FINITE GROUP SCHEMES OVER BASES WITH LOW RAMIFICATION

BRIAN CONRAD

Abstract. Let A' be a complete characteristic $(0,p)$ discrete valuation ring with absolute ramification degree e and a perfect residue field. We are interested in studying the category $\mathcal{FF}_{A'}$ of finite flat commutative group schemes over A' with p-power order. When $e = 1$, Fontaine formulated the purely 'linear algebra' notion of a *finite Honda system over* A' and constructed an anti-equivalence of categories between $\mathcal{FF}_{A'}$ and the category of finite Honda systems over A' when $p > 2$. We generalize this theory to the case $e \leq p-1$.

Introduction

This paper lays the foundations for generalizing Ramakrishna's work [16] on deformations of Galois representations to settings in which a small amount of ramification is allowed. The motivation is the problem of proving the Shimura-Taniyama Conjecture in non-semistable cases, and this requires extending the results of [16] to cases in which there is ramification. The application of our group scheme results to the deformation theory of Galois representations is given in [4] (below, we will formulate a simplified version of the main result of [4]). In [5], these deformation-theoretic results are used to establish the Shimura-Taniyama Conjecture for elliptic curves over $\mathbf{Q}$ which acquire semistable reduction over a tamely ramified extension of $\mathbf{Q}_3$ (and in [3] the remaining 'wild' cases of the Shimura-Taniyama Conjecture are handled by [2], which generalizes the results of this paper via much more sophisticated techniques). At the end of this Introduction we make some remarks on these matters.

First, let's describe the basic setting which we will consider. Let $(A', \mathfrak{m})$ be a complete mixed characteristic discrete valuation ring with perfect residue field k having characteristic p, and let $A = W(k)$. We are interested in studying the category $\mathcal{FF}_{A'}$ of finite flat commutative A'-group schemes with p-power order. When $p > 2$ and $A' = A$, Fontaine constructs in [8] a fully faithful, essentially surjective functor from $\mathcal{FF}_{A'}$ to the category $SH^f_{A'}$ of *finite Honda systems over* A', whose objects consist of finite-length $W(k)$-modules with various extra structures. Fontaine's central tool is the theory he develops in his book [7]. He obtains a similar result when $p = 2$ for unipotent group schemes. But what if one does not require $e(A') = 1$?

It follows from [17, Cor 3.3.6(1)] that the category $\mathcal{FF}_{A'}$ is abelian whenever $e = e(A') < p-1$, using scheme-theoretic kernel as the kernel, so it is natural to ask if Fontaine's results can be extended to cover this general case. We have developed such a generalization and following Fontaine, we call the corresponding category $SH^f_{A'}$ of module structures *finite Honda systems over* A'. When $e \leq p-1$, we define categories $SH^{f,u}_{A'}$ and $SH^{f,c}_{A'}$ of *unipotent* and *connected finite Honda systems over* A' and obtain similar results, extending those of Raynaud and Fontaine for such ramification values.

When $e < p-1$, we define a contravariant additive functor $LM_{A'} : \mathcal{FF}_{A'} \to SH^f_{A'}$ (Theorem 3.4) which we prove is fully faithful and essentially surjective (Theorem 3.6). The abelian category structure on $SH^f_{A'}$ is made explicit too (Theorem 4.3). We have similar results for the full subcategories of unipotent and connected objects when $e \leq p-1$. For $e = 1$, we recover Fontaine's original construction.

The full details of the proof of Fontaine's result in the unramified case have never been published ([8] is a brief announcement outlining the main steps of the proof). These details are essential for an understanding of the more general arguments, so we begin by writing them out fully in §1. We use ideas introduced by Fontaine in [7] in order to generalize everything to the case in which $e \leq p-1$. The calculations required for

Date: Sept 8, 1999.
1991 *Mathematics Subject Classification.* Primary 14L15; Secondary 14L05.
Key words and phrases. group scheme, Dieudonné module, Fontaine.
This research was partially supported by a DoD grant.

the case $e > 1$ are far more cumbersome than in the unramified case and some of our arguments will only work when $e > 1$, so we first present the $e = 1$ proof. It should be emphasized that [7] is vital for everything that we do.

We construct a 'base change' functor for finite Honda systems (Theorem 4.8) and we verify that this construction is compatible with base change of finite flat group schemes (of course only allowing base changes which preserve the $e \leq p-1$ condition). The base change formalism has some interesting applications. For example, it can be used to prove a theorem about good reduction of abelian varieties (Theorem 5.3). Also, this formalism allows us to translate generic fiber Galois descent into the language of finite Honda systems, thereby laying the groundwork for generalizing the work of Ramakrishna [16] to ramified situations.

This second application is briefly described in §5 and is more fully developed in [4]; it is concerned with a deformation-theoretic study of certain continuous representations $\overline{\rho} : \mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p) \to \mathrm{GL}_2(\mathbf{F}_p)$. Fix a finite extension $K/\mathbf{Q}_p$ inside of $\overline{\mathbf{Q}}_p$, with $e = e(K/\mathbf{Q}_p)$ satisfying $e \leq p-1$. We assume that $\overline{\rho}|_{\mathrm{Gal}(\overline{\mathbf{Q}}_p/K)}$ is the generic fiber of a finite flat group scheme G over $\mathcal{O}_K$ which is connected and has a connected Cartier dual. There is also the mild technical hypothesis that if M is the Dieudonné module of the closed fiber of G, then the sequence of groups

$$0 \to M/VM \xrightarrow{F} M/pM = M \to M/FM \to 0.$$

should be exact (this is automatically satisifed if G is the p-torsion of a p-divisible group). For the motivating application to the study of modularity of certain elliptic curves over $\mathbf{Q}$, these conditions are satisfied. As long as $\overline{\rho}$ has trivial centralizer, there is a universal deformation ring $R_K(\overline{\rho})$ classifying deformations ρ of $\overline{\rho}$ to complete local noetherian $\mathbf{Z}_p$-algebras R with residue field $\mathbf{F}_p$ such that $\rho|_{\mathrm{Gal}(\overline{\mathbf{Q}}_p/K)} \bmod \mathfrak{m}_R^n$ is the generic fiber of a finite flat group scheme over $\mathcal{O}_K$ for all $n \geq 1$. In [4], we use the results in this paper to prove

Theorem. The representation $\overline{\rho}$ has trivial centralizer and $R_K(\overline{\rho}) \simeq \mathbf{Z}_p[\![T_1, T_2]\!]$.

We also obtain in [4] similar results in somewhat more general settings.

After the writing of this paper was completed, the author found that the general problem of extending Fontaine's results on finite flat group schemes to a setting with $e > 1$ has been considered before, in [18]. However, the methods and results in [18] are very different from ours. Let us explain this point more carefully. We develop a theory which classifies group schemes in terms of 'intrinsic' finite-length module data. This theory makes it possible to do explicit calculations, even if we are interested in studying maps between group schemes (as opposed to studying a single group scheme). Such computability is essential in the proof of the deformation theory result mentioned above. The theory in [18], which applies under less restrictive conditions on the ramification, is motivated by the theorem of Oort which asserts that any object in $\mathcal{FF}_{A'}$ arises as the kernel of an isogeny of p-divisible groups. The classification of finite flat group schemes in [18], which uses very different techniques of proof, is given in terms of pairs of finite free modules with maps between them [18, pp. 13-15].

That is, in some sense [18] works with a presentation of a finite-length module rather than directly with the finite-length module itself. This leads to serious difficulties once one tries to study maps between group schemes. For example, if G and G' are two objects in $\mathcal{FF}_{A'}$ and $\Gamma_1 \to \Gamma_2$, $\Gamma_1' \to \Gamma_2'$ are isogenies of p-divisible groups over A' with respective kernels G and G', then it is not generally true that any map $f : G \to G'$ in $\mathcal{FF}_{A'}$ is induced by a compatible pair of maps $\Gamma_1 \to \Gamma_1'$, $\Gamma_2 \to \Gamma_2'$. Thus, any attempt to study morphisms in $\mathcal{FF}_{A'}$ by means of [18] requires frequently 'changing the presentation', and this makes explicit computations difficult or impossible to carry out.

The approach in [18], on the other hand, is useful in the study of lifting questions for a single fixed group scheme. For example, for any $e > 1$ and $p \geq 5$, the theory in [18] enables one to construct 'lifts to characteristic 0' of any object in $\mathcal{FF}_k$. This is something our approach cannot establish for $e > p-1$.

Due to absent-mindedness of the author, this paper is appearing in print somewhat later than it should have. It therefore seems appropriate to discuss subsequent developments. In [2], Breuil constructs a 'linear algebra' theory for finite flat group schemes (subject to some flatness conditions on p-power torsion levels, and with $p > 2$) without any restrictions on the ramification. When $e < p-1$, Breuil's category of 'linear algebra' objects is equivalent to (but not literally the same as) the category studied in this paper. However, whereas our theory is given in terms of filtered modules over a discrete valuation ring, Breuil's more general theory works with filtered modules over the p-adic completion of a certain divided power envelope and depends upon a *choice* of uniformizer. In the case of p-torsion objects, Breuil's category of 'linear algebra' objects can be identified with a simpler category of finite-length filtered modules over a small artin ring. This theory provides the necessary local tools to complete the proof of the remaining 'wild' cases of the Shimura-Taniyama Conjecture [3].

There are several reasons why the results in this paper seem to still be of interest (if one is in a situation with low ramification). First of all, the methods are certainly much more elementary; e.g., there is no use of the techniques of crystalline cohomology. Also, we make *no* flatness restriction on the p-power torsion levels and the intrinsic description of base change (preserving the low ramification condition) is very simple, whereas base change in the setting of [2] is somewhat complicated; this is mainly due to the fact that the theory in [2] depends upon a choice of uniformizer of the base. However, the main distinction between the two approaches is seen if one wants to do explicit calculations with group schemes which are *not necessarily* killed by p (over bases with absolute ramification $e < p-1$). Without a p-torsion hypothesis, the theory in [2] is well-suited to theoretical considerations and analysis of p-divisible groups, but it does not yet seem amenable to explicit calculations "at finite level". At some future time, this problem will no doubt be overcome. In the meantime, we should be grateful that the local calculations in [3] only require working with objects killed by p.

Acknowledgements I would like to thank Wiles for suggesting the problem of generalizing Fontaine's theory to ramified settings. I am also grateful to Fred Diamond, Vinayak Vatsal, and (especially) J.-M. Fontaine for comments and suggestions which led to the removal of some unneccessary hypotheses in earlier versions of some of the results.

Summary of some results of Fontaine

Fontaine's book [7] is absolutely essential in everything that we will do. It develops the foundations for Dieudonné modules as we will use them and also supplies the results on formal group schemes which will be the starting point for our study of finite flat group schemes. As a convenience to the reader we will now give an overview of the basic results and notation that we take from [7]. We will only formulate the results in the most common cases of application for our arguments, but the reader should keep in mind that much greater generality is needed in order to carry out the proofs of the main results in [7], including ones we will invoke later on (e.g., Fontaine's classification of p-divisible groups).

Let k be a perfect field with characteristic $p > 0$. For any finite k-algebra R, we define the *R-valued Witt covectors* $CW_k(R)$ to be the set of sequences $\mathbf{a} = (\dots, a_{-n}, \dots, a_0)$ of elements $a_i \in R$ indexed by non-positive integers, with a_i nilpotent for large i. This is to be thought of as analogous to $\mathbf{Q}_p/\mathbf{Z}_p$. Letting $S_m \in \mathbf{Z}[X_0, \dots, X_m, Y_0, \dots, Y_m]$ denote the mth addition polynomial for p-Witt vectors [7, pp. 71-2], and choosing $\mathbf{a}, \mathbf{b} \in CW_k(R)$, the nilpotence condition ensures that the sequence

$$\{S_m(a_{-n-m}, \dots, a_{-n}, b_{-n-m}, \dots, b_{-n})\}_{m \geq 0}$$

is stationary. Denoting the limit by c_{-n}, it is true that $\mathbf{c} = (c_{-n}) \in CW_k(R)$ and defining

$$\mathbf{a} + \mathbf{b} \stackrel{\text{def}}{=} \mathbf{c}$$

makes $CW_k(R)$ into a commutative group with identity $(\dots, 0, \dots, 0)$ [7, Prop 1.4, Ch II]. For $R = k'$ a finite extension of k, $CW_k(k')$ is exactly $K'/W(k')$, with K' the fraction field of $W(k')$.

