Compositio Math. 143 (2007) 566–602
doi:10.1112/S0010437X07002813

The canonical subgroup for families of abelian varieties

F. Andreatta and C. Gasbarri

Abstract

Let V be a complete discrete valuation ring with residue field k of characteristic $p > 0$ and fraction field K of characteristic zero. Let $\mathcal{S}$ be a formal scheme over V and let $\mathfrak{X} \to \mathcal{S}$ be a locally projective formal abelian scheme. In this paper we prove that, under suitable natural conditions on the Hasse–Witt matrix of $\mathfrak{X} \otimes_V V/pV$, the kernel of the Frobenius morphism on $\mathfrak{X}_k$ can be canonically lifted to a finite and flat subgroup scheme of $\mathfrak{X}$ over an admissible blow-up of $\mathcal{S}$, called the 'canonical subgroup of $\mathfrak{X}$'. This is done by a careful study of torsors under group schemes of order p over $\mathfrak{X}$. We also present a filtration on $\mathrm{H}^1(\mathfrak{X}, \mu_p)$ in the spirit of the Hodge–Tate decomposition.

1. Introduction

In the seminal paper [Kat73], Katz developed the theory of p-adic modular forms in one variable. One of the most interesting features is the introduction of p-adic modular forms with growth condition. This has been the starting point of the theory of overconvergent eigenforms in one variable with astonishing applications to the theory of two-dimensional Galois representations. In order to go further in the comprehension of the Galois representations, one feels the need for a higher-dimensional analogue of [Kat73]. The first serious difficulty one meets is the construction of the canonical subgroup.

Let V be a complete discrete valuation ring (dvr) of unequal characteristic $(0, p)$ with residue field k and fraction field K. Let X be a g-dimensional abelian scheme over V with special fiber X_k. The problem of constructing the canonical subgroup is the problem of lifting functorially in X the kernel of Frobenius H_k on X_k to a subgroup scheme of X (finite and flat of rank p^g over V).

If X_k is ordinary, one proves that H_k can be lifted uniquely to a closed subgroup scheme H_X of $X[p]$, finite and flat of rank p^g over V; see Proposition 3.4. In the general case, one looks for conditions on X so that the canonical subgroup can be constructed. One can not hope to be able to find the canonical subgroup in general, i.e. for any X. Indeed, in characteristic p, associating the kernel of Frobenius to an elliptic curve gives rise to a canonical section of the modular curves $X_0(p) \otimes \mathbb{F}_p \to X_0(1) \otimes \mathbb{F}_p$, but such a section can not exist over $\mathbf{Z}_p$.

In this paper we give a construction of the canonical subgroup in the setting of rigid analytic spaces à la Raynaud and in the setting of formal schemes. This is what is needed for a natural generalization to higher dimensions of Katz's approach to p-adic modular forms. We refer the reader to § 3 for precise statements of our results. Furthermore, with this approach we provide the following.

(i) We give a geometric reinterpretation and a generalization of the Bloch–Kato filtration on $\mathrm{H}^1_{\mathrm{et}}(X_K, \mu_p)$ (X_K being the generic fiber of X), see § 6, and we explain its relation to the canonical subgroup, see § 12.

Received 6 October 2006, accepted in final form 26 November 2006.
2000 Mathematics Subject Classification 11G10, 14G20, 11F33 (primary).
Keywords: canonical subgroup, torsors, Frobenius endomorphism, abelian scheme, Bloch–Kato filtration.

https://doi.org/10.1112/S0010437X07002813 Published online by Cambridge University Press

(ii) For $p > 3$ we provide $\mathrm{H}^1_{\mathrm{et}}(X_{\overline{K}}, \mu_p)$ with a two-step filtration in the spirit of the Hodge–Tate decomposition, see § 13.6. In particular, this answers a question asked in [AM04, Remark 6.1]. We also explain how it relates to the canonical subgroup and we show that, if X_k is not ordinary, a 'true' Hodge–Tate decomposition does not exist.

We now give an outline of the main ideas in our approach. Let v be the valuation on K^* normalized so that $\mathrm{v}(p) = 1$. Let $\mathfrak{X} \to \mathcal{S}$ be a g-dimensional locally projective abelian formal scheme with $\mathcal{S}$ a formal scheme over V. If $\iota_k \colon G_k \to \mathfrak{X}_k$ is the kernel of Frobenius, the problem of constructing the canonical subgroup is twofold: (1) to lift G_k to a finite and flat group scheme G over $\mathcal{S}$ and (2) to lift the closed immersion ι_k and these functorially in $\mathfrak{X}$ and $\mathcal{S}$. If G is a finite and flat group scheme over $\mathcal{S}$, one has a canonical isomorphism

$$\mathrm{H}^1_{\mathrm{fppf}}(\mathfrak{X}^\vee, G^\vee)/\mathrm{H}^1_{\mathrm{fppf}}(\mathcal{S}, G^\vee) \xrightarrow{\sim} \mathrm{Hom}(G, \mathfrak{X}),$$

where $G^\vee$ is the Cartier dual of G and $\mathfrak{X}^\vee$ is the dual abelian scheme of $\mathfrak{X}$; see [Mil80, Proposition III.4.16]. This allows us to translate problem (2) to the problem of lifting $G^\vee$-torsors over $\mathfrak{X}^\vee$. In the ordinary case this approach is very natural: the group scheme $G_k^\vee$ is étale so that it lifts uniquely and, consequently, $G_k^\vee$-torsors over X_k lift uniquely as well.

In § 11 we show how to reduce the problem to the case that $\mathcal{S} = \mathrm{Spf}(R)$ with R a p-adically complete and separated, flat, normal, noetherian V-algebra and $\mathfrak{X} \to \mathcal{S}$ is the formal completion of an abelian scheme $X \to \mathrm{Spec}(R)$. On the generic fiber $R_K := R \otimes_R K$, the canonical subgroup is, if it exists, a twisted form of $(\mathbf{Z}/p\mathbf{Z})^g$ and corresponds, possibly after extending the base R, to g 'linearly independent' subgroup schemes of $X \otimes_R R_K$ of order p. Let F be the Frobenius on $\mathrm{H}^1(X \otimes R/pR, \mathcal{O}_{X\otimes R/pR})$. If the ideal of R/pR defined by the determinant of F contains an element of V/pV of valuation $w < (p-1)/(2p-1)$, we show that, indeed, there exist a finite and normal extension $R \subset W$, étale over R_K, and a finite and flat group scheme G_λ of order p over W, parameterized by $\lambda \in V$, such that $\mathrm{H}^1_{\mathrm{fppf}}(X \otimes_R W, \mathrm{G}_\lambda)/\mathrm{H}^1_{\mathrm{fppf}}(W, \mathrm{G}_\lambda)$ is a $\mathbb{F}_p$-vector space of dimension g. In the ordinary case this is a consequence of Artin–Schreier theory. Our approach is a generalization of this. We proceed as follows. In § 7 we give an analogue of Hensel's lemma for G_λ-torsors which allows us to reduce the problem to estimating the number of G_λ-torsors modulo p^r $(0 \leqslant r = r(\lambda) \leqslant 1)$. In § 8 we further translate this problem into the question of finding zeroes of the operator Frobenius$-a$, with $a = a(\lambda) \in \overline{V}$, on $\mathrm{H}^1(X \otimes W/pW, \mathcal{O}_{X\otimes W/pW})$ for a suitable W (in the ordinary case $a = 1$). We deal with this question in § 9. The main ingredient in proving the results in §§ 7–8 is the explicit description of torsors under group schemes of order p developed in [AG] and briefly recalled in § 5. We then define the subgroup scheme $\mathbb{G}_K$ of $X_K^\vee$ as the image of the induced map $(\mathrm{G}_\lambda{}^\vee)^g \to X^\vee \otimes_R W_K$. This makes sense, i.e. it descends to a closed subgroup scheme of $X_K^\vee$. It follows from § 12 that there exists an admissible blow-up $S' \to S$ over which the schematic closure of $\mathbb{G}_K$ in $X \times_S S'$ is a closed subgroup scheme finite and flat over S'. Eventually, we define the canonical subgroup H_X as the Cartier dual of $X^\vee \times_S S'[p]/\mathbb{G}$. We prove that H_X has the required properties. See § 12 for the detailed argument.

In § 4 we show that the solution of the canonical subgroup problem, if it exists, is unique. This allows us to prove that all possible constructions agree with ours, when comparable.

The problem of constructing the canonical subgroup has been solved completely in [Kat73] for elliptic curves. The first solution in the higher-dimensional case is due to [AM04] for abelian schemes over dvr's in the case $p \geqslant 3$. In [AM04] the authors show how a solution of the canonical subgroup problem implies the existence of generalized Atkin U operators on overconvergent Siegel p-adic modular forms. In their case, the canonical subgroup is constructed when the determinant of F contains an element of V/pV of valuation $w < b(g,p)$, where $b(g,p)$ is an explicit constant depending on p and g with $b(g,p) \to 0$ when $g \to +\infty$. The methods employed are, however, quite different and rely on the ramification theory developed in [AS02] and syntomic cohomology.

https://doi.org/10.1112/S0010437X07002813 Published online by Cambridge University Press

Subsequent constructions of the canonical subgroup in the rigid analytic setting, based on techniques of rigid analytic geometry, have recently been proposed in [KL05] in the Hilbert–Blumenthal case, in [GK06] for Shimura curves and in [Con05] in general. Another approach, based on a detailed study of formal groups, can be found in [Nev03] for Hilbert–Blumenthal abelian schemes over dvr's.

2. Notation and terminology

We let V be a complete discrete valuation ring of unequal characteristic 0–p with maximal ideal $\mathfrak{m}$, fraction field K and residue field k. Let $\overline{K}$ be an algebraic closure of K and let v be the induced valuation on $\overline{K}$ normalized so that $\mathrm{v}(p) = 1$. By abuse of notation, if $w \in \mathbb{Q}_{>0}$, we denote by p^w an (any) element in $\overline{K}$ of valuation w. For every rational number r in $\mathrm{v}(\mathfrak{m})$, let $V_r := V/p^rV$.

In this paper we follow the terminology and conventions of [BL93] concerning formal rigid geometry à la Raynaud. In particular, an *admissible V-algebra* is a p-adically complete and separated flat V-algebra topologically of finite type as in [BL93, § 1]. Formal schemes over V will always be assumed to be *admissible* in the sense of [BL93, § 5], i.e. quasi-compact and with a covering by open formal subschemes spectra of admissible V-algebras.

We say that a formal scheme $\mathfrak{X}$ over $\mathcal{S}$ is projective if there exists $n \in \mathbf{N}$ such that $\mathfrak{X}$ is a closed formal subscheme of the formal n-dimensional projective space $\widehat{\mathbf{P}}^n_{\mathcal{S}}$ over $\mathcal{S}$. We say that a formal scheme $\mathfrak{X}$ over $\mathcal{S}$ is locally projective if there exists a covering $\{\mathfrak{U}_i\}_i$ of $\mathcal{S}$ by open formal subschemes such that $\mathfrak{X} \times_{\mathcal{S}} \mathfrak{U}_i$ is projective over $\mathfrak{U}_i$.

If X (respectively, $\mathfrak{X}$) is a (formal) scheme over V, we denote by X_r (respectively, $\mathfrak{X}_r$) the pullback of X (respectively, $\mathfrak{X}$) to V_r and by $\iota_r \colon X_r \to X$ (respectively, $\iota_r \colon \mathfrak{X}_r \to \mathfrak{X}$) the canonical closed immersion. We denote by X_K (respectively, $\mathfrak{X}^{\mathrm{an}}$) the fiber product $X \times_V \operatorname{Spec}(K)$ (respectively, the associated rigid analytic space as in [BL93, § 5]).

We will have different notions of admissible blow-ups depending on the context. To avoid confusion we gather them in the following definition.

Definition 2.1. (1) Let S be a scheme and $i \colon U \hookrightarrow S$ be an open subscheme. A *U-admissible blow-up* of S is a blow-up $f \colon S' \to S$ along a closed subscheme $C \hookrightarrow S$ disjoint from U and defined by an ideal of $\mathcal{O}_S$ of finite presentation.

(2) If S is a scheme flat over V, a *K-admissible blow-up* of S is an admissible blow-up of S with respect to the open subscheme $S_K \hookrightarrow S$.

(3) If $\mathcal{S}$ is a formal scheme over V, an *admissible formal blow-up* $\mathcal{S}' \to \mathcal{S}$ is a formal $\mathcal{S}$-scheme

$$\mathcal{S}' \cong \lim_{h\to\infty} \quad \operatorname{Proj} \bigoplus_{n=0}^{\infty} (A^n \otimes_{\mathcal{O}_{\mathfrak{X}}} \mathcal{O}_{\mathfrak{X}}/p^{h+1}\mathcal{O}_{\mathfrak{X}}),$$

where $A \subset \mathcal{O}_{\mathfrak{X}}$ is a coherent open ideal sheaf. See [BL93, § 2].

Recall that the category $\mathfrak{T}$ of quasi-separated paracompact rigid K-spaces of Tate is equivalent to the category of admissible formal V-schemes, localized by admissible formal blow-ups [Ray74a], [BL93, Theorem 4.1].

3. The main theorems

Let $\mathcal{S}$ be a formal scheme over V. Let $f \colon \mathfrak{X} \to \mathcal{S}$ be a g-dimensional formal abelian scheme. Let F be the Frobenius morphism on $\mathrm{R}^1 f_* \mathcal{O}_{\mathfrak{X}_1}$. We denote by $\det(\mathrm{F})\mathcal{O}_{\mathcal{S}_1}$ the ideal locally generated by the determinant of the matrix of F with respect to a basis of $\mathrm{R}^1 f_* \mathcal{O}_{\mathfrak{X}_1}$. Observe that it is well defined.

https://doi.org/10.1112/S0010437X07002813 Published online by Cambridge University Press

Definition 3.1. Let $0 \leqslant w < 1$ be a rational number. We define a formal (w, g)-situation to be $f \colon \mathfrak{X} \to \mathcal{S}$ where:

(a) $\mathcal{S}$ is a formal scheme;

(b) f is a locally projective g-dimensional formal abelian scheme;

(c) $p^w \in \det(\mathrm{F})\mathcal{O}_{\mathcal{S}_1}$.

Remark 3.2. To require that $f \colon \mathfrak{X} \to \mathcal{S}$ is a formal $(0, g)$-situation is equivalent to requiring that its geometric fibers are ordinary. Since being ordinary is an open condition, there exists a maximal formal open subscheme $\mathcal{S}(0)$ of $\mathcal{S}$ such that $\mathfrak{X} \times_{\mathcal{S}} \mathcal{S}(0) \to \mathcal{S}(0)$ is a formal $(0, g)$-situation.

In the next lemma we determine the maximal locus where $\mathfrak{X} \to \mathcal{S}$ is a (w, g)-situation.

Lemma 3.3. *Let $\mathfrak{X} \to \mathcal{S}$ be a locally projective formal abelian scheme over a formal scheme $\mathcal{S}$. For every rational number $0 \leqslant w < 1$ with $p^w \in \Gamma(\mathcal{S}, \mathcal{O}_{\mathcal{S}})$, there exists a formal scheme $\mathcal{S}(w)$ over $\mathcal{S}$ such that:*

(1) *$\mathfrak{X} \times_{\mathcal{S}} \mathcal{S}(w) \to \mathcal{S}(w)$ is a (w, g)-situation;*

(2) *every morphism $\mathfrak{T} \to \mathcal{S}$ of formal schemes for which $\mathfrak{X} \times_{\mathcal{S}} \mathfrak{T} \to \mathfrak{T}$ is a (w, g)-situation, factors uniquely via $\mathcal{S}(w) \to \mathcal{S}$.*

Furthermore, $\mathcal{S}(w)$ is an open formal subscheme of an admissible blow-up of $\mathcal{S}$. In particular, $\mathcal{S}(w)^{\mathrm{an}}$ is an open rigid analytic subspace of $\mathcal{S}^{\mathrm{an}}$.

Proof. Due to property (2) it suffices to construct $\mathcal{S}(w)$ and to prove its claimed properties locally on $\mathcal{S}$. We may then assume that $\mathcal{S} = \mathrm{Spf}(R)$ is affine and that $\mathrm{H}^1(\mathfrak{X}, \mathcal{O}_{\mathfrak{X}})$ is free as an $\mathcal{O}_{\mathcal{S}}$-module. Then, with the notation of Definition 3.1, we have that $\det(\mathrm{F})R_1$ is generated by one element of R_1. Fix a generator $\overline{\alpha}$ and a lifting $\alpha \in R$. Define $R(w) := R\{Y\}/(Y\alpha - p^w)$ and $\mathcal{S}(w) := \mathrm{Spf}(R(w))$. One verifies that properties (1) and (2) hold. The last claims follow from the construction of $\mathcal{S}(w)$. □

Proposition 3.4. *Let $\mathfrak{X} \to \mathcal{S}$ be a $(0, g)$-situation. There is a unique closed subgroup scheme $H^{\mathrm{ord}}_{\mathfrak{X}}$ of $\mathfrak{X}$ finite and flat over $\mathcal{S}$ such that $H^{\mathrm{ord}}_{\mathfrak{X}} \otimes_V k$ is the kernel of the relative Frobenius on $\mathfrak{X} \otimes_V k$. In particular, it is multiplicative and of order p^g. Furthermore, the construction of $H^{\mathrm{ord}}_{\mathfrak{X}}$ is functorial for $(0, g)$-situations and commutes with base-change.*

It is not difficult to deduce the proposition from the general fact that the étale topos of $\mathcal{S}$ (respectively, $\mathfrak{X}$) is the same as the étale topos of $\mathcal{S} \otimes_V k$ (respectively, of $\mathfrak{X} \otimes_V k$). Nevertheless, we prefer to give a different, probably less-efficient proof which follows closely and thus hopefully clarifies the strategy for proving one of the main theorems of the paper (Theorem 3.5).

Proof. Due to the claimed uniqueness it suffices to construct $H^{\mathrm{ord}}_{\mathfrak{X}}$, and prove that it is unique, Zariski locally on $\mathcal{S}$. In particular, we may assume that $\mathcal{S} = \mathrm{Spf}(R)$ is affine and that $\mathrm{H}^1(\mathfrak{X}, \mathcal{O}_{\mathfrak{X}})$ is a free $\mathcal{O}_{\mathcal{S}}$-module of rank g. By Artin–Schreier theory [Mil80, Proposition III.4.12] we have an exact sequence

$$0 \longrightarrow \mathrm{H}^1(\mathfrak{X}_1, \mathbf{Z}/p\mathbf{Z})/\mathrm{H}^1(\mathcal{S}_1, \mathbf{Z}/p\mathbf{Z}) \longrightarrow \mathrm{H}^1(\mathfrak{X}_1, \mathcal{O}_{\mathfrak{X}_1}) \xrightarrow{\mathrm{F}-1} \mathrm{H}^1(\mathfrak{X}_1, \mathcal{O}_{\mathfrak{X}_1}), \qquad (3.4.1)$$

where F is defined by Frobenius. Note that $\mathrm{Ker}(\mathrm{F} - 1)$ is a $\mathbb{F}_p$-vector space. We claim that there exists a finite, étale and Galois morphism $\mathcal{S}_1' \to \mathcal{S}_1$ such that, if we put $\mathfrak{X}_1' := \mathfrak{X}_1 \times_{\mathcal{S}_1} \mathcal{S}_1'$, the kernel of $\mathrm{F} - 1$ on $\mathrm{H}^1(\mathfrak{X}_1', \mathcal{O}_{\mathfrak{X}_1'})$ is a $\mathbb{F}_p$-vector space of dimension g.

Indeed, fix a basis $B = \{e_1, \ldots, e_g\}$ of $\mathrm{H}^1(\mathfrak{X}_1, \mathcal{O}_{\mathfrak{X}_1})$ as an R_1-module and let U be the matrix of Frobenius on $\mathrm{H}^1(\mathfrak{X}_1, \mathcal{O}_{\mathfrak{X}_1})$ with respect to B. The ordinarity of $\mathfrak{X} \to \mathcal{S}$ is equivalent to requiring

https://doi.org/10.1112/S0010437X07002813 Published online by Cambridge University Press

that U is invertible. Let $W \to \mathcal{S}_1$ be the closed subscheme of $\mathrm{Spec}(R_1[z_1, \ldots, z_g])$ defined by the equations

$$U \begin{pmatrix} z_1^p \\ \vdots \\ z_g^p \end{pmatrix} - \begin{pmatrix} z_1 \\ \vdots \\ z_g \end{pmatrix} = 0.$$

Since U is invertible, $W \to \mathcal{S}_1$ is finite and flat of rank p^g. By the Jacobian criterion it is also étale. We then let $\mathcal{S}_1' \to \mathcal{S}_1$ be a finite, étale and Galois morphism such that $W \times_{\mathcal{S}_1} \mathcal{S}_1'$ splits as the disjoint sum of p^g-copies of $\mathcal{S}_1'$.

Let $\mathcal{S}' \to \mathcal{S}$ be the unique finite, étale and Galois morphism lifting $\mathcal{S}_1' \to \mathcal{S}_1$. Let G be the Galois group. Define $\mathfrak{X}' := \mathfrak{X} \times_{\mathcal{S}} \mathcal{S}'$. Since any $\mathbf{Z}/p\mathbf{Z}$-torsor over $\mathfrak{X}_1'$ can be uniquely lifted to a $\mathbf{Z}/p\mathbf{Z}$-torsor over $\mathfrak{X}'$, then $\mathrm{H}^1(\mathfrak{X}', \mathbf{Z}/p\mathbf{Z})/\mathrm{H}^1(\mathcal{S}', \mathbf{Z}/p\mathbf{Z})$ is an $\mathbb{F}_p$-vector space of dimension g and it is endowed with an action of G given by the pull-back of torsors. This group is isomorphic to $\mathrm{Hom}_{\mathcal{S}'}(\mu_p, (\mathfrak{X}')^\vee)$ as a G-module (where G acts on the latter via its action on $\mathfrak{X}'$); see § 5.12. We then obtain a homomorphism $\Psi\colon \mu_p^g \to (\mathfrak{X}')^\vee$. Since μ_p^g is finite over $\mathcal{S}$, the map Ψ is finite. Using again (3.4.1) for every geometric point of $\mathcal{S}_1$, we deduce that the kernel of $\Psi \times_{\mathcal{S}} \mathcal{S}_1$ is trivial fiberwise over $\mathcal{S}_1$ and, hence, is trivial. In particular, $\Psi \times_{\mathcal{S}} \mathcal{S}_1$ is a closed immersion. Owing to [EGAIII, 4.8.10], this implies that Ψ is a closed immersion. By étale descent, Ψ descends to a closed subgroup scheme $\mathbb{G} \subset \mathfrak{X}^\vee$. It is finite and flat of rank p^g over $\mathcal{S}$, it is annihilated by p and it is of multiplicative type. Define $H_{\mathfrak{X}}^{\mathrm{ord}}$ as the Cartier dual of $\mathfrak{X}^\vee[p]/\mathbb{G}$. It is a finite and flat group scheme over $\mathcal{S}$ of rank p^g and it is a closed subgroup scheme of $\mathfrak{X}[p]$. Since $\mathfrak{X}^\vee$ is also ordinary, $\mathfrak{X}^\vee[p]/\mathbb{G}$ is an étale group scheme and, hence, $H_{\mathfrak{X}}^{\mathrm{ord}}$ is of multiplicative type. In particular, it lifts the kernel of Frobenius on $\mathfrak{X} \otimes_V k$. □

One of the main theorems of this paper is the following analogue of a classical theorem of Lubin as stated in [Kat73, Theorem 3.1].

Theorem 3.5. *There is the only way to attach to every formal (w, g)-situation $\mathfrak{X} \to \mathcal{S}$, with $0 \leqslant w < (p-1)/(2p-1)$, a rigid analytic subgroup scheme $H_{\mathfrak{X}}^{\mathrm{an}}$ of $\mathfrak{X}^{\mathrm{an}}$ finite and flat of rank p^g over $\mathcal{S}^{\mathrm{an}}$, called the canonical subgroup of $\mathfrak{X}^{\mathrm{an}}$, such that:*

(i) *it depends only on the isomorphism class of $\mathfrak{X}^{\mathrm{an}} \to \mathcal{S}^{\mathrm{an}}$;*

(ii) *its construction commutes with base-change;*

(iii) *the restriction of $H_{\mathfrak{X}}^{\mathrm{an}}$ to $\mathcal{S}(0)^{\mathrm{an}}$ is $(H_{\mathfrak{X} \times_{\mathcal{S}} \mathcal{S}(0)}^{\mathrm{ord}})^{\mathrm{an}}$.*

Remark 3.6. In part (i) we mean that for every formal (w', g)-situation $\mathfrak{X}' \to \mathcal{S}'$, with $0 \leqslant w' < (p-1)/(2p-1)$ and with rigid analytic fiber $\mathfrak{X}^{\mathrm{an}} \to \mathcal{S}^{\mathrm{an}}$, we have $H_{\mathfrak{X}}^{\mathrm{an}} = H_{\mathfrak{X}'}^{\mathrm{an}}$ as rigid analytic subgroups of $\mathfrak{X}^{\mathrm{an}}$.

In part (ii), besides base-change via formal schemes over V, we also allow base-change via formal schemes defined over different complete discrete valuation rings.

Proposition 3.7. *Let $\mathfrak{X}_1 \to \mathcal{S}$ (respectively, $\mathfrak{X}_2 \to \mathcal{S}$) be a formal (w_1, g_1)-situation (respectively, a formal (w_2, g_2)-situation) with $0 \leqslant w_1, w_2 < (p-1)/(2p-1)$. Let $h\colon \mathfrak{X}_1 \to \mathfrak{X}_2$ be a morphism of formal abelian schemes. Then, h^{an} restricted to $H_{\mathfrak{X}_1}^{\mathrm{an}}$ factors via $H_{\mathfrak{X}_2}^{\mathrm{an}} \hookrightarrow \mathfrak{X}_2^{\mathrm{an}}$.*

In particular, if one takes $\mathfrak{X}_1 = \mathfrak{X}_2 = \mathfrak{X}$ and h to be the identity, the proposition implies that $H_{\mathfrak{X}}^{\mathrm{an}}$ does not depend on whether we consider $\mathfrak{X} \to \mathcal{S}$ as a formal (w, g) or as a formal (w', g) situation.

Let $f\colon \mathfrak{X} \to \mathcal{S}$ be a formal (w, g)-situation with $0 \leqslant w < (p-1)/(2p-1)$. We now show that we can be more precise at the level of formal schemes, i.e. regarding the formal models of $H_{\mathfrak{X}}^{\mathrm{an}}$. More precisely, one knows from [BL93, Theorem 4.1] that there exists a formal scheme whose rigid analytic fiber is $H_{\mathfrak{X}}^{\mathrm{an}}$, but one has very little control on such a formal model. We can show that there exists an admissible formal blow-up $\mathcal{S}' \to \mathcal{S}$ and a closed subgroup scheme of $\mathfrak{X} \times_{\mathcal{S}} \mathcal{S}'$, finite

https://doi.org/10.1112/S0010437X07002813 Published online by Cambridge University Press

and flat of rank p^g over $\mathcal{S}'$, whose rigid analytic fiber is $H_{\mathfrak{X}}^{\mathrm{an}}$. Furthermore, one can find a formal scheme over $\mathcal{S}$ which is minimal in the following sense.