We topologize $CW_k(R)$ by viewing it as a subset of the product space $\prod_{n \leq 0} R$, where each factor is discrete. This makes $CW_k(R)$ a topological group. Moreover, it admits a unique compatible structure of topological $W(k)$-module such that for all $x \in k$, with Teichmüller lift $[x] \in W(k)$, we have

$$[x] \cdot \mathbf{a} = (\dots, x^{p^{-n}} a_{-n}, \dots, x^{p^{-1}} a_{-1}, a_0).$$

The operations $F, V : CW_k(R) \to CW_k(R)$ given by

$$F(\mathbf{a}) = (\dots, a_{-n}^p, \dots, a_0^p), \quad V(\mathbf{a}) = (\dots, a_{-n-1}, \dots, a_{-1})$$

are additive, continuous, satisfy $FV = VF = p$, and with respect to the $W(k)$-module structure are σ and σ^{-1}-semilinear respectively, where $\sigma : W(k) \to W(k)$ is the Frobenius morphism.

In other words, $CW_k(R)$ is a module over the Dieudonné ring $D_k = W(k)[F, V]$ generated by two commuting variables with the usual relations $FV = VF = p$, $F\alpha = \sigma(\alpha)F$, $V\alpha = \sigma^{-1}(\alpha)V$ (for $\alpha \in W(k)$), and there is a compatible structure of topological $W(k)$-module with respect to which F and V act continuously. We abbreviate this by saying that $CW_k(R)$ is a *topological D_k-module* (though note that we do not put a topology on D_k). This is all functorial in R. For proofs, see [7, pp. 79-82]. When $R = k'$ is a finite extension of k, the topology and D_k-module structure on $CW_k(k') \simeq K'/W(k')$ are as usual.

If R is a complete local noetherian $W(k)$-algebra with residue field a finite extension of k, we define the topological D_k-module

$$\widehat{CW}_{W(k)}(R) = \varprojlim CW_k(R/\mathfrak{m}_R^n),$$

where $\mathfrak{m}_R$ is the maximal ideal of R. This is a Hausdorff topological D_k-module, functorial in R. In fact, if R is *any* separated and complete topological $W(k)$-algebra with a base of open ideals, one can define a topological D_k-module $\widehat{CW}_{W(k)}(R)$ functorially in R [7, Ch II, Prop 2.3]. However, due to pathologies which arise from the relation between product topologies and direct limit topologies [12, Exer 40A], one needs to be extremely careful when dealing with such general R. The only such pathological R that will really arise for us are rings such as the valuation ring of $\mathbf{C}_p$, with the p-adic topology (the problem is that the quotients of this ring by powers of p do not have a nilpotent nilradical). This ring only arises in formulating an 'explicit' dictionary between 'linear algebra data' and Galois representations; since this is not relevant to our classification theorems, we won't address this issue any further.

The functor CW_k on finite k-algebras is pro-represented by a formal affine commutative k-group scheme, denoted $\widehat{CW}_k$ [7, §4.2, Ch II]. If R is a complete local noetherian k-algebra with residue field a finite extension of k, then $\widehat{CW}_k(R) = \widehat{CW}_{W(k)}(R)$. For any p-formal commutative group scheme G over k — i.e., one for which $G \simeq \varinjlim G[p^n]$ (e.g., a finite flat commutative k-group scheme with p power order, or a p-divisible group over k) — we define the *Dieudonné module*

$$\mathcal{M}(G) = \mathrm{Hom}(G, \widehat{CW}_k),$$

the group of formal k-group scheme maps from G to $\widehat{CW}_k$. This is motivated by the functor

$$G \rightsquigarrow \mathrm{Hom}(G, \mathbf{C}^\times) \simeq \mathrm{Hom}(G, \mathbf{Q}_p/\mathbf{Z}_p)$$

for finite abelian p-groups. The action of D_k on the functor CW_k gives rise to an action of D_k on $\mathcal{M}(G)$. One can also define a suitable topology on $\mathcal{M}(G)$ with respect to which it is a topological D_k-module [7, §1.2, Ch III]. All of the standard properties of the classical Dieudonné module theory are proven in [7, Ch III] based on this definition. The main result of this theory is that the functor $\mathcal{M}$ sets up an antiequivalence of abelian categories between p-formal commutative group schemes over k and certain topological D_k-modules. There are various specializations of this theorem to finite commutative k-group schemes with p-power order, connected commutative p-formal k-group schemes, etc.

The main result in [7] is that one can 'enhance' this theory to classify p-divisible groups over suitable bases (up to isogeny or isomorphism, depending on ramification) in terms of 'linear algebra' data.

NOTATION. Throughout this paper, we fix a perfect field k with characteristic $p > 0$ and let A denote $W(k)$ and K its fraction field. The Dieudonné ring $A[F, V]$ of k as introduced above is denoted D_k. Note that for $k \neq \mathbf{F}_p$, this is not commutative. We let $(A', \mathfrak{m})$ be the valuation ring of a finite *totally ramified* extension K' of K, with $e = e(A') = [K' : K]$ the absolute ramification index of A'. The category of finite flat commutative group schemes over A with p power order is denoted $\mathcal{FF}_A$, and $\mathcal{FF}_A^c$, $\mathcal{FF}_A^u$ are the full subcategories consisting of connected and unipotent (i.e., connected Cartier dual) objects, respectively. We define $\mathcal{FF}_k$, $\mathcal{FF}_{A'}$, etc. in a similar manner.

A *p-adic A'-ring* is a flat A'-algebra which is p-adically separated and complete. The main examples to keep in mind are power series rings $A'[\![X_1, \ldots, X_n]\!]$, finite flat A'-algebras, and the valuation ring of the completion of an algebraic closure of K'.

1. Finite Flat Group Schemes: The Case $e = 1$

We wish to develop a 'linear algebra' theory of finite flat group schemes. It will always be assumed that the absolute ramification index $e = e(A')$ satsifies $e \leq p-1$. Our aim is to construct an equivalence of categories between $\mathfrak{FF}_{A'}$ (resp. $\mathfrak{FF}^c_{A'}$, $\mathfrak{FF}^u_{A'}$) and a certain category of 'linear algebra data' when $e < p-1$ (resp. $e \leq p-1$).

In the case $e = 1$, a theorem in this direction has been proven by Fontaine. His brief announcement [8] sketches the outline of the proof, but omits some technical details. This section is just a technical exposition of Fontaine's announcement and contains nothing new (note that we formulate the main result to include connected group schemes when $p = 2$, but the argument is essentially the same as Fontaine's in the unipotent case). Some of these details are essential for understanding the motivation behind the generalization we will prove. Therefore, in the interest of completeness (and since the arguments in the case $e = 1$ are far simpler to explain), we will first review Fontaine's proof in full detail for the case $e = 1$. Then this method will be generalized in the sections which follow.

It may be instructive to first explain the general strategy. When $e < p-1$, Fontaine constructs an essentially surjective, fully faithful contravariant additive functor $LM_{A'}$ from the category of p-divisible groups over A' to a certain category of 'linear algebra data' in which the objects are pairs $(\mathcal{L}, M)$ with $\mathcal{L}$ a finite free A'-module and M a finite free A-module, together with various extra structures and properties required [7, Ch IV, §5, Prop 5.1(i)]. The construction of such a functor depends heavily on the condition $e < p-1$. When $e \leq p-1$, the method applies to connected and unipotent objects. For *arbitrary* e, Fontaine can only describe the category of p-divisible groups over A' up to isogeny [7, Ch IV, §5, Prop 5.2]. One can think of the constraint on e as being related to forcing the convergence of the p-adic logarithm on $\mathfrak{m}$, which is relevant because in some sense, the failure of Fontaine's method to yield a fully faithful functor for large e is related to the failure of the torsion points of a p-divisible group over A' to *inject* into the torsion points of the closed fiber for large e. A large radius of convergence for the logarithm can ensure such injectivity (though the logarithm is not explicitly used in Fontaine's arguments).

The functor $LM_{A'}$ on p-divisible groups suggests that objects in $\mathfrak{FF}_{A'}$ which occur inside p-divisible groups over A' ought to correspond to analogous 'linear algebra data' in which the A and A'-modules have finite length. When $e = 1$, Fontaine carries out this idea while simulataneously showing that for odd p *all* objects in $\mathfrak{FF}_A$ occur inside a p-divisible group over A, and similarly for $\mathfrak{FF}^u_A$ and unipotent p-divisible groups for all p. It is a (non-trivial) theorem that *every* object in $\mathfrak{FF}_{A'}$ occurs in a p-divisible group over A' (with *no* conditions on e or p). This suggests that we should try to use Fontaine's classification of p-divisible groups over A' in conjunction with a generalization of his method for analyzing $\mathfrak{FF}_A$ using p-divisible groups in order to describe $\mathfrak{FF}_{A'}$ via 'linear algebra data'. We will not use the theorem about embedding objects in $\mathfrak{FF}_{A'}$ into p-divisible groups over A', though our methods rederive this result in the cases we consider.

Briefly, the underlying principle is summed up as follows. *Smooth* finite-dimensional commutative formal group schemes over A' are extensions of etale ones by connected ones, with the connected ones having as their affine ring a formal power series ring in finitely many variables. This is how Fontaine is able to get decisive results on such formal group schemes [7, Ch IV, §4.8, Thm 2]. Since p-divisible groups are special examples of such formal group schemes and they provide a convenient setting in which objects in $\mathfrak{FF}_{A'}$ arise 'in nature,' a classification theory for p-divisible groups over A' can be expected to lead to a classification theory for finite flat closed subgroup schemes of p-divisible groups (and fortunately all objects in $\mathfrak{FF}_{A'}$ arise in this way). Thus, the result of Serre and Tate [19, Prop 1] that connected p-divisible groups are necessarily *smooth* (in the formal sense) is the main starting point for everything that follows.

Let's now derive Fontaine's results in the case $e = 1$. Choose an object G in $\mathfrak{FF}_A$, with $M = \mathcal{M}(G_k)$ the Dieudonne module of the closed fiber G_k of G. By viewing formal k-group scheme homomorphisms $G \to \widehat{CW}_k$ as just formal k-scheme homomorphisms, we get a natural embedding of the D_k-module M as a finite-length A-submodule of the topological D_k-module $CW_k(\mathcal{R}_k)$, where $\mathcal{R}$ is the finite flat A-algebra which is the affine ring of G (the induced topology on M is exactly the p-adic topology). We denote by $\mathcal{R}_k$ and $\mathcal{R}_K$ the closed and generic fibers respectively of $\mathcal{R}$ over A. Also, Δ will be our notation for a comultiplication map (Δ_G, Δ_{G_k}, etc.). Let $L = L_A(G) \subseteq M$ denote kernel of the A-linear composite map

$$M \hookrightarrow CW_k(\mathcal{R}_k) \xrightarrow{w_{\mathcal{R}}} \mathcal{R}_K\,/p\,\mathcal{R},$$

where $w_{\mathcal{R}}$ is the continuous A-linear map given by

$$w_{\mathcal{R}}((a_{-n})) = \sum_{n\geq 0} p^{-n}\widehat{a}_{-n}^{p^n} \bmod p\,\mathcal{R},$$

with $\widehat{a}_{-n} \in \mathcal{R}$ any lift of $a_{-n} \in \mathcal{R}_k$. For a proof that $w_{\mathcal{R}}$ is well-defined, A-linear, and continuous, see [7, Ch II, §5.2].

The motivation for considering this particular L will become clear in the arguments below. At this point it should be remarked that the topology issues involved are far too cumbersome to review here, but a careful reading of [7] shows that all formal manipulations we will carry out with limits and infinite sums are valid; for a ring like $\mathcal{R}$ which is a finite flat A-algebra, the topology we use on $\mathcal{R}_K$ is it's natural topology as a finite-dimensional K-vector space, the topology we use on $\mathcal{R}$ is the p-adic one, and the topology we use on $\mathcal{R}_k$ is the discrete one.

Observe that since M/FM is killed by p, there is a natural k-linear map $L/pL \to M/FM$. We are now ready to establish some essential properties of the pair (L, M). It should be pointed out that the first of the properties we prove is quite natural to expect; cf. [7, Ch IV, Prop 1.6].