Definition 3.8. We say that a morphism of formal schemes $\pi\colon \mathcal{S}' \to \mathcal{S}$ is *minimal* with respect to the given (w, g)-situation if:

(a) π is locally projective and it induces an isomorphism of the associated rigid analytic spaces;

(b) there exists a closed subgroup scheme H' of $\mathfrak{X} \times_{\mathcal{S}} \mathcal{S}'$, finite and flat of order p^g over $\mathcal{S}'$, whose rigid analytic fiber is $H_{\mathfrak{X}}^{\mathrm{an}}$;

(c) for every admissible blow-up $h\colon \mathfrak{T} \to \mathcal{S}$, such that $\mathfrak{X} \times_{\mathcal{S}} \mathfrak{T}$ admits a closed subgroup scheme H finite and flat over $\mathfrak{T}$ and whose rigid analytic fiber is $H_{\mathfrak{X}}^{\mathrm{an}} \times_{\mathcal{S}^{\mathrm{an}}} \mathfrak{T}^{\mathrm{an}}$, the morphism h factors via π and $H = H' \times_{\mathcal{S}'} \mathfrak{T}$.

We first prove a lemma which guarantees that a flat formal model of $H_{\mathfrak{X}}^{\mathrm{an}}$, if it exists, is unique.

Lemma 3.9. *Let $f\colon \mathfrak{X}_1 \to \mathfrak{X}_2$ be a morphism of formal schemes over a formal scheme $\mathfrak{T}$. Let H_1 (respectively, H_2) be a formal closed subscheme of $\mathfrak{X}_1$ (respectively, $\mathfrak{X}_2$) such that H_1 is flat over $\mathfrak{T}$. Assume that f^{an} restricted to H_1^{an} factors via H_2^{an}. Then, f restricted to H_1 factors via H_2.*

Proof. Let $g\colon \mathfrak{U}_1 \to \mathfrak{U}_2$ be the restriction of f to affine open formal subschemes of $\mathfrak{X}_1$ and $\mathfrak{X}_2$, respectively. For $i = 1$, 2 we have the following commutative diagram.

$$\begin{tikzcd}
\Gamma(\mathfrak{U}_i, \mathcal{O}_{\mathfrak{X}_i}) \arrow[r] \arrow[d, "\iota_i"'] & \Gamma(\mathfrak{U}_i^{\mathrm{an}}, \mathcal{O}_{\mathfrak{X}_i^{\mathrm{an}}}) \arrow[d] \\
\Gamma(\mathfrak{U}_i, \mathcal{O}_{H_i}) \arrow[r, "j_i"] & \Gamma(\mathfrak{U}_i^{\mathrm{an}}, \mathcal{O}_{H_1^{\mathrm{an}}})
\end{tikzcd}$$

The vertical arrows are surjective since $H_i \hookrightarrow \mathfrak{X}_i$ and $H_i^{\mathrm{an}} \hookrightarrow \mathfrak{X}_i^{\mathrm{an}}$ are closed immersions (as formal schemes and as rigid analytic spaces, respectively). Let J_i be the kernel of ι_i. The map j_1 is injective because $\Gamma(\mathfrak{U}_1^{\mathrm{an}}, \mathcal{O}_{H_1^{\mathrm{an}}})$ is $\Gamma(\mathfrak{U}_1, \mathcal{O}_{H_1}) \otimes_V K$ and H_1 is flat over $\mathfrak{T}$ by assumption. By assumption, $(g^{\mathrm{an}})^*(J_2) = j_1 \circ \iota_1 \circ g^*(J_2)$ is zero in $\Gamma(\mathfrak{U}_1^{\mathrm{an}}, \mathcal{O}_{H_1^{\mathrm{an}}})$. Hence, $\iota_1 \circ g^*(J_2) = 0$. The conclusion follows. □

The following theorem shows us that a flat formal model of $H_{\mathfrak{X}}^{\mathrm{an}}$ exists over an admissible blow-up of $\mathcal{S}$ with no need for further blow-ups (of the base-change) of $\mathfrak{X}$.

Theorem 3.10. *Let $f\colon \mathfrak{X} \to \mathcal{S}$ be a formal (w, g)-situation with $0 \leqslant w < (p-1)/(2p-1)$.*

(1) There exists a minimal morphism, unique up to $\mathcal{S}$-isomorphism, $\mathcal{S}^{\mathfrak{X}} \to \mathcal{S}$ with respect to the given (w, g)-situation.

(2) The formation of $\mathcal{S}^{\mathfrak{X}}$ commutes with flat base-change, i.e. if $\mathfrak{T}$ is a formal scheme flat over $\mathcal{S}$, we have $\mathfrak{T}^{\mathfrak{X}} \cong \mathfrak{T} \times_{\mathcal{S}} \mathcal{S}^{\mathfrak{X}}$.

In particular, there exists an admissible blow-up $\mathcal{S}' \to \mathcal{S}$ and a closed subgroup scheme $H_{\mathfrak{X}}^{\mathrm{form}}$ of $\mathfrak{X} \times_{\mathcal{S}} \mathcal{S}'$, finite and flat of order p^g over $\mathcal{S}'$, whose rigid analytic fiber is $H_{\mathfrak{X}}^{\mathrm{an}}$.

Remark 3.11. Property (1) and Raynaud's theorem [BL93, Theorem 4.1] imply that there exists an admissible blow-up $\mathcal{S}' \to \mathcal{S}$ factoring via $\mathcal{S}^{\mathfrak{X}} \to \mathcal{S}$. This proves the last statement of the theorem. We thank the referee for pointing out that this does not necessarily imply that $\mathcal{S}^{\mathfrak{X}} \to \mathcal{S}$ is an admissible blow-up.

As in the ordinary case we can also show that the special fiber of $H_{\mathfrak{X}}^{\mathrm{form}}$ is the kernel of Frobenius on the special fiber of the pull-back of $\mathfrak{X}$ to $\mathcal{S}'$.

https://doi.org/10.1112/S0010437X07002813 Published online by Cambridge University Press

Proposition 3.12. *With the notation of Theorem 3.10 we have*

$$H_{\mathfrak{X}}^{\mathrm{form}} \times_{\mathcal{S}'} (\mathcal{S}' \otimes_V k)^{\mathrm{red}} = \mathrm{Ker}(\mathrm{F}) \times_{\mathcal{S}} (\mathcal{S}' \otimes_V k)^{\mathrm{red}},$$

where $(\mathcal{S}' \otimes_V k)^{\mathrm{red}}$ is the scheme $\mathcal{S}' \otimes_V k$ with reduced induced structure and F is the relative Frobenius on $\mathfrak{X} \otimes_V k$.

The formal model of the canonical subgroup is functorial in $\mathfrak{X}$. Indeed, we deduce from Lemma 3.9 the following.

Proposition 3.13. *Let $f_1 \colon \mathfrak{X}_1 \to \mathcal{S}$ (respectively, $f_2 \colon \mathfrak{X}_2 \to \mathcal{S}$) be a formal (w, g_1)-situation (respectively, a formal (w, g_2)-situation) with $0 \leqslant w < (p-1)/(2p-1)$. Let $h \colon \mathfrak{X}_1 \to \mathfrak{X}_2$ be a morphism of formal abelian schemes. Denote by $\mathcal{S}' \to \mathcal{S}$ an admissible blow-up such that there exist group schemes $H_{\mathfrak{X}_1}^{\mathrm{form}} \subset \mathfrak{X}_1 \times_{\mathcal{S}} \mathcal{S}'$ and $H_{\mathfrak{X}_2}^{\mathrm{form}} \subset \mathfrak{X}_2 \times_{\mathcal{S}} \mathcal{S}'$ extending $H_{\mathfrak{X}_1}^{\mathrm{an}}$ and $H_{\mathfrak{X}_2}^{\mathrm{an}}$ as in Theorem 3.10. Then, $h \times_{\mathcal{S}} \mathcal{S}'$ restricted to $H_{\mathfrak{X}_1}^{\mathrm{form}}$ factors via $H_{\mathfrak{X}_2}^{\mathrm{form}}$.*

4. Proof of the uniqueness

In this section we prove that the canonical subgroup, if it exists, is unique. More precisely, we show in Proposition 4.6 that two rules satisfying Theorem 3.5(i)–(iii) coincide.

First of all we prove a general result on the rigid analytic connected components of suitable tubes of moduli spaces of abelian varieties over V. This is the key ingredient in proving Proposition 4.6. We start by recalling the notion of rigid analytic connectedness.

Definition 4.1 (Berthelot [Ber96, (0.1.12)]). Let Y be a rigid analytic space over K. We say that Y is *connected* if one of the following equivalent conditions are satisfied:

(i) $\Gamma(Y, \mathcal{O}_Y)$ does not contain idempotents different from 0 and 1;

(ii) Y does not admit an admissible covering consisting of two disjoint non-empty open rigid analytic subspaces.

Proposition 4.2. *Let R be an admissible V-algebra. Fix $\alpha \in R$, a generator π of the maximal ideal of V and a non-negative rational number w such that $p^w \in R$. Denote by $\mathfrak{X}$ the formal scheme* $\mathrm{Spf}(R)$ *and by $\mathfrak{X}(w)$ the formal scheme* $\mathrm{Spf}(R(w))$ *with $R(w) := R\{Y\}/(\alpha Y - p^w)$. If (π, α) is a regular sequence in R, every connected component of $\mathfrak{X}(w)^{\mathrm{an}}$ has non-empty intersection with $\mathfrak{X}(0)^{\mathrm{an}}$.*

Proof. Write $\mathfrak{X}(w)^{\mathrm{an}}$ as the disjoint union of its connected components $\amalg_h \mathfrak{X}(w)_h^{\mathrm{an}}$. For every h let e_h in $\Gamma(\mathfrak{X}(w)^{\mathrm{an}}, \mathcal{O}_{\mathfrak{X}(w)^{\mathrm{an}}})$ be the function which is 1 on $\mathfrak{X}(w)_h^{\mathrm{an}}$ and 0 elsewhere. The set $\{e_h\}_h$ consists of idempotents of $R(w) \otimes_V K$ such that $1 = \sum_h e_h$ and $e_h e_\ell = 0$ if $\ell \neq h$. In particular, $R(w) \otimes_V K$ decomposes accordingly into the product $\prod_h (R(w) \otimes_V K) e_h$. The proposition follows if we prove that for every h the map $(R(w) \otimes_V K) e_h \to (R(0) \otimes_V K) e_h$ is injective. This is proven in the following lemmas. □

Lemma 4.3. *The map $R/p^n R \to R/p^n R[\alpha^{-1}]$ is injective for every $n \in \mathbf{N}$. In particular, $p^i R = (p^i \widehat{R[\alpha^{-1}]}) \cap R_K$ (in $\widehat{R[\alpha^{-1}]} \otimes_V K$).*

Proof. The regularity of the sequence (π, α) implies that α is neither zero nor a zero divisor in $R \otimes_V k$, i.e. the map $R \otimes_V k \to R[\alpha^{-1}] \otimes_V k$ is injective. Since π is not a zero divisor in R, for every $n \in \mathbf{N}$ the sequence

$$0 \longrightarrow R/\pi R \xrightarrow{\cdot \pi^{n-1}} R/\pi^n R \longrightarrow R/\pi^{n-1} R \longrightarrow 0$$

is exact. Proceeding inductively on n, one deduces that $R/\pi^n R \to R[\alpha^{-1}]/\pi^n R[\alpha^{-1}]$ is injective for every n. We leave it to the reader to check that the second statement of the lemma is equivalent to

https://doi.org/10.1112/S0010437X07002813 Published online by Cambridge University Press

showing that $p^s\widehat{R[\alpha^{-1}]} \cap R = p^sR$ for every $s \in \mathbf{N}$. This follows from the injectivity of $R/\pi^{rs}R \to R/\pi^{rs}R[\alpha^{-1}]$ where $pV = \pi^r V$. □

Lemma 4.4. *The map* $(R\{Y\}/(\alpha Y - p^w)) \otimes_V K \to \widehat{R[\alpha^{-1}]} \otimes_V K$ *is injective.*

Proof. Write $\beta := \alpha/p^w$. Consider the following commutative diagram.

$$\begin{tikzcd}
R_K\{Y\} \arrow[r, "\iota"] \arrow[d, "\rho"'] & (\widehat{R[\alpha^{-1}]} \otimes_V K)\{Y\} \arrow[d] & \\
R_K\{Y\}/(\beta Y - 1) \arrow[r, "j"] & (\widehat{R[\alpha^{-1}]} \otimes_V K)\{Y\}/(\beta Y - 1) \arrow[r, equal] & \widehat{R[\alpha^{-1}]} \otimes_V K
\end{tikzcd}$$

The lemma asserts that j is injective. Due to Lemma 4.3 the map $R \to \widehat{R[\alpha^{-1}]}$ is injective since R is p-adically complete and separated. Hence, the map ι is also injective. Let $B = \sum_i b_i Y^i \in R_K\{Y\}$ be such that $j(\rho(B)) = 0$, i.e. $\iota(B) = C(1-Y\beta)$ with $C = \sum_i c_i Y^i \in (\widehat{R[\alpha^{-1}]}\otimes_V K)\{Y\}$. To have $\iota(B) = C(1 - Y\beta)$ is equivalent to requiring that $c_0 = b_0$ and $c_n = c_{n-1}\beta + b_n$ for $n \geqslant 1$. It follows by induction that $c_n \in R_K$, i.e. $C \in R_K[\![Y]\!]$. For every $s \in \mathbf{N}$ there exists $N \in \mathbf{N}$ such that c_n lies in $p^s\widehat{R[\alpha^{-1}]}$ for $n \geqslant N$. Hence, c_n lies in $(p^s\widehat{R[\alpha^{-1}]}) \cap R_K$ which is p^sR by Lemma 4.3. Hence, C lies in $\iota(R_K\{Y\})$. In particular, $\rho(B) = 0$. The conclusion follows. □

We apply Proposition 4.2 in the following geometric context. Fix positive integers n and d such that $n \geqslant 3$, $(n,p) = 1$ and $(n,d) = 1$. Denote by $\mathcal{A}_{g,d,n}$ (respectively, $\mathcal{A}_{g,d,n}^{(p)}$) the moduli space over V of g-dimensional abelian varieties with full level n structure, i.e. with a fixed isomorphism of the n-torsion with $(\mathbf{Z}/n\mathbf{Z})^{2g}$, and a polarization of degree d^2 (respectively, and a subgroup scheme finite and flat over the base of order p^g). They exist by [Mum65, Theorem 7.9], they are quasi-projective and they are fine moduli spaces due to our assumption on n. In particular, there exists a universal abelian scheme $X^{\mathrm{univ}} \to \mathcal{A}_{g,d,n}$. Let $\rho\colon \mathcal{A}_{g,d,n}^{(p)} \to \mathcal{A}_{g,d,n}$ be the morphism induced by the forgetful functor. Over K these moduli spaces are smooth and ρ is finite and étale. Let $\mathfrak{A}_{g,d,n}$ be the formal scheme associated to $\mathcal{A}_{g,d,n}$. For $0 \leqslant w < 1$ define $(\mathfrak{A}_{g,d,n})(w)$ as in Lemma 3.3.

Proposition 4.5. *Every connected component of* $(\mathfrak{A}_{g,d,n})(w)^{\mathrm{an}}$*, in the sense of Definition 4.1, has non-empty intersection with* $(\mathfrak{A}_{g,d,n})(0)^{\mathrm{an}}$.

Proof. Let $\mathcal{A}_{g,d,n}^{\mathrm{norm}}$ be the normalization of $\mathcal{A}_{g,d,n}$ and let $\mathfrak{T}$ be the associated formal scheme. Since $\mathcal{A}_{g,d,n} \otimes_V K$ is smooth we have $\mathfrak{T}(w)^{\mathrm{an}} = (\mathfrak{A}_{g,d,n})(w)^{\mathrm{an}}$ so that it suffices to prove the lemma for $\mathfrak{T}(w)^{\mathrm{an}}$. Since $\mathcal{A}_{g,d,n}$ is of finite type over V, it is an excellent scheme and its normalization is finite over $\mathcal{A}_{g,d,n}$ and it is itself excellent. Since $\mathcal{A}_{g,d,n}^{\mathrm{norm}}$ is flat over V and V is universally catenary, by [EGAIV, 5.6.1] the irreducible components of $\mathcal{A}_{g,d,n}^{\mathrm{norm}} \otimes_V k$ all have the same dimension equal to $g(g+1)/2$. By [NO80, Theorem 3.1] every irreducible component of $\mathcal{A}_{g,d,n} \otimes_V k$ has dimension $g(g+1)/2$. Since the map $\mathcal{A}_{g,d,n}^{\mathrm{norm}} \otimes_V k \to \mathcal{A}_{g,d,n} \otimes_V k$ is finite, we deduce by dimension reasons that every irreducible component of $(\mathcal{A}_{g,d,n})^{\mathrm{norm}} \otimes_V k$ dominates an irreducible component of $\mathcal{A}_{g,d,n} \otimes_V k$. By [NO80, Theorem 3.1] the generic point of every irreducible component of $\mathcal{A}_{g,d,n} \otimes_V k$ is ordinary. We conclude that the same holds for every irreducible component of the special fiber $\mathcal{A}_{g,d,n}^{\mathrm{norm}} \otimes_V k$.

Let $\{U_i\}_i$ be a covering of $\mathcal{A}_{g,d,n}$ by affine open subschemes each dominating $\mathrm{Spec}(V)$ and such that, if $U_i = \mathrm{Spec}(A_i)$ and $X_i^{\mathrm{univ}} \to U_i$ is the restriction of the universal abelian scheme X^{univ} to U_i, then $H^1(X_i^{\mathrm{univ}}, \mathcal{O}_{X_i^{\mathrm{univ}}})$ is a free A_i-module. For every i let α_i be a lift of a generator of the ideal generated by $\det(\mathrm{F})$ on $\mathrm{H}^1(X_i^{\mathrm{univ}}, \mathcal{O}_{X_i^{\mathrm{univ}}})/p\mathrm{H}^1(X_i^{\mathrm{univ}}, \mathcal{O}_{X_i^{\mathrm{univ}}})$. Each A_i is a V-algebra of finite type and, hence, it is an excellent ring. In particular, the p-adic completion R_i of the normalization of A_i is normal by [EGAIV, 7.8.3(v)]. Furthermore, $\{\mathrm{Spf}(R_i)\}_i$ is a covering of $\mathfrak{T}$ by affine open formal subschemes. It follows from Lemma 3.3 that $\{\mathrm{Spf}(R_i(w))\}_i$, with $R_i(w) := R_i\{Y_i\}/(\alpha_i Y_i - p^w)$, is a covering of $\mathfrak{T}(w)$ by affine open formal subschemes. Since $\mathrm{Spec}((R_i \otimes_V k)[\alpha_i^{-1}])$ is the ordinary locus in $\mathrm{Spec}(R_i \otimes_V k)$, the conclusion of the previous paragraph translates into the fact that α_i is not contained in any minimal prime ideal of R_i containing π. Since R_i is normal, we conclude from [Bou98, IV.1.1, Proposition 2 and Corollary 3] that α_i is not a zero divisor in $R_i \otimes_V k$. Hence, the hypotheses of Proposition 4.2 are satisfied for $R = R_i$ and $\alpha = \alpha_i$ and the proposition follows. □

We now prove the main result of this section: the uniqueness of the canonical subgroup.

Proposition 4.6. *Suppose that we have two rules H^{an} and G^{an} satisfying Theorem 3.5(i)–(iii). Then, H^{an} and G^{an} coincide.*

Proof. Let $\mathfrak{X} \to \mathcal{S}$ be a formal (w, g)-situation, with w as in Theorem 3.5. We have to prove that $H^{\mathrm{an}}_{\mathfrak{X}} = G^{\mathrm{an}}_{\mathfrak{X}}$. If $w = 0$ this follows from property (iii). We then assume $w > 0$. We remark that we can work locally in the fppf topology. By this we mean the following: let $\mathcal{S}' \to \mathcal{S}$ be a fppf morphism of formal schemes and let $\mathfrak{X}' := \mathfrak{X} \times_{\mathcal{S}} \mathcal{S}' \to \mathcal{S}'$ be the (w, g)-situation obtained by base-change, then $H^{\mathrm{an}}_{\mathfrak{X}'} = G^{\mathrm{an}}_{\mathfrak{X}'}$, as rigid analytic subspaces of $\mathfrak{X}'$, if and only if $H^{\mathrm{an}}_{\mathfrak{X}} = G^{\mathrm{an}}_{\mathfrak{X}}$. Indeed, $H^{\mathrm{an}}_{\mathfrak{X}}$ and $G^{\mathrm{an}}_{\mathfrak{X}}$ define closed rigid analytic subspaces of $\mathfrak{X}[p]^{\mathrm{an}}$ and the latter is finite over $\mathcal{S}^{\mathrm{an}}$. The same applies replacing $\mathfrak{X}$ with $\mathfrak{X}'$. Since the map of rigid analytic spaces associated to $\mathcal{S}' \to \mathcal{S}$ is fppf, in the sense of [BL93, pp. 313–314], the claim follows from property (ii).

In particular, considering the base-change to a dvr finite over V, we may assume that $p^w \in V$. Possibly after localization on $\mathcal{S}$, we may also suppose that $\mathfrak{X}$ is projective over $\mathcal{S}$ and, in particular, that it admits a polarization of degree d^2 for some d. Eventually, we may suppose that $\mathfrak{X}$ is endowed with a full level n structure with $n \geqslant 3$, $(n, p) = 1$ and $(n, d) = 1$.

The formal abelian scheme $\mathfrak{X} \to \mathcal{S}$ is obtained by a pull-back of the universal formal abelian scheme $\mathfrak{X}^{\mathrm{univ}}$ over $\mathfrak{A}_{g,d,n}$. Property (ii) reduces the proof of the uniqueness to the case of the universal family over $(\mathfrak{A}_{g,d,n})(w)$; see Lemma 3.3 for the notation. Note that $H^{\mathrm{an}}_{\mathfrak{X}}$ and $G^{\mathrm{an}}_{\mathfrak{X}}$ define two closed immersions

$$\sigma_H, \sigma_G \colon (\mathfrak{A}_{g,d,n})(w)^{\mathrm{an}} \hookrightarrow (\rho^{\mathrm{an}})^{-1}((\mathfrak{A}_{g,d,n})(w)).$$

By property (iii) they coincide on the rigid analytic open subspace $\mathfrak{A}_{g,d,n}(0)^{\mathrm{an}}$. We deduce from Proposition 4.5 that the latter has non-empty intersection with every connected component of $(\mathfrak{A}_{g,d,n})(w)^{\mathrm{an}}$. The conclusion then follows from the following lemma. □

Lemma 4.7. *Let X and Y be rigid analytic spaces. Assume that X is connected and that for every $x \in X$ the local ring $\mathcal{O}_{X,x}$ is integral. Assume that we are given two closed immersions $\alpha, \beta \colon X \hookrightarrow Y$ coinciding on a non-empty open rigid analytic subspace $U \subset X$. Then, $\alpha = \beta$.*

Proof. One proves that the ideal sheaves in $\mathcal{O}_Y$ defining α and β coincide. One proceeds as in [Ber96, Proposition 0.1.13]. Details are left to the reader. □

Remark 4.8. One may observe that the main difficulty in the proof of the uniqueness is showing that every connected component of $(\mathfrak{A}_{g,d,n})(w)^{\mathrm{an}}$ intersects the ordinary locus; if one is interested just in principally polarized abelian varieties, this is obvious.

5. Torsors under group schemes of order p

In this section we review some of the results of [AG], in the special case needed in this paper, concerning a description of torsors under group schemes of order p. This allows us to give explicit equations for such torsors in the Zariski topology. We refer to [AG] for proofs, applications and generalizations.

https://doi.org/10.1112/S0010437X07002813 Published online by Cambridge University Press

Definition 5.1. For every $\lambda \in V$ define $\mathcal{G}^{(\lambda)}$ to be the V-scheme

$$\mathrm{Spec}\biggl(V\biggl[T, \frac{1}{1+\lambda T}\biggr]\biggr).$$

It has the structure of a V-group scheme defining the comultiplication by $T \mapsto T \otimes 1 + 1 \otimes T + \lambda T \otimes T$, the counit by $T = 0$ and the coinverse by $T \mapsto -T/(1+\lambda T)$.

For $\lambda \in V$ with $\mathrm{v}(\lambda) \leqslant 1/(p-1)$ let P_λ be the polynomial

$$P_\lambda(T) := \frac{(1+\lambda T)^p - 1}{\lambda^p}.$$

Then, the map $\phi_\lambda \colon \mathcal{G}^{(\lambda)} \to \mathcal{G}^{(\lambda^p)}$, defined at the level of Hopf algebras by $T \mapsto P_\lambda(T)$, is an isogeny of degree p. Let

$$\mathrm{G}_\lambda := \mathrm{Spec}(V[T]/(P_\lambda(T)))$$

be the kernel of ϕ_λ. It is a commutative, finite and flat group scheme over $\mathrm{Spec}(V)$ of rank p.

Example 5.2. (a) If $\lambda = 0$, then $\mathcal{G}^{(0)} \simeq \mathbf{G}_a$. For future use, in this case, we pose $T = W$, consequently $\mathbf{G}_a = \mathrm{Spec}(V[W])$ with comultiplication $W \mapsto W \otimes 1 + 1 \otimes W$, coinverse $W \mapsto -W$ and counit $W \mapsto 0$.

(b) If λ is a unit, then $\mathcal{G}^{(\lambda)} \cong \mathbf{G}_{m,V}$. Write $\mathbf{G}_{m,V}$ as $\mathrm{Spec}(V[Z, \frac{1}{Z}])$ with comultiplication given by $Z \mapsto Z \otimes Z$ and counit defined by $Z \mapsto 1$; then, the isomorphism $\mathcal{G}^{(\lambda)} \xrightarrow{\sim} \mathbf{G}_{m,V}$ is given by $Z \mapsto 1 + \lambda T$.

(c) The group scheme G_λ is étale if and only if $\mathrm{v}(\lambda) = 1/(p-1)$. It is multiplicative, i.e. its Cartier dual is étale, if and only if λ is a unit.

5.3 Compatibilities

Let λ and ν be elements of V with $\mathrm{v}(\nu) \leqslant \mathrm{v}(\lambda)$. We have a natural morphism $\eta_{\lambda,\nu} \colon \mathcal{G}^{(\lambda)} \longrightarrow \mathcal{G}^{(\nu)}$ of V-group schemes given by $T \mapsto (\lambda/\nu)T$. It is an isomorphism over K. Assume that $0 \leqslant \mathrm{v}(\nu) \leqslant \mathrm{v}(\lambda) \leqslant 1/(p-1)$. Then, one checks that the diagram

$$\begin{tikzcd}
\mathcal{G}^{(\lambda)} \arrow[r, "\Phi_\lambda"] \arrow[d, "\eta_{\lambda,\nu}"'] & \mathcal{G}^{(\lambda^p)} \arrow[d, "\eta_{\lambda^p,\nu^p}"] \\
\mathcal{G}^{(\nu)} \arrow[r, "\Phi_\nu"] & \mathcal{G}^{(\nu^p)}
\end{tikzcd}$$

commutes. Hence, we obtain a homomorphism of V-group schemes $\eta_{\lambda,\nu} \colon \mathrm{G}_\lambda \to \mathrm{G}_\mu$, which is an isomorphism over K. In the case ν is a unit, thanks to Example 5.2(b), we obtain a homomorphism

$$\eta_\lambda \colon \mathrm{G}_\lambda \longrightarrow \mathrm{G}_\nu \xrightarrow{\sim} \mu_p.$$

For ν not necessarily a unit, one verifies that $\eta_\lambda = \eta_\nu \circ \eta_{\lambda,\nu}$.

5.4 Relation with Oort–Tate theory

Although we do not need it explicitly, we describe here the relation with the Oort–Tate description of group schemes of order p. For elements a, c in V satisfying $ac = p$, denote by $G_{(a,c)}$ the group scheme over V defined in [OT70]: the structure as a V-scheme is given by $G_{(a,c)} := \mathrm{Spec}(V[y]/(y^p - ay))$, the co-multiplication by

$$y \mapsto y \otimes 1 + 1 \otimes y + \frac{cw_{p-1}}{1-p} \sum_{i=1}^{p-1} \frac{y^i}{w_i} \otimes \frac{y^{p-i}}{w_{p-i}}$$

and the counit by $y = 0$. Here, $w_1, \dots, w_{p-1}$ are the universal constants in V introduced in [OT70, p. 9].

Under the further *assumption* that cw_{p-1} admits a $(p-1)$th root β in V, put $\lambda(a) := \beta/(1-p)$. Then, we have the isomorphism $G_{(a,c)} \to \mathrm{G}_{\lambda(a)}$ defined at the level of the underlying Hopf algebras by $T \mapsto \sum_{i=1}^{p-1} \beta^{i-1}(y^i/w_i)$. *Vice versa*, given λ and letting $c(\lambda) := (\lambda(1-p))^{p-1}/w_{p-1}$ and $a(\lambda) := p/c(\lambda)$, we have $\mathrm{G}_\lambda \cong \mathrm{G}_{(a(\lambda),c(\lambda))}$.

Oort–Tate have proved that, Zariski locally on V, any finite and flat group scheme of rank p over V is of the form above. In particular, the G_λ give an alternative description of all V-group schemes of order p (possibly after a ramified extension of V).

Definition 5.5. Assume that λ satisfies $0 < \mathrm{v}(\lambda) \leqslant 1/(p-1)$. Let X be a scheme over V. Define $\mathrm{CD}^{(\lambda)}(X)$ to be the category of global classifying data over X. The objects consist of triples (L, E, Ψ) where:

(1) L is an invertible $\mathcal{O}_X$-module;

(2) E is an extension of L by $\mathcal{O}_X$;

(3) $\Psi\colon E \to E$ is a $\mathcal{O}_X$-linear map such that

  (a) defining $E_0 := \mathrm{Ker}(\Psi)$, we have $E_0 = \mathcal{O}_X$;

  (b) the map $E/E_0 \to E/E_0$ induced by Ψ is multiplication by λ on L;

  (c) the $\mathcal{O}_X$-module $E/\Psi(E)$ is invertible.

A morphism $\Xi\colon (L, E, \Psi) \to (L', E', \Psi')$ is given by isomorphisms $\Xi_L\colon L \to L'$ and $\Xi_E\colon E \to E'$ as $\mathcal{O}_X$-modules such that the following two diagrams are commutative.

$$\begin{tikzcd}
0 \arrow[r] & \mathcal{O}_{\mathfrak{X}} \arrow[r] \arrow[d, "\mathrm{Id}"'] & E \arrow[r] \arrow[d, "\Xi_E"] & L \arrow[r] \arrow[d, "\Xi_L"] & 0 \\
0 \arrow[r] & \mathcal{O}_{\mathfrak{X}} \arrow[r] & E' \arrow[r] & L' \arrow[r] & 0
\end{tikzcd}$$

$$\begin{tikzcd}
E \arrow[r, "\Psi"] \arrow[d, "\Xi_E"'] & E \arrow[d, "\Xi_E"] \\
E' \arrow[r, "\Psi'"] & E'
\end{tikzcd}$$

The following theorem is proven in [AG] and gives a description of $\mathcal{G}^{(\lambda)}$-torsors in terms of global classifying data.

Theorem 5.6 [AG, § 2]. *The category of $\mathcal{G}^{(\lambda)}$-torsors for the fppf topology over X is quasi-equivalent to the category* $\mathrm{CD}^{(\lambda)}(X)$.

Remark 5.7. Given global classifying data one can always find a covering $\{U_i\}_i$ of X by open affine subschemes and $e_i \in \Gamma(U_i, E)$ such that $E|_{U_i} = \mathcal{O}_{U_i} \oplus \mathcal{O}_{U_i} e_i$ and $\Psi(e_i) = 1 + \lambda e_i$. Then, the associated $\mathcal{G}^{(\lambda)}$-torsor $Y^{(\lambda)} \to X$ is locally defined by

$$Y^{(\lambda)}_{|U_i} \cong \mathrm{Spec}(\mathcal{O}_{U_i}[e_i])$$

with coaction $Y^{(\lambda)}_{|U_i} \times_V \mathcal{G}^{(\lambda)} \to Y^{(\lambda)}_{|U_i}$ given by $e_i \mapsto e_i \otimes 1 + \Psi(e_i) \otimes T$. Furthermore, for every $i, j \in I$ one can write $e_i = (1 + \lambda u_{ij})e_j + u_{ij}$ as sections of $E|_{U_i \cap U_j}$. The gluing of $Y^{(\lambda)}_{|U_i}$ and $Y^{(\lambda)}_{|U_j}$ on $U_{ij} := U_i \cap U_j$ is then given by $e_i = (1+\lambda u_{ij})e_j + u_{ij}$. One checks that $Y^{(\lambda)}$ is indeed a $\mathcal{G}^{(\lambda)}$-torsor; see [AG] for details.

Definition 5.8. Define $\mathrm{CD}_\lambda(X)$ to be the category of classifying data over X. The objects consist of the quadruples $(L, E, \Psi, \{(U_i, e_i, \alpha_i)\}_{i \in I})$ where:

(i) (L, E, Ψ) are global classifying data;

(ii) $\{U_i\}_i$ is a covering of X by open affine subschemes such that:

https://doi.org/10.1112/S0010437X07002813 Published online by Cambridge University Press

(a) for every $i \in I$ we have $\alpha_i \in \Gamma(U_i, \mathcal{O}_X)$ and $e_i \in \Gamma(U_i, E)$ such that $E|_{U_i} = \mathcal{O}_{U_i} \oplus \mathcal{O}_{U_i} e_i$ and $\Psi(e_i) = 1 + \lambda e_i$;

(b) for every i, $j \in I$, writing $e_i = v_{ij} e_j + u_{ij}$, we have

$$v_{ij} = 1 + \lambda u_{i,j} \quad \text{and} \quad v_{ij}^p \alpha_j - \alpha_i = -P_\lambda(u_{ij}).$$

A morphism $\Xi\colon (L, E, \Psi, \{(U_i, e_i, \alpha_i)\}_{i\in I}) \to (L', E', \Psi', \{(U'_j, e'_j, \alpha'_j)\}_{j\in J})$ is a morphism $\Xi\colon (L, E, \Psi) \to (L', E', \Psi')$ in the sense of Definition 5.5 such that there exists a common refinement $\{V_h\}_h$ of $\{U_i\}_i$ and $\{U'_j\}_j$ such that, if $V_h \subset U_i \cap U'_j$ and writing $\Xi_E(e_i) = v_h e'_j + u_h$ over V_h, we have

$$v_h = 1 + \lambda u_h \quad \text{and} \quad v_h^p \alpha'_j - \alpha_i = -P_\lambda(u_h).$$

One of the key results of [AG] is the following theorem characterizing G_λ-torsors in terms of classifying data.

Theorem 5.9 [AG, Theorems 2.2 and 3.4]. *Assume that $0 < \mathrm{v}(\lambda) \leqslant 1/(p-1)$. The category of G_λ-torsors $Y \to X$ for the fppf topology is quasi-equivalent to the category $\mathrm{CD}_\lambda(X)$ of classifying data over X.*

Remark 5.10. (a) Given classifying data $\mathcal{C}$ as in the theorem, let $Y^{(\lambda)} \to X$ be the $\mathcal{G}^{(\lambda)}$-torsor associated to the global classifying data (L, E, Ψ) as in Remark 5.7. Then, the G_λ-torsor $Y \to X$ corresponding to $\mathcal{C}$ can be realized as the closed subscheme $Y \subset Y^{(\lambda)}$ locally defined by $\mathrm{Spec}(\mathcal{O}_{U_i}[e_i]/(P_\lambda(e_i) - \alpha_i))$ endowed with the unique action of G_λ compatible with the one of $\mathcal{G}^{(\lambda)}$ on $Y^{(\lambda)}$.

(b) One can show that Kummer and Artin–Schreier theories are instances of Theorem 5.9; see [AG].

Remark 5.11. Let $\mathfrak{X}$ be a formal V-scheme. With minor changes, one can show that similar descriptions of formal torsors over $\mathfrak{X}$ in terms of formal classifying data exist. The key observation is that giving a formal torsor over $\mathfrak{X}$ is equivalent to giving compatible torsors over $X_n := \mathfrak{X} \otimes_V V_n$ for n varying in $\mathbf{N}$. We leave the details to the reader.

5.12 Torsors and subgroups

Let S be a V-scheme. Assume that $X \to S$ is a locally projective abelian scheme (which is the case of interest for us in this paper). Denote by Pic_X the Picard presheaf, by $\mathrm{Pic}_{X/S}$ the relative Picard sheaf and by $X^\vee = \mathrm{Pic}^0_{X/S}$ the dual abelian scheme.

Let $Y \to X$ be a G_λ-torsor. Let T be a scheme over S and consider a T-valued point of the Cartier dual ${\mathrm{G}_\lambda}^\vee$ of G_λ, i.e. a homomorphism $f\colon \mathrm{G}_\lambda \otimes_V T \to \mathbf{G}_{m,T}$. Then, the push-forward of $Y \times_S T \to X \times_S T$ via f defines a $\mathbf{G}_{m,T}$-torsor over $X \times_S T$ and, hence, an element of $\mathrm{Pic}_X(T)$. This defines a homomorphism $\mathrm{H}^1(X, \mathrm{G}_\lambda) \to \mathrm{Hom}_S({\mathrm{G}_\lambda}^\vee, \mathrm{Pic}_X)$ and, hence, a homomorphism $\tau\colon \mathrm{H}^1(X, \mathrm{G}_\lambda)/\mathrm{H}^1(S, \mathrm{G}_\lambda) \longrightarrow \mathrm{Hom}_S({\mathrm{G}_\lambda}^\vee, \mathrm{Pic}_{X/S})$. Then, τ clearly factors via $\mathrm{Hom}_S({\mathrm{G}_\lambda}^\vee, X^\vee)$. Furthermore, the homomorphism

$$\tau\colon \mathrm{H}^1(X, \mathrm{G}_\lambda)/\mathrm{H}^1(S, \mathrm{G}_\lambda) \longrightarrow \mathrm{Hom}_S({\mathrm{G}_\lambda}^\vee, X^\vee)$$

is an isomorphism; cf. [Mil80, Proposition III.4.16].

For later purposes we make the following remark. Let r be a rational number in $\mathrm{v}(\mathfrak{m})$.

Proposition 5.13. *If R is a p-adically complete and separated V-algebra, the reduction map $\mathrm{H}^1(R, \mathrm{G}_\lambda) \to \mathrm{H}^1(R_r, \mathrm{G}_\lambda)$ is surjective.*

Proof. In [AG, § 4] an infinitesimal deformation theory for G_λ-torsors is developed. The obstruction space to lift G_λ-torsors infinitesimally is a subgroup of an extension of $\mathrm{H}^2(\mathrm{Spec}(R \otimes_V k), \mathcal{G}^{(\lambda)}) \cong \mathrm{H}^2(\mathrm{Spec}(R \otimes_V k), \mathcal{O}) = \{0\}$ by $\mathrm{H}^1(\mathrm{Spec}(R \otimes_V k), \mathcal{G}^{(\lambda^p)}) \cong \mathrm{H}^1(\mathrm{Spec}(R \otimes_V k), \mathcal{O}) = \{0\}$, where $\mathcal{O}$ is the structure sheaf. The proposition follows. □

https://doi.org/10.1112/S0010437X07002813 Published online by Cambridge University Press

6. G_λ-torsors and the Bloch–Kato filtration

In this section we assume that R is a p-adically complete, separated, noetherian and normal flat V-algebra. We also fix an algebraically closed field Ω containing R. We denote by S the scheme $\mathrm{Spec}(R)$. Let $\pi\colon X \to S$ be a projective abelian scheme over S.

Definition 6.1. Define $\mathcal{W} := \{W\}$ as the set of all finite extensions of R, which are normal integral domains, are contained in Ω and $R_K \subset W_K$ is étale. Let $\overline{R} := \lim_{\to} W$.

We observe that the direct limit $\lim_{\to} W_K$ is also the limit of all finite, étale and irreducible extensions of R_K contained in Ω. Indeed, by [Eis95, Proposition 13.14] if $R_K \subset T$ is a finite and étale extension, the normalization of R in T is finite as an R-module. We now introduce a filtration, called the G_λ-filtration, on $\mathrm{H}^1_{\mathrm{et}}(X_K \otimes_R \overline{R}, \mu_p)$.

Lemma 6.2. *The group* $\mathrm{H}^1(\overline{R}, \mathrm{G}_\lambda)$ *is trivial.*

Proof. Let $f\colon Y \to \mathrm{Spec}(\overline{R})$ be a G_λ-torsor. Since f is finite, Y is obtained by a pull-back from a G_λ-torsor $f'\colon Y' \to \mathrm{Spec}(W)$ such that $W \subset \overline{R}$ is a normal and integral domain, it is finite as an R-module and étale over R_K. Since $\mathrm{H}^1(\overline{R}_K, \mathrm{G}_\lambda) = 0$, we may further assume that f' admits a section σ over W_K. The schematic closure $\overline{\sigma}$ of σ is finite over W. Since W is normal, it is a section of f'. Hence, f admits a section as well. □

Lemma 6.3. *For every* $W \in \mathcal{W}$ *the map*

$$\mathrm{H}^1_{\mathrm{fppf}}(X \otimes_R W, \mu_p)/\mathrm{H}^1_{\mathrm{fppf}}(W, \mu_p) \longrightarrow \mathrm{H}^1_{\mathrm{fppf}}(X_K \otimes_R W, \mu_p)/\mathrm{H}^1_{\mathrm{fppf}}(W_K, \mu_p)$$

is an isomorphism. In particular, the map $\mathrm{H}^1_{\mathrm{fppf}}(X \otimes_R \overline{R}, \mu_p) \to \mathrm{H}^1_{\mathrm{fppf}}(X_K \otimes_R \overline{R}, \mu_p)$ *is an isomorphism.*

Proof. By § 5.12 the first statement amounts to proving that $\mathrm{Hom}(\mathbf{Z}/p\mathbf{Z}, X^\vee \otimes_R W) \to \mathrm{Hom}(\mathbf{Z}/p\mathbf{Z}, X^\vee_K \otimes_R W)$ is an isomorphism. This is equivalent to proving that the application $\mathrm{Hom}(\mathbf{Z}/p\mathbf{Z}, X^\vee[p] \otimes_R W) \to \mathrm{Hom}(\mathbf{Z}/p\mathbf{Z}, X^\vee[p]_K \otimes_R W)$ is an isomorphism. Since $X^\vee[p]$ is finite over $\mathrm{Spec}(W)$ and W is normal, this follows from the valuative criterion of properness and [EGAIV, 20.4.12]. □

Lemma 6.4. *Let* $\lambda \in \overline{V}$ *satisfying* $0 \leqslant \mathrm{v}(\lambda) \leqslant 1/(p-1)$. *Let* $W \in \mathcal{W}$ *be such that* $\lambda \in W$. *The map* $\mathrm{H}^1_{\mathrm{fppf}}(X \otimes_R W, \mathrm{G}_\lambda)/\mathrm{H}^1_{\mathrm{fppf}}(W, \mathrm{G}_\lambda) \to \mathrm{H}^1_{\mathrm{fppf}}(X \otimes_R W, \mu_p)/\mathrm{H}^1_{\mathrm{fppf}}(W_K, \mu_p)$, *defined using the homomorphism* η_λ *of* § 5.3, *is injective. In particular, the homomorphism*

$$\theta_\lambda\colon \mathrm{H}^1_{\mathrm{fppf}}(X \otimes_R \overline{R}, \mathrm{G}_\lambda) \longrightarrow \mathrm{H}^1_{\mathrm{fppf}}(X_K \otimes_R \overline{R}, \mu_p)$$

is injective.

Proof. Using § 5.12 the claim amounts to proving that the map $\mathrm{Hom}({\mathrm{G}_\lambda}^\vee, X^\vee \otimes_R W) \to \mathrm{Hom}(\mu_p^\vee, X^\vee_K \otimes_R W)$ defined by composing with η_λ is injective. The base-change of $\eta_\lambda\colon \mathrm{G}_\lambda \to \mu_p$ via $\otimes_V K$ is an isomorphism. The claim is then equivalent to proving that any homomorphism ${\mathrm{G}_\lambda}^\vee \to X^\vee \otimes_R W$ which is trivial over K is itself trivial. Since ${\mathrm{G}_\lambda}^\vee$ is a flat group scheme over W and $W \to W \otimes_V K$ is injective, this is clear. □

Definition 6.5. For every λ in $\overline{V}$ with $0 \leqslant \mathrm{v}(\lambda) \leqslant 1/(p-1)$, define $\mathrm{H}^1_{\mathrm{fppf}}(X_K \otimes_R \overline{R}, \mu_p)^{[\lambda]}$ as the subgroup $\theta_\lambda(\mathrm{H}^1_{\mathrm{fppf}}(X \otimes_R \overline{R}, \mathrm{G}_\lambda))$ of $\mathrm{H}^1_{\mathrm{fppf}}(X_K \otimes_R \overline{R}, \mu_p)$.

Proposition 6.6. *Let* λ *and* ν *be elements of* $\overline{V}$ *with* $0 \leqslant \mathrm{v}(\nu) \leqslant \mathrm{v}(\lambda) \leqslant 1/(p-1)$. *Then,*

$$\mathrm{H}^1_{\mathrm{fppf}}(X_K \otimes_R \overline{R}, \mu_p)^{[\lambda]} \subset \mathrm{H}^1_{\mathrm{fppf}}(X_K \otimes_R \overline{R}, \mu_p)^{[\nu]}.$$

In particular:

https://doi.org/10.1112/S0010437X07002813 Published online by Cambridge University Press

(1) $\mathrm{H}^1(X \otimes \overline{R}, \mu_p)^{[\lambda]}$ *depends on* $\mathrm{v}(\lambda)$ *and not on* λ;

(2) $\mathrm{H}^1(X \otimes \overline{R}, \mu_p)^{[\lambda]}$ *is invariant under* $\mathrm{Gal}(\overline{R_K}/R_K)$;

(3) $\{\mathrm{H}^1(X \otimes \overline{R}, \mu_p)^{[\lambda]} \mid 0 \leqslant \mathrm{v}(\lambda) \leqslant 1/(p-1)\}$ *is a decreasing filtration of* $\mathrm{H}^1_{\mathrm{fppf}}(X_K \otimes_R \overline{R}, \mu_p)$.

Proof. The first statement follows using the homomorphism $\eta_{\lambda,\nu}$ of § 5.3 and the fact that $\eta_\nu \circ \eta_{\lambda,\nu} = \eta_\lambda$. This implies claim (1) and claim (3). If $\sigma \in \mathrm{Gal}(\overline{R_K}/R_K)$, then σ acts on $\mathrm{H}^1_{\mathrm{fppf}}(X_K \otimes_R \overline{R}, \mu_p)$ by a pull-back and the image of $\mathrm{H}^1(X \otimes \overline{R}, \mu_p)^{[\lambda]}$ is $\mathrm{H}^1(X \otimes \overline{R}, \mu_p)^{[\sigma(\lambda)]}$. Claim (2) then follows from claim (1). □

6.7 Relation with the Bloch–Kato filtration

In this section we further assume that R is a dvr. We consider the following descending filtration on $\mathrm{H}^1(X_K \otimes_R \overline{R}, \mu_p)$ introduced and studied in the ordinary case in [BK86, § 1] and in more generality in [AM04]. Consider the following diagram.

$$\begin{tikzcd}
X_k \otimes_R \overline{R} \arrow[r, "i"] \arrow[d] & X \otimes_R \overline{R} \arrow[d] & X_K \otimes_R \overline{R} \arrow[l, "j"'] \arrow[d] \\
\mathrm{Spec}(k \otimes_V \overline{R}) \arrow[r] & \mathrm{Spec}(\overline{R}) & \mathrm{Spec}(K \otimes_V \overline{R}) \arrow[l]
\end{tikzcd}$$

Let M^1_1 be the étale sheaf on $X_k \otimes_R \overline{R}$ given by

$$\mathrm{M}^1_1 := i^* \mathrm{R}^1 j_*(\mu_p).$$

The exact sequence

$$0 \longrightarrow \mu_p \longrightarrow \mathbf{G}_m \xrightarrow{\_^p} \mathbf{G}_m \longrightarrow 0$$

on $X_K \otimes_R \overline{R}$ and the fact that $X \otimes_R W$ is locally factorial (for every finite and normal extension $R \subset W$, étale over R_K as in Definition 6.1) give an exact sequence

$$i^* j_*(\mathcal{O}^*_{X_K \otimes_R \overline{R}}) \xrightarrow{\_^p} i^* j_*(\mathcal{O}^*_{X_K \otimes_R \overline{R}}) \xrightarrow{h} \mathrm{M}^1_1 \longrightarrow 0. \tag{6.7.1}$$

For every $\lambda \in \overline{V}$ we denote by $U^\lambda \mathrm{M}^1_1$ the subsheaf locally generated by local sections of $i^* j_*(\mathcal{O}^*_{X_K \otimes_R \overline{R}})$ congruent to 1 modulo λ^p (note that $U^\lambda \mathrm{M}^1_1$ corresponds to the sheaf $U^{\mathrm{v}(\lambda^p)} \mathrm{M}^1_1$ in [BK86]; our choice of notation is more suitable for Theorem 6.8). Consider the natural map

$$u \colon \mathrm{H}^1_{\mathrm{et}}(X_K \otimes_R \overline{R}, \mu_p) \longrightarrow \mathrm{H}^0_{\mathrm{et}}(X_k \otimes_R \overline{R}, \mathrm{M}^1_1)$$

obtained from the Leray spectral sequence and the properness of $X \to S$. Define

$$U^\lambda \mathrm{H}^1_{\mathrm{et}}(X_K \otimes_R \overline{R}, \mu_p) := u^{-1}(\mathrm{H}^0_{\mathrm{et}}(X_k \otimes_R \overline{R}, U^\lambda \mathrm{M}^1_1)).$$

It follows from [BK86, Corollary 1.4.1] that for $\mathrm{v}(\lambda) > 1/(p-1)$ one has $U^\lambda \mathrm{H}^1_{\mathrm{et}}(X_K \otimes_R \overline{R}, \mu_p) = 0$. We now prove that this filtration, called *the Bloch–Kato filtration*, can be reinterpreted in terms of G_λ-torsors on $X \otimes_R \overline{R}$. As a corollary one deduces that the G_λ-filtration is Galois invariant providing an alternative proof of Proposition 6.6.

Theorem 6.8. *The filtrations* $\{\mathrm{H}^1_{\mathrm{et}}(X_K \otimes_R \overline{R}, \mu_p)^{[\lambda]}\}_\lambda$ *and* $\{U^\lambda \mathrm{H}^1_{\mathrm{et}}(X_K \otimes_R \overline{R}, \mu_p)\}_\lambda$, *with* $\lambda \in \overline{V}$ *satisfying* $0 \leqslant \mathrm{v}(\lambda) \leqslant 1/(p-1)$, *coincide.*

Proof. We start by giving an explicit description of the map u. Let $Y \to X \otimes_R \overline{R}$, a μ_p-torsor. Since $X \to S$ is smooth, X is locally factorial and, hence, $\mathrm{R}^1 j_*(\mathcal{O}^*_{X \otimes_R \overline{R}}) = 0$. Thus, there exists a finite and normal extension $R \subset W$ and a covering $\{U_i\}_i$ of $X \otimes_R W$ by affine open subschemes such that Y is defined over $X \otimes_R W$ and $Y|_{U_i \otimes_V K}$ is defined by the equation $z_i^p - \gamma_i$ with $\gamma_i \in \Gamma(U_i \otimes_V K, \mathcal{O}^*_{U_i \otimes_V K})$. The elements γ_i define a global section γ of $j_*(\mathcal{O}^*_{X_K \otimes_R \overline{R}})/j_*((\mathcal{O}^*_{X_K \otimes_R \overline{R}})^p)$. Then, via the identification $\mathrm{H}^0_{\mathrm{et}}(X_k \otimes_R \overline{R}, M^1_1) = \mathrm{H}^0_{\mathrm{et}}(X \otimes_R \overline{R}, j_*(\mathcal{O}^*_{X_K \otimes_R \overline{R}})/j_*((\mathcal{O}^*_{X_K \otimes_R \overline{R}})^p))$ the

https://doi.org/10.1112/S0010437X07002813 Published online by Cambridge University Press

element $u([Y])$ coincides with γ. It lies in $U^\lambda \mathrm{H}^1_{\mathrm{et}}(X_K \otimes_R \overline{R}, \mu_p)$ if and only if each γ_i, up to pth powers, lies in $\Gamma(U_i, 1 + \lambda^p \mathcal{O}_{U_i})$.

Assume that Y arises as the restriction to $X_K \otimes_R W$ of the push-forward via η_λ of a G_λ-torsor $Q \to X \otimes_R W$. Suppose also that Q is defined on each U_i by an equation $P_\lambda(e_i) - \alpha_i$ as explained in Remark 5.10. Then, Y is defined on $U_i \otimes_V K$ by the equation $z_i^p - (1 + \lambda^p \alpha_i)$. Hence, $u([Y])$ lies in $U^\lambda \mathrm{H}^1_{\mathrm{et}}(X_K \otimes_R \overline{R}, \mu_p)$.

Conversely, assume that $\gamma_i = 1 + \lambda^p \alpha_i$ with $\alpha_i \in \Gamma(U_i, \mathcal{O}_{U_i})$ for every i. Define a G_λ-torsor $Q \to X \otimes_R W$ as follows. Let $Q|_{U_i}$ be the G_λ-torsor associated to the classifying data with trivial line bundle, trivial extension and datum (U_i, e_i, α_i) as in Remark 5.10. Then, $\mathcal{O}_{Q|_{U_i}}$ is a $\mathcal{O}_{U_i}$-subalgebra of $\mathcal{O}_{Y|_{U_i}}$ via the map $e_i \mapsto 1 + \lambda z_i$ and the inclusion is compatible with the action of G_λ (the action on Y being given via $\eta_\lambda \colon \mathrm{G}_\lambda \to \mu_p$). Thus, the $Q|_{U_i}$ glue to a G_λ-torsor and the restriction to $X_K \otimes_R W$ of its push-forward via η_λ is Y as required. □

7. Hensel's lemma for torsors

In this section we prove an analogue of Hensel's lemma for torsors under group schemes of type G_λ. We fix a p-adically complete and separated, noetherian, flat V-algebra R. Let $S := \mathrm{Spec}(R)$ and fix a projective abelian scheme $X \to S$.