Theorem 1.1. *The natural k-linear map $L/pL \to M/FM$ is an isomorphism and the restriction of V to $L \subseteq M$ is injective.*

Proof. We first need to prove the following sufficient criteria for an element of $CW_k(\mathcal{R}_k)$ to actually lie in M: if $\mathbf{a} \in CW_k(\mathcal{R}_k)$, $w_{\mathcal{R}}(\mathbf{a}) = 0$, and $V\mathbf{a} \in M$, then $\mathbf{a} \in M$ (in this proof, we reserve the boldface font for covectors, and sometimes for elements of M when we wish to emphasize their nature as covectors). In order to prove this, we write $\mathbf{a} = (a_{-n})$ and because M is *by definition* the group of formal k-group scheme homomorphisms from G_k to $\widehat{CW}_k$, we need to verify that

$$(\Delta_{G_k}(a_{-n})) \stackrel{?}{=} (a_{-n}\otimes 1) + (1 \otimes a_{-n}).$$

Since V is additive and $V\mathbf{a} \in M$ by hypothesis, applying V does yield an equality. Hence, it remains to compare the 0th-coordinates on both sides, which is to say that we must check

$$\Delta_{G_k}(a_0) \stackrel{?}{=} \lim_{m\to\infty} S_m(a_{-m}\otimes 1, \ldots, a_0 \otimes 1; 1\otimes a_{-m}, \ldots, 1\otimes a_0)$$

in $\mathcal{R}_k \otimes_k \mathcal{R}_k \simeq (\mathcal{R}\otimes_A \mathcal{R})_k$. Here, S_m is the usual mth-coordinate addition polynomial for p-Witt vectors (and indeed this sequence in the discrete $\mathcal{R}_k \otimes_k \mathcal{R}_k$ in we are taking a limit does eventually becomes constant).

Since $w_{\mathcal{R}}(\mathbf{a}) = 0$, in $\mathcal{R}_K$ we have

$$\sum_{n\geq 0} p^{-n}\widehat{a}_{-n}^{p^n} = py$$

for some $y \in \mathcal{R}$. Replacing $\widehat{a}_0$ by $\widehat{a}_0 - py$, we may assume $y = 0$. That is,

$$\widehat{a}_0 = -\sum_{n\geq 1} p^{-n}\widehat{a}_{-n}^{p^n}.$$

Now G is a lift of G_k as a *group scheme*, so $\Delta_{G_k}(a_0) \in (\mathcal{R}\otimes_A \mathcal{R})_k$ is represented by the element $\Delta_G(\widehat{a}_0) \in \mathcal{R}\otimes_A \mathcal{R}$. Since $\mathcal{R}\otimes_A \mathcal{R}$ is a *p-adic A-ring* (i.e, a flat A-algebra which is separated and complete with respect to the p-adic topology), the addition formulas for $\widehat{CW}_A(\mathcal{R}\otimes_A \mathcal{R})$ permit us to define

$$\mathcal{L}_{-m}(\widehat{\mathbf{a}}) = \lim_{N\to\infty} S_N(\widehat{a}_{-N-m}\otimes 1, \ldots, \widehat{a}_{-m}\otimes 1; 1\otimes \widehat{a}_{-N-m}, \ldots, 1\otimes \widehat{a}_{-m})$$

in $\mathcal{R}\otimes_A \mathcal{R}$, where $\widehat{\mathbf{a}} = (\widehat{a}_{-n}) \in \widehat{CW}_A(\mathcal{R})$. We are given that for all $m \geq 1$,

$$\Delta_G(\widehat{a}_{-m}) \equiv \mathcal{L}_{-m}(\widehat{\mathbf{a}}) \bmod p(\mathcal{R}\otimes_A \mathcal{R}).$$

We need to prove this when $m = 0$.

Combining our expression for $\widehat{a}_0$ in terms of the $\widehat{a}_{-n}$ for $n \geq 1$ with the above congruences for $m \geq 1$, it suffices to show that the element

$$\sum_{n \geq 0} p^{-n} \mathcal{L}_{-n}(\widehat{\mathbf{a}})^{p^n} \in (\mathcal{R} \otimes_A \mathcal{R})_K$$

lies in $p(\mathcal{R} \otimes_A \mathcal{R})$. In other words, we wish to prove

$$w_{\mathcal{R} \otimes_A \mathcal{R}}\left((\mathcal{L}_{-n}(\widehat{\mathbf{a}}) \bmod p(\mathcal{R} \otimes_A \mathcal{R}))\right) \stackrel{?}{=} 0.$$

However, *by definition*

$$(\mathcal{L}_{-n}(\widehat{\mathbf{a}}) \bmod p(\mathcal{R} \otimes_A \mathcal{R})) = (a_{-n} \otimes 1) + (1 \otimes a_{-n}).$$

Since $w_{\mathcal{R} \otimes_A \mathcal{R}}$ is additive, we conclude that

$$w_{\mathcal{R} \otimes_A \mathcal{R}}\left((\mathcal{L}_{-n}(\widehat{\mathbf{a}}) \bmod p(\mathcal{R} \otimes_A \mathcal{R}))\right) = w_{\mathcal{R} \otimes_A \mathcal{R}}(a_{-n} \otimes 1) + w_{\mathcal{R} \otimes_A \mathcal{R}}(1 \otimes a_{-n}).$$

This is equal to $w_{\mathcal{R}}(\mathbf{a}) \otimes 1 + 1 \otimes w_{\mathcal{R}}(\mathbf{a})$ in $(\mathcal{R} \otimes_A \mathcal{R})_K / p(\mathcal{R} \otimes_A \mathcal{R}) \simeq (\mathcal{R}_K / p\,\mathcal{R}) \otimes_A (\mathcal{R}_K / p\,\mathcal{R})$ and $w_{\mathcal{R}}(\mathbf{a}) = 0$, so we are done.

Now that we have established a criteria for membership in M, we can begin the proof of the theorem. First, let's prove that $pL = (FM) \cap L$, so the map $L/pL \to M/FM$ is at least injective. Since one inclusion is obvious, choose $a \in (FM) \cap L$, so $a = Fb$ with $b \in M$. Define

$$\mathbf{b} = (\ldots, b_{-n+1}, \ldots, b_0, b_1) \in CW_k(\mathcal{R}_k),$$

with $b_1 \in \mathcal{R}_k$ to be chosen later and $b = (b_{-n}) = V\mathbf{b}$. Observe that $p\mathbf{b} = FV\mathbf{b} = Fb = a$, so if $w_{\mathcal{R}}(\mathbf{b}) = 0$ then $V\mathbf{b} = b \in M$ implies (by our criteria) that $\mathbf{b}$ lies in M, thus in L, and so $a \in pL$ as desired.

It remains to choose $b_1 \in \mathcal{R}_k$ so that $w_{\mathcal{R}}(\mathbf{b}) = 0$. If $\widehat{b}_{-n} \in \mathcal{R}$ is a lift of b_{-n} (so we *define* $\widehat{a}_{-n} = \widehat{b}^{p}_{-n}$) and $\widehat{b}_1 \in \mathcal{R}$ is a lift of b_1, then $w_{\mathcal{R}}(\mathbf{b})$ is represented by the element of $\mathcal{R}_K$ given by

$$\widehat{b}_1 + \sum_{n \geq 1} p^{-n} \widehat{b}^{p^n}_{-n+1} = \widehat{b}_1 + \frac{1}{p} \sum_{n \geq 0} p^{-n} \widehat{a}^{p^n}_{-n}.$$

The sum

$$\sum_{n \geq 0} p^{-n} \widehat{a}^{p^n}_{-n}$$

is a representative for $w_{\mathcal{R}}(\mathbf{a})$, which vanishes in $\mathcal{R}_K / p\,\mathcal{R}$, so this sum lies in $p\,\mathcal{R}$. Thus, we can choose

$$\widehat{b}_1 = -\frac{1}{p} \sum_{n \geq 0} p^{-n} \widehat{a}^{p^n}_{-n} \in \mathcal{R}$$

and this ensures $w_{\mathcal{R}}(\mathbf{b}) = 0$, as desired.

The surjectivity of $L/pL \hookrightarrow M/FM$ will be proven by a length calculation. In order to compute the relevant lengths, and in order to prove the injectivity of the restricted semilinear map $V : L \to M$, we will first show that the natural map

$$L[p] \oplus \ker V \to M[p]$$

is a surjection. Choose $\mathbf{x} = (x_{-n}) \in M[p]$, so $x^{p}_{-n} = 0$ for all $n \geq 1$ (recall $p = FV$). We will prove that there exists a decomposition (in $CW_k(\mathcal{R}_k)$)

$$\mathbf{x} = \mathbf{y} + (\ldots, 0, \ldots, 0, z)$$

with $y^{p}_{-n} = 0$ for all $n \geq 1$ and $w_{\mathcal{R}}(\mathbf{y}) = 0$. Note that if this holds, then $y_{-n} = x_{-n}$ for all $n \geq 1$, so $V\mathbf{y} = V\mathbf{x} \in M$ and so by our criteria above, $\mathbf{y} \in M$ and so $\mathbf{y} \in L$. Furthermore, since $p\mathbf{y} = VF\mathbf{y} = 0$, $\mathbf{y} \in L[p]$. Since this also forces $(\ldots, 0, \ldots, 0, z) = \mathbf{x} - \mathbf{y} \in M$ as well, the existence of a decomposition as indicated above is sufficient in order to establish the desired surjectivity.

Hence, we want to find $y, z \in \mathcal{R}_k$ such that

$$\mathbf{x} = (\ldots, x_{-n}, \ldots, x_{-1}, y) + (\ldots, 0, \ldots, 0, z)$$

with $w_{\mathcal{R}}(\mathbf{y}) = 0$, where $\mathbf{y}$ denotes the first covector on the right side. Clearly if $y \in \mathcal{R}_k$ exists so that $w_{\mathcal{R}}(\mathbf{y}) = 0$, then equating 0th-coordinates shows the existence of z. In other words, it suffices to check that if $\widehat{x}_{-n} \in \mathcal{R}$ is a lift of x_{-n} for $n \geq 1$, then

$$\sum_{n \geq 1} p^{-n} \widehat{x}_{-n}^{p^n} \in \mathcal{R},$$

where the sum a priori lies in $\mathcal{R}_K$. We can then set y to be the reduction modulo $p\,\mathcal{R}$ of the negative of this sum.

But $x_{-n}^p = 0$ for all $n \geq 1$, so we have for such n that

$$p^{-n} \widehat{x}_{-n}^{p^n} = p^{-n} (\widehat{x}_{-n}^p)^{p^{n-1}} \in p^{p^{n-1}-n}\,\mathcal{R}\,.$$

Combining this with $p^{n-1} - n \geq 0$ for all $n \geq 1$ then completes the proof that $L[p] \oplus \ker V \to M[p]$ is surjective. This surjection yields the length relation $\ell_A(L/pL) \geq \ell_A(M/pM) - \ell_A(M/VM)$, so in order to prove that $L/pL \hookrightarrow M/FM$ is an isomorphism, it is sufficient to check that the sequence

$$0 \to M/VM \xrightarrow{F} M/pM \to M/FM \to 0,$$

which is at least right exact, is in fact exact. Since $p = FV$, this is clearly equivalent to the assertion that the kernel of F lies in the image of V. This is a very special property of M (e.g., it implies that $\alpha_{p/k}$ cannot arise as the closed fiber of an object in $\mathcal{FF}_A$, though this is also clear by [15, §2, Rem 3]).

To verify this exactness, suppose for some $\mathbf{x} \in M \subseteq CW_k(\mathcal{R}_k)$ that $F\mathbf{x} = 0$, so $x_{-n}^p = 0$ for all $n \geq 0$. We want to find some $y \in \mathcal{R}_k$ so that $\mathbf{y} = (\ldots, x_{-n+1}, \ldots, x_0, y)$ lies in M (so then $\mathbf{x} = V\mathbf{y}$ is in the image of V). Thanks to the criteria for membership in M, it is enough to find y so that $w_{\mathcal{R}}(\mathbf{y}) = 0$. If $\widehat{x}_{-n} \in \mathcal{R}$ is a lift of x_{-n}, then as above we see that for $n \geq 1$,

$$p^{-n} \widehat{x}_{-n+1}^{p^n} \in p^{p^{n-1}-n}\,\mathcal{R} \subseteq \mathcal{R}\,.$$

Thus, simply define

$$y = -\sum_{n \geq 1} p^{-n} \widehat{x}_{-n+1}^{p^n} \bmod p\,\mathcal{R}\,.$$

We may now also conclude that

$$\ell_A(L/pL) = \ell_A(M/pM) - \ell_A(M/VM),$$

so the surjection

$$L[p] \oplus \ker V \twoheadrightarrow M[p]$$

is an isomorphism. This clearly implies the injectivity of $V|_L$.

■

Thanks to this theorem, we are motivated to make the definition (following Fontaine):

Definition 1.2. A *finite Honda system over A* is a pair (L, M) where M is a D_k-module with finite A-length and $L \subseteq M$ is an A-submodule such that $V|_L$ is injective and the natural k-linear map

$$L/pL \to M/FM$$

is an isomorphism. These objects form a category SH_A^f in an obvious manner. The full subcategory $SH_A^{f,u}$ of *unipotent finite Honda systems over A* consists of those objects (L, M) for which the action of V on M is nilpotent. The full subcategory $SH_A^{f,c}$ of *connected finite Honda systems* consists of those objects (L, M) for which the action of F on M is nilpotent.

It is because the group schemes μ_2 and $\underline{\mathbf{Z}/2}$ over $\mathbf{Z}_2$ have isomorphic generic fibers that we need a restriction for $p = 2$.

Lemma 1.3. *The category SH_A^f is abelian. For a morphism $\varphi : (L_1, M_1) \to (L_2, M_2)$, $\ker\varphi = (L', M')$, where $M' = \ker(M_1 \to M_2)$ and $L' = L_1 \cap M'$. Also, $\operatorname{coker}\varphi = (L'', M'')$, where $M'' = \operatorname{coker}(M_1 \to M_2)$ and L'' is the image of the composite map of A-modules*

$$L_2 \to M_2 \to M''.$$

This category is also artinian.

The same statements are true for $SH_A^{f,u}$ and $SH_A^{f,c}$. The forgetful functors $SH_A^{f,c}, SH_A^{f,u} \to SH_A^f$ are exact.

Proof. One way to prove this is to observe that by [9, Prop 8.10], we have an equivalence of categories between SH_A^f and the category denoted $\underline{MF}^{f,2}_{A,\sigma,p,\mathrm{tor}}$ (in [9]), with explicit functors in both directions. Now simply examine the proof in [9, Prop 1.8] that this latter category is abelian (and artinian). Similar arguments apply in the unipotent and connected settings.

A direct proof could also be given by translating the arguments in [9, §1] through the above equivalence of categories, but this is unnecessary and so we won't bother with it. ∎

The above lemma can also be deduced from the main results below. This will be explained after Corollary 1.6 and will be useful in the proof of our generalization to cases with $e > 1$.

Theorem 1.1 allows us to define the functor

$$LM = LM_A : \mathfrak{FF}_A \to SH_A^f$$

via $LM(G) = (L_A(G), \mathcal{M}(G_k))$. This is an additive contravariant functor. Since unipotence and connectedness can be detected on the closed fiber, we can 'restrict' LM to get an additive contravariant functor

$$LM^u = LM_A^u : \mathfrak{FF}_A^u \to SH_A^{f,u},$$

and $LM^c = LM_A^c$ is defined similarly. The main theorem in the present setting ($e = 1$) is

Theorem 1.4. *If $p > 2$, then LM is fully faithful and essentially surjective. The same is true for LM^u and LM^c for all p.*

In other words, LM (resp. LM^u, LM^c) is an equivalence of categories for odd p (resp. for all p) in the usual weak sense. That is, we don't yet claim to construct an explicit quasi-inverse functor, but for all practical purposes we can regard LM (resp. LM^u) as an equivalence of categories (this is also the sense in which Fontaine uses this notion in [7, Ch IV] and [8]). With further work, one can construct explicit quasi-inverses. We'll say more about this later.

Before proving Theorem 1.4, we record two corollaries as noted in [7]. These are special cases of Raynaud's result [17, Cor 3.3.6] (together with an analogous argument when $e = 1 = p - 1$), and Raynaud's proof of the first corollary below is by somewhat different methods.

Corollary 1.5. *If $p > 2$, then $\mathfrak{FF}_A$ is stable under the formation of scheme-theoretic kernels and is an abelian category. A morphism is a kernel if and only if it is a closed immersion and is a cokernel if and only if it is faithfully flat. The formation of the cokernel of a closed immersion is as usual.*

For all p, the same statements are true for $\mathfrak{FF}_A^u$ and $\mathfrak{FF}_A^c$ (the full subcategory of connected objects). Moreover, the forgetful functors from $\mathfrak{FF}_A^u$ and $\mathfrak{FF}_A^c$ to $\mathfrak{FF}_A$ are exact for odd p.

Proof. We give the argument for odd p and $\mathfrak{FF}_A$. The arguments for $\mathfrak{FF}_A^u$ and $\mathfrak{FF}_A^c$ are done similarly.

By Theorem 1.1 and Lemma 1.3, $\mathfrak{FF}_A$ is an abelian category. If $f : G \to G'$ is a morphism and $\mathcal{K}$ denotes the (abstract) kernel object in the abelian category $\mathfrak{FF}_A$, then a consideration of Dieudonne modules on the closed fiber and the *definition* of LM shows that the natural map $\mathcal{K}_k \to \ker(f_k)$ is an isomorphism, with $\ker(f_k)$ denoting the scheme-theoretic kernel of f_k. Thus, the map $\mathcal{K} \to G$ is a closed immersion on the closed fiber and so is a closed immersion. This factors through the scheme-theoretic kernel $\ker f \hookrightarrow G$, so we get a closed immersion $\mathcal{K} \hookrightarrow \ker f$ of finite A-group schemes which is an isomorphism on the closed fibers. Since $\mathcal{K}$ is also *flat* over A, a standard argument shows this map is an isomorphism. The rest is now easy. ∎

Corollary 1.6. *If $p > 2$, then the functor which associates to each G in $\mathcal{FF}_A$ its generic fiber K-group scheme G_K is a fully faithful functor. For arbitrary p, the same statement is true for the categories $\mathcal{FF}_A^u$ and $\mathcal{FF}_A^c$.*

Proof. Faithfulness is clear by flatness. Now suppose $p > 2$ and we're given a morphism $f : G_K \to H_K$ of K-group schemes. We want it to arise from a morphism $f : G \to H$ in $\mathcal{FF}_A$. Let $\mathcal{K}_K = \ker f_K$ and let $\mathcal{K}$ denote the scheme-theoretic closure of this in G. Thus, $\mathcal{K}$ is a finite flat closed subgroupscheme of G and f_K factors through $(G/\mathcal{K})_K \simeq G_K/\mathcal{K}_K$. We see now that we may replace G by $G/\mathcal{K}$ and so without loss of generality f_K is a closed immersion. By Cartier duality, we may assume that the dual of f_K is a closed immersion, so a consideration of orders shows that f_K is an isomorphism.

By Corollary 1.5, a morphism in $\mathcal{FF}_A$ is an isomorphism if and only if the induced map on generic fibers is an isomorphism. Now use Raynaud's result on the existence of a 'maximal' prolongation of G_K over A to obtain the desired f [17, Prop 2.2.2].

The same arguments apply to $\mathcal{FF}_A^u$ and $\mathcal{FF}_A^c$ for any p. ∎

As we noted above, Raynaud independently deduces Corollary 1.5 and from this one can readily obtain both Corollary 1.6 and (more importantly) Lemma 1.3 by formal arguments based on Theorem 1.4 (see the proof of Theorem 4.3 for how this is carried out in a more general setting). In order for this not to be circular, note that the proof of Theorem 1.4 below does *not* use Lemma 1.3. This clarifies the comment following Lemma 1.3 and will also be the means by which we deduce the analogue of Lemma 1.3 in the general case $e \leq p-1$, as the analogue of Corollary 1.5 for $e \leq p-1$ is proven independently by Raynaud. One could perhaps avoid using Raynaud's results in the proof of the analogue of Lemma 1.3 for $e \leq p-1$, instead using just linear algebra manipulations, but we'll need Raynaud's explicit formulas anyway in the proof of Theorem 1.4 and its generalization for $e \leq p-1$.

We now are ready to prove Theorem 1.4.

Proof. (of Theorem 1.4) The proof consists of five steps. The formulation of these steps is due to Fontaine [8]; here, we supply some extra technical details. For now, if $p = 2$ we shall require G to be *unipotent*. We will come back to the connected case at the end.

Step 1. Let $\mathcal{S}$ be a finite flat A-algebra. Then we claim that the reduction map

$$G(\mathcal{S}) \to G(\mathcal{S}_k) = G_k(\mathcal{S}_k)$$

is injective (this is false for $G = \mu_2$, $\mathcal{S} = \mathbf{Z}_2$).

Before checking this, note that this not only permits us to identify $G(\mathcal{S})$ with a subgroup of $G_k(\mathcal{S}_k)$ in a manner which is functorial in both G and $\mathcal{S}$, but it also implies (by Yoneda's Lemma) that the functor $G \rightsquigarrow G_k$ from $\mathcal{FF}_A$ to the category of finite commutative k-group schemes is a faithful functor. Since $LM(G)$ encodes the Dieudonne module of G_k, it follows that LM is at least faithful for odd p and LM^u is faithful for all p.

In order to verify Step 1, we can base extend by the completion of the strict Henselization of A, so we may suppose that k is algebraically closed and A is strictly Henselian. Also, if

$$0 \to G' \to G \to G'' \to 0$$

is a short exact sequence in $\mathcal{FF}_A$ and the assertion is true for G' and G'', then it is trivially true for G. Hence, the method of scheme-theoretic closure reduces us to the case in which the generic fiber G_K is a simple finite commutative group scheme over K with p-power order.

By [17, Prop 3.2.1, Prop 3.3.2], G is an $\mathbf{F}$-vector scheme with $\mathbf{F}$ a finite field of order equal to that of G. Choosing r so that $\mathbf{F}$ has size p^r, [17, Cor 1.5.1, Prop 3.3.2(1), Prop 3.3.2(3)] implies that as an A-scheme,

$$G \simeq \mathrm{Spec}(A[X_1, \dots, X_r]/(X_i^p - \delta_i X_{i+1})),$$

where $\delta_i \in A$ satisfies $\mathrm{ord}_A(\delta_i) \le p-1$ for all i and some $\mathrm{ord}_A(\delta_{i_0}) < p-1$. Here we adopt the convention that the set of indices are a principal homogenous space for $\mathbf{Z}/r$, and the final condition with i_0 is where we have used the unipotence hypothesis in case $e = 1 = p-1$ (see the proof of [17, Prop 3.3.2(3)]).

Choose $g \in G(\mathcal{S})$ vanishing in $G(\mathcal{S}_k)$, so g corresponds to a choice of $x_1, \dots, x_r \in p\mathcal{S}$ satisfying $x_{i+1}^p = \delta_i x_i$ (and again we view the indices as a principal homogenous space for $\mathbf{Z}/r$). Iterating this condition, we obtain

$$x_i^{p^r} = \delta x_i,$$

with $\delta = \prod \delta_i \in A$ satisfying $\mathrm{ord}_A(\delta) < r(p-1)$. Writing $x_i = py_i$ for $y_i \in \mathcal{S}$ and using $p^r - r(p-1) \ge 1$, A-flatness of $\mathcal{S}$ allows us to cancel p's to get $y_i \in py_i\mathcal{S}$ for all i. Thus,

$$y_i \in \bigcap_{m \ge 1} p^m \mathcal{S} = 0,$$

so $g(I_G) = 0$. That is, $G(\mathcal{S}) \to G(\mathcal{S}_k)$ is injective.

Step 2. For each $g \in G(\mathcal{S})$, with $\mathcal{S}$ a finite flat A-algebra, we get maps $g_K : \mathcal{R}_K \to \mathcal{S}_K$ and $g_k : \mathcal{R}_k \to \mathcal{S}_k$, the latter giving rise to

$$CW_k(g_k) : CW_k(\mathcal{R}_k) \to CW_k(\mathcal{S}_k).$$

The commutative diagram of A-modules

$$\begin{array}{ccc} CW_k(\mathcal{R}_k) & \xrightarrow{CW_k(g_k)} & CW_k(\mathcal{S}_k) \\ {\scriptstyle w_{\mathcal{R}}}\downarrow & & \downarrow{\scriptstyle w_{\mathcal{S}}} \\ \mathcal{R}_K/p\mathcal{R} & \xrightarrow{g_K} & \mathcal{S}_K/p\mathcal{S} \end{array}$$

(with $w_{\mathcal{S}}$ defined by the same formula as $w_{\mathcal{R}}$) shows (via Step 1) that we can identify $G(\mathcal{S})$ with a subgroup of

$$\underline{G}(\mathcal{S}) \stackrel{\mathrm{def}}{=} \{\gamma \in G_k(\mathcal{S}_k) \mid CW_k(\gamma)(L) \subseteq \ker w_{\mathcal{S}}\}$$

in a manner which is functorial in both G and $\mathcal{S}$. Clearly $\underline{G}$ is a functor from finite flat A-algebras to $\mathbf{Ab}$ in an obvious manner. Recall that $G_k(\mathcal{S}_k) \simeq \mathrm{Hom}_{D_k}(\mathcal{M}(G_k), \widehat{CW}_k(\mathcal{S}_k))$ [7, Ch III, §1.5, Prop 1.2]

Though G is a priori just a subgroup functor of the functor $\underline{G}$ on finite flat A-algebras, we'll show below that $G(\mathcal{S}) = \underline{G}(\mathcal{S})$ and so the natural transformation $G \to \underline{G}$ is an isomorphism of group functors.