We recall the statement of the classical Hensel's lemma. Assume that R is complete and separated with respect to an ideal $\mathfrak{m}$. Let $f(X)$ be a polynomial with coefficients in R. Let $a \in R$ be such that $f(a) \equiv 0$ modulo $f'(a)^2\mathfrak{m}$. Hensel's lemma asserts that there exists a zero b of f congruent to a modulo $f'(a)\mathfrak{m}$. Furthermore, if $f'(a)$ is not a zero divisor, b is unique with this property; see, for instance, [Eis95, Theorem 7.3].

The Grothendieck algebraization theorem implies that the group $\mathrm{H}^1(X, \mathrm{G}_\lambda)$ coincides with the inverse limit $\lim_n \mathrm{H}^1(X_n, \mathrm{G}_\lambda)$. In particular, given two non-isomorphic G_λ-torsors over X there exists an r, *a priori* depending on X and the two torsors, such that the base-change of the two torsors to X_r are non-isomorphic. This can be interpreted as the analogue of uniqueness of solutions in the classical Hensel's lemma. Proposition 7.1 gives an effective upper bound on r which depends on λ, but not on X. The main tool is the theory of [AG] briefly recalled in § 3. This result is one of the main ingredients in the proof of the existence of the canonical subgroup.

Proposition 7.1. *Suppose that V contains a $(p-1)$th root of p. Let $\lambda \in V$ be such that $\mathrm{v}(\lambda) \leqslant 1/(p-1)$. Assume that r is a rational number such that $p/(p-1) - p\mathrm{v}(\lambda) < r \leqslant 1$. The map $\iota_r^* \colon \mathrm{H}^1(X, \mathrm{G}_\lambda) \to \mathrm{H}^1(X_r, \mathrm{G}_\lambda)$ is injective.*

Proof. Let $\mathfrak{X}$ be the formal R-scheme associated to X. By the Grothendieck algebraization theorem the map $\mathrm{H}^1(X, \mathrm{G}_\lambda) \to \mathrm{H}^1(\mathfrak{X}, \mathrm{G}_\lambda)$, obtained by associating to a torsor its formal completion, is an isomorphism. Indeed, the surjectivity follows remarking that G_λ is finite over V and, thus, every formal G_λ-torsor over $\mathfrak{X}$ is finite and, thus, algebraizable by [EGAIII, 5.4.4]. The injectivity follows from the fact that, given a torsor $f \colon Y \to X$, a section at the level of the associated formal schemes arises from a section of f by [EGAIII, 5.4.1]. Thus, we can replace X by its formal completion.

Let $\mathcal{Y} \to \mathfrak{X}$ be a G_λ-torsor such that $\mathcal{Y}_r$ is trivial. Let $(L, E, \Psi, \{(\mathfrak{U}_i, e_i, \alpha_i)\}_{i \in I})$ be the associated (formal) classifying data. We assume that $\{\mathfrak{U}_i\}_i$ is a covering by formal affine open subschemes of $\mathfrak{X}$. The triviality of Y_r allows us to assume that E and L are trivial modulo p^r and, for every $i \in I$, that $\alpha_i \equiv 0$ modulo p^r. Fix $i \in I$. Consider the polynomial $Q_i(T) := (1 + \lambda T)^p \alpha_i + P_\lambda(T)$ in the variable T and with coefficients in $\Gamma(\mathfrak{U}_i, \mathcal{O}_{\mathfrak{X}})$. It is a polynomial of degree p. Let $a := a(\lambda)$ be as in § 5.4. It is equal to p/λ^{p-1} times a unit of V. By hypothesis, since p admits a $p-1$-root, a admits a $p-1$-root $a^{1/(p-1)}$. The linear term of $P_\lambda(T)$ is a times a unit of $\Gamma(\mathfrak{U}_i, \mathcal{O}_{\mathfrak{X}})$ which is congruent to 1 modulo $\mathfrak{m}$. For every $2 \leqslant h \leqslant p-1$ the coefficient of T^h in $P_\lambda(T)$ is divisible by $a\lambda$.

https://doi.org/10.1112/S0010437X07002813 Published online by Cambridge University Press

The constant term of $P_\lambda(T)$ is zero. Let $S_i(T) := Q_i(a^{1/(p-1)}T)a^{-p/(p-1)}$. Since $r > \mathrm{v}(a^{p/(p-1)})$, the polynomial $S_i(T)$ has coefficients in $\Gamma(\mathfrak{U}_i, \mathcal{O}_{\mathfrak{X}})$, has derivative congruent to 1 modulo $\mathfrak{m}$ and has 0 as a root modulo $\mathfrak{m}$. By Hensel's lemma [Eis95, Theorem 7.3] we deduce that $S_i(T)$ admits a *unique* zero t_i congruent to 0 modulo $\mathfrak{m}$. Thus, $u_i := a^{1/(p-1)}t_i$ is a root of $Q_i(T)$. The element $e_i' := (1+\lambda u_i)e_i + u_i$ satisfies $\Psi(e_i') = 1 + \lambda e_i'$ and in the symmetric algebra of $E|_{\mathfrak{U}_i}$ over $\mathcal{O}_{\mathfrak{U}_i}$ we have

$$\begin{aligned}
P_\lambda(e_i') &= P_\lambda((1+\lambda u_i)e_i + u_i)\\
&= (1+\lambda u_i)^p\biggl(\frac{(1+\lambda e_i)^p - 1}{\lambda^p}\biggr) + \frac{(1+\lambda u_i)^p - 1}{\lambda^p}\\
&= (1+\lambda u_i)^p\alpha_i + P_\lambda(u_i) = Q_i(u_i) = 0.
\end{aligned}$$

Over $\mathfrak{U}_{ij}$ we compute

$$\begin{aligned}
(1+\lambda u_i)^p(1+\lambda u_{ij})^p\alpha_j &= (1+\lambda u_i)^p\alpha_i - (1+\lambda u_i)^p P_\lambda(u_{ij})\\
&= -P_\lambda(u_i) - (1+\lambda u_i)^p P_\lambda(u_{ij})\\
&= -P_\lambda(u_i + u_{ij} + \lambda u_i u_{ij}).
\end{aligned}$$

Thus, $u_i + u_{ij} + \lambda u_i u_{ij}$ satisfies the equation $(1+\lambda T)^p\alpha_j + P_\lambda(T) = 0$. The triviality of $\mathcal{Y}_r$ allows to assume $u_{ij} \equiv 0$ modulo p^r. Thus, $u_i + u_{ij} + \lambda u_i u_{ij} \equiv 0$ modulo $a^{1/(p-1)}\mathfrak{m}$. Put $u_j' := u_i + u_{ij} + \lambda u_i u_{ij}$ and $t_j' := a^{-1/(p-1)}u_j'$. Then, t_j' is an element of $\Gamma(\mathfrak{U}_{ij}, \mathcal{O}_{\mathfrak{X}})$, congruent to 0 modulo $\mathfrak{m}$ and satisfies $S_j(t_j') = 0$. Hence, by the uniqueness of solutions in Hensel's lemma, $t_j' = t_j$ and $u_j = u_j' = u_i + u_{ij} + \lambda u_i u_{ij}$ in $\Gamma(\mathfrak{U}_{ij}, \mathcal{O}_{\mathfrak{X}})$. We compute

$$\begin{aligned}
e_i' &= (1+\lambda u_i)e_i + u_i\\
&= (1+\lambda u_i)(1+\lambda u_{ij})e_j + (1+\lambda u_i)u_{ij} + u_i\\
&= \frac{(1+\lambda u_i)(1+\lambda u_{ij})}{(1+\lambda u_j)}e_j' + (1+\lambda u_i)u_{ij} + u_i - \frac{(1+\lambda u_i)(1+\lambda u_{ij})u_j}{(1+\lambda u_j)}\\
&= \frac{(1+\lambda u_i)(1+\lambda u_{ij})}{(1+\lambda u_j)}e_j' + (1+\lambda u_i)u_{ij} + u_i - u_j\\
&= \frac{(1+\lambda u_i)(1+\lambda u_{ij})}{(1+\lambda u_j)}e_j'.
\end{aligned}$$

Thus, $e_i' := 0$ for every i defines a section of $\mathcal{Y} \to \mathfrak{X}$. This implies that $\mathcal{Y} \to \mathfrak{X}$ is the trivial formal G_λ-torsor as claimed. □

The classical Hensel's lemma provides sufficient conditions for the existence of zeroes of polynomial equations once given approximate solutions. The following proposition can be seen as an analogue of this in our context.

Proposition 7.2. *Let r be a rational number satisfying $2(1-(p-1)\mathrm{v}(\lambda)) < r \leqslant 1$. Let $r' := r - 1 + (p-1)\mathrm{v}(\lambda)$. In the commutative diagram*

$$\begin{tikzcd}
\mathrm{H}^1(X, \mathrm{G}_\lambda) \arrow[r, "\iota_r^*"] \arrow[dr, "\iota_{r'}^*"] & \mathrm{H}^1(X_r, \mathrm{G}_\lambda) \arrow[d, "\iota_{r,r'}^*"]\\
& \mathrm{H}^1(X_{r'}, \mathrm{G}_\lambda)
\end{tikzcd}$$

the image of $\iota_{r'}^*$ coincides with the image of $\iota_{r,r'}^*$.

Proof. As in Proposition 7.1 we may replace X with its associated formal R-scheme $\mathfrak{X}$. Let $Y_r \to X_r$ be a G_λ-torsor and let $(\overline{L}, \overline{E}, \overline{\Psi}, \{(\overline{U}_i, \overline{e}_i, \overline{\alpha}_i)\}_{i\in I})$ be its associated classifying data. We may (and we do) assume that $\{\overline{U}_i\}_i$ is a covering by open affine subschemes of X_r. For every $i \in I$, let $\mathfrak{U}_i$

be the formal open affine subscheme of $\mathfrak{X}$ defined by $\overline{U}_i$ and let $\alpha_i \in \Gamma(\mathfrak{U}_i, \mathcal{O}_{\mathfrak{X}})$ be a lifting of $\overline{\alpha}_i$. Consider the polynomial $Q_{ij}(T) = (1+\lambda T)^p \alpha_j - \alpha_i + P_\lambda(T)$ with coefficients in $\Gamma(\mathfrak{U}_i \cap \mathfrak{U}_j, \mathcal{O}_{\mathfrak{X}})$. Then $Q_{ij}(T)$ is a polynomial with coefficients in $\Gamma(\mathfrak{U}_i \cap \mathfrak{U}_j, \mathcal{O}_{\mathfrak{X}})$ of degree p. Let $a := a(\lambda)$ be as in § 5.4; it is an element of V of valuation $1-(p-1)\mathrm{v}(\lambda)$. The derivative of $Q_{ij}(T)$ has constant coefficient equal to a times a unit and it has the coefficients of terms of higher degree congruent to 0 modulo $a\mathfrak{m}$. Let $\overline{u}_{ij} \in \Gamma(\overline{U}_i \cap \overline{U}_j, \mathcal{O}_{X_r})$ be as in Definition 5.8. Let $\gamma_{ij} \in \Gamma(\mathfrak{U}_i \cap \mathfrak{U}_j, \mathcal{O}_{\mathfrak{X}})$ be a lifting of $\overline{u}_{ij}$. Then $Q'_{ij}(\gamma_{ij}) = a$ times a unit. Since $Q_{ij}(\gamma_{ij})$ is congruent to zero modulo p^r, we conclude from Hensel's lemma [Eis95, Theorem 7.3] that $Q_{ij}(T)$ admits a root $u_{ij} \in \Gamma(\mathfrak{U}_i \cap \mathfrak{U}_j, \mathcal{O}_{\mathfrak{X}})$ which is congruent to γ_{ij}, and thus to $\overline{u}_{ij}$, modulo $p^{r'} = p^r a^{-1}$. Since $\mathfrak{X}$ is V-flat, a is not a zero divisor in $\Gamma(\mathfrak{U}_i \cap \mathfrak{U}_j, \mathcal{O}_{\mathfrak{X}})$. Hence, u_{ij} is *unique* with these properties. For i, j and k in I we have

$$\begin{aligned}(1+\lambda u_{ki})^p(1+\lambda u_{ij})^p\alpha_j &= (1+\lambda u_{ki})^p(\alpha_i - P_\lambda(u_{ij}))\\ &= \alpha_k - P_\lambda(u_{ki}) - (1+\lambda u_{ki})^p P_\lambda(u_{ij})\\ &= \alpha_k - P_\lambda(u_{ki}+u_{ij}+\lambda u_{ki}u_{ij}).\end{aligned}$$

Since there exists a unique zero of $Q_{ij}(T)$ congruent to $\overline{u}_{ij}$ modulo $p^{r'}$, as guaranteed by Hensel's lemma, we conclude that $u_{kj} = u_{ki} + u_{ij} + \lambda u_{ki}u_{ij}$. Over $\mathfrak{U}_i$ define L as $\mathcal{O}_{\mathfrak{U}_i} e_i$ and E as $\mathcal{O}_{\mathfrak{U}_i} \oplus \mathcal{O}_{\mathfrak{U}_i} e_i$. Over $\mathfrak{U}_i \cap \mathfrak{U}_j$ impose the gluing condition $e_i := (1+\lambda u_{ij})e_j + u_{ij}$. Since $u_{kj} = u_{ki} + u_{ij} + \lambda u_{ki}u_{ij}$, we have

$$\begin{aligned}e_k &= (1+\lambda u_{ki})e_i + u_{ki}\\ &= (1+\lambda u_{ki})(1+\lambda u_{ij})e_j + (1+\lambda u_{ki})u_{ij} + u_{ki}\\ &= (1+\lambda u_{kj})e_j + u_{kj}.\end{aligned}$$

In particular, we obtain an invertible sheaf L over $\mathfrak{X}$ and an extension E of L by $\mathcal{O}_{\mathfrak{X}}$. Furthermore, there is a unique morphism of $\mathcal{O}_{\mathfrak{X}}$-modules $\Psi\colon E \to E$ defined over each $\mathfrak{U}_i$ by $\Psi(e_i) = 1 + \lambda e_i$. One verifies that (L, E, Ψ) is a global classifying datum, in the sense of Definition 5.5, and hence defines a formal $\mathcal{G}^{(\lambda)}$-torsor $\mathcal{Y}^{(\lambda)} \to \mathfrak{X}$. Proceeding as in Remark 5.10 we get a formal G_λ-torsor $\mathcal{Y} \to \mathfrak{X}$. Its algebraization $Y \to X$ defines a G_λ-torsor. By construction, it lifts $Y_{r'} \to X_{r'}$ as claimed. □

Corollary 7.3. *Fix $\lambda \in V$ such that*

$$\frac{p}{(p-1)(2p-1)} < \mathrm{v}(\lambda) \leqslant \frac{1}{p-1}.$$

Then, the natural morphism

$$\iota^*_{(p-1)\mathrm{v}(\lambda)}\colon \mathrm{H}^1(X, \mathrm{G}_\lambda) \longrightarrow \mathrm{Im}(\iota^*_{1,(p-1)\mathrm{v}(\lambda)}\colon \mathrm{H}^1(X_1, \mathrm{G}_\lambda) \to \mathrm{H}^1(X_{(p-1)\mathrm{v}(\lambda)}, \mathrm{G}_\lambda))$$

is an isomorphism.

Proof. Since

$$\frac{p}{(p-1)(2p-1)} < \mathrm{v}(\lambda),$$

the injectivity follows from Proposition 7.1 with $r = (p-1)\mathrm{v}(\lambda)$. Note that $2(1-(p-1)\mathrm{v}(\lambda)) < 2 - 2(p/(2p-1)) < 1$. Hence, the surjectivity follows from Proposition 7.2 with $r = 1$. □

Remark 7.4. If $p > 2$, then

$$\frac{1}{p} \leqslant \mathrm{v}(\lambda) \leqslant \frac{1}{p-1}$$

implies that

$$\frac{p}{(p-1)(2p-1)} < \mathrm{v}(\lambda) \leqslant \frac{1}{p-1}.$$

https://doi.org/10.1112/S0010437X07002813 Published online by Cambridge University Press

8. Torsors modulo p

Let R be a p-adically complete and separated, noetherian, flat V-algebra and let $X \to \operatorname{Spec}(R)$ be a projective abelian scheme. We can interpret, under suitable hypothesis on λ, the elements of $\mathrm{H}^1(X, \mathrm{G}_\lambda)$ as torsors à la Artin–Schreier on the reduction of X modulo p^r with r depending only on λ. Remark that a crucial point is that $r \leqslant 1$.

Suppose that $\mathrm{v}(\lambda) \leqslant 1/(p-1)$. Let $r \in \mathbb{Q}$ be such that $\max\{1/p, (p-1)\mathrm{v}(\lambda)\} \leqslant r \leqslant 1$. Denote by F the Frobenius homomorphism on X_1 and let $a(\lambda)$ be as in § 5.4. Then, $\mathrm{F} - a(\lambda) \colon \mathrm{H}^1(X_1, \mathcal{O}_{X_1}) \to \mathrm{H}^1(X_1, \mathcal{O}_{X_1})$ factors via $\mathrm{H}^1(X_1, \mathcal{O}_{X_1}) \to \mathrm{H}^1(X_r, \mathcal{O}_{X_r})$. By abuse of notation we call $\mathrm{F} - a(\lambda) : \mathrm{H}^1(X_r, \mathcal{O}_{X_r}) \to \mathrm{H}^1(X_1, \mathcal{O}_{X_1})$ the induced map. The main result of this section is the following.

Theorem 8.1. *Assume that*

$$\frac{p}{(p-1)(2p-1)} < \mathrm{v}(\lambda) \leqslant \frac{1}{p-1}.$$

Let $r := (p-1)\mathrm{v}(\lambda)$. *Then,*

$$\mathrm{H}^1(X, \mathrm{G}_\lambda)/\mathrm{H}^1(R, \mathrm{G}_\lambda) \xrightarrow{\sim} \operatorname{Ker}(\mathrm{H}^1(X_r, \mathcal{O}_{X_r}) \xrightarrow{\mathrm{F} - a(\lambda)} \mathrm{H}^1(X_1, \mathcal{O}_{X_1})).$$

The proof of the theorem is based on two main ingredients. One is our version of Hensel's lemma for torsors, Corollary 7.3. The other is the analysis of the kernel of $\mathrm{F} - a(\lambda)$. This is based on the crucial Lemma 8.2 and also Lemma 8.3.

Lemma 8.2. *Let* λ *be an element of* V *satisfying* $\mathrm{v}(\lambda) \leqslant 1/(p-1)$ *and* $\lambda^{p-1} \equiv 0 \mod p^r$ *with* $r \leqslant 1$. *Let* $\rho_r^\lambda \colon \mathcal{G}_r^{(\lambda)} \to \mathbf{G}_{a,r}$ *be the map defined by* $W \mapsto \sum_{i=1}^{p-1} (-\lambda)^{i-1}(T^i/i)$. *Then,* ρ_r^λ *defines an isomorphism of group schemes. Furthermore, the following diagram commutes.*

$$\begin{tikzcd}
\mathcal{G}_r^{(\lambda)} \arrow[r, "\phi_\lambda"] \arrow[d, "\rho_r^\lambda"'] & \mathcal{G}_r^{(\lambda^p)} \arrow[d, "\varrho_r^{\lambda^p}"] \\
\mathbf{G}_{a,r} \arrow[r, "\mathrm{F} - a(\lambda)"] & \mathbf{G}_{a,r}
\end{tikzcd}$$

In particular, ρ_r^λ *identifies* $\mathrm{G}_{(a(\lambda), c(\lambda))}$ *with* G_λ *over* $\operatorname{Spec}(V_r)$*; see Definition 5.1 and § 5.4 for notation.*

Proof. Let $\log(1+W) := \sum_{i=1}^{\infty} (-1)^{i+1}(W^i/i) \in K[\![W]\!]$; it defines an isomorphism between the formal groups $\widehat{\mathbf{G}_{m,K}}$ and $\widehat{\mathbf{G}_{a,K}}$; in particular we have a formal identity of power series $\log((1+W) \otimes (1+W)) = \log(1+W) \otimes 1 + 1 \otimes \log(1+W)$. From this we deduce

$$\sum_{i=1}^{p-1} (-\lambda)^{i-1} \frac{(T \otimes 1 + 1 \otimes T + \lambda T \otimes T)^i}{i} = \left(\sum_{i=1}^{p-1} (-\lambda)^{i-1} \frac{T^i}{i} \right) \otimes 1 + 1 \otimes \left(\sum_{i=1}^{p-1} (-\lambda)^{i-1} \frac{T^i}{i} \right)$$

in the ring $V[T] \otimes_V V[T]$ up to terms in $\lambda^{p-1}(T \otimes 1, 1 \otimes T)^p$ and, thus, the equality above holds in $V_r[T] \otimes_{V_r} V_r[T]$ since $\lambda^{p-1} \equiv 0$ in V_r. This implies that ρ_r^λ is compatible with the two comultiplications. Since $\sum_{i=1}^{p-1} (-\lambda)^{i-1}(T^i/i)$ is equal to T times a unit in $V_r[T]$ congruent to 1 modulo λ, we deduce that ρ_r^λ sends the ideal (W) to the ideal (T) and induces an isomorphism of tangent spaces at the origin. We conclude that ρ_r^λ is a homomorphism of V_r-group schemes and it is étale. Since ρ_r^λ is an isomorphism modulo λ and $V_r[T]$ is λ-adically complete and separated, ρ_r^λ is surjective at the level of underlying algebras and, hence, it is a closed immersion. We conclude that ρ_r^λ is an isomorphism.

Regarding the commutativity of the diagram in Lemma 8.2, we argue as follows. Since $\lambda^{p-1} = 0$ in V_r, the homomorphism $\rho_r^{\lambda^p}$ is $W \mapsto T$. Thus, we may identify $\mathcal{G}_r^{(\lambda^p)}$ with $\mathbf{G}_{a,r}$ via $\rho_r^{\lambda^p}$. We have to prove that $P_\lambda(T) = \phi_\lambda(W) = \rho_r^\lambda(\mathrm{F}(W) - a(\lambda)(W))$. Since $p \equiv 0$ in V_r, we have $a(\lambda) \equiv -p/\lambda^{p-1}$

https://doi.org/10.1112/S0010437X07002813 Published online by Cambridge University Press

in V_r and $\rho_r^\lambda(\mathrm{F}(W)) = T^p$. Thus, the commutativity of the diagram is equivalent to the equality $P_\lambda(T) \equiv T^p - a(\lambda)\rho_r^\lambda(T)$ modulo p. It suffices, then, to show that

$$\sum_{i=1}^{p-1} \frac{1}{p}\binom{p}{i}\lambda^{i-1}T^i \equiv \sum_{i=1}^{p-1}(-\lambda)^{i-1}\frac{T^i}{i} \quad \mathrm{mod}(p). \tag{8.2.1}$$

It is easy to see, by induction on i, that, for $1 \leqslant i \leqslant p-1$, one has

$$\frac{1}{p}\binom{p}{i} \equiv \frac{(-1)^{i-1}}{i} \quad \mathrm{mod}(p),$$

and from this we conclude. □

Lemma 8.3. *Let $\lambda \in V$ be such that*

$$\frac{1}{p(p-1)} \leqslant \mathrm{v}(\lambda) \leqslant \frac{1}{p-1}$$

and write $r := (p-1)\mathrm{v}(\lambda)$. The following diagram is commutative.

$$\begin{tikzcd}
\mathcal{G}_1^{(\lambda)} \arrow[rr, "\phi_\lambda"] \arrow[d] & & \mathcal{G}_1^{(\lambda^p)} \arrow[d, "\varrho_1^{\lambda^p}"] \\
\mathcal{G}_r^{(\lambda)} \arrow[r, "\varrho_r^\lambda"] & \mathbf{G}_{a,r} \arrow[r, "\mathrm{F}-a(\lambda)"] & \mathbf{G}_{a,1}
\end{tikzcd}$$

Proof. Let U be a scheme over V_1. Let $u \in \mathcal{G}_1^{(\lambda)}(U)$ and let $\overline{u}$ be the reduction of u modulo p^r. Since $a(\lambda) \equiv -p/\lambda^{p-1}$ modulo p, the element $((\mathrm{F}-a(\lambda))\varrho_r^\lambda)(\overline{u})$ is

$$\left(\sum_{h=1}^{p-1}(-\lambda)^{(h-1)}\frac{u^h}{h}\right)^p + \frac{p}{\lambda^{p-1}}\left(\sum_{h=1}^{p-1}(-\lambda)^{(h-1)}\frac{u^h}{h}\right)$$

modulo p^r. On the other hand, $(\varrho_1^{\lambda^p}\phi_\lambda)(u)$ is the element $\sum_{t=1}^{p-1}(-\lambda^p)^{t-1}(P_\lambda(u)^t/t)$. Since $P_\lambda(u) = ((1+\lambda u)^p - 1)/\lambda^p$ and $(p/\lambda^{p-1})^t\lambda^{p(t-1)} \equiv 0$ modulo p for $t \geqslant 2$, we have

$$\sum_{t=1}^{p-1}(-\lambda^p)^{t-1}\frac{P_\lambda(u)^t}{t} \equiv \sum_{t=1}^{p-1}(-\lambda^p)^{t-1}\frac{u^{pt}}{t} + (P_\lambda(u) - u^p).$$

It suffices to prove that $P_\lambda(u) - u^p$ is congruent to $(p/\lambda^{p-1})(\sum_{h=1}^{p-1}(-\lambda)^{(h-1)}(u^h/h))$ modulo p. This follows from (8.2.1). □

Consider the following commutative diagram with exact rows.

$$\begin{tikzcd}
\mathrm{H}^0(R_1, \mathcal{G}^{(\lambda^p)}) \arrow[r] \arrow[d] & \mathrm{H}^1(R_1, \mathrm{G}_\lambda) \arrow[r] \arrow[d] & \mathrm{H}^1(R_1, \mathcal{G}^{(\lambda)}) \arrow[r, "\phi_\lambda"] \arrow[d] & \mathrm{H}^1(R_1, \mathcal{G}^{(\lambda^p)}) \arrow[d] \\
\mathrm{H}^0(X_1, \mathcal{G}^{(\lambda^p)}) \arrow[r] & \mathrm{H}^1(X_1, \mathrm{G}_\lambda) \arrow[r] & \mathrm{H}^1(X_1, \mathcal{G}^{(\lambda)}) \arrow[r, "\phi_\lambda"] & \mathrm{H}^1(X_1, \mathcal{G}^{(\lambda^p)})
\end{tikzcd}$$