Step 3. If $1 < p-1$ and $f : \Gamma \to \Gamma'$ is an isogeny of p-divisible groups over A with G isomorphic to the kernel, then we claim $G \simeq \underline{G}$ in Step 2. The same holds for all p if Γ, Γ', and G are all unipotent (i.e., have connected duals).

In order to show that $G(\mathcal{S}) \subseteq \underline{G}(\mathcal{S})$ fills up the entire group, we need to use Fontaine's classification of p-divisible groups over A. More precisely, by [7, Ch IV, §1.10, Rem 2,3] (which covers both the case $1 < p-1$ and the unipotent case when $1 = p-1$), for any finite flat A-algebra $\mathcal{S}$, we have functorially as groups that $\Gamma_{\mathrm{tor}}(\mathcal{S}) \stackrel{\mathrm{def}}{=} \varinjlim \Gamma[p^n](\mathcal{S})$ is identified via reduction with

$$\{\gamma \in \Gamma_k(\mathcal{S}_k) \,|\, L_A(\Gamma) \hookrightarrow \mathcal{M}(\Gamma_k) \subseteq \widehat{CW}_k(\mathcal{O}(\Gamma_k)) \xrightarrow{\widehat{CW}_k(\gamma)} \widehat{CW}_k(\mathcal{S}_k) \xrightarrow{w_{\mathcal{S}}} \mathcal{S}_K/p\mathcal{S} \text{ is } 0\}$$

(recall that $\widehat{CW}_k(\mathcal{S}_k) = CW_k(\mathcal{S}_k)$ since $\mathcal{S}_k$ is a finite k-algebra), and likewise for $\Gamma'_{\mathrm{tor}}(\mathcal{S})$. The A-submodule of 'logarithms' $L_A(\Gamma) \subseteq \mathcal{M}(\Gamma_k)$ has a somewhat complicated definition as an A-module mapping to $\mathcal{M}(\Gamma_k)$ [7, p. 167], and [7, Ch IV, Prop 1.1] shows that $L_A(\Gamma)$ is finite and free as an A-module, with $L_A(\Gamma) \to \mathcal{M}(\Gamma_k)$ injective (here we use that $\mathcal{M}(\Gamma_k)$ is a finite free A-module, as Γ_k is a p-divisible group [7, Ch III, §6.1, Rem 3]). In particular, this functorial description of torsion implies that the natural map of groups $\Gamma'_{\mathrm{tor}}(\mathcal{S}) \to \Gamma'_k(\mathcal{S}_k)$ is *injective*.

Now choose $g \in G_k(\mathcal{S}_k)$. Of course $G(\mathcal{S}) \hookrightarrow \Gamma_{\mathrm{tor}}(\mathcal{S})$. Assume $CW_k(g)(L) \subseteq \ker w_{\mathcal{S}}$ (i.e., $g \in \underline{G}(\mathcal{S})$). We need to show $g \in G(\mathcal{S})$. We first make the crucial claim that $\mathcal{M}(\Gamma_k) \twoheadrightarrow \mathcal{M}(G_k)$ takes $L_A(\Gamma)$ over into $L_A(G)$. In fact, this is the reason for defining $L_A(G)$ as we did in the first place. To prove this claim, simply observe that the given closed immersion of formal A-group schemes $i : G \hookrightarrow \Gamma$ gives an element of $\Gamma(\mathcal{R})$ which lies in

$\Gamma_{\rm tor}(\mathcal{R})$ (G is annihilated by its order!), so by the description of $\Gamma_{\rm tor}(\mathcal{R})$ above, we get *precisely* the desired condition.

The functoriality of $\widehat{CW}_k$ now implies that $i_{\mathcal{S}_k}(g) \in \Gamma_k(\mathcal{S}_k)$ satisfies the conditions describing $\Gamma_{\rm tor}(\mathcal{S})$. Thus, there is some $\gamma \in \Gamma_{\rm tor}(\mathcal{S})$ such that $\gamma_k = i_{\mathcal{S}_k}(g)$, so $(f_{\mathcal{S}}(\gamma))_k = f_{\mathcal{S}_k}(i_{\mathcal{S}_k}(g)) = 0$ (recall $G = \ker f$). But $f_{\mathcal{S}}(\gamma)$ lies in ${\Gamma'}_{\rm tor}(\mathcal{S})$, which *injects* into ${\Gamma'}_k(\mathcal{S}_k)$ via reduction. Hence, $f_{\mathcal{S}}(\gamma) = 0$.

Exactness of the sequence

$$0 \to G(\mathcal{S}) \to \Gamma(\mathcal{S}) \to \Gamma'(\mathcal{S})$$

implies that $\gamma = i_{\mathcal{S}}(g_0)$ for some $g_0 \in G(\mathcal{S})$, so $i_{\mathcal{S}_k}((g_0)_k) = \gamma_k = i_{\mathcal{S}_k}(g)$. That is, $g = (g_0)_k$ is in $G(\mathcal{S})$, viewed inside of $G_k(\mathcal{S}_k)$. This shows that $G(\mathcal{S}) = \underline{G}(\mathcal{S})$.

We note in passing that if Γ and Γ' are unipotent, then G is automatically unipotent.

Step 4. Let (L, M) be an object in SH_A^f with $p \neq 2$. We claim there is an object $G_{(L,M)}$ in $\mathcal{FF}_A$ which is the kernel of an isogeny of p-divisible groups over A and for which $(L, M) \simeq LM(G_{(L,M)})$; in other words, LM is essentially surjective. If p is arbitrary and (L, M) is an object in $SH_A^{f,u}$, we make an analogous claim with $G_{(L,M)}$ in $\mathcal{FF}_A^u$ the kernel of an isogeny of unipotent p-divisible groups. Beware that we don't (yet) claim to construct $G_{(L,M)}$ in a manner which is functorial in (L, M).

This step is the heart of the proof and is the most important detail omitted in [8]. First, we will construct a short exact sequence of D_k-modules

$$0 \to M_2 \to M_1 \to M \to 0$$

with M_1 and M_2 finite free A-modules (so by [7, Ch III, §6.1, Rem 3], $M_i \simeq \mathcal{M}(\overline{\Gamma}_i)$ for $\overline{\Gamma}_i$ a p-divisible group over k). In addition, we will choose M_1 and M_2 with topologically nilpotent V action (i.e., with $\overline{\Gamma}_i$ unipotent) when M has nilpotent V action (i.e., when M is the Dieudonne module of a unipotent finite commutative k-group scheme). Obviously we only need to construct $M_1 \twoheadrightarrow M$ and then can set M_2 to be the kernel. We exploit Cartier duality in order to decompose M into a product of étale-connected, connected-étale, and connected-connected components, so it suffices to consider these three cases separately (and just the first and third cases are needed in the unipotent setting). See [7, Ch III, §1.7] for the definitions of the notions of *étale* and *connected* in the setting of suitable Dieudonne modules; one can also see from the arguments in [7, Ch III] that these notions are compatible with the functor between finite flat commutative k-group schemes of p-power order and their Dieudonne modules. By [7, Ch III, §5.3, Cor 2], one can also explicitly translate Cartier duality of finite flat commutative k-group schemes with p-power order into the language of their Dieudonne modules.

If M is étale, then let M_1 be a free A-module of finite rank, together with a surjection of M_1 onto M inducing an isomorphism modulo p. Since $F : M \to M$ is a Frobenius-semilinear *automorphism*, we can lift it to a Frobenius-semilinear automorphism F_1 of M_1. Defining $V_1 = pF_1^{-1}$ gives an M_1 of the desired sort (with V_1 topologically nilpotent). If M has an étale dual, we can proceed similarly using V in place of F. There remains the connected-connected case, so $V^n = F^n = 0$ for some suitably large n. Choosing A-module generators of M allows us to take for M_1 a product of finitely many copies of $A[F, V]/I$, with I the left ideal generated by $F^n - V^n$. This M is a finite free A-module having topologically nilpotent F and V actions.

Next, we will construct A-submodules $\mathcal{L}_i \subseteq M_i$ such that the natural k-linear maps $\mathcal{L}_i/p\mathcal{L}_i \to M_i/FM_i$ are isomorphisms, $M_2 \hookrightarrow M_1$ takes $\mathcal{L}_2$ over into $\mathcal{L}_1$ (we do *not* claim $\mathcal{L}_2 = M_2 \cap \mathcal{L}_1$), and the image of $\mathcal{L}_1$ under $M_1 \twoheadrightarrow M$ is precisely L. It is this construction that will use the injectivity of $V|_L$. In particular, we'll have a map

$$\psi : (\mathcal{L}_2, M_2) \to (\mathcal{L}_1, M_1)$$

in the category H_A^d when $p \neq 2$ [7, Ch IV, §1.10, Rem 1] and in the category $H_A^{d,u}$ in the unipotent case [7, loc. cit.]. Recall that H_A^d is the category of pairs (L, M) with L an A-submodule of a D_k-module M such that M is finite free with rank d as an A-module and the natural k-linear map $L/pL \to M/FM$ is an isomorphism (the definition of morphism is obvious, as are the definitions of the corresponding 'unipotent' and 'connected' full subcategories $H_A^{d,u}$, $H_A^{d,c}$).

Suppose for the moment that we have carried out the construction of $\mathcal{L}_1$ and $\mathcal{L}_2$. Let's see how to use this to construct $G_{(L,M)}$ of the desired sort. When $1 < p-1$, we can let $\Gamma_{i/A}$ be the 'unique' p-divisible group over A (up to isomorphism) such that in H_A^d,

$$(\mathcal{L}_i, M_i) \simeq LM_A(\Gamma_i).$$

When $1 \leq p-1$ and we are in the unipotent setting, we can uniquely choose such Γ_i which are unipotent. Here we are invoking the main classification theorem [7, Ch IV, §1.2, Thm 1], but see [7, Ch IV, §1.2, §1.10] for the definition of LM_A as just used; the discussion in Step 3 shows that, in a reasonable sense, this is compatible with the notion of LM_A on $\mathfrak{FF}_A$ (and similarly in the unipotent case); also see Lemma 4.12 below. Thus, there is a unique morphism $f : \Gamma_1 \to \Gamma_2$ of p-divisible groups such that

$$LM_A(f) : (\mathcal{L}_2, M_2) \to (\mathcal{L}_1, M_1)$$

is the map ψ we mentioned above. On the closed fibers, which satisfy $(\Gamma_i)_k \simeq \overline{\Gamma}_i$, the induced morphism f_k corresponds to the map

$$M_2 = \mathcal{M}(\overline{\Gamma}_2) \to \mathcal{M}(\overline{\Gamma}_1) = M_1$$

which is our original inclusion. As this is injective with a cokernel M that has finite A-length, the morphism f_k is an isogeny. Therefore, f is itself an isogeny and so is 'formally faithfully flat' over A (i.e., 'faithfully flat' with respect to the functor $\widehat{\otimes}_A$ on 'profinite' A-modules in the sense of [7, Ch I, §3]).

Hence, $G \overset{\text{def}}{=} \ker f$ is an object in $\mathfrak{FF}_A$ (in particular, it is *flat* over A) and $M \simeq \mathcal{M}(G_k)$. When Γ_1 and Γ_2 are unipotent, so is G. Under the D_k-module isomorphism $M \simeq \mathcal{M}(G_k)$, we claim that $L_A(G)$ corresponds to L. Since $\mathcal{L}_1 \to L$ is surjective, certainly L lies inside of $L_A(G)$ (see the discussion in Step 3). But the commutative diagram of k-vector spaces

$$\begin{array}{ccc} L/pL & \longrightarrow & L_A(G)/pL_A(G) \\ \simeq \big\downarrow & & \big\downarrow \simeq \\ M/FM & \xrightarrow{\sim} & \mathcal{M}(G_k)/F\mathcal{M}(G_k) \end{array}$$

shows that the top row is an isomorphism, whence $L_A(G)$ does correspond precisely to L, so $(L, M) \simeq LM(G)$. Let $G_{(L,M)} = G$.