Then, $\mathrm{H}^0(X_1, \mathcal{G}^{(\lambda^p)}) = \mathrm{H}^0(R_1, \mathcal{G}^{(\lambda^p)})$ since $X \to \mathrm{Spec}(R)$ is an abelian scheme. Furthermore, $\mathrm{H}^1(R_1, \mathcal{G}^{(\lambda)}) = 0$. Indeed, every $\mathcal{G}^{(\lambda)}$-torsor Y over R_r admits a section σ_k over R_k because $\mathrm{H}^1(R_k, \mathcal{G}^{(\lambda)}) \cong \mathrm{H}^1(R_k, \mathbf{G}_a) = \{0\}$. Since $\mathcal{G}^{(\lambda)}$ is a smooth group scheme, Y is smooth over R_r. Since R_r is affine, σ_k can be lifted to a section of Y over R_r. In particular, the map $\mathrm{H}^0(R_1, \mathcal{G}^{(\lambda^p)}) \to \mathrm{H}^1(R_1, \mathrm{G}_\lambda)$ is surjective. Thus, the image of $\mathrm{H}^0(X_1, \mathcal{G}^{(\lambda^p)})$ in $\mathrm{H}^1(X_1, \mathrm{G}_\lambda)$ is the image of $\mathrm{H}^1(R_1, \mathrm{G}_\lambda)$ in $\mathrm{H}^1(X_1, \mathrm{G}_\lambda)$. The composite

$$\mathrm{H}^1(R_1, \mathrm{G}_\lambda) \longrightarrow \mathrm{H}^1(X_1, \mathrm{G}_\lambda) \longrightarrow \mathrm{H}^1(X_r, \mathrm{G}_\lambda) \longrightarrow \mathrm{H}^1(X_r, \mathcal{G}^{(\lambda)}) \xrightarrow{\varrho_r^\lambda} \mathrm{H}^1(X_r, \mathcal{O}_{X_r}),$$

https://doi.org/10.1112/S0010437X07002813 Published online by Cambridge University Press

factors via $\mathrm{H}^1(R_r, \mathcal{O}_{R_r}) = \{0\}$. We then get a *complex*

$$\begin{tikzcd}
\mathrm{H}^1(X_1, \mathrm{G}_\lambda)/\mathrm{H}^1(R_1, \mathrm{G}_\lambda) \arrow[r, "j_r"] \arrow[d, equal] & \mathrm{H}^1(X_r, \mathcal{O}_{X_r}) \arrow[r, "\mathrm{F}-a(\lambda)"] & \mathrm{H}^1(X_1, \mathcal{O}_{X_1}). \\
\mathrm{H}^1(X_1, \mathrm{G}_\lambda)/\mathrm{H}^0(X_1, \mathcal{G}^{(\lambda^p)}) & &
\end{tikzcd} \tag{8.3.1}$$

Proposition 8.4. *If* $\mathrm{H}^1(X_1, \mathcal{G}^{(\lambda)}) \to \mathrm{H}^1(X_r, \mathcal{G}^{(\lambda)})$ *is surjective, then* (8.3.1) *is an exact sequence.*

Proof. Using Lemma 8.3 and taking the associated map of torsors over Y, the surjectivity of ϱ_r^λ and the fact that $\varrho_1^{\lambda^p}$ is an isomorphism, we deduce that the map from the kernel of $\phi_\lambda \colon \mathrm{H}^1(X_1, \mathcal{G}^{(\lambda)}) \to \mathrm{H}^1(X_1, \mathcal{G}^{(\lambda^p)})$ to the kernel of $\mathrm{F} - a(\lambda) \colon \mathrm{H}^1(X_r, \mathbf{G}_a) \to \mathrm{H}^1(X_1, \mathbf{G}_a)$ is an isomorphism. The kernel of ϕ_λ is $\mathrm{H}^1(X_1, \mathrm{G}_\lambda)/\mathrm{H}^0(X_1, \mathcal{G}^{(\lambda^p)})$. The proposition follows. □

Lemma 8.5. *For every* $r' \geqslant r \geqslant \mathrm{v}(\lambda)$ *the map* $\mathrm{H}^1(X_{r'}, \mathcal{G}^{(\lambda)}) \to \mathrm{H}^1(X_r, \mathcal{G}^{(\lambda)})$ *is surjective.*

Proof. Since there exists n such that $2^n r \geqslant r'$, by induction it suffices to prove the lemma for $r' = 2r$. Let $\eta \colon \mathcal{G}^{(\lambda)} \to \mathbf{G}_m = \mathrm{Spec}(V[Z, Z^{-1}])$ be the homomorphism of V-group schemes defined at the level of algebras by $Z \mapsto 1 + \lambda T$; cf. § 5.3. Consider the following exact sequence of Zariski sheaves on X_{2r}:

$$\begin{tikzcd}
0 \arrow[r] & \mathcal{O}_{X_r} \arrow[r, "\alpha_\lambda"] \arrow[d, equal] & \mathcal{G}^{(\lambda)}_{X_{2r}} \arrow[r] \arrow[d, "\eta"'] & \mathcal{G}^{(\lambda)}_{X_r} \arrow[r] \arrow[d, "\eta"'] & 0 \\
0 \arrow[r] & \mathcal{O}_{X_r} \arrow[r, "\alpha_1"] & \mathbf{G}_{m,X_{2r}} \arrow[r] & \mathbf{G}_{m,X_r} \arrow[r] & 0
\end{tikzcd}$$

where α_s is the homomorphism locally given by $a \mapsto 1 + \lambda(p^r s^{-1})a$ for every $s \in V$ with $r \geqslant \mathrm{v}(s)$. Taking the associated long exact sequences of cohomology and using that $\mathrm{H}^1(\_, \mathcal{G}^{(\lambda)})$ (respectively, $\mathrm{H}^1(\_, \mathbf{G}_m)$) for the Zariski or fppf topologies are the same [AG, Corollary 2.5], we get the following commutative diagram with exact rows.

$$\begin{tikzcd}
\mathrm{H}^1(X_{2r}, \mathcal{G}^{(\lambda)}) \arrow[r] \arrow[d, "\eta"'] & \mathrm{H}^1(X_r, \mathcal{G}^{(\lambda)}) \arrow[r] \arrow[d, "\eta"'] & \mathrm{H}^2(X_r, \mathcal{O}_{X_r}) \arrow[d, equal] \\
\mathrm{H}^1(X_{2r}, \mathbf{G}_m) \arrow[r] & \mathrm{H}^1(X_r, \mathbf{G}_m) \arrow[r] & \mathrm{H}^2(X_r, \mathcal{O}_{X_r})
\end{tikzcd}$$

The image of η in $\mathrm{Pic}(X_r/R_r)$ is contained in the connected component $\mathrm{Pic}^0(X_r/R_r)$ of the identity; indeed, since $\mathrm{v}(\lambda) > 0$, over R_k the image of η is the trivial invertible sheaf. The obstruction to lift invertible sheaves algebraically equivalent to 0 over X_r to X_{2r} is given by a group scheme homomorphism $\mathrm{ob} \colon \mathrm{Pic}^0(X_r/R_r) \to \mathrm{H}^2(X_r, \mathcal{O}_{X_r})$. Since X is an abelian scheme over $\mathrm{Spec}(R)$, then $\mathrm{Pic}^0(X_r/R_r)$ is proper and geometrically connected. Since $\mathrm{H}^2(X_r, \mathcal{O}_{X_r})$ is affine, the obstruction map ob is trivial. In particular, the map $\mathrm{H}^1(X_r, \mathcal{G}^{(\lambda)}) \to \mathrm{H}^1(X_r, \mathbf{G}_m) \to \mathrm{H}^2(X_r, \mathcal{O}_{X_r})$ is zero. The conclusion follows. □

8.6 Proof of Theorem 8.1

Consider the composite map

$$\begin{tikzcd}
\mathrm{H}^1(X, \mathrm{G}_\lambda)/\mathrm{H}^1(R, \mathrm{G}_\lambda) \arrow[d, "\iota_1"'] & \\
\mathrm{H}^1(X_1, \mathrm{G}_\lambda)/\mathrm{H}^1(R_1, \mathrm{G}_\lambda) \arrow[r, "j_r"] & \mathrm{Ker}(\mathrm{F} - a(\lambda) \colon \mathrm{H}^1(X_r, \mathcal{O}_{X_r}) \to \mathrm{H}^1(X_1, \mathcal{O}_{X_1})),
\end{tikzcd}$$

where j_r is the homomorphism introduced in (8.3.1). It suffices to prove that $j_r \circ \iota_1$ is an isomorphism. By Proposition 8.4 the map j_r is surjective. By construction, j_r factors via

$$\mathrm{H}^1(X_1, \mathrm{G}_\lambda)/\mathrm{H}^1(R_1, \mathrm{G}_\lambda) \to \mathrm{H}^1(X_r, \mathrm{G}_\lambda)/\mathrm{H}^1(R_r, \mathrm{G}_\lambda) \hookrightarrow \mathrm{H}^1(X_r, \mathcal{G}^{(\lambda)}) \xrightarrow{\sim} \mathrm{H}^1(X_r, \mathcal{O}_{X_r}),$$

where the latter isomorphism is defined using Lemma 8.2. Since the hypotheses of Proposition 7.2 are satisfied, the map $j_r \circ \iota_1$ is surjective. One verifies that the conditions in Proposition 7.1 apply in our case so that the reduction map $\iota_r \colon \mathrm{H}^1(X, \mathrm{G}_\lambda) \to \mathrm{H}^1(X_r, \mathrm{G}_\lambda)$ is injective. By Proposition 5.13 the map $\mathrm{H}^1(X, \mathrm{G}_\lambda)/\mathrm{H}^1(R, \mathrm{G}_\lambda) \to \mathrm{H}^1(X_r, \mathrm{G}_\lambda)/\mathrm{H}^1(R_r, \mathrm{G}_\lambda)$ is injective. Thus, $j_r \circ \iota_1$ is injective as well. This proves the theorem.

Remark 8.7. If $f \colon Y \to X$ is a morphism of projective abelian schemes over $\mathrm{Spec}(R)$. One verifies that the following diagram commutes.

$$\begin{tikzcd}
\mathrm{H}^1(X_1, \mathrm{G}_\lambda)/\mathrm{H}^1(R_1, \mathrm{G}_\lambda) \arrow[r, "j_r"] \arrow[d, "f^*"'] & \mathrm{H}^1(X_r, \mathcal{O}_{X_r}) \arrow[r, "\mathrm{F}-a(\lambda)"] \arrow[d, "f^*"'] & \mathrm{H}^1(X_1, \mathcal{O}_{X_1}) \arrow[d, "f^*"] \\
\mathrm{H}^1(Y_1, \mathrm{G}_\lambda)/\mathrm{H}^1(R_1, \mathrm{G}_\lambda) \arrow[r, "j_r"] & \mathrm{H}^1(Y_r, \mathcal{O}_{Y_r}) \arrow[r, "\mathrm{F}-a(\lambda)"] & \mathrm{H}^1(Y_1, \mathcal{O}_{Y_1})
\end{tikzcd}$$

8.8 Relation to the Lie algebra of Pic

Let M be an R-scheme and let $X_M := X \times_R M$. Let

$$\tau_M \colon \mathrm{H}^1(X_M, \mathrm{G}_\lambda)/\mathrm{H}^1(M, \mathrm{G}_\lambda) \longrightarrow \mathrm{Hom}(\mathrm{G}_{\lambda,M}^\vee, \mathrm{Pic}_{X_M/M})$$

be the map defined in § 5.12.

Assume that $M := \mathrm{Spec}(R_r)$ and that $\lambda^{p-1} \equiv 0$ modulo p^r, $r \leqslant 1$. Let $R_r[\varepsilon]$ be the ring of dual numbers on R_r. Let $\delta \in \mathrm{Lie}(\mathrm{G}_{\lambda,R_r}^\vee)$ be the element defined by the map

$$\delta \colon \mathrm{G}_\lambda \times_{R_r} \mathrm{Spec}(R_r[\varepsilon]) \longrightarrow \mathbf{G}_m \times_{R_r} \mathrm{Spec}(R_r[\varepsilon])$$

given by the composite of the inclusion $\mathrm{G}_\lambda \to \mathcal{G}^{(\lambda)}$, the map $\rho_r^\lambda \colon \mathcal{G}_r^{(\lambda)} \to \mathbf{G}_{a,r}$ defined in Lemma 8.2 and the map $\mathbf{G}_a \times_{R_r} \mathrm{Spec}(R_r[\varepsilon]) \to \mathbf{G}_m \times_{R_r} \mathrm{Spec}(R_r[\varepsilon])$ given by $Z \to 1 + \varepsilon W$.

Proposition 8.9. *Let $Y_r \to X_r$ be a G_λ-torsor, r as above. Let $[Y_r] \in \mathrm{H}^1(X_r, \mathcal{G}^{(\lambda)})$ be the associated class. Let $\varrho_r^\lambda \colon \mathrm{H}^1(X_r, \mathcal{G}^{(\lambda)}) \to \mathrm{H}^1(X_r, \mathbf{G}_a)$ be the application induced by the map ϱ_λ^r in Lemma 8.2. The homomorphism*

$$\mathrm{Lie}(\tau_{R_r}([Y_r])) \colon \mathrm{Lie}(\mathrm{G}_{\lambda,R_r}^\vee) \longrightarrow \mathrm{Lie}(\mathrm{Pic}_{X_r/R_r}) = \mathrm{H}^1(X_r, \mathcal{O}_{X_r}),$$

sends δ to $\varrho_r^\lambda([Y_r])$.

Proof. Let $(L, E, \Psi, \{(U_i, e_i, \alpha_i)\}_{i \in I})$ be the classifying data associated to $Y_r \to X_r$; see Definition 5.8. Then $Y_r|_{U_i} = \mathrm{Spec}(\mathcal{O}_{U_i}[e_i]/(P_\lambda(e_i) - \alpha_i))$. The gluing morphisms are defined by $e_i = (1 + \lambda u_{i,j})e_j + u_{ij}$ for suitable $u_{ij} \in \Gamma(U_i \cap U_j, \mathcal{O}_{X_r})$. The $\mathcal{G}^{(\lambda)}$-torsor associated to $Y_r \to X_r$ is defined by the 1-cocycle $(u_{ij})_{i,j}$. The push-forward of $Y_r \to X_r$ via ρ_r^λ is the $\mathbf{G}_a$-torsor defined by the 1-cocycle $(\sum_{s=1}^{p-1}(-\lambda)^{s-1}(u_{ij}^s/s))_{i,j}$. This cocycle represents $\varrho_r^\lambda([Y_r])$. On the other hand, $\tau_{R_r}([Y_r])(\delta)$ is the $\mathbf{G}_m$-torsor over $X_r \times_{R_r} \mathrm{Spec}(R_r[\varepsilon])$ defined by the 1-cocycle $(1 + \varepsilon(\sum_{s=1}^{p-1}(-\lambda)^{s-1}(u_{ij}^s/s)))_{i,j}$. This proves the claim. □

We conclude the section by showing the following.

Lemma 8.10. *The element δ generates $\mathrm{Lie}(\mathrm{G}_{\lambda,R_r}^\vee)$ as an R_r-module.*

https://doi.org/10.1112/S0010437X07002813 Published online by Cambridge University Press

Proof. By Nakayama's lemma, we may assume that $\lambda \equiv 0$ in R_r. Take $\delta' \in \mathrm{Lie}(\mathrm{G}^\vee_{\lambda,R_r})$. View it as a homomorphism $\mathrm{G}_\lambda \times_{R_r} \mathrm{Spec}(R_r[\varepsilon]) \to \mathbf{G}_m \times_{R_r} \mathrm{Spec}(R_r[\varepsilon])$ reducing to the identity modulo ε. Then, δ' is of the form $Z \mapsto 1 + \varepsilon f(T)$ with $f(T)$ a polynomial with coefficients in R_r of degree at most $p-1$. Since δ' is a group homomorphism we have $f(0) = 0$ and $f(T \otimes 1 + 1 \otimes T) = f(T) \otimes 1 + 1 \otimes f(T)$. An easy computation shows that $f(T) = cT$ with $c \in R_r$. Hence, $\delta' = c\delta$. □

9. Hasse–Witt equations

Let R be a p-adically complete and separated, noetherian, normal flat V-algebra. Let M be a free R-module of rank g. For every $r \in \mathrm{v}(\mathfrak{m})$ denote $M_r := M/p^r M$. Let $\mathrm{F}\colon M_1 \to M_1$ be a Frobenius linear homomorphism, i.e. $\mathrm{F}(c_1 m_1 + c_2 m_2) = c_1^p \mathrm{F}(m_1) + c_2^p \mathrm{F}(m_2)$ for every $m_1,\ m_2 \in\ M$ and c_1, $c_2 \in R_1$. We denote by $\det(\mathrm{F}) R_1$ the ideal defined by the determinant of a matrix of F; note that, although the determinant depends on the choice of the matrix representing F, the ideal it generates does not.

Let $a \in V$ with $\mathrm{v}(a) = w$ satisfying $0 \leqslant w \leqslant (p-1)/p$. Consider the induced map

$$\mathrm{F} - a\colon M_{1-w} \longrightarrow M_1$$

(observe that this makes sense due to the assumption on w). Then we have the following.

Proposition 9.1. *If $w < \frac{1}{2}$ and $p^w \in \det(\mathrm{F}) R_1$, then:*

(i) *$\mathrm{Ker}(\mathrm{F} - a)$ is a $\mathbb{F}_p$-vector space of dimension $\leqslant g$;*

(ii) *there exists a finite, normal extension $R \subset R'$, étale over $R_K := R \otimes_V K$, such that the dimension of the kernel $\mathrm{Ker}_{R'}(\mathrm{F} - a)$ of $\mathrm{F} - a\colon M_{1-w} \otimes_R R' \to M_1 \otimes_R R'$ is exactly g;*

(iii) *for every morphism of normal, p-adically complete and separated V-algebras $R' \to R''$, the map $\mathrm{Ker}_{R'}(\mathrm{F} - a) \to \mathrm{Ker}_{R''}(\mathrm{F} - a)$ is an isomorphism.*

Remark 9.2. In the case we are interested in, one has $a = a(\lambda) \equiv p/\lambda^{p-1}$ modulo p. If λ satisfies

$$\frac{p}{(p-1)(2p-1)} < \mathrm{v}(\lambda) \leqslant \frac{1}{p-1},$$

then $0 \leqslant \mathrm{v}(a(\lambda)) = 1 - (p-1)\mathrm{v}(\lambda) < (p-1)/(2p-1) < \frac{1}{2}$. Thus, the condition on w in Proposition 9.1 is automatically satisfied.

Remark 9.3. The statement of Proposition 9.1 and the strategy of the proof is similar to (and inspired by) [AM04, § 5].

Proof. Fix a basis $\mathcal{B}$ of M. Let $U_1 \in M_{g \times g}(R_1)$ be a matrix of F with respect to $\mathcal{B}$. Let U be a lift of U_1 in $M_{g \times g}(R)$. Remark that there exists $c \in R$ and $u \in R^*$ such that $\det(U)c = p^w u$. In particular, U is invertible in R_K. Indeed, by assumption, there exists $c \in R$ such that $p^w \equiv \det(U)c$ modulo p. Thus, there exists $s \in R$ satisfying $\det(U)c = p^w - ps = p^w(1 - sp^{1-w})$ and $u := 1 - sp^{1-w}$ is a unit in R since the latter is p-adically complete and separated.

The choice of $\mathcal{B}$ allows us to identify M with R^g. We view an element m of M as a column vector $\underline{X}$. If $\underline{X} = {}^{\mathrm{t}}(x_1, \ldots, x_g)$, then denote $\underline{X}^p := {}^{\mathrm{t}}(x_1^p, \ldots, x_g^p)$. Define

$$\mathbf{Z}_R(a) := \{\underline{X} \in R^g \mid U\underline{X}^p - a\underline{X} = 0\} \quad \text{and} \quad \mathbf{Z}(a,r) := \{\underline{X} \in R_r^g \mid U\underline{X}^p - a\underline{X} = 0\}$$

for $r \geqslant 0$. For $0 \leqslant r' \leqslant r''$ denote by $\mathrm{red}_{r'',r'}$ the reduction map $\mathbf{Z}(a, r'') \to R^g_{r'}$. Define $\mathrm{red}_{r''}$ as the map $\mathbf{Z}_R(a) \to R^g_{r''}$. Remark that $\mathbf{Z}(a,1)$ is a $\mathbb{F}_p$-vector space and that $\mathrm{Ker}(\mathrm{F} - a)$ is identified with $\mathrm{red}_{1,1-w}(\mathbf{Z}(a,1))$. Thus, the proposition follows from the following. □

https://doi.org/10.1112/S0010437X07002813 Published online by Cambridge University Press

Lemma 9.4. *The following hold:*

(i) $\mathbf{Z}_R(a)$ *has cardinality less than or equal to* p^g*;*

(ii) *there exists a finite, normal extension* $R \subset R'$*, étale over* $R_K := R \otimes_V K$*, such that the set* $\mathbf{Z}_{R'}(a)$ *has cardinality exactly* p^g*;*

(iii) *for every normal extension* $R' \subset R''$ *the map* $\mathbf{Z}_{R'}(a) \to \mathbf{Z}_{R''}(a)$ *is a bijection.*

Lemma 9.5. *The map* red_{1-w} *induces a bijection* $\mathbf{Z}_R(a) \xrightarrow{\sim} \mathrm{red}_{1,1-w}(\mathbf{Z}(a,1))$*.*

Proof of Lemma 9.4. We start by proving that aU^{-1} is a matrix with coefficients in R. Let $V \in M_{g\times g}(R)$ such that $VU = UV = \det(U)\mathbf{1}_g$. Then, $aU^{-1} = (a/\det(U))V$. By the above there exists $c \in R$ and $u \in R^*$ such that $\det(U)c = p^w u$. However, $\mathrm{v}(a) = w$, thus $a/\det(U) = ac/p^w u \in R$.

Let W be the closed subscheme of $\mathbb{A}^g_R$ defined by the equations $\underline{X}^p - aU^{-1}\underline{X} = 0$. It is finite and flat over R of rank p^g. In particular, it is an affine scheme p-adically complete and separated. Due to the normality of R we conclude from the valuative criterion of properness and [EGAIV, 20.4.12], that $\mathbf{Z}_R(a) = W(R) = W(R_K)$. To conclude the proof of the lemma it is enough to show that W is unramified over R_K. We compute the determinant of the Jacobian matrix of the equations defining W:

$$\det\left(p\begin{pmatrix} X_1^{p-1} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & X_p^{p-1}\end{pmatrix} - aU^{-1}\right) = \det(aU^{-1})\det\left(\frac{p}{a}U\begin{pmatrix} X_1^{p-1} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & X_p^{p-1}\end{pmatrix} - \mathbf{1}_g\right).$$

Note that $\det(aU^{-1})$ is in R and it is invertible in R_K. The second factor on the right-hand side is an invertible element in the ring of functions B_W of W. Indeed, it is congruent to 1 modulo $\mathfrak{m}B_W$ and B_W is $\mathfrak{m}$-adically complete and separated. □

Proof of Lemma 9.5. The method is an adaptation of the usual proof of Hensel's lemma. A straightforward application of Hensel's lemma, as found in the (standard) literature, would give us bounds depending on g (the rank of M). We thus prefer to give some details.

The lemma is equivalent to proving that given $\underline{x} \in R^g$, whose reduction modulo p lies in $\mathbf{Z}(a,1)$, there exists a sequence $\{\underline{y}_n \in \mathbf{Z}(a,(n+1)(1-w))\}_n$ with:

(a) $\underline{y}_1 \equiv \underline{x}$ modulo p/a;

(b) $\underline{y}_n \equiv \underline{y}_{n-1}$ modulo p^n/a^{n+1} for every $n \geqslant 2$;

(c) the sequence $\{\underline{y}_n \mod (p^{n+1}/a^{n+2})\}_n$ is independent of the choice of $\{\underline{y}_n\}$ satisfying parts (a) and (b).

Indeed, since $w < \frac{1}{2}$ we have $p^n/a^{n+1} \to 0$ for $n \to \infty$. Hence, by parts (a) and (b) the limit $\underline{y} := \lim_n \underline{y}_n$ is an element of $\mathbf{Z}_R(a)$ lifting $\underline{x}$ modulo p/a. By part (c) it is also the unique element of $\mathbf{Z}_R(a)$ with these properties. We proceed by induction on n.

Let $\mathcal{R}_g := R\langle X_1, \ldots, X_g\rangle$ be the p-adic completion of the ring of polynomials in the variables $X_1, \ldots, X_g$ and coefficients in R. Define the matrix Δ in $M_{g\times g}(\mathcal{R}_g)$ as

$$\Delta := \frac{p}{a}U\begin{pmatrix} X_1^{p-1} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & X_p^{p-1}\end{pmatrix} - \mathbf{1}_g.$$

Since $\mathrm{v}(p) > \mathrm{v}(a)$, the matrix Δ is in $\mathrm{Gl}_{g\times g}(\mathcal{R}_g)$. The Jacobian matrix J of $U\underline{X}^p - a\underline{X}$ is $a\Delta$.

https://doi.org/10.1112/S0010437X07002813 Published online by Cambridge University Press

Write $U\underline{x}^p - a\underline{x} = p\underline{t}$. Let $\underline{y}_1 = \underline{x} + (p/a)\underline{Z}$ with $\underline{Z} := \Delta(\underline{x})^{-1}\underline{t}$. Then, modulo p^2/a^2, one has

$$U\underline{y}_1^p - a\underline{y}_1 = (U\underline{x}^p - a\underline{x}) + J(\underline{x})\frac{p}{a}\underline{Z} = p(\underline{t} - \Delta(\underline{x})\underline{Z}) = 0.$$

One easily verifies that this uniquely determines the class of $\underline{Z}$ modulo p/a^2.

Assume $\underline{y}_n$ has been constructed with the properties above. Let $\tilde{\underline{y}}_n$ be a lift of $\underline{y}_n$ in $R^g_{(n+2)(1-w)}$. Hence, we have $U\tilde{\underline{y}}_n^p - a\tilde{\underline{y}}_n = (p/a)^{n+1}\underline{t}$ for a suitable $\underline{t}$. Let $\underline{Z} := \Delta(\tilde{\underline{y}}_n)^{-1}\underline{t}$. Define $\underline{y}_{n+1} := \tilde{\underline{y}}_n + (p^{n+1}/a^{n+2})\underline{Z}$. Then, modulo $(p/a)^{n+2}$ we have

$$U\underline{y}_{n+1}^p - a\underline{y}_{n+1} = (U\tilde{\underline{y}}_n^p - a\tilde{\underline{y}}_n) + J(\tilde{\underline{y}}_n)\frac{1}{a}\left(\frac{p}{a}\right)^{n+1}\underline{Z} = \left(\frac{p}{a}\right)^{n+1}(\underline{t} - \Delta(\underline{x})\underline{Z}) = 0.$$

The class of $\underline{Z}$ modulo p/a is uniquely determined by this equation. The lemma follows. □

Remark 9.6. Let $g\colon M \to M'$ be a morphism of R-modules. Assume that M_1 and M_1' are endowed with Frobenius linear homomorphisms F and F' such that $g \circ \mathrm{F} = \mathrm{F}' \circ g$. Fix a as above, then g induces a $\mathbb{F}_p$-linear map $\mathrm{Ker}(\mathrm{F} - a) \to \mathrm{Ker}(\mathrm{F}' - a)$.

Assume now that R is a p-adically complete dvr with valuation v_R and a flat V-algebra. Let M be as in Proposition 9.1. Let $\{x_1, \ldots, x_s\}$ be $\mathbb{F}_p$-linearly independent elements of $\mathrm{Ker}(\mathrm{F} - a)$. We prove that they are 'almost' R-linearly independent.

Lemma 9.7. *Suppose that there exists $r_1, \ldots, r_s$ in R such that $r_1x_1 + \cdots + r_sx_s = 0$ in M_{1-w}, then $\mathrm{v}_R(r_i) > 0$.*

Proof. By hypothesis $w = \mathrm{v}(a)$ and M is a free R-module. Thus, multiplication by a induces an injection $M_{1-w} \to M_1$. Since $x_i \in \mathrm{Ker}(\mathrm{F} - a)$ for $i = 1, \ldots, s$, we get $0 = \mathrm{F}(\sum_i r_ix_i) = \sum_i r_i^p \mathrm{F}(x_i) = a \cdot (\sum_i r_i^p x_i)$. Hence, $\sum_i r_i^p x_i = 0$ in M_{1-w}. We conclude that for every natural number t we have $\sum_i r_i^{p^t} x_i = 0$.