Now let's see how to construct $\mathcal{L}_1$ and $\mathcal{L}_2$ as described above. The first thing we need to do is to check that an abstract object (L, M) in SH_A^f enjoys some properties noted earlier (in the proof of Theorem 1.1) for the essential image of LM. More precisely, we claim that the kernel of F lies in the image of V and

$$L[p] \oplus \ker V = M[p].$$

In order to establish this decomposition of $M[p]$, note that there is certainly an injection from the left side to the right side ($V|_L$ is injective!) and so a comparsion of the length of both sides (using $L/pL \simeq M/FM$) yields the inequality

$$\ell_A(M/FM) + \ell_A(M/VM) \leq \ell_A(M/pM).$$

In order to establish the reverse inequality, just note that the sequence

$$0 \to M/VM \xrightarrow{F} M/pM \to M/FM \to 0,$$

is always right exact. Hence, we not only get the decomposition of $M[p]$, but the equality of lengths shows that the right exact sequence above is in fact exact. However, this exactness is equivalent to the other claim the kernel of F lies in the image of V.

With these initial observations settled, let $\overline{e}_1, \ldots, \overline{e}_r \in M_1/FM_1$ be a basis for the image of M_2/FM_2, with representatives $e_i \in M_2 \subseteq M_1$. Let $\overline{e}_{r+1}, \ldots, \overline{e}_n$ extend this to a full basis of M_1/FM_1, so their images in M/FM give a basis of $M/FM \xleftarrow{\sim} L/pL$. Note that we are implicitly using the obvious fact that the sequence

$$M_2/FM_2 \to M_1/FM_1 \to M/FM \to 0$$

is exact. We may (and do) choose representatives $e_{r+1}, \ldots, e_n \in M_1$ so that their images in M lie in L and constitute a minimal A-basis of L. Define $\mathcal{L}_1 = \sum Ae_i$. Clearly $\mathcal{L}_1/p\mathcal{L}_1 \simeq M_1/FM_1$ and

$$\mathcal{L}_1 \hookrightarrow M_1 \twoheadrightarrow M$$

has image precisely L.

We now seek to find $\epsilon_{r+1}, \ldots, \epsilon_m \in M_2 \cap FM_1$ so that $\overline{e}_1, \ldots, \overline{e}_r, \overline{\epsilon}_{r+1}, \ldots, \overline{\epsilon}_m$ is a basis of M_2/FM_2 and all ϵ_j lie in $\mathcal{L}_1$ (note that $\overline{e}_1, \ldots, \overline{e}_r$ now denote elements of M_2/FM_2 and not M_1/FM_1, but this won't cause any confusion). Defining

$$\mathcal{L}_2 = Ae_1 + \cdots + Ae_r + A\epsilon_{r+1} + \ldots A\epsilon_m$$

will complete our construction. More generally, choose any $\epsilon \in M_2 \cap FM_1$. It suffices to shows that its image in M_2/FM_2 can be represented by an element of M_2 which lies in $\mathcal{L}_1$.

Well, $\epsilon = Fy$ with the projection $\mathcal{P} : M_1 \twoheadrightarrow M$ killing ϵ, so $\mathcal{P}(y) \in \ker F_M$. We claim, however, that $V_M(L[p]) = \ker F_M$. Indeed, '$\subseteq$' is clear and if $Fx = 0$, then x lies in the image of V, say $x = Vz$ for $z \in M$. But $pz = FVz = Fx = 0$, so $z \in M[p] = L[p] \oplus \ker V$. Thus, we can take $z \in L[p]$. Consequently,

$$\mathcal{P}(y) = V\left(\sum_{j=r+1}^{n} a_j\, \mathcal{P}(e_j)\right),$$

so

$$y \equiv V\left(\sum_{j=r+1}^{n} a_j e_j\right) \bmod M_2.$$

Applying F, we obtain

$$\epsilon = Fy \equiv \sum_{j=r+1}^{n} a_j p e_j \bmod FM_2,$$

which then gives what we sought to prove.

Step 5. We will now show that $G(\mathcal{S}) = \underline{G}(\mathcal{S})$ for all finite flat A-algebras $\mathcal{S}$. Note that the formula for $\underline{G}(\mathcal{S})$ and some compatibility checks then will imply that LM is fully faithful for odd p and LM^u is fully faithful for all p, thereby completing the proof of Theorem 1.4.

For $p \neq 2$ and $(L, M) = LM(G)$ (resp. for arbitrary p and $(L, M) = LM^u(G)$), choose $G_{(L,M)}$ as in Step 4 so that $LM(G_{(L,M)}) \simeq LM(G)$ (resp. so that $LM^u(G_{(L,M)}) \simeq LM^u(G)$). By Step 3, $\underline{G} \simeq G_{(L,M)}$ as functors on finite flat A-algebras, so $G \hookrightarrow G_{(L,M)}$ as group functors. But the induced map on closed fibers corresponds to the isomorphism of Dieudonne modules $\mathcal{M}(\left(G_{(L,M)}\right)_k) \simeq \mathcal{M}(G_k)$, so the map on closed fibers is an isomorphism. Hence, by flatness over A, the map of A-group schemes $G \to G_{(L,M)}$ is an isomorphism also. From this it follows that $G(\mathcal{S}) = \underline{G}(\mathcal{S})$ and we are done with the case of odd p and unipotent G for $p = 2$.

Step 6. The case $p = 2$ and G connected.
We saw above that for any odd p and any G in $\mathcal{FF}_A$, or for $p = 2$ and unipotent G, there is an isomorphism $G \simeq G_{(L_A(G), \mathcal{M}(G_k))}$, so G arises as the kernel of an isogeny of p-divisible groups over A. Now suppose $p = 2$ and G is connected. The dual $\widehat{G}$ is unipotent, so is the kernel of an isogeny of p-divisible groups over A. The dual isogeny has kernel isomorphic to $\widehat{\widehat{G}} \simeq G$, so there is a short exact sequence of formal A-group schemes

$$0 \to G \to \Gamma_1 \to \Gamma_2 \to 0.$$

Moreover, G lands inside of the connected component of Γ_1, so we can easily suppose the Γ_i are connected.

Now we invoke Fontaine's classification of p-divisible groups in the connected case over A for $p = 2$. The definition of the functor $\underline{G}$ is slightly different in this case. Since G is connected, $\mathcal{M}(G_k)$ has a nilpotent F-action, so $\mathcal{M}(G_k) \hookrightarrow CW_k(\mathcal{R}_k)$ lies in the 'connected factor' $CW_k^c(\mathcal{R}_k) = CW_k(\mathfrak{r}_{\mathcal{R}_k})$, where $\mathfrak{r}_{\mathcal{R}_k}$ denotes the nilpotent maximal ideal given by augmentation. Since every element of $\mathfrak{r}_{\mathcal{R}_k}$ lifts to an element of the augmentation ideal $\mathfrak{r}_{\mathcal{R}}$ of $\mathcal{R}$, and $w_{\mathcal{R}}$ is well-defined, we can define a variant continuous group map

$$w_{\mathcal{R}}^{\varepsilon} : CW_k(\mathfrak{r}_{\mathcal{R}_k}) \to \mathcal{R}_K\,/p\mathfrak{r}_{\mathcal{R}}$$

using liftings to the augmentation ideal in the formula for $w_{\mathcal{R}}$.

Observe that the composite of $w_{\mathcal{R}}^{\varepsilon}$ with projection $\mathcal{R}_K\,/p\mathfrak{r}_{\mathcal{R}} \to \mathcal{R}_K\,/p\,\mathcal{R}$ is exactly $w_{\mathcal{R}}$ and the two maps have the *same* kernel (since $\mathfrak{r}_{\mathcal{R}}$ is an A-module direct summand of $\mathcal{R}$)! We now interpret $L_A(G)$ as the kernel of $w_{\mathcal{R}}^{\varepsilon}$, since it is this map which will have a more useful analogue in the setting of connected p-divisible groups for $p = 2$. It follows from [7, Ch IV, Prop 1.4′] (and the definitions preceding this Proposition) that an analogue of [7, Ch IV, §1.10, Rem 2] is true. More precisely, suppose $p = 2$, Γ is a connected p-divisible group over A, and $\mathcal{S}$ is a p-adic A-ring with $\mathfrak{r}_{\mathcal{S}}$ the ideal of topologically nilpotent elements. There is a functorial identification of the group $\Gamma_{\mathrm{tor}}(\mathcal{S})$ with the group of all D_k-linear maps

$$\gamma : \mathcal{M}(\Gamma_k) \to CW_k(\mathfrak{r}_{\mathcal{S}}/p\mathfrak{r}_{\mathcal{S}})$$

for which the composite map

$$L_A(\Gamma) \hookrightarrow \mathcal{M}(\Gamma_k) \xrightarrow{\gamma} CW_k(\mathfrak{r}_{\mathcal{S}}/p\mathfrak{r}_{\mathcal{S}}) \xrightarrow{w_{\mathcal{S}}^{c}} \mathcal{S}_K/p\mathfrak{r}_{\mathcal{S}}$$

is zero. Here, $w_{\mathcal{S}}^{c}$ is a 'connected' variant on $w_{\mathcal{S}}$ defined with the same formula, but using liftings to the ideal $\mathfrak{r}_{\mathcal{S}}$; cf. [7, pp. 181-2] (where slightly different notation is used).

We define the functor $\underline{G}$ on p-adic A-rings $\mathcal{S}$ to be given by the group of D_k*-linear* maps

$$\underline{G}(\mathcal{S}) = \{\gamma : \mathcal{M}(G_k) \to CW_k(\mathfrak{r}_{\mathcal{S}}/p\mathfrak{r}_{\mathcal{S}}) \,|\, w_{\mathcal{S}}^{c} \circ \gamma(L_A(G)) = 0\}.$$

Pick any exact sequence $0 \to G \to \Gamma_1 \to \Gamma_2 \to 0$ with Γ_i connected. The induced exact sequence of D_k-modules

$$0 \to \mathcal{M}((\Gamma_2)_k) \to \mathcal{M}((\Gamma_1)_k) \to \mathcal{M}(G_k)$$

induces a map $L_A(\Gamma_1) \to L_A(G)$ for the same reasons as used earlier. Also, the exactness of

$$0 \to G(\mathcal{S}) \to (\Gamma_1)_{\mathrm{tor}}(\mathcal{S}) \to (\Gamma_2)_{\mathrm{tor}}(\mathcal{S})$$

and the above functorial description of torsion in a connected p-divisible group for $p = 2$ gives rise to an injective map

$$j_{G,\mathcal{S}} : G(\mathcal{S}) \to \underline{G}(\mathcal{S})$$

which is functorial in $\mathcal{S}$ and is independent of the choice of 'resolution' of G by connected p-divisible groups; from this, functoriality of $j_{G,\mathcal{S}}$ in G is clear also.

Now we show that the inclusion $G(\mathcal{S}) \to \underline{G}(\mathcal{S})$ is also surjective. In the earlier discussion, we used injectivity of 'passage to closed fiber' on 'points', which is not true anymore (again, recall μ_2 over $\mathbf{Z}_2$). But an alternate argument based on the modified definition of $\underline{G}$ will work, as we now explain. Choose $g \in \underline{G}(\mathcal{S})$, so composing with $\pi : \mathcal{M}((\Gamma_1)_k) \twoheadrightarrow \mathcal{M}(G_k)$ gives an element $\gamma = g \circ \pi \in (\Gamma_1)_{\mathrm{tor}}(\mathcal{S})$. If γ vanishes in $(\Gamma_2)_{\mathrm{tor}}(\mathcal{S})$, then it comes from an element of $G(\mathcal{S})$ which is easily seen to map to g under $j_{G,\mathcal{S}}$. Since the composite map

$$\mathcal{M}((\Gamma_2)_k) \to \mathcal{M}((\Gamma_1)_k) \to \mathcal{M}(G_k) \xrightarrow{g} CW_k(\mathfrak{r}_{\mathcal{S}}/p\mathfrak{r}_{\mathcal{S}})$$

is certainly zero, we get the desired vanishing.