Suppose that there exists a relation $r_1x_1 + \cdots + r_sx_s = 0$ with $\mathrm{v}_R(r_j) = 0$ for some j. Eventually replacing the r_i with their p^tth powers for t large enough, we may assume that, for every i, r_i is either a unit or it is 0. We deduce that there exists a subset J of $\{1, \ldots, s\}$ and units $r_j \in R^*$ for $j \in J$ such that $\sum_{j \in J} r_jx_j = 0$. Take J of minimal cardinality with these properties. Eventually, renumbering the x_i and reducing s we may assume that $J = \{1, \ldots, s\}$. We may also suppose that $r_1 = 1$. Then, $x_1 = -\sum_{i \neq 1} r_ix_i = -\sum_{i \neq 1} r_i^p x_i$. Hence, $\sum_{i \neq 1}(r_i^p - r_i)x_i = 0$. The minimality of the cardinality of J implies that $r_i^p - r_i$ is not a unit in R. Thus, the class of r_i in the residue field of R lies in $\mathbb{F}_p$. Hence, $r_i \equiv a_i$ for some $a_i \in \mathbf{Z}$ modulo the maximal ideal of R. Taking suitable pth powers, we get $\sum_i a_i^{p^t} x_i = 0$, contradicting the $\mathbb{F}_p$-independence of $\{x_1, \ldots, x_s\}$. □

10. Extensions of subgroup schemes generically defined

Let S be a flat V-scheme and let $G \to S$ be a group scheme over S. Let $H_K \subset G_K$ be a closed subgroup scheme, flat over S_K. In this section we investigate the problem of extending H_K to a closed subgroup scheme of G. As the following example shows, this is not always possible even if S is integral.

Example 10.1. Let p be a prime number. Let $A := \mathbf{Z}_p[\![X, Y]\!]/(XY - p)$. Let $N \to \mathrm{Spec}(A)$ be the group scheme, finite and flat of order p over $\mathrm{Spec}(A)$ defined by the elements $a := X$ and $c := Y$ of A via the Oort–Tate classification [OT70]; in particular, $N = \mathrm{Spec}(A[T]/(T^p - XT))$. Let $R := \mathbf{Z}_p[\![X_1, X_2, Y_1, Y_2]\!]/(X_1Y_1 - p, X_2Y_2 - p)$ and let $p_i\colon \mathrm{Spec}(R) \to \mathrm{Spec}(A)$ with $i = 1, 2$ be the morphism $X \mapsto X_i$ and $Y \mapsto Y_i$. Let $P := \mathrm{Spec}(B)$ with

$$B := \mathrm{Spec}(R[Z, Z^{-1}]/(Z^{p-1}X_1 - X_2)).$$

https://doi.org/10.1112/S0010437X07002813 Published online by Cambridge University Press

We denote by N_i the base-change of N, respectively, via p_i. The base-change of N_1 and N_2 to P are isomorphic via the isomorphism α given by $1 \otimes T \mapsto ZT \otimes 1$. Over $\mathrm{Spec}(R_K)$ the scheme P is given by the equation $Z^{p-1} - X_2 X_1^{-1}$; by Kummer theory it is then a torsor under μ_{p-1}. In particular, it is finite and étale of rank $p-1$. Let $S := \mathrm{Spec}(C)$ with

$$C := R[W]/(W^{p-1} - X_2^{p-1} X_1^{p-2}).$$

It is a scheme finite and flat over $\mathrm{Spec}(R)$. Let $u \colon P \to S$ be the morphism of R-schemes given by $W \mapsto ZX_1$. Via the map u, we have $B = C[Z, Z^{-1}]/(ZX_1 - W)$. In particular, note that u is an isomorphism over $\mathrm{Spec}(R_K)$ and it is surjective on points.

Let G be the base-change of $N_1 \times_R N_2$ via $S \to \mathrm{Spec}(R)$ and let $H_K \subset G_K$ be the closed subgroup scheme defined as the graph of $\alpha_K \colon N_{1,K} \to N_{2,K}$ over $S_K = P_K$. The isomorphism α is defined over P and its graph gives a closed subscheme $H_P \subset G \times_S P$. Since P is a flat $\mathbf{Z}_p$-scheme, P_K is schematically dense in P. Assume that H_K can be extended to a closed subgroup scheme H of G, flat over S. Then $H_P = H \times_S P$ as closed subgroup schemes of $G \times_S P$. Since the map u is surjective, it follows that the morphism $f_i \colon H \to N_i$ is an isomorphism for $i = 1, 2$. By [OT70] the isomorphism $f_2 \circ f_1^{-1}$ is defined by $1 \otimes T \mapsto cT \otimes 1$ for a unique $c \in C^*$ satisfying $c^{p-1} X_1 - X_2$. We then get a map $S \to P$ given by $Z \to c$. The composite with u is the identity over S_K and, hence, it is the identity. Since P is an affine chart of the blow-up of S at the ideal (W, X_1) intersecting the exceptional divisor, u does not admit any section.

The main result of this section states that if S is noetherian, one can find a K-admissible blow-up S' of S such that the schematic closure of the subgroup H_K of G_K in $G_{S'} := G \times_S S'$ is a *subgroup scheme* of $G_{S'}$ *flat* over S'. In particular, if G is an abelian scheme over S and H_K is finite and flat, the schematic closure of H_K in $G_{S'}$ will also be finite and flat. When S is the spectrum of a dvr, this is a classical result due to Raynaud [Ray74b].

10.2 Admissible blow-ups

For the convenience of the reader, we recall the following definitions and properties from [RG71, § 5.1]. Assume that S is a noetherian scheme and let $f \colon S' \to S$ be a K-admissible blow-up with center C; see Definition 2.1. If Z is an S-scheme, flat over V, we denote by $Z_{S'}$ the fiber product $Z \times_S S'$. Let A be the open subscheme of S given by $S \backslash C$. If $Y \subset Z$ is a closed subscheme, we define the *strict transform* $\widetilde{Y}$ of Y in $Z_{S'}$ as the schematic closure of $Y_A := Y \times_S A$ in $Z_{S'}$. Here and in what follows we identify $f^{-1}(A)$ with A via f and consequently we view Y_A as a locally closed subscheme of $Z_{S'}$. Note that, since C is of finite presentation and S is noetherian, $A \to S$ is quasi-compact so that $Y_A \to Z_{S'}$ is quasi-compact as well, and the schematic closure exists by [EGAI, I.9.5.2]. Then:

(i) if Z is flat over S, we have $Z_{S'} = \widetilde{Z}$, i.e. $Z_{S'}$ is the strict transform of Z;

(ii) if Y_A is flat over A, then Y_K is schematically dense in Y_A; the latter is schematically dense in $\widetilde{Y}$ by construction, hence, Y_K is schematically dense in $\widetilde{Y}$; in particular, the strict transform of Y in $Z_{S'}$ coincides with the schematic closure of Y_K in $Z_{S'}$;

(iii) if Y is flat over S, then $Y_{S'}$ is the strict transform of Y in $Z_{S'}$;

(iv) let $f \colon S' \to S$ and $g \colon S'' \to S'$ be K-admissible blow-ups, then $f \circ g \colon S'' \to S$ is a K-admissible blow-up; cf. [RG71, Lemma 5.1.4].

The following proposition is the key to the solution of the problem.

Proposition 10.3. *Assume that S is a noetherian scheme, flat over V and let Z be a scheme projective over S. Suppose that $Y_K \subset Z_K$ is a closed subscheme flat over S_K and let Y be the schematic closure of Y_K in Z. Then, there exists a scheme S^Y and a projective morphism $S^Y \to S$ such that:*

https://doi.org/10.1112/S0010437X07002813 Published online by Cambridge University Press

(a) *S^Y is flat over V, the induced map $S^Y_K \to S_K$ is an isomorphism and the schematic closure of Y_K in $Z \times_S S^Y$ is flat over S^Y;*

(b) *S^Y is minimal among the S-schemes satisfying condition (a).*

Furthermore:

(i) *let S' be a K-admissible blow-up of S, then $S' \to S$ factors via $S^Y \to S$ if and only if the schematic closure of Y_K in $Z_{S'}$ is flat over S'; in this case, such schematic closure coincides with the pull-back of the schematic closure of Y_K in $Z \times_S S^Y$ via $S' \to S^Y$;*

(ii) *there exists a K-admissible blow-up $S' \to S$ and a morphism of S-schemes $S' \to S^Y$;*

(iii) *if $T \to S$ is a flat morphism of noetherian schemes, T^Y is $T \times_S S^Y$.*

In the statement above, condition (b) means that for every other S-scheme S' satisfying condition (a), there exists a unique S-morphism $S' \to S^Y$ so that the schematic closure of Y_K in $Z' := Z \times_S S'$ is the base-change of the schematic closure of Y_K in $Z \times_S S^Y$.

Proof. We follow closely [RG71, § 5.2].

(a) The subscheme Y_K of Z_K defines a S_K-point s in the Hilbert scheme $\mathbf{Hilb}(Z/S)$ of Z over S. The latter is the disjoint union of projective schemes over S. Define S^Y as the schematic closure of s in $\mathbf{Hilb}(Z/S)$. Since S_K is schematically dense in S^Y, the latter is flat over V. By the universal property of the Hilbert scheme, one has a closed subscheme of $Z_{S^Y} := Z \times_S S^Y$, flat over S^Y and coinciding with Y_K over S_K.

(b) Let S' be an S-scheme so that condition (a) holds. Then, S_K is schematically dense in S' since the latter is flat over V. By assumption, the schematic closure of Y_K in $Z_{S'}$ is flat over S' and, in particular, defines an S' valued point of $\mathbf{Hilb}(Z/S)$. By construction it factors via S^Y and the claim follows.

(i) The implication $\Longleftarrow$ follows from condition (b).

We prove the implication $\Longrightarrow$ and the last claim. Suppose that $S' \to S$ factors via S^Y. Denote by $\widetilde{Y}$ the schematic closure of Y_K in Z_{S^Y}. Since S' and S^Y are flat V-schemes and since $S'_K = S_K = S^Y_K$, then $S' \to S^Y$ is the admissible blow-up with center equal to the inverse image of the center of the blow-up $S' \to S$ via the morphism $S^Y \to S$. In particular, the base-change $\widetilde{Y}_{S'}$ of $\widetilde{Y}$ via $S' \to S^Y$ is the strict transform of $\widetilde{Y}$ in $Z_{S'}$ by condition (iii) of § 10.2 and it is flat over S'. In particular, $\widetilde{Y}_{S'} \otimes_V K = Y_K$ and Y_K is schematically dense in $\widetilde{Y}_{S'}$ by condition (ii) of § 10.2.

(ii) By [RG71, Theorem 5.2.2] there exists a K-admissible blow-up $f\colon S' \to S$ such that the strict transform $\widetilde{\mathcal{O}_Y}$ of the coherent $\mathcal{O}_Z$-module $\mathcal{O}_Y$ is S'-flat. Recall from [RG71, Definition 5.1.1] that $\widetilde{\mathcal{O}_Y}$ is the $\mathcal{O}_{Z'_S}$-module defined as the quotient of $\mathcal{O}_{Y_{S'}}$ by the submodule of sections supported on $f^{-1}(C)$, where C is the center of the blow-up f. In particular, $\widetilde{\mathcal{O}_Y}$ is a quotient of $\mathcal{O}_{Z'_S}$ and, by the S'-flatness, it is the structure sheaf of the schematic closure of Y_K in $Z_{S'}$. By property (c) the morphism $S' \to S$ factors via S^Y.

(iii) This follows from the fact that the formation of the Hilbert scheme commutes with base-change and the fact that taking schematic closures commutes with flat base-change. □

Lemma 10.4. *Let W and Z be S-schemes. Let $Y \subset Z$ and $X \subset W$ be closed subschemes. Assume that X_K is schematically dense in X. Then, any morphism $u\colon W \to Z$ as S-schemes, inducing a morphism $v_K\colon X_K \to Y_K$ such that $X_K \xrightarrow{v_K} Y_K \subset Z_K$ is $X_K \subset W_K \xrightarrow{u_K} Z_K$, induces a unique morphism $v\colon X \to Y$ such that the following diagram commutes.*

$$\begin{tikzcd}
X \arrow[r, hook] \arrow[d, "v"'] & W \arrow[d, "u"] \\
Y \arrow[r, hook] & Z
\end{tikzcd}$$

https://doi.org/10.1112/S0010437X07002813 Published online by Cambridge University Press

Proof. Consider $i\colon X_K \to X$ and $j\colon Y_K \to Y$. Let $\mathcal{I}$ be the ideal sheaf defining Y in Z and $\mathcal{J}$ be the ideal sheaf defining X in W. We then have the following commutative diagram.

$$\begin{tikzcd}
\mathcal{O}_Z \arrow[r] \arrow[d, "u^*"'] & \mathcal{O}_Y \arrow[r, "j^*"] & j_*(\mathcal{O}_{Y_K}) \arrow[d, "v_K^*"] \\
u_*(\mathcal{O}_W) \arrow[r] & u_*(\mathcal{O}_X) \arrow[r, "i^*"] & u_* \circ i_*(\mathcal{O}_{X_K})
\end{tikzcd}$$

Since X_K is schematically dense in X, the map i^* is injective. Since $i^*(u^*(\mathcal{I})) = 0$, we conclude that $u^*(\mathcal{I}) \subset u_*(\mathcal{J})$. Thus, there exists a unique morphism $v^*\colon \mathcal{O}_Y \to u_*(\mathcal{O}_X)$ compatible with u^* and v_K^*, as claimed. □

Corollary 10.5. *Let Z be a group scheme over S. Let $Y \subset Z$ be a closed subscheme flat over S. If $Y_K \subset Z_K$ is a closed subgroup scheme, then $Y \subset Z$ is a closed subgroup scheme.*

Proof. Denote by f the morphism $f\colon Y \to S$ and by j the morphism $j\colon Y_K \to Y$. Since $i\colon S_K \to S$ is quasi-compact, $i_*(\mathcal{O}_{S_K})$ is quasi-coherent by [EGAI, I.9.4.1]. Since $Y \times_S Y$ is flat over S, the natural map $(f \times f)^*(i_*(\mathcal{O}_{S_K})) \to (j \times j)_*(\mathcal{O}_{Y_K} \otimes_{\mathcal{O}_{S_K}} \mathcal{O}_{Y_K})$ is an isomorphism. Applying $(f \times f)^*$ to the injective map $\mathcal{O}_S \to i_*(\mathcal{O}_{S_K})$ and using the flatness of $Y \times_S Y$ over S, we conclude that $Y_K \times_{S_K} Y_K$ is schematically dense in $Y \times_S Y$. Furthermore, $Y \times_S Y$ is a closed subscheme of $Z \times_S Z$ and is flat over S. It then follows from Lemma 10.4 that the multiplication map $m\colon Z \times_S Z \to Z$ restricted to $Y \times_S Y$ factors via $Y \subset Z$. Analogously, the inverse map $\iota\colon Z \to Z$ sends Y to Y. Hence, the map

$$m \circ (id \times \iota)\colon Z \times_S Z \longrightarrow Z, \quad (x, y) \mapsto x - y$$

restricted to $Y \times_S Y$ factors via $Y \subset Z$. Thus, Y is a closed subgroup scheme of Z as claimed. □

We summarize the results obtained so far in the following theorem.

Theorem 10.6. *Let $Z \to S$ be a projective abelian scheme over S. Let $Y_K \subset Z_K$ be a closed subgroup scheme, flat over S_K. Then, there exists an S-scheme S^Y and a projective morphism $S^Y \to S$ such that the induced map $S_K^Y \to S_K$ is an isomorphism and the schematic closure of Y_K in $Z \times_S S^Y$, denoted by Y, is a subgroup scheme of $Z \times_S S^Y$, flat over S^Y. Furthermore, we have the following.*

(i) (Admissibility) *There exists a K-admissible blow-up $S' \to S$ and a morphism of S-schemes $S' \to S^Y$.*

(ii) (Minimality) *A morphism $S' \to S$, such that S' is flat over V and the morphism induces an isomorphism of generic fibers $S'_K \to S_K$, factors via $S^Y \to S$ if and only if the schematic closure Y' of Y_K in $Z' := Z \times_S S'$ is flat over S'. In particular, Y' is a closed subgroup scheme of Z' and it coincides with $Y \times_{S^Y} S'$.*

(iii) (Base-change) *If $T \to S$ is a flat morphism of noetherian schemes, T^Y is $T \times_S S^Y$.*

(iv) (Functoriality) *Let $W \to S$ and $Z \to S$ be projective abelian schemes. Let $U_K \subset W_K$ and $Y_K \subset Z_K$ be closed subgroup schemes, flat over S_K. Let $S' \to S$ be an admissible blow-up such that the schematic closure U' of U_K in $W' = W \times_S S'$ (respectively, Y' of Y_K in $Z' = Z \times_S S'$) is a subgroup scheme, flat over S'. Then, every homomorphism $W \to Z$ of group schemes, inducing a homomorphism $U_K \to Y_K$, induces a homomorphism $U' \to Y'$ as well.*

Remark 10.7. One can relax the hypotheses of Theorem 10.6. Let S be a quasi-compact and quasi-separated scheme and let $U \hookrightarrow S$ be an open, schematically dense, quasi-compact subscheme of S. Let $Z \to S$ be a group scheme, of finite presentation as an S-scheme. Let $Y_U \subset Z_U$ be a closed subgroup scheme of $Z_U := Z \times_S U$, flat over U. Using [RG71, Theorem 5.2.2], one can then deduce

https://doi.org/10.1112/S0010437X07002813 Published online by Cambridge University Press

that there exists a U-admissible blow-up $S' \to S$ such that the strict transform of Y in $Z' := Z \times_S S'$ is a closed subgroup scheme of Z', flat over S'. Observe, however, that the existence of an S-scheme S^Y with the properties of Proposition 10.3 is not guaranteed in this more general setting.

11. Proof of the main theorems: first reductions

In this section we show that the existence of the canonical subgroup and of a formal model for special (w, g)-situations (as in Definition 11.1) implies its existence and the existence of a formal model in the general case. The main point of this reduction is the fact that, due to property (ii) of Theorem 3.5, we can work with strict neighborhoods of the ordinary locus in suitable moduli spaces of abelian varieties; the restriction of the universal family to the normalization of sufficiently small open formal subschemes of these *are* special (w, g)-situations.

Definition 11.1. We define a *special* (w, g)*-situation* to be $X \to S$ where:

(a) S is $\mathrm{Spec}(R)$ with R a normal admissible V-algebra;

(b) $X \to S$ is a projective g-dimensional abelian scheme;

(c) $\mathrm{H}^1(X_1, \mathcal{O}_{X_1})$ is a free R_1-module;

(d) the determinant of Frobenius F on $\mathrm{H}^1(X_1, \mathcal{O}_{X_1})$ satisfies $p^w \in \det(\mathrm{F})R_1$.

Denote by $\mathfrak{X}$ (respectively, $\mathcal{S}$) the formal completion of X (respectively, S). We then have the following.

Theorem 11.2. *Suppose that there is a way of associating to every* special (w, g)*-situation* $X \to S$*, with* $0 \leqslant w < (p-1)/(2p-1)$*, a rigid analytic subgroup scheme* $H^{\mathrm{an}}_{\mathfrak{X}}$ *of* $\mathfrak{X}^{\mathrm{an}}$ *finite and flat of rank* p^g *over* $\mathcal{S}^{\mathrm{an}}$*, satisfying (the analogue of) properties (i)–(iii) of Theorem 3.5 and the (the analogue of the) functoriality of Proposition 3.7. Then, Theorem 3.5 and Proposition 3.7 hold true.*

Moreover, if Theorem 3.10 and Proposition 3.12 hold for special (w, g)*-situations* $X \to S$*, with* $0 \leqslant w < (p-1)/(2p-1)$*, then Theorem 3.10 and Proposition 3.12 hold true.*

Proof. We first construct a canonical subgroup in the rigid and in the formal settings for universal families of abelian varieties. We then deduce the general case.

Let $0 \leqslant w < (p-1)/(2p-1)$ and assume that $p^w \in V$. Let n and d be positive integers such that $n \geqslant 3, (n, d) = 1$ and $(p, n) = 1$. Denote by $\mathcal{A}_{g,d,n}$ the moduli space of abelian varieties of dimension g over V with full level n structure and a polarization of degree d^2, and by $X^{\mathrm{univ}} \to \mathcal{A}_{g,d,n}$ the universal abelian scheme. Consider a covering $\{U_i\}_i$ of $\mathcal{A}_{g,d,n}$ by affine open subschemes, say $U_i := \mathrm{Spec}(R_i)$, with the property that each U_i dominates $\mathrm{Spec}(V)$ and the R_i-module $H^1(U_i, \mathcal{O}_{X^{\mathrm{univ}}})$ is free. For each i fix a lifting $\alpha_i \in R_i$ of the principal ideal defined by the determinant of Frobenius on $H^1(U_i, \mathcal{O}_{X^{\mathrm{univ}}}) \otimes_V V_1$. Let $R_i(w) := R_i[Y]/(Y\alpha_i - p^w)$ and A_i be the normalization of $R_i(w)$. Since $R_i(w)$ is of finite type over V, it is excellent by [EGAIV, 7.8.3]. Consequently, A_i is finite as an $R_i(w)$-module and it is itself excellent. Thus, its p-adic completion $\widehat{A}_i$ is normal by [EGAIV, 7.8.3(v)]. In particular, $X^{\mathrm{univ}}_i := X^{\mathrm{univ}} \times_{\mathcal{A}_{g,d,n}} \mathrm{Spec}(\widehat{A}_i) \to \mathrm{Spec}(\widehat{A}_i)$ is a special (w, g)-situation. By hypothesis we can define a rigid analytic subgroup H^{an}_i of $(\mathfrak{X}^{\mathrm{univ}}_i)^{\mathrm{an}}$, a minimal morphism of formal schemes $\mathfrak{T}_i^{\mathfrak{X}^{\mathrm{univ}}_i} \to \mathfrak{T}_i := \mathrm{Spf}(\widehat{A}_i)$ relative to $\mathfrak{X}^{\mathrm{univ}}_i \to \mathfrak{T}_i$ and a finite and flat closed subgroup scheme $H^{\mathrm{form}}_{\mathfrak{X}^{\mathrm{univ}}_i}$ of $\mathfrak{X}^{\mathrm{univ}}_i \times_{\mathfrak{T}_i} \mathfrak{T}_i^{\mathfrak{X}^{\mathrm{univ}}_i}$ extending H^{an}_i. Furthermore, $H^{\mathrm{form}}_{\mathfrak{X}^{\mathrm{univ}}_i}$ also satisfies Proposition 3.12. Write $U_i \cap U_j$ as $\mathrm{Spec}(R_{ij})$. Let A_{ij} be the normalization of $R_{ij}[Y]/(Y\alpha_i - p^w)$ and let $\widehat{A}_{ij}$ be its completion. It is easy to see that $\widehat{A}_{ij}$ is canonically isomorphic to $\widehat{A}_{ji}$. Analogously, $X^{\mathrm{univ}}_{ij} := X^{\mathrm{univ}} \times_{\mathcal{A}_{g,d,n}} \mathrm{Spec}(\widehat{A}_{ij}) \to \mathrm{Spec}(\widehat{A}_{ij})$ is a special (w, g)-situation. Hence, denoting $\mathfrak{T}_{ij} := \mathrm{Spm}(\widehat{A}_{ji})$, there exists a rigid analytic subgroup H^{an}_{ij} of $(\mathfrak{X}^{\mathrm{univ}}_{ij})^{\mathrm{an}}$, a minimal morphism of

https://doi.org/10.1112/S0010437X07002813 Published online by Cambridge University Press

formal schemes up $\mathfrak{T}_{ij}^{\mathfrak{X}_{ij}^{\mathrm{univ}}} \to \mathfrak{T}_{ij}$ relative to $\mathfrak{X}_{ij}^{\mathrm{univ}} \to \mathfrak{T}_{ij}$ and a finite and flat closed subgroup scheme $H^{\mathrm{form}}_{\mathfrak{X}_{ij}^{\mathrm{univ}}}$ of $\mathfrak{X}_{ij}^{\mathrm{univ}} \times_{\mathfrak{T}_{ij}} \mathfrak{T}_{ij}^{\mathfrak{X}_{ij}^{\mathrm{univ}}}$ extending H_{ij}^{an}. Since H^{an} depends only on the isomorphism classes and commutes with base-change for special (w, g)-situations (properties (i) and (ii) of Theorem 3.5), the restriction of H_i^{an} to $\mathfrak{T}_{ij}^{\mathrm{an}}$ is H_{ij}^{an}. Using Theorem 3.10, which we are assuming to be valid for special (w, g)-situations, we also deduce that $\mathfrak{T}_{ij}^{\mathfrak{X}_{ij}^{\mathrm{univ}}}$ is an open formal subscheme of $\mathfrak{T}_i^{\mathfrak{X}_i^{\mathrm{univ}}}$ and that $H^{\mathrm{form}}_{\mathfrak{X}_{ij}^{\mathrm{univ}}}$ coincides with the pull-back of $H^{\mathrm{form}}_{\mathfrak{X}_i^{\mathrm{univ}}}$ to $\mathfrak{T}_{ij}^{\mathfrak{X}_{ij}^{\mathrm{univ}}}$.

Let $\mathfrak{A}_{g,d,n}$ be the formal scheme associated to $\mathcal{A}_{g,d,n}$. Denote by $\mathfrak{X}^{\mathrm{univ}}(w)$ the universal formal abelian scheme over $\mathfrak{A}_{g,d,n}(w)$. By construction, the covering $\{\mathfrak{T}_i^{\mathrm{an}}\}_i$ of $\mathfrak{A}_{g,d,n}(w)^{\mathrm{an}}$ coincides with the covering $\{\mathrm{Spm}(\widehat{R_i(w)} \otimes_V K)\}_i$, which is admissible since it is associated to a covering by open formal subschemes of $\mathfrak{A}_{g,d,n}(w)$. Thus, the groups $\{H_i^{\mathrm{an}}\}_i$ glue and define a rigid analytic subgroup $H^{\mathrm{an}}_{\mathfrak{X}^{\mathrm{univ}}(w)}$ of $(\mathfrak{X}^{\mathrm{univ}}(w))^{\mathrm{an}}$. By construction it satisfies property (iii) of Theorem 3.5; in particular, it is preserved by the automorphisms of $\mathcal{A}_{g,d,n}$, for example those of the level structure. Analogously, $\{\mathfrak{T}_i\}_i$ and $\{\mathfrak{T}_i^{\mathfrak{X}_i^{\mathrm{univ}}}\}_i$ also glue and define formal schemes $\mathfrak{T}$ and $\mathfrak{T}^{\mathfrak{X}^{\mathrm{univ}}}$ over $\mathfrak{A}_{g,d,n}(w)$, and we have a morphism $\mathfrak{T}^{\mathfrak{X}^{\mathrm{univ}}} \to \mathfrak{T}$ as formal schemes over $\mathfrak{A}_{g,d,n}(w)$. At the level of associated rigid analytic spaces, we obtain isomorphisms

$$(\mathfrak{T}^{\mathfrak{X}^{\mathrm{univ}}})^{\mathrm{an}} \xrightarrow{\sim} \mathfrak{T}^{\mathrm{an}} \xrightarrow{\sim} \mathfrak{A}_{g,d,n}(w)^{\mathrm{an}}.$$

We also obtain a formal closed subgroup scheme $H^{\mathrm{form}}_{\mathfrak{X}^{\mathrm{univ}}(w)}$ of the base-change of $\mathfrak{X}^{\mathrm{univ}}(w)$ to $\mathfrak{T}^{\mathfrak{X}^{\mathrm{univ}}}$, finite and flat over $\mathfrak{T}^{\mathfrak{X}^{\mathrm{univ}}}$, extending $H^{\mathrm{an}}_{\mathfrak{X}^{\mathrm{univ}}(w)}$. It follows that Definition 3.8(b) and (c) and Proposition 3.12 hold true in this case.

The strategy to construct the canonical subgroup in general is to work first under some restrictive hypotheses and eventually show how to remove them. Assume that we are given a formal (w, g)-situation $\mathfrak{X} \to \mathcal{S}$ such that $\mathfrak{X}$ admits a polarization of degree d^2 and full level n structure with n a positive integer $n \geqslant 3$ prime to pd, i.e., $\mathfrak{X}^{\mathrm{an}}[n] \cong (\mathbf{Z}/n\mathbf{Z})^g$. Suppose, furthermore, that $p^w \in V$. Then, $\mathfrak{X} \to \mathcal{S}$ is obtained as the pull-back of $\mathfrak{X}^{\mathrm{univ}}(w)$ via a morphism $f \colon \mathcal{S} \to \mathfrak{A}_{g,d,n}(w)$. We *define* $H_{\mathfrak{X}}^{\mathrm{an}}$ as the pull-back of $H^{\mathrm{an}}_{\mathfrak{X}^{\mathrm{univ}}}$ via f^{an}.

We now prove that $H_{\mathfrak{X}}^{\mathrm{an}}$ is independent of the choices of the polarization and level structure. Indeed, assume that there exists d' and $n' \geqslant 3$ with $(n', pd') = 1$ and a morphism $f' \colon \mathcal{S} \to \mathfrak{A}_{g,d',n'}(w)$ such that $\mathfrak{X}$ is the pull-back of the universal formal abelian scheme $\mathfrak{X}'^{\mathrm{univ}}$ via f'. It suffices to prove that the pull-back H of $H^{\mathrm{an}}_{\mathfrak{X}^{\mathrm{univ}}}$ via f^{an} and the pull-back H' of $H^{\mathrm{an}}_{\mathfrak{X}'^{\mathrm{univ}}}$ via f'^{an} coincide. Since $\mathfrak{X}^{\mathrm{an}}[p]$ is étale over $\mathcal{S}^{\mathrm{an}}$ and the two groups H and H' are contained in $\mathfrak{X}^{\mathrm{an}}[p]$, it is enough to show that they coincide over the rigid points of $\mathcal{S}^{\mathrm{an}}$. Any such point extends to a morphism $h \colon \mathrm{Spm}(V') \to \mathcal{S}$ for some finite extension $V \subset V'$ of discrete valuation rings. The pull-back $\mathfrak{X}_h \to \mathrm{Spm}(V')$ of $\mathfrak{X} \to \mathcal{S}$ via h is a special (w, g)-situation and the pull-backs of H and H' via h^{an} coincide with $H^{\mathrm{an}}_{\mathfrak{X}_h}$ due to the definition of $H^{\mathrm{an}}_{\mathfrak{A}_{g,d,n}(w)}$ (respectively, $H^{\mathrm{an}}_{\mathfrak{A}_{g,d',n'}(w)}$) and the hypothesis that the formation of H^{an} commutes with base change-for special (w, g)-situations.

Eventually, assume that $\mathfrak{X} \to \mathcal{S}$ is a (w, g)-situation. Take a finite extension $V \subset W$ of dvrs, a covering by open formal subschemes $\{\mathfrak{U}_i\}_i$ of $\mathcal{S} \otimes_V W$ and a finite and étale extension $\mathfrak{Z}_i \to \mathfrak{U}_i$ for every i such that $p^w \in W$, the pull-back of $\mathfrak{X}$ to $\mathfrak{U}_i$ admits a polarization of degree d_i^2 and the pull-back of $\mathfrak{X}$ to $\mathfrak{Z}_i$ is endowed with a full level n_i structure for some n_i and d_i with $(n_i, pd_i) = 1$. By the above, we may construct $H^{\mathrm{an}}_{\mathfrak{X} \times_{\mathcal{S}} \mathfrak{Z}_i}$ independently of any choice. The extension $\mathfrak{Z}_i^{\mathrm{an}} \to \mathfrak{U}_i^{\mathrm{an}}$ is finite and étale as rigid analytic spaces over $W \otimes_V K$ and the morphism $(\mathcal{S} \otimes_V W)^{\mathrm{an}} \to \mathcal{S}^{\mathrm{an}}$ is finite and étale as rigid analytic spaces over K. Remark that $H^{\mathrm{an}}_{\mathfrak{X} \times_{\mathcal{S}} \mathfrak{Z}_i}$ is a closed rigid analytic subspace of $\mathfrak{X}[p] \times_{\mathcal{S}} \mathfrak{Z}_i^{\mathrm{an}}$. Then, the usual étale descent for coherent modules suffices to descend $H^{\mathrm{an}}_{\mathfrak{X} \times_{\mathcal{S}} \mathfrak{Z}_i}$ to a unique closed rigid analytic subgroup $H_{\mathfrak{X}}^{\mathrm{an}}$ of $\mathfrak{X}[p]$. By construction it satisfies property (iii)

https://doi.org/10.1112/S0010437X07002813 Published online by Cambridge University Press

of Theorem 3.5. Reducing once more to the case of $\mathcal{S}$ equal to the formal spectrum of a complete discrete valuation ring and using the assumption of the theorem, one shows that $H_{\mathfrak{X}}^{\mathrm{an}}$ depends only on the isomorphism class of $\mathfrak{X} \to \mathcal{S}$, that its formation commutes with base-change and is functorial in $\mathfrak{X}$. This concludes the proof of the existence of the canonical subgroup and shows its main properties. We are left to discuss its formal models.

We assume first that $\mathcal{S} = \mathrm{Spf}(R)$, with R an admissible V-algebra, and that $\mathfrak{X} \to \mathcal{S}$ is projective. Let $S := \mathrm{Spec}(R)$ and let $X \to S$ be the abelian scheme whose associated formal scheme is $\mathfrak{X} \to \mathcal{S}$. Since $\mathfrak{X}[p]^{\mathrm{an}}$ is finite over $\mathcal{S}^{\mathrm{an}}$ and $H_{\mathfrak{X}}^{\mathrm{an}}$ is a closed analytic subgroup scheme, there exists a unique closed subgroup scheme H_{X_K} of $X_K[p]$, finite and étale over S_K, whose associated rigid analytic subgroup scheme of $\mathfrak{X}[p]^{\mathrm{an}}$ is $H_{\mathfrak{X}}^{\mathrm{an}}$. By Theorem 10.6 there exists a projective morphism $S^X \to S$ and a closed subgroup scheme $H_X \subset X \times_S S^X$ such that $(H_X)_K = H_{X_K}$. We let $\mathcal{S}^{\mathfrak{X}}$ (respectively, $H_{\mathfrak{X}}^{\mathrm{form}}$) be the p-adic formal scheme associated to S^X (respectively, H_X). Due to Theorem 10.6, the requirements (a) and (b) of Definition 3.8 are satisfied. We prove that requirement (c) also holds. Let $\mathfrak{T} \to \mathcal{S}$ be an admissible blow-up such that $\mathfrak{X}[p] \times_{\mathcal{S}} \mathfrak{T}$ admits a closed subgroup scheme $\mathcal{H}$ finite and flat over $\mathfrak{T}$ whose rigid analytic fiber is $H_{\mathfrak{X}}^{\mathrm{an}} \times_{\mathcal{S}^{\mathrm{an}}} \mathfrak{T}^{\mathrm{an}}$. Then, $\mathfrak{T} \to \mathcal{S}$ is obtained as the p-adic completion of an admissible blow-up $T \to S$. Let $H_T \subset X[p] \times_S T$ be the schematic closure of $H_{X_K} \times_S T$. Passing to an affine covering of T and using that the schematic closure commutes with flat base-change (such as taking p-adic completion), one sees that $\mathcal{H}$ is the p-adic completion of H_T. Since R is p-adically complete by construction, its maximal ideals contain p so that the closed points of S and $\mathcal{S}$ are identified with the closed points of S_k. Since T is proper over S and $\mathfrak{T}$ is proper over $\mathcal{S}$, we deduce that the closed points of T and $\mathfrak{T}$ are the closed points of the special fiber T_k and are identified. For any such point x, the p-adic completion of the local ring of T at x and of $\mathfrak{T}$ at x coincide. Since $\mathcal{H}$ is flat over $\mathfrak{T}$, we conclude that H_T is flat passing to the p-adic completion of the local ring of T at every closed point and, hence, that H_T is flat over T. Thus, by Corollary 10.5, it is a closed subgroup scheme of $X[p] \times_S T$. Then, $T \to S$ factors uniquely via $S^X \to S$ and $\mathfrak{T} \to \mathcal{S}$ factors via $\mathcal{S}^{\mathfrak{X}}$. We conclude that $\mathcal{S}^X \to \mathcal{S}$ satisfies the requirement of Theorem 3.10, apart from the uniqueness. Any minimal morphism is, by definition, locally projective and, hence, there is a Zariski covering of $\mathcal{S}$ by affine formal subschemes over which it is algebraizable by Grothendieck's existence theorem. Applying Theorem 10.6 we then deduce that it must coincide with $\mathcal{S}^{\mathfrak{X}} \to \mathcal{S}$ proving also the uniqueness.

In general, consider a covering $\{\mathfrak{U}_i\}_i$ of $\mathcal{S}$ by open formal affine subschemes such that $\mathfrak{X} \times_{\mathcal{S}} \mathfrak{U}_i \to \mathfrak{U}_i$ is projective. One then obtains $\mathfrak{U}_i^{\mathfrak{X}} \to \mathfrak{U}_i$ satisfying Theorem 3.10 for every i. By Theorem 3.10, the formal scheme $\mathfrak{U}_i^{\mathfrak{X}} \times_{\mathcal{S}} \mathfrak{U}_j$ coincides with $\mathfrak{U}_j^{\mathfrak{X}} \times_{\mathcal{S}} \mathfrak{U}_i$ for every i and j so that one can glue the formal schemes $\mathfrak{U}_i^{\mathfrak{X}} \to \mathfrak{U}_i$ to a formal scheme $\mathcal{S}^{\mathfrak{X}} \to \mathcal{S}$. By construction it satisfies Definition 3.8(b) and (c). We claim that Definition 3.8(a) holds as well. This is true for each $\mathfrak{U}_i^{\mathfrak{X}}$, i.e. there exists an admissible blow-up $\mathfrak{U}'_i$ of $\mathfrak{U}_i$ and a map $\mathfrak{U}'_i \to \mathfrak{U}_i^{\mathfrak{X}}$ as $\mathfrak{U}_i$-schemes. By [BL93, Lemma 2.6], for every i there exists an admissible blow-up $\mathcal{S}'_i \to \mathcal{S}$ extending $\mathfrak{U}'_i \to \mathfrak{U}_i$ and there exists an admissible blow-up $\mathcal{S}' \to \mathcal{S}$ factoring through each $\mathcal{S}'_i$. The natural maps $\mathcal{S}' \times_{\mathcal{S}} \mathfrak{U}_i \to \mathfrak{U}'_i \to \mathfrak{U}_i^{\mathfrak{X}}$ glue by the universal property of $\mathfrak{T}^{\mathfrak{X}}$ (Definition 3.8(c)). We then get a morphism $\mathcal{S}' \to \mathcal{S}^{\mathfrak{X}}$ of $\mathcal{S}$-schemes as required. This shows that Definition 3.8(a) holds as well. Since the uniqueness claimed in Theorem 3.10 holds if it holds locally on $\mathcal{S}$, this completes the proof of Theorem 3.10.

We now prove that Proposition 3.12 holds. Let $\mathcal{S}' \to \mathcal{S}$ be an admissible blow-up over which a formal model $H_{\mathfrak{X}}^{\mathrm{form}}$ of $H_{\mathfrak{X}}^{\mathrm{an}}$ exists. Using the notation introduced above, we know that there exists a Zariski covering $\{\mathfrak{Z}_i\}_i$ of $\mathcal{S}$ and admissible blow-ups $\{\mathfrak{Z}'_i\}_i$ such that for every i a formal model H_i of $H_{\mathfrak{X}}^{\mathrm{an}} \times_{\mathcal{S}}^{\mathrm{an}} \mathfrak{Z}_i^{\mathrm{an}}$ exists and satisfies Proposition 3.12. For every i, let $\mathcal{S}''_i$ be a blow-up dominating both $\mathfrak{Z}'_i$ and $\mathcal{S}' \times_{\mathcal{S}} \mathfrak{Z}_i$. Then, Proposition 3.12 holds for $H_i \times_{\mathfrak{Z}'_i} \mathcal{S}''_i$ since it holds for H_i. This group scheme coincides with $H_{\mathfrak{X}}^{\mathrm{form}} \times_{\mathcal{S}} \mathcal{S}''_i$ by Lemma 3.9. Note that $\amalg_i \mathcal{S}''_i \to \mathcal{S}'$ is surjective on points since it is an admissible blow-up of a fppf covering of $\mathcal{S}'$. Hence, $H_{\mathfrak{X}}^{\mathrm{form}} \times_{\mathcal{S}'} (\mathcal{S}' \otimes_V k)^{\mathrm{red}}$ is annihilated

https://doi.org/10.1112/S0010437X07002813 Published online by Cambridge University Press

by Frobenius for every geometric point of $(\mathcal{S}'\otimes_V k)^{\mathrm{red}}$ and, thus, it is annihilated by Frobenius. Since $H_{\mathfrak{X}}^{\mathrm{form}}$ has rank p^g, we conclude that Proposition 3.12 holds for $H_{\mathfrak{X}}^{\mathrm{form}}$ as claimed. □

12. Proof of the main theorems for special (w, g)-situations

In this section we prove the theorems and propositions of § 3 for special (w, g)-situations.

We start with Theorem 3.5. Let $X \to S$ be a special (w, g)-situation with $0 \leqslant w < (p-1)/(2p-1)$. In particular, $S = \mathrm{Spec}(R)$ with R a normal, admissible V-algebra. Let $\overline{R}$ be the direct limit of a maximal chain of finite and normal R-algebras, which are integral domains and are étale over R_K. Let $\overline{V}$ be the integral closure of V in $\overline{R}$. It is the ring of integers of an algebraic closure of K. Fix $\lambda \in \overline{V}$ so that $\mathrm{v}(\lambda) = (1-w)/(p-1)$. The assumption on w implies that

$$\frac{p}{(p-1)(2p-1)} < \mathrm{v}(\lambda) \leqslant \frac{1}{p-1}.$$

Proposition 12.1. *We have the following.*

1. *Let λ be as above. Then, $\mathrm{H}^1(X \otimes \overline{R}, \mathrm{G}_\lambda) \cong \mathbb{F}_p^g$.*
2. *Let $0 \leqslant w < w' < (p-1)/(2p-1)$ and let λ, $\mu \in \overline{V}$ be such that $\mathrm{v}(\lambda) = (1-w)/(p-1)$ and $\mathrm{v}(\mu) = (1-w')/(p-1)$. The map $\mathrm{H}^1(X \otimes \overline{R}, \mathrm{G}_\lambda) \to \mathrm{H}^1(X \otimes \overline{R}, \mathrm{G}_\mu)$, induced by the homomorphism $\eta_{\lambda,\nu} \colon \mathrm{G}_\lambda \to \mathrm{G}_\mu$ of § 5.3, is an isomorphism.*

Proof. (1) By Theorem 8.1, Proposition 9.1 and Remark 9.2 there exists a finite, normal R-algebra W étale over R_K such that $\mathrm{H}^1(X \otimes W, \mathrm{G}_\lambda)/\mathrm{H}^1(W, \mathrm{G}_\lambda)$ is a $\mathbb{F}_p$-vector space of dimension g. Furthermore, for every extension $W \subset W'$ which is finite, normal and étale over W_K, the map $\mathrm{H}^1(X \otimes W, \mathrm{G}_\lambda)/\mathrm{H}^1(W, \mathrm{G}_\lambda) \to \mathrm{H}^1(X \otimes W', \mathrm{G}_\lambda)/\mathrm{H}^1(W', \mathrm{G}_\lambda)$ is an isomorphism. The claim follows.

(2) The given map is injective due to Lemma 6.4. Then, the claim follows from claim (1). □

Consider the map $\tau_{\overline{R}} \colon \mathrm{H}^1(X \otimes \overline{R}, \mathrm{G}_\lambda) \longrightarrow \mathrm{Hom}_{\overline{R}}({\mathrm{G}_\lambda}^\vee, \mathrm{Pic}^0_{X/R})$ as in § 5.12. Choose an $\mathbb{F}_p$-basis $\{x_1, \dots, x_g\}$ of $\mathrm{H}^1(X \otimes \overline{R}, \mathrm{G}_\lambda)$ and let

$$\Psi \colon ({\mathrm{G}_\lambda}^\vee_{,\overline{R}})^g \longrightarrow \mathrm{Pic}^0_{X/R} \otimes_R \overline{R}$$

be the map $\tau_{\overline{R}}(x_1) + \dots + \tau_{\overline{R}}(x_g)$.

Lemma 12.2. *The map Ψ is a closed immersion over $\overline{R}_K$.*

Proof. Since ${\mathrm{G}_\lambda}^\vee_{,\overline{R}_K} \cong \mathbf{Z}/p\mathbf{Z}$, it suffices to prove that for any non-trivial homomorphism $\mathbf{Z}/p\mathbf{Z} \to ({\mathrm{G}_\lambda}^\vee_{,\overline{R}_K})^g$, the composite with Ψ is non-zero. For every $(a_1, \dots, a_g) \in \mathbb{F}_p^g$ consider the homomorphism $\xi_{a_1,\dots,a_g} \colon {\mathrm{G}_\lambda}^\vee \to ({\mathrm{G}_\lambda}^\vee)^g$ defined on points by $g \mapsto (g^{a_1}, \dots, g^{a_g})$. It suffices to prove that, for every $0 \neq (a_1, \dots, a_g) \in \mathbb{F}_p^g$ the map $\Psi \circ \xi_{a_1,\dots,a_g}$ is non-zero. By Proposition 8.9 and Lemma 8.10, the image of the Lie algebra of ${\mathrm{G}_\lambda}^\vee_{,\overline{R}}$, via $\Psi \circ \xi_{a_1,\dots,a_g}$, in $\mathrm{Lie}(\mathrm{Pic}^0_{X/R} \otimes_R \overline{R}_1) = \mathrm{H}^1(X, \mathcal{O}_X) \otimes_R \overline{R}_1$ is identified with the $\overline{R}_1$-submodule generated by the non-zero element $a_1 x_1 + \dots + a_g x_g$. The lemma follows because of the injectivity in Theorem 8.1. □

Lemma 12.3. *The image of $\Psi \otimes \overline{R}_K$ is* $\mathrm{Gal}(\overline{R}_K/R_K)$*-invariant.*

Proof. Consider the following diagram:

$$\begin{tikzcd}
\mathrm{H}^1(X \otimes \overline{R}, \mu_p) \arrow[r, hook] & \mathrm{H}^1(X \otimes \overline{R}_K, \mu_p) \arrow[r, "\sim"] & \mathrm{Pic}^0_{X/R}[p](\overline{R}_K) \\
\mathrm{H}^1(X \otimes \overline{R}, \mu_p)^{[\lambda]} \arrow[u, phantom, "\cup"] \arrow[r, equal] & \mathrm{H}^1(X \otimes \overline{R}, \mathrm{G}_\lambda) &
\end{tikzcd}$$

https://doi.org/10.1112/S0010437X07002813 Published online by Cambridge University Press

see Definition 6.5. The group $\mathrm{Gal}(\overline{R}_K/R_K)$ acts equivariantly on the terms in the upper part of the diagram. By Proposition 6.6, the subgroup $\mathrm{H}^1(X\otimes\overline{R},\mu_p)^{[\lambda]}\subset\mathrm{H}^1(X\otimes\overline{R},\mu_p)$ is also $\mathrm{Gal}(\overline{R}_K/R_K)$-invariant.

Let $\eta_\lambda\colon \mathrm{G}_\lambda\to\mu_p$ be the map defined in § 5.3. We view it as an element $\eta_\lambda\in{\mathrm{G}_\lambda}^\vee(R)$; it generates ${\mathrm{G}_\lambda}^\vee(\overline{K})$. It follows by the definition of $\tau_{\overline{R}}$ that, for every G_λ-torsor $Y\to X\otimes\overline{R}$, the image of the class $[Y]$ in $\mathrm{Pic}^0_{X/R}[p](\overline{R}_K)$ obtained via the diagram above coincides with the element $\tau_{\overline{R}}([Y])(\eta_\lambda)$. The lemma follows.

Using the lemmas above we deduce that $\Psi\otimes\overline{R}_K$ descends to a closed subgroup scheme $\mathbb{G}_K\subset\mathrm{Pic}^0_{X_K/R_K}$. It is finite and flat of rank p^g and it is annihilated by multiplication by p. □

DEFINITION 12.4. Let H_{X_K} be the closed subgroup scheme of $X_K[p]$ given by

$$H_{X_K}:=(\mathrm{Pic}^0_{X_K/S_K}[p]/\mathbb{G}_K)^\vee.$$

We let $H^{\mathrm{an}}_{\mathfrak{X}}$ be the rigid analytic subgroup scheme of $\mathfrak{X}^{\mathrm{an}}[p]$ associated to subgroup scheme H_{X_K} of $X_K[p]$.

PROPOSITION 12.5. *The rule associating to a special (w,g)-situation $X\to S$ the group scheme $H^{\mathrm{an}}_{\mathfrak{X}}$ given in Definition 12.4 satisfies properties (i)–(iii) of Theorem 3.5 and Proposition 3.7.*

Proof. Note that $H^{\mathrm{an}}_{\mathfrak{X}}$ is a closed subgroup scheme of $\mathfrak{X}^{\mathrm{an}}[p]$, finite and flat of rank p^g over $\mathcal{S}^{\mathrm{an}}$.

(i) By construction $H^{\mathrm{an}}_{\mathfrak{X}}$ depends only on the isomorphism class of $\mathfrak{X}\to\mathcal{S}$.

(ii) *(Base-change)* The formation of $H^{\mathrm{an}}_{\mathfrak{X}}$ commutes with base change associated to extensions $R\to R'$ of normal admissible V-algebras thanks to Proposition 9.1(iii).
(Functoriality) Let $X_1\to S$ (respectively, $X_2\to S$) be a special (w_1,g)-situation (respectively, a special (w_2,g)-situation) with $0\leqslant w_1,w_2<(p-1)/(2p-1)$. Let $h:X_1\to X_2$ be a morphism of abelian schemes. We deduce from Remarks 8.7 and 9.6 that Proposition 3.7 holds, i.e. h^{an} restricts to a group scheme homomorphism from $H^{\mathrm{an}}_{\mathfrak{X}_1}$ to $H^{\mathrm{an}}_{\mathfrak{X}_2}$.

(iii) *(Ordinary case)* If X has ordinary reduction, by the functoriality just proven one can take $w=0$. In particular, we can suppose $\mathrm{G}_\lambda\cong\mathbf{Z}/p\mathbf{Z}$. Then, the construction above coincides with that in Proposition 3.4. Hence, $H^{\mathrm{an}}_{\mathfrak{X}}=H^{\mathrm{ord}}_{\mathfrak{X}}$. □

12.6 Proof of Theorem 3.10

The notation is as in Definition 12.4. It follows from Theorem 10.6 that there exists a projective morphism $S^X\to S$, inducing an isomorphism over S_K, and a closed subgroup scheme

$$H_X\hookrightarrow X\times_S S^X,$$

which is finite and flat over S^X of rank p^g and extends H_{X_K}. Furthermore, S^X is minimal with these properties and its formation commutes with flat extensions $T\to S$ by Theorem 10.6. We then define $\mathcal{S}^{\mathfrak{X}}$ (respectively, $H^{\mathrm{form}}_{\mathfrak{X}}$) as the completion of S^X (respectively, H_X) along its special fiber. By construction $\mathcal{S}^{\mathfrak{X}}$ and $H^{\mathrm{form}}_{\mathfrak{X}}$ satisfy the requirements of Theorem 3.10; cf. the proof of Theorem 11.2.

12.7 Proof of Proposition 3.12

The notation is as in § 12.6. Let $\mathbb{G}$ be the closed subgroup scheme of $\mathrm{Pic}^0(X/S)\times_S S^X$ defined as the Cartier dual of $(X[p]\times_S S^X)/H_X$. It is a finite and flat over S^X of rank p^g and it is annihilated by p. Since $H_X\times_V k=H^{\mathrm{form}}_{\mathfrak{X}}\times_V k$, by Cartier duality, Proposition 3.12 follows if we prove the following.

LEMMA 12.8. *The group scheme $\mathbb{G}\times_{S^X}(S^X\otimes_V k)^{\mathrm{red}}$ coincides with the kernel of Frobenius on $\mathrm{Pic}^0_{X/S}\times_S(S^X\otimes_V k)^{\mathrm{red}}$.*

https://doi.org/10.1112/S0010437X07002813 Published online by Cambridge University Press

Proof. Since $\mathbb{G}$ is a subgroup of $\mathrm{Pic}^0_{X/S}\times_S S^X$ of rank p^g, it suffices to prove that $\mathbb{G}\times_{S^X}(S^X\otimes_V k)^{\mathrm{red}}$ is killed by Frobenius. For every generic point s of $(S^X\otimes_V k)^{\mathrm{red}}$, let $k(s)$ be its residue field. We claim that for every s the Lie algebra of $\mathbb{G}\otimes k(s)$ is a $k(s)$-vector space of dimension at least g. Consequently, [Mum70, p. 139] implies that the kernel of Frobenius on $\mathbb{G}\otimes k(s)$ has rank at least p^g. Since $\mathbb{G}\otimes k(s)$ has rank equal to p^g, it is then killed by Frobenius. This proves the lemma for the generic points of $(S^X\otimes k)^{\mathrm{red}}$. Since in a reduced ring A, the map from A to the product of the localizations at all its height 0 ideals is injective, it follows that $\mathbb{G}\times_{S^X}(S^X\otimes_V k)^{\mathrm{red}}$ (respectively, $\mathrm{Ker}(\mathrm{F})$ on $\mathrm{Pic}^0_{X/S}\times_S(S^X\otimes_V k)^{\mathrm{red}}$), being flat, coincides with the schematic closure in $\mathrm{Pic}^0_{X/S}\times_S(S^X\otimes_V k)^{\mathrm{red}}$ of its restriction to the generic points. The lemma follows.