The isomorphism of functors $G \simeq \underline{G}$ on p-adic A-rings, together with naturality in the connected G, yields full faithfulness of LM^c for $p = 2$. Essential surjectivity is proven by exactly the same argument as we used in Step 4 above.

■

For its independent interest, we now record a corollary mentioned above:

Corollary 1.7. *For $p > 2$, any G in $\mathcal{FF}_A$ arises as the kernel of an isogeny of p-divisible groups over A. The same statement is true with unipotent and connected group objects for all p.*

Next, note that for odd p and any G in $\mathcal{FF}_A$ (resp. for arbitrary p and G in $\mathcal{FF}_A^u$), both G and $\underline{G}$ make sense as functors on p-adic A-rings and as such there is a natural map $G \to \underline{G}$.

Corollary 1.8. *$G(\mathcal{S}) \simeq \underline{G}(\mathcal{S})$ for all p-adic A-rings $\mathcal{S}$.*

Proof. Note that $\underline{G}(\mathcal{S})$ makes sense, because $w_{\mathcal{S}}$ makes sense, using the same formula as when $\mathcal{S}$ is finite flat over A; [7, Ch II, §5.1,§5.2] has a discussion of this. For odd p, let $\Gamma \to \Gamma'$ be an isogeny of p-divisible groups over A such that G is the kernel. In the unipotent setting with arbitrary p, choose such p-divisible groups which are unipotent (the connected case for $p = 2$ was settled above, so we ignore this case now). The map $G(\mathcal{S}) \to \Gamma(\mathcal{S})$ is injective, with image inside of $\Gamma_{\mathrm{tor}}(\mathcal{S})$, and by [7, Ch IV, §1.10, Rem 3],

$$\Gamma_{\mathrm{tor}}(\mathcal{S}) \to \Gamma_{\mathrm{tor}}(\mathcal{S}_k)$$

is injective. From this it easily follows that $G(\mathcal{S}) \to G(\mathcal{S}_k)$ is injective, so $G(\mathcal{S}) \to \underline{G}(\mathcal{S})$ is injective.

Consequently, Step 1 is now valid for *all* p-adic A-rings $\mathcal{S}$. But this step was the *only* reason to restrict to finite flat A-algebras rather than to p-adic A-rings above (as this restriction was needed in order to permit the base extension argument involving passage to the strictly Henselian case). All other steps in the proof of Theorem 1.4 go through for p-adic A-rings once Step 1 does. One simply replaces 'finite flat A-algebra' with 'p-adic A-ring' everywhere and the references to [7] remain applicable. ∎

Note that as we promised earlier, Lemma 1.3 was never used in the proof of Theorem 1.4. We'll later return to this point in our discussion of the case $e \leq p - 1$.

We conclude our discussion of the $e = 1$ case with an explicit description of a quasi-inverse functor to LM for odd p and to LM^u, LM^c for arbitrary p. This result is implicit in [8] but is not explicitly stated there (though it is given in a slightly less precise form in [9, Prop 9.12]). Let $\mathbf{C}_K$ denote the completion of a chosen algebraic closure $\overline{K}$ of K, with valuation ring $(\mathcal{O}_{\mathbf{C}_K}, \mathfrak{m}_{\mathbf{C}_K})$. For arbitrary $p > 2$ and (L, M) in SH_A^f (or $p = 2$ and (L, M) in $SH_A^{f,u}$), define

$$\rho_{(L,M)} = \{\phi \in \mathrm{Hom}_{D_k}(M, \widehat{CW}_k(\mathcal{O}_{\mathbf{C}_K}/p)) \mid \phi(L) \subseteq \ker w_{\mathcal{O}_{\mathbf{C}_K}}\}$$

as a $\mathbf{Z}[\mathrm{Gal}(\overline{K}/K)]$-module (via the canonical isomorphism $\mathrm{Gal}(\overline{K}/K) \simeq \mathrm{Aut}_{\mathrm{cont}}(\mathbf{C}_K/K)$). For $p = 2$ and (L, M) in $SH_A^{f,c}$, define $\rho^c_{(L,M)}$ in a similar way, using $\widehat{CW}(\mathfrak{m}_{\mathbf{C}_K}/p\mathfrak{m}_{\mathbf{C}_K})$ and $w^c_{\mathcal{O}_{\mathbf{C}_K}}$. Note that if $p = 2$ and G is connected and unipotent, there is a natural map $\rho^c_{(L,M)} \to \rho_{(L,M)}$ of $\mathbf{Z}[\mathrm{Gal}(\overline{K}/K)]$-modules (since F is nilpotent on M, any $\phi \in \rho_{(L,M)}$ has image in $\widehat{CW}_k(\mathfrak{m}_{\mathbf{C}_K}/p\mathcal{O}_{\mathbf{C}_K})$).

Theorem 1.9. *Assume $p \neq 2$ or else that (L, M) lies in $SH_A^{f,u}$ or $SH_A^{f,u}$. The abelian group underlying $\rho_{(L,M)}$ is* finite p-group *and* $\mathrm{Gal}(\overline{K}/K)$ *acts through the quotient by an open normal subgroup. Consider the finite flat commutative group scheme $G(\rho_{(L,M)})$ of p-power order over K which is canonically attached to $\rho_{(L,M)}$ (using our fixed choice of $\overline{K}$). This is the generic fiber of a canonically determined object $G_{(L,M)}$ in $\mathcal{FF}_A$ if $p \neq 2$, and similarly with $\mathcal{FF}_A^u$ if (L, M) lies in $SH_A^{f,u}$ and p is arbitrary. In this way, we get a functor $(L, M) \rightsquigarrow G_{(L,M)}$ which is a quasi-inverse to LM for odd p and which is a quasi-inverse to LM^u for arbitrary p.*

If $p = 2$, the same assertions holds for connected objects, using $\rho^c_{(L,M)}$. If in addition (L, M) is unipotent, then $\rho^c_{(L,M)} \to \rho_{(L,M)}$ is an isomorphism.

Proof. Since $(L, M) \simeq LM(G)$ for *some* G in $\mathcal{FF}_A$, with G unipotent if (L, M) lies in $SH_A^{f,u}$, $\rho_{(L,M)} \simeq \underline{G}(\mathcal{O}_{\mathbf{C}_K})$ as a $\mathbf{Z}[\mathrm{Gal}(\overline{K}/K)]$-module (this is where the definition of $\rho_{(L,M)}$ comes from). By Corollary 1.8, this can be identified with $G(\mathcal{O}_{\mathbf{C}_K})$ in a manner which is functorial in $\mathcal{O}_{\mathbf{C}_K}$ — that is, as a $\mathbf{Z}[\mathrm{Gal}(\overline{K}/K)]$-module. Since this is canonically the same as $G(\overline{K})$, we obtain the claim that $\rho_{(L,M)}$ has an underlying abelian group which is a finite p-group on which $\mathrm{Gal}(\overline{K}/K)$ acts continuously.

Because $\rho_{(L,M)} \simeq G(\overline{K})$ as a Galois module, it follows from Corollary 1.5 and [17, Cor 2.2.3(2)] that the affine K-algebra of $G(\rho_{(L,M)})$ contains a *unique* finite (flat) A-subalgebra which has generic fiber $G(\rho_{(L,M)})$ and which admits a (necessarily unique, commutative, p-power order) group scheme structure over A compatible with this generic fiber identification, with the added condition of unipotence or connectedness for $p = 2$. Also, if (L, M) lies in $SH_A^{f,u}$ for $p > 2$, the resulting A-group scheme must be unipotent (resp.

connected). Define $G_{(L,M)}$ to be the corresponding object in $\mathcal{FF}_A$ (and it lies in $\mathcal{FF}_A^u$ when (L, M) lies in $SH_A^{f,u}$). Note that the passage from $G(\rho_{(L,M)})$ to $G_{(L,M)}$ does not depend on our choice of $\overline{K}$; it is only the passage from $\rho_{(L,M)}$ to $G(\rho_{(L,M)})$ that depends on this choice.

It is now straightfoward to check that

$$(L, M) \rightsquigarrow G_{(L,M)}$$

is a functor of (L, M) in an obvious manner and that this is a quasi-inverse to LM for odd p and to LM^u for arbitrary p. If we change $\overline{K}$, upon choosing an isomorphism between the two algebraic closures we easily get an explicit isomorphism between the resulting functors (the only point of the construction that really changes is the passage from a Galois representation to a finite group scheme over K).

In the connected case with $p = 2$, the same arguments carry over for ρ^c. Finally, if $p = 2$ and (L, M) is unipotent and connected, then a G in $\mathcal{FF}_A^u$ with $LM^u(G) \simeq (L, M)$ has $\mathcal{M}(G_k) \simeq M$, so G lies in $\mathcal{FF}_A^c$. Thus, $LM^c(G) \simeq (L, M)$ and we have a commutative diagram

$$\begin{array}{ccc} \underline{G}(\mathcal{O}_{\mathbf{C}_K}) & \simeq & \rho^c_{(L,M)} \\ \| & & \downarrow \\ \underline{G}(\mathcal{O}_{\mathbf{C}_K}) & \simeq & \rho_{(L,M)} \end{array}$$

This proves that $\rho^c_{(L,M)} \to \rho_{(L,M)}$ is an isomorphism.

■

2. Defining Honda Systems when $e \leq p - 1$

We now wish to extend all of the arguments in §1 to the case where $e \leq p - 1$. The first main point is to figure out what the definition of a Honda system should be. Before getting into the details, we should emphasize that a potentially serious technical problem for us when $e > 1$ is the fact that for G in $\mathcal{FF}_{A'}$ and $M = \mathcal{M}(G_k)$, the sequence

$$0 \to M/V \xrightarrow{F} M/p \to M/F \to 0,$$

which is always right exact, does *not* have to be exact. The fact that this is always exact when $e = 1$ was critical for Fontaine's argument in §1 to work (see Step 4). The formulas of Oort-Tate in [15, §2, Rem 3] show that when $e > 1$, there always exists G in $\mathcal{FF}_{A'}$ with closed fiber $\alpha_{p/k}$, in which case the above sequence is

$$0 \to M \xrightarrow{0} M \xrightarrow{\mathrm{id}} M \to 0,$$

which is not exact. Fortunately, the case $e > 1$ has other significant features that will enable us to circumvent this issue.

Before giving the definitions (or, rather, the motivation), we need to recall a crucial general construction, due to Fontaine, which attaches to a D_k-module a certain A'-module (note that it generally makes no sense to have F or V operators on an A'-module when $e > 1$ because Frobenius-semilinearity wouldn't make any sense). We will only discuss this construction in the case $e \leq p - 1$, as that's all we'll need and quite fortunately it is possible to make things very explicit in this case. This explicitness will be useful when carrying out various computations.

It should be emphasized that the computations in this section are very formal and so if we consider the construction below without conditions on e, the basic formalism still goes through for tame extensions (though it does not coincide with Fontaine's general construction in [7, Ch IV, §2] once $e > p - 1$). In later sections, the restriction $e \leq p - 1$ will be essential.

Let M be a D_k-module. We define $M^{(j)}$ to be the D_k-module whose underlying A-module is $A \otimes_A M$, using $\sigma^j : A \simeq A$ (σ denoting the Frobenius map), $F(\lambda \otimes x) = \sigma(\lambda) \otimes F(x)$, and $V(\lambda \otimes x) = \sigma^{-1}(\lambda) \otimes V(x)$. Thus, we obtain A-*linear* maps

$$F_j : M^{(j+1)} \to M^{(j)}, \qquad V_j : M^{(j)} \to M^{(j+1)},$$

satisfying $F_j V_j = p_{M^{(j)}}$, $V_j F_j = p_{M^{(j+1)}}$. We'll only use $M^{(0)} = M$ and $M^{(1)}$. We will not abuse notation and write F, V for F_0, V_0, as this might cause confusion with respect to issues of A-linearity.

Definition 2.1. We define $M_{A'}$ to be the direct limit of the diagram

$$\begin{array}{ccc} \mathfrak{m}\otimes_A M & \xrightarrow{V^M} & p^{-1}\mathfrak{m}\otimes_A M^{(1)} \\ \varphi_0^M\big\downarrow & & \big\uparrow\varphi_1^M \\ A'\otimes_A M & \xleftarrow{F^M} & A'\otimes_A M^{(1)} \end{array}$$

in the category of A'-modules, where φ_0^M, φ_1^M are the obvious 'inclusion' maps (which might not be injective!), $V^M(\lambda\otimes x) = p^{-1}\lambda\otimes V_0(x)$, and $F^M(\lambda\otimes x) = \lambda\otimes F_0(x)$.