We are left to prove the claim. Possibly, after replacing S^X with the p-adic completion of the normalization of $\mathcal{O}_{S^X,s}$, we may assume that $S=S^X=\mathrm{Spec}(R)$ is the spectrum of a complete dvr with residue field $\mathbb{F}$. By construction, Ψ factors through $\mathbb{G}\otimes_R\overline{R}$. Reducing modulo $\overline{R}_{1-w}$, with $w=1-(p-1)\mathrm{v}(\lambda)$ and λ as in Proposition 12.1, and taking the associated map on Lie algebras, we get $\overline{R}$-linear maps

$$\mathrm{Lie}(\mathrm{G}_\lambda{}^\vee)^g\otimes_R\overline{R}_{1-w}\longrightarrow\mathrm{Lie}(\mathbb{G}\otimes_R\overline{R}_{1-w})\subset\mathrm{Lie}(\mathrm{Pic}^0_{X/R}\otimes_R\overline{R}_{1-w})=\mathrm{H}^1(X,\mathcal{O}_X)\otimes_R\overline{R}_{1-w}.$$

By § 8.8, the image I contains the $\overline{R}$-module generated by the image of the map from $\mathrm{H}^1(X\otimes_R\overline{R},\mathrm{G}_\lambda)$ to $\mathrm{H}^1(X,\mathcal{O}_X)\otimes_R\overline{R}_{1-w}$ given in Theorem 8.1. It follows from Lemma 9.7 that I is generated as an $\overline{R}$-module by at least g elements. This implies that $\mathrm{Lie}(\mathbb{G}\otimes_R\overline{R}_{1-w})$ and, hence, the module J of invariant differentials of $\mathbb{G}\otimes_R\overline{R}_{1-w}$ are generated as an $\overline{R}$-modules by at least g elements. If the invariant differentials of $\mathbb{G}\otimes_R\mathbb{F}$ were generated by less than g elements, the same would apply to J by Nakayama. We conclude that the invariant differentials of $\mathbb{G}\otimes_R\mathbb{F}$ form a vector space of dimension at least g as claimed. □

13. Final considerations

In this section we assume that R is a complete discrete valuation ring. We fix an abelian scheme $X\to\mathrm{Spec}(R)$. We first show that our construction of the canonical subgroup coincides with that in [AM04].

13.1 Relation with [AM04]

Suppose that $p\geqslant 3$. Suppose that X satisfies the assumptions in [AM04, Theorem 1.1]. Take $\lambda\in\overline{R}$ to be an element of valuation $\mathrm{v}(\lambda)=1/p$. Thanks to Definition 6.5 and Proposition 12.1 the canonical subgroup $H_X\otimes\overline{R}_K$ is also with the orthogonal of $\mathrm{H}^1(X\otimes\overline{R},\mu_p)^{[\lambda]}$ via the Weil pairing

$$(X\otimes\overline{R}_K)[p]\times\mathrm{H}^1(X\otimes\overline{R}_K,\mu_p)\longrightarrow\mu_p.$$

It follows from [AM04, Theorem 3.1.2] that $H_X\otimes\overline{R}_K$ coincides with the subgroup $X[p]^{j+}$, constructed in [AM04, Corollary 6.1.2], base-changed to $\overline{R}_K$. This implies that our canonical subgroup and the canonical subgroup defined in [AM04] coincide in this case.

We now give an alternative description of $\mathrm{H}^1(X\otimes\overline{R},\mu_p)^{[p^{1/p}]}\subset\mathrm{H}^1(X\otimes\overline{R},\mu_p)$ (see Definition 6.5) using the map $d\log$.

13.2 The map $d\log$

Let $\overline{R}$ be as in Definition 6.1. Define the map

$$d\log\colon\mathrm{H}^1_{\mathrm{fppf}}(X_1\otimes_R\overline{R},\mu_p)\longrightarrow\mathrm{H}^0(X_1\otimes_R\overline{R},\Omega_{X_1\otimes_R\overline{R}/\overline{R}})$$

as follows. Let $Y_1\to X_1\otimes_R W$ be a μ_p-torsor with $R\subset W$ finite and étale over R_K and W normal. There exist a covering by open affine subschemes $\{U_i\}_i$ of $X\otimes_R W$ and elements $\gamma_i\in\Gamma(U_i,\mathcal{O}^*_{U_i})$

https://doi.org/10.1112/S0010437X07002813 Published online by Cambridge University Press

such that $Y_1|_{U_i}$ is defined by the affine algebra $z_i^p = \gamma_i$. Furthermore, there exists a one cocycle v_{ij} for $\mathcal{O}^*_{X_1 \otimes_R W}$ relative to the covering $\{U_i\}_i$ such that $\gamma_i = \gamma_j v_{ij}^p$ on $U_i \cap U_j$. Then, $d\log(\gamma_i) = d\log(\gamma_j)$ on $U_i \cap U_j$ and we get a section of $\mathrm{H}^0(X_1 \otimes_R W, \Omega_{X_1 \otimes_R W/W})$ denoted by $d\log(Y_1)$.

Lemma 13.3. *With the notation above we have $d\log(Y_1) = 0$ if and only if the γ_i are pth powers in $\Gamma(U_i, \mathcal{O}_{X_1 \otimes_R \overline{R}})$.*

Proof. If the γ_i are pth powers, clearly $d\log(Y_1) = 0$. Assume that $d\log(\gamma_i) = 0$ for every i. This holds only if $d\gamma_i = 0$. Fix i. Let π be a uniformizer of W. The proposition is known for the special fiber of $X \otimes_R W \to \mathrm{Spec}(W)$ since it is regular. Let π be a uniformizer of W. Then, there exists $a_1 \in \Gamma(U_i, \mathcal{O}_{X_1 \otimes_R W})$ such that $\gamma_i = a_1^p + \pi b_1$ for some b_1 in $\Gamma(U_i, \mathcal{O}_{X_1 \otimes_R W})$. Analogously, $\pi d(b_1) = 0$. Thus, there exists $a_2 \in \Gamma(U_i, \mathcal{O}_{X_1 \otimes_R W})$ such that $\pi b_1 = \pi a_2^p + \pi^2 b_2$ for some b_2 in $\Gamma(U_i, \mathcal{O}_{X_1 \otimes_R W})$. Continuing in this fashion we get a π-adic expansion of γ_i of the form $\gamma_i = \sum_n \pi^n a_n^p$. Let $\pi^{1/p}$ be an element of $\overline{R}$ whose pth power is π. Then, $\gamma_i = (\sum_n \pi^{n/p} a_n)^p$ is a pth power as claimed. □

Proposition 13.4. *Let $\lambda \in \overline{R}$ be an element of valuation $\mathrm{v}(\lambda) = \frac{1}{p}$. Then, the kernel of the map*

$$\mathrm{H}^1(X \otimes \overline{R}, \mu_p) \longrightarrow \mathrm{H}^1(X_1 \otimes_R \overline{R}, \mu_p) \xrightarrow{d\log} \mathrm{H}^0(X_1 \otimes \overline{R}, \Omega_{X_1 \otimes_R \overline{R}/\overline{R}})$$

coincides with $\mathrm{H}^1(X \otimes \overline{R}, \mu_p)^{[\lambda]}$.

Proof. We prove first that the image of η_λ is contained in the kernel of $d\log$. Let $Y \to X \otimes W$ be a G_λ-torsor. By Theorem 5.9 and Remark 5.10, if $(L, E, \Psi, \{(U_i, e_i, \alpha_i)\}_{i \in I})$ are the associated classifying data, the torsor is locally defined by $\mathrm{Spec}(\mathcal{O}_{U_i}[e_i]/(P_\lambda(e_i) - \alpha_i))$. The associated μ_p-torsor is then defined by $\mathrm{Spec}(\mathcal{O}_{U_i}[z_i]/(z_i - 1 + \lambda^p \alpha_i))$ and $d\log(1 + \lambda^p \alpha_i) \equiv 0$ modulo p by the assumption on $\mathrm{v}(\lambda)$.

Let Y be a μ_p-torsor over $X \otimes_R W$ such that $d\log(Y) = 0$. Let $\mathcal{Y}$ be the associated formal μ_p-torsor over $\mathfrak{X} \otimes_R W$. Let $\{\mathfrak{U}_i\}_i$ be a covering of $\mathfrak{X} \otimes W$ by open affine formal subschemes and let $\gamma_i \in \Gamma(\mathfrak{U}_i, (\mathcal{O}_{\mathfrak{X}} \otimes_R W)^*)$ be such that $\mathcal{Y}|_{\mathfrak{U}_i} \cong \mathrm{Spec}(\mathcal{O}_{\mathfrak{U}_i}[z_i]/(z_i^p - \gamma_i))$. By Lemma 13.3, we may assume that $\gamma_i \equiv 1$ modulo p. Since $\mathrm{v}(\lambda^p) = 1$, we can write $\gamma_i = 1 + \lambda^p \alpha_i$ with $\alpha_i \in \Gamma(\mathfrak{U}_i, \mathcal{O}_{\mathfrak{X}} \otimes W)$. Let $\{v_{ij}\}$ be a cocycle for $\mathcal{O}^*_{\mathfrak{X} \otimes W}$ relative to the covering $\{\mathfrak{U}_i\}_i$ such that $\gamma_i = \gamma_j v_{ij}^p$ on $\mathfrak{U}_i \cap \mathfrak{U}_j$ for every i and j. Then, $v_{ij} \equiv 1$ modulo $p^{1/p}$. Thus, we may write $v_{ij} = 1 + \lambda u_{ij}$ with $u_{ij} \in \Gamma(\mathfrak{U}_i \cap \mathfrak{U}_j, \mathcal{O}_{\mathfrak{X}} \otimes W)$. Let $Y'|_{\mathfrak{U}_i}$ be the spectrum of the subalgebra of $\mathcal{O}_{\mathfrak{U}_i}[z_i]/(z_i^p - \gamma_i) \otimes_W \mathrm{Frac}(W)$ defined by $\mathcal{O}_{\mathfrak{U}_i}[e_i]/(P_\lambda(e_i) - \alpha_i)$ with $e_i := (z_i - 1)/\lambda$. Note that $\mathcal{Y}'\ |_{\mathfrak{U}_i}$ is a G_λ-torsor over $\mathfrak{U}_i$. Since $e_i = v_{ij} e_j + u_{ij}$ and $v_{ij}^p \alpha_j - \alpha_i = -P_\lambda(u_{ij})$ on $\mathfrak{U}_i \cap \mathfrak{U}_j$, the G_λ-torsors $\mathcal{Y}'|_{\mathfrak{U}_i} \to \mathfrak{U}_i$ glue to a global G_λ-torsor $\mathcal{Y}' \to \mathfrak{X} \otimes W$. By construction, $\eta_\lambda(\mathcal{Y}') = \mathcal{Y}$. Since X is projective, it algebraizes to a G_λ-torsors $Y' \to X \otimes W$ such that $\eta_\lambda(Y') = Y$. □

We also have another map

$$d\,\mathrm{Log}_1 \colon X_1^\vee[p](\overline{R}_1) \longrightarrow \mathrm{H}^0(X_1 \otimes \overline{R}, \Omega_{X_1 \otimes \overline{R}/\overline{R}})$$

defined as follows. Let $\rho \colon X_1 \otimes \overline{R}[p] \to \mu_p$ be a $\overline{R}_1$-point of $X_1^\vee[p]$. Define $d\,\mathrm{Log}_1(\rho)$ as the pull-back of the canonical invariant differential dz/z on μ_p via ρ. Here we use that the invariant differentials of $X_1[p]$ coincide with the invariant differentials of X_1, i.e. with $\mathrm{H}^0(X_1, \Omega_{X_1/R_1})$. The following proposition answers a question raised in [AM04, Remark 6.1].

Proposition 13.5. *The following diagram is commutative.*

$$\begin{tikzcd}
\mathrm{H}^1(X \otimes \overline{R}, \mu_p) \arrow[r, "d\log"] \arrow[d, "\wr"'] & \mathrm{H}^0(X_1 \otimes \overline{R}, \Omega_{X_1 \otimes \overline{R}/\overline{R}}) \\
X^\vee[p](\overline{R}) \arrow[r] & X_1^\vee[p](\overline{R}_1) \arrow[u, "d\,\mathrm{Log}_1"']
\end{tikzcd}$$

https://doi.org/10.1112/S0010437X07002813 Published online by Cambridge University Press

Proof. To simplify the notation we assume $R = \overline{R}$ and that every μ_p-torsor over X is rigidified at the origin. Let $f : Y_1 \to X_1$ be a (rigidified) μ_p-torsor. Due to the rigidification it has a unique group scheme structure such that f is a homomorphism of group schemes (with kernel μ_p). The isomorphism $\varphi\colon \mathrm{Ext}^1(X_1, \mu_p) \xrightarrow{\sim} \mathrm{Hom}(X_1[p], \mu_p)$ has the following explicit description. The pull-back $[p]^*(Y_1)$ of Y_1 via multiplication by p on X_1 is canonically trivial since $\mathrm{Hom}(X_1, \mu_p) = 0$, i.e. $[p]^*(Y_1) \cong \mu_p \times X_1$. We thus get an induced homomorphism $h\colon X_1 \to Y_1$ such that $f \circ h = [p]$; this induces the required map $\varphi([Y_1])\colon X_1[p] \to \mu_p$.

Let F_{S_1} (respectively, F_{X_1}) be the absolute Frobenius on S_1 (respectively, X_1). Denote by $X_1^{(p)}$ the fiber product of $X_1 \to S_1$ via F_{S_1} and by $W : X_1^{(p)} \to X_1$ the projection. Let $V : X_1^{(p)} \to X_1$ be Verschiebung, we then get two maps V^* and W^* from $\mathrm{H}^1(X_1, \mu_p)$ to $\mathrm{H}^1(X_1^{(p)}, \mu_p)$. Consider the map V^*; via the isomorphisms

$$\mathrm{H}^1(X_1, \mu_p) \xrightarrow{\sim} \mathrm{Hom}(\mathbf{Z}/p\mathbf{Z}, X_1^\vee), \quad \mathrm{H}^1(X_1^{(p)}, \mu_p) \xrightarrow{\sim} \mathrm{Hom}(\mathbf{Z}/p\mathbf{Z}, (X_1^{(p)})^\vee)$$

it coincides with the homomorphism $v\colon \mathrm{Hom}(\mathbf{Z}/p\mathbf{Z}, X_1^\vee) \to \mathrm{Hom}(\mathbf{Z}/p\mathbf{Z}, (X_1^{(p)})^\vee)$ induced by $V^\vee\colon X_1^\vee \to (X_1^{(p)})^\vee$. Since $V^\vee\colon X_1^\vee \to (X_1^{(p)})^\vee = (X_1^\vee)^{(p)}$ is the relative Frobenius and Frobenius is the identity on $\mathbf{Z}/p\mathbf{Z}$, the map v coincide with the map $\varphi \mapsto F_{S_1}^*(\varphi)$. We conclude that $W^* = V^*$.

Suppose that the μ_p-torsor Y_1 is given on a covering by open affine subschemes $\mathfrak{U} = \{U_i\}_i$ of X_1 by local equations $Z_i^p = \gamma_i$ with $\gamma_i \in \Gamma(U_i, \mathcal{O}_{U_i}^*)$. Then, $(dZ_i/Z_i)_i \in C^0(\mathfrak{U}, \Omega_{Y_1/R_1})$ lifts the invariant differential dz/z of μ_p and $d\,\mathrm{Log}_1([Y_1])$ is the global differential of X_1 given by the pull-back of $(dZ_i/Z_i)_i$ via h. Since $[p]$ is the composite of Verschiebung V and (the relative) Frobenius F, the μ_p-torsor $[p]^*(Y_1)$ is $F^*(V^*[Y_1]) = F^*(W^*[Y_1]) = F_{X_1}^*[Y_1]$. The latter is defined on U_i by the equation $Z_i^p - \gamma_i^p$ and admits the trivialization $Z_i = \gamma_i$ so that the pull-back of $(dZ_i/Z_i)_i$ via h is locally given by $(d\gamma_i/\gamma_i)_i$. The conclusion follows.

Proposition 13.5 is motivated by the following weak integral analogue of the Hodge–Tate decomposition as suggested in [AM04, Remark 6.1]. □

13.6 Relations with the Hodge–Tate decomposition

Suppose that $p \geqslant 3$. Let $\overline{K}$ be an algebraic closure of K and let $\overline{V}$ be the integral closure of V in $\overline{K}$. Let $\mathbf{C}_p$ (respectively, $\mathcal{O}_{\mathbf{C}_p}$) be the p-adic completion of $\overline{K}$ (respectively, $\overline{V}$). Let $\lambda \in \overline{V}$ be an element of valuation $\mathrm{v}(\lambda) := 1/p$. The Hodge–Tate decomposition is a canonical isomorphism of Galois modules

$$\mathrm{H}^1(X_{\overline{K}}, \mathbb{Q}_p) \otimes_{\mathbb{Q}_p} \mathbf{C}_p \cong (\mathrm{H}^1(X, \mathcal{O}_X) \oplus \mathrm{H}^0(X, \Omega^1_{X/V})(-1)) \otimes_V \mathbf{C}_p;$$

see [Tat67, Remark on p. 180]. To simplify the following heuristic considerations we will ignore the Galois action from now on. We will discuss it in a more general situation in a future paper.

In Proposition 13.4 and 13.5 we proved that we have an exact sequence of $\mathbb{F}_p$-vector spaces:

$$0 \longrightarrow \mathrm{H}^1(X \otimes \overline{V}, \mathrm{G}_\lambda) \longrightarrow \mathrm{H}^1(X \otimes \overline{K}, \mu_p) \xrightarrow{d\,\mathrm{Log}_1} \mathrm{H}^0(X_1 \otimes \overline{V}, \Omega^1_{X_1 \otimes \overline{V}/\overline{V}}). \tag{13.6.1}$$

If X_k is ordinary, we can obtain from (13.6.1) a generalization of the Hodge–Tate decomposition to p-torsion coefficients. Indeed, we remark the following.

(1) the kernel of $d\,\mathrm{Log}_1$ has dimension g as $\mathbb{F}_p$-vector space by Proposition 12.1(1).

(2) By Proposition 12.1(2) the kernel of $d\,\mathrm{Log}_1$ with $\mathrm{H}^1(X \otimes \overline{V}, \mathbf{Z}/p\mathbf{Z})$ because $\mathbf{Z}/p\mathbf{Z} \simeq G_{p^{1/p-1}}$; the reduction modulo p gives $\mathrm{H}^1(X \otimes \overline{V}, \mathbf{Z}/p\mathbf{Z}) \xrightarrow{\sim} \mathrm{H}^1(X_1 \otimes \overline{V}, \mathbf{Z}/p\mathbf{Z})$. By Artin–Schreier theory, cf. Theorem 8.1, we have an exact sequence

$$0 \longrightarrow \mathrm{H}^1(X_1 \otimes \overline{V}, \mathbf{Z}/p\mathbf{Z}) \longrightarrow \mathrm{H}^1(X_1, \mathcal{O}_{X_1}) \otimes_V \overline{V} \xrightarrow{\mathrm{F}-1} \mathrm{H}^1(X_1, \mathcal{O}_{X_1}) \otimes_V \overline{V}.$$

Furthermore, we have $\mathrm{H}^1(X_1, \mathcal{O}_{X_1}) \otimes_V \overline{V} \cong \mathrm{H}^1(X_1 \otimes \overline{V}, \mathbf{Z}/p\mathbf{Z}) \otimes_{\mathbb{F}_p} \overline{V}/p\overline{V}$. This is deduced

https://doi.org/10.1112/S0010437X07002813 Published online by Cambridge University Press

using Nakayama's lemma since it holds modulo the maximal ideal of $\overline{V}$ by [Mum70, Corollary on p. 143];

(3) We have that $\mathrm{H}^0(X_1 \otimes \overline{V}, \Omega^1_{X_1 \otimes \overline{V}/\overline{V}})$ coincides with $\mathrm{Im}(d\,\mathrm{Log}_1) \otimes_{\mathbb{F}_p} \overline{V}/p\overline{V}$. Indeed, using the Cartier operator and relating the Hodge to de Rham and the conjugate spectral sequences on $\mathbb{H}^1_{\mathrm{dR}}(X_1 \otimes \overline{V}/\overline{V})$ (see [Kat73, § 2], especially Corollary 2.3.1.2) we obtain a Frobenius linear homomorphism

$$C^{-1} : \mathrm{H}^0(X_1 \otimes \overline{V}, \Omega^1_{X_1 \otimes \overline{V}/\overline{V}}) \to \mathrm{H}^0(X_1 \otimes \overline{V}, \Omega^1_{X_1 \otimes \overline{V}/\overline{V}}).$$

The ordinarity of X implies that it is an isomorphism, cf. [Kat72, (2.3.4.1.4)]. By [Kat72, (2.1.2.1)] it is the identity on the image of $d\,\mathrm{Log}_1$. One concludes using [Mum70, Corollary on p. 143] once more.

One then deduces from (13.6.1) the exact sequence

$$0 \to \mathrm{H}^1(X, \mathcal{O}_X) \otimes_V (\overline{V}/p\overline{V}) \to \mathrm{H}^1(X \otimes \overline{K}, \mu_p) \otimes_{\mathbf{Z}} \overline{V} \to \mathrm{H}^0(X, \Omega^1_{X/V}) \otimes_V (\overline{V}/p\overline{V}) \to 0.$$

This can be seen as a weak Hodge–Tate decomposition with torsion coefficients.

Condition (3) is equivalent to asking whether X_k is ordinary: if it holds, $\mathrm{H}^0(X_k, \Omega^1_{X_k/k})$ is generated by logarithmic differential forms so that the Cartier operator is an isomorphism and this is equivalent to requiring that X_k is ordinary.

Consequently, if X_k is not ordinary, one does not expect such a decomposition to exist. Nevertheless, suppose that $X \to S$ is a (w, g)-situation with $w < 1/p$ (and $p > 3$). Then, we still have an exact sequence

$$0 \longrightarrow \mathrm{H}^1(X \otimes \overline{K}, \mu_p)^{[1/p]} \longrightarrow \mathrm{H}^1(X \otimes \overline{K}, \mu_p) \xrightarrow{d\,\mathrm{Log}_1} \mathrm{H}^0(X_1 \otimes \overline{V}, \Omega^1_{X_1 \otimes \overline{V}/\overline{V}}).$$

Moreover, $\mathrm{H}^1(X \otimes \overline{K}, \mu_p)^{[1/p]}$ is a $\mathbb{F}_p$-vector space of dimension g by Proposition 12.1. Thus, in this case, one has an exact sequence in the flavor of the Hodge–Tate decomposition for torsion coefficients. The authors believe that a similar phenomenon should occur for $\mathrm{H}^1(X \otimes \overline{K}, \mu_{p^n})$ (for every $n \geqslant 1$) and will return to this topic in a future paper.

Acknowledgements

We warmly thank Ahmed Abbes for discussions which lead us into the realm of the canonical subgroup, for his supporting enthusiasm and encouragement and for his suggestions. We also thank the referee for his careful reading and his very useful comments on the manuscript.

References

AG F. Andreatta and C. Gasbarri, *Torsors under some group schemes of order p^n*, Preprint http://www.mat.uniroma2.it/∼gasbarri.

AM04 A. Abbes and A. Mokrane, *Sous-groupes canoniques et cycles évanescents p-adiques pour les variétés abéliennes*, Publ. Math. Inst. Hautes Études Sci. **99** (2004), 117–162.

AS02 A. Abbes and T. Saito, *Ramification of local fields with imperfect residue fields*, Amer. J. Math. **124** (2002), 879–902.

Ber96 P. Berthelot, *Cohomologie rigide et cohomologie rigide à supports propres*, première partie (version provisoire 1991), Preprint (1996), IRMAR 96–03, Université de Rennes.

BK86 S. Bloch and K. Kato, *p-adic étale cohomology*, Publ. Math. Inst. Hates Études Sci. **63** (1986), 107–152.

Bou98 N. Bourbaki, *Commutative algebra*, Elements of Mathematics (Springer, Berlin, 1998), ch. 1–7.

https://doi.org/10.1112/S0010437X07002813 Published online by Cambridge University Press

BL93 S. Bosch and S. Lütkebohmert, *Formal and rigid geometry. I. Rigid spaces*, Math. Ann. **295** (1993), 291–317.

Con05 B. Conrad, *Higher-level canonical subgroups in abelian varieties*, Preprint (2005).

Eis95 D. Eisenbud, *Commutative algebra. With a view toward algebraic geometry*, Graduate Texts in Mathematics, vol. 150 (Springer, New York, 1995).

GK06 E. Z. Goren and P. Kassaei, *The canonical subgroup: a 'subgroup-free' approach*, Comment Math. Helv. **81** (2006), 617–641.

EGAI A. Grothendieck, *Éléments de géométrie algébrique. I. Le Langage des schemas*, Publ. Math. Inst. Hautes Études Sci. **4** (1960).

EGAII A. Grothendieck, *Éléments de géométrie algébrique. II. Étude globale élémentaire de quelques classes de morphismes*, Publ. Math. Inst. Hautes Études Sci. **8** (1961).

EGAIII A. Grothendieck, *Éléments de géométrie algébrique. III. Étude cohomologique des faiceaux cohérents. I*, Publ. Math. Inst. Hautes Études Sci. **11** (1961); *II*, idem. **17** (1963).

EGAIV A. Grothendieck, *Éléments de géométrie algébrique. IV. Étude locale des schemas et des morphismes de schemas. I*, Publ. Math. Inst. Hautes Études Sci. **20** (1964); *II*, idem. **24** (1965); *III*, idem. **28** (1966); *IV*, idem. **32** (1967).

Kat72 N. Katz, *Algebraic solutions of differential equations (p-curvature and the Hodge filtration)*, Invent. Math. **18** (1972), 1–118.

Kat73 N. Katz, *p-adic properties of modular schemes and modular forms*, In *Modular functions of one variable, III*, Lecture Notes in Mathematics, vol. 350, (Springer, Berlin, 1973), 69–190.

KL05 M. Kisin and K. F. Lai, *Overconvergent Hilbert modular forms*, Amer. J. Math. **127** (2005), 735–783.

Mil80 J. Milne, *Étale cohomology* (Princeton University Press, Princeton, NJ, 1980).

Mum65 D. Mumford, *Geometric invariant theory*, Ergebnisse der Mathematik und ihrer Grenzgebiete. Neue Folge, vol. 34 (Springer, New York, 1965).

Mum70 D. Mumford, *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics, No. 5 (Oxford University Press, London, 1970).

Nev03 E. Nevens, *The Hecke operator U_p for overconvergent Hilbert modular forms*, PhD thesis, Imperial College, London (2003).

NO80 P. Norman and F. Oort, *Moduli of abelian varieties*, Ann. of Math. (2) **112** (1980), 413–439.

OT70 F. Oort and J. Tate, *Group schemes of prime order*, Ann. Sci. École Norm. Sup. (4)**3** (1970), 1–21.

Ray74a M. Raynaud, *Géométrie analytique rigide d'aprés Tate, Kiehl, ...*, in *Table Ronde d'Analyse non archimédienne*, Paris, 1972, Bull. Soc. Math. France **39**–**40** (1974), 319–327.

Ray74b M. Raynaud, *Schémas en groupes de type* $(p, \dots, p)$, Bull. Soc. Math. France **102** (1974), 241–280.

RG71 M. Raynaud and L. Gruson, *Critéres de platitude et de projectivité. Techniques de 'platification' d'un module*, Invent. Math. **13** (1971), 1–89.

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

F. Andreatta fandreat@math.unipd.it
Dipartimento di Matematica 'Federigo Enriques', Università di Milano, Via C. Saldini 50, 20133 Milano, Italy

C. Gasbarri gasbarri@mat.uniroma2.it
Dipartimento di Matematica dell'Università di Roma 'Tor Vergata', Viale della Ricerca Scientifica, 00133 Roma, Italy

https://doi.org/10.1112/S0010437X07002813 Published online by Cambridge University Press