More explicitly, $M_{A'}$ is the quotient of $(A'\otimes_A M)\oplus(p^{-1}\mathfrak{m}\otimes_A M^{(1)})$ by the submodule

$$\{(\varphi_0^M(u) - F^M(w), \varphi_1^M(w) - V^M(u)) \mid u\in\mathfrak{m}\otimes_A M, w\in A'\otimes_A M^{(1)}\}.$$

For $x\in A'\otimes_A M$ and $y\in p^{-1}\mathfrak{m}\otimes_A M^{(1)}$, we let $\overline{(x,y)}$ denote the residue class in $M_{A'}$ represented by (x,y). Trivially $M\rightsquigarrow M_{A'}$ is a covariant additive functor from D_k-modules to A'-modules. When $e=1$, the obvious A-module isomorphism $pA\otimes_A M\simeq M$ shows that M_A is isomorphic to the direct limit of the diagram

$$\begin{array}{ccc} M & \xrightarrow{V_0} & M^{(1)} \\ p\big\downarrow & & \big\| \\ M & \xleftarrow{F_0} & M^{(1)} \end{array}$$

in the category of A-modules and so the natural A-module map $\iota_M : M\to M_A$ given by $\iota_M(m) = \overline{(m,0)}$ is an isomorphism. This will motivate how we define and study finite Honda systems over A'.

There are maps

$$\iota_M : A'\otimes_A M\to M_{A'}$$

and

$$\mathcal{F}_M : p^{-1}\mathfrak{m}\otimes_A M^{(1)}\to M_{A'}$$

of A'-modules, natural in M. Also, it is easy to check that the A'-linear maps

$$1\otimes V_0 : A'\otimes_A M\to A'\otimes_A M^{(1)},\ \ p\otimes\mathrm{id} : p^{-1}\mathfrak{m}\otimes_A M^{(1)}\to A'\otimes_A M^{(1)}$$

satisfy the necessary compatibilies to induce an A'-linear map

$$\mathcal{V}_M : M_{A'}\to A'\otimes_A M^{(1)}$$

on the direct limit $M_{A'}$. For accuracy these maps should be denoted $\iota_{M,A'}$, $\mathcal{F}_{M,A'}$, and $\mathcal{V}_{M,A'}$ (and likewise we should have written $V^{M,A'}$, $F^{M,A'}$, $\varphi_0^{M,A'}$, $\varphi_1^{M,A'}$ above), but we'll only use the more precise notation when the less precise notation may cause confusion (e.g., in our discussion of base change in §4). Also, observe that via $\iota_{M,A} : M\simeq M_A$, $\mathcal{F}_{M,A}$ is exactly $F_0 : M^{(1)}\to M$ and $\mathcal{V}_{M,A}$ is exactly $V_0 : M\to M^{(1)}$.

Using the natural A-linear maps $M\to A'\otimes_A M\overset{\iota_M}{\to} M_{A'}$ and $M^{(1)}\to p^{-1}\mathfrak{m}\otimes_A M^{(1)}$, it is easy to check that the diagram

$$\begin{array}{ccccc} M^{(1)} & \xrightarrow{F_0} & M & \xrightarrow{V_0} & M^{(1)} \\ \downarrow & & \downarrow & & \downarrow \\ p^{-1}\mathfrak{m}\otimes_A M^{(1)} & \xrightarrow{\mathcal{F}_M} & M_{A'} & \xrightarrow{\mathcal{V}_M} & A'\otimes_A M^{(1)} \end{array}$$

commutes.

Warning In [7, Ch IV, §2.4ff], $p^{-1}\mathfrak{m}\otimes_A M^{(1)}$ is denoted $M_{A'}[1]$.

Before proceeding further, we should remark that since K'/K is a tamely totally ramified extension, we can choose a uniformizer π of A' such that $\pi^e = p\epsilon$ for a suitable unit $\epsilon\in A^\times$. Fix such a choice of π now and forever. This will be essential for many of our calculations, since it makes the matrix for multiplication by π on A' extremely simple with respect to the A-basis $1,\dots,\pi^{e-1}$.

Lemma 2.2. *If $\ell_A(M) < \infty$, then*

$$\ell_{A'}(M_{A'}) = \ell_{A'}(p^{-1}\mathfrak{m} \otimes_A M^{(1)}) = \ell_{A'}(A' \otimes_A M) = e\ell_A(M).$$

Also, the functor $M \rightsquigarrow M_{A'}$ is exact on the category of D_k-modules with finite A-length.

Remark 2.3. This extends [7, Ch IV, §2.6, Cor 1] to the finite-length case.

Proof. It is not hard to check 'by hand' that $M \rightsquigarrow M_{A'}$ is right exact as asserted. Thus, exactness will follow from the length result. The essential point here and for what follows is the simple observation that because $A \to A'$ induces an isomorphism of residue fields, for any A'-module N we have the equality $\ell_{A'}(N) = \ell_A(N)$. It is now obvious that $\ell_{A'}(p^{-1}\mathfrak{m} \otimes_A M^{(1)}) = e\ell_A(M) = \ell_{A'}(A' \otimes_A M)$. As for $\ell_{A'}(M_{A'})$, which is at least a priori finite, we see from the explicit description of $M_{A'}$ that $\ell_{A'}(M_{A'})$ is equal to the A'-length of

$$\{(u, w) \in (\mathfrak{m} \otimes_A M) \oplus (A' \otimes_A M^{(1)}) \mid \varphi_0^M(u) = F^M(w), \varphi_1^M(w) = V^M(u)\}.$$

We will show that as an A-module, this is (non-canonically) isomorphic to

$$M \oplus (M^{(1)})^{\oplus(e-1)},$$

so $\ell_{A'}(M_{A'}) = \ell_A(M_{A'}) = e\ell_A(M)$ as desired.

In order to get the A-module isomorphism mentioned above, recall our uniformizer π. Any $u \in \mathfrak{m} \otimes_A M$ and $w \in A' \otimes_A M^{(1)}$ can be uniquely written in the form

$$u = \sum_{j=1}^{e} \pi^j \otimes u_j, \qquad w = \sum_{j=0}^{e-1} \pi^j \otimes w_j,$$

with $u_j \in M$, $w_j \in M^{(1)}$. The condition $\varphi_0^M(u) = F^M(w)$ says that in $A' \otimes_A M$,

$$1 \otimes p\epsilon u_e + \sum_{j=1}^{e-1} \pi^j \otimes u_j = 1 \otimes F_0 w_0 + \sum_{j=1}^{e-1} \pi^j \otimes F_0 w_j,$$

so the precise conditions are $p\epsilon u_e = F_0 w_0$ and $u_j = F_0 w_j$ for $1 \leq j \leq e-1$. Meanwhile, $\varphi_1^M(w) = V^M(u)$ says that in $p^{-1}\mathfrak{m} \otimes_A M^{(1)}$,

$$1 \otimes \epsilon V_0 u_e + \sum_{j=1}^{e-1} p^{-1}\pi^j \otimes V_0 u_j = 1 \otimes w_0 + \sum_{j=1}^{e-1} p^{-1}\pi^j \otimes p w_j,$$

so the precise conditions are $\epsilon V_0 u_e = w_0$ and $V_0 u_j = p w_j$ for $1 \leq j \leq e-1$.

Hence, we see that we are free to choose $u_e \in M$ and $w_1, \ldots, w_{e-1} \in M^{(1)}$, with everything else uniquely determined. This gives rise to the desired A-module isomorphism. ■

Lemma 2.4. *If $\ell_A(M) < \infty$, then*

$$\ell_{A'}(\ker \iota_M) = \ell_{A'}(\operatorname{coker} \iota_M) = (e-1)\ell_A(\ker V),$$

$$\ell_{A'}(\ker \mathcal{F}_M) = \ell_{A'}(\operatorname{coker} \mathcal{F}_M) = \ell_A(\ker F),$$

and

$$\ell_{A'}(\ker \mathcal{V}_M) = \ell_{A'}(\operatorname{coker} \mathcal{V}_M) = \ell_A(\ker V).$$

Also, the kernels and cokernels of $\mathcal{F}_M$ and $\mathcal{V}_M$ are annihilated by $\mathfrak{m}$ (this is true even without a finiteness assumption on $\ell_A(M)$). Finally, the commutative diagram above Lemma 2.2 *induces k-linear isomorphisms*

$$\ker F_0 \simeq \ker \mathcal{F}_M, \ \ \operatorname{coker} F_0 \simeq \operatorname{coker} \mathcal{F}_M,$$

and

$$\ker V_0 \simeq \ker \mathcal{V}_M, \ \ \operatorname{coker} V_0 \simeq \operatorname{coker} \mathcal{V}_M\,.$$

Remark 2.5. This lemma extends [7, Ch IV, §2.5, Cor 2] to the finite-length case.

Proof. Certainly $\ell_{A'}(\ker \iota_M) = \ell_{A'}(\operatorname{coker} \iota_M)$, since ι_M is an A'-linear map between A'-modules with the same finite A'-length, and likewise for $\mathcal{F}_M$ and $\mathcal{V}_M$. We'll now explicitly compute the lengths of the kernels.

By definition, $\ker \iota_M = \{\varphi_0^M(u) - F^M(w) \mid \varphi_1^M(w) = V^M(u)\}$. Writing

$$u = \sum_{j=1}^{e} \pi^j \otimes u_j \in \mathfrak{m} \otimes_A M, \quad w = \sum_{j=0}^{e-1} \pi^j \otimes w_j \in A' \otimes_A M^{(1)}$$

as usual, $\varphi_1^M(w) = V^M(u)$ says exactly that $w_0 = \epsilon V_0 u_e$ and, for $1 \le j \le e-1$, $pw_j = V_0 u_j$. In this case, we compute in $A' \otimes_A M$ that

$$\varphi_0^M(u) - F^M(w) = 1 \otimes (p\epsilon u_e - F_0 w_0) + \sum_{j=1}^{e-1} \pi^j \otimes (u_j - F_0 w_j).$$

But

$$p\epsilon u_e - F_0 w_0 = p\epsilon u_e - F_0 \epsilon V_0 u_e = \epsilon(p - F_0 V_0) u_e = 0$$

and for $1 \le j \le e-1$,

$$V_0(u_j - F_0 w_j) = V_0 u_j - pw_j = 0,$$

so easily

$$\ker \iota_M = \left\{ \sum_{j=1}^{e-1} \pi^j \otimes u'_j | V u'_j = 0 \right\}.$$

This enables us to see that

$$\ell_{A'}(\ker \iota_M) = \ell_A(\ker \iota_M) = (e-1)\ell_A(\ker V).$$

Meanwhile,

$$\ker \mathcal{F}_M = \{\varphi_1^M(w) - V^M(u) \mid \varphi_0^M(u) = F^M(w)\}.$$

Doing a similar computation as above (in fact, just extending the one in the proof of Lemma 2.2), we find

$$\ker \mathcal{F}_M = \{1 \otimes w \in p^{-1}\mathfrak{m} \otimes_A M^{(1)} \mid F_0 w = 0\}.$$

Note that if $1 \otimes w \in \ker \mathcal{F}_M$, then $\pi(1 \otimes w) = p^{-1}\pi \otimes pw = 0$, so $\ker \mathcal{F}_M$ is annihilated by $\mathfrak{m}$ and clearly

$$\ell_{A'}(\ker \mathcal{F}_M) = \ell_A(\ker \mathcal{F}_M) = \ell_A(\ker F).$$

The description of $\ker \mathcal{F}_M$ also shows that the natural k-linear map $\ker F_0 \to \ker \mathcal{F}_M$ is an isomorphism.

Let's next check that $\mathfrak{m}$ annihilates $\operatorname{coker} \mathcal{F}_M$. Choose $x \in M$. We need to show that for $1 \otimes x \in A' \otimes_A M$, $\pi \cdot \iota_M(1 \otimes x)$ maps to 0 in $\operatorname{coker} \mathcal{F}_M$. This says that $\iota_M(\pi \otimes x)$ is in the image of $\mathcal{F}_M$. But this is obvious:

$$\iota_M(\pi \otimes x) = \mathcal{F}_M(V^M(\pi \otimes x))$$

(the careful reader will note the harmless fact that the two $\pi \otimes x$'s in the above equality live in different tensor product modules; with this point clarified, above we are implicitly using $\pi \otimes x = \varphi_M^0(\pi \otimes x)$).

Observe also that for $x \in M^{(1)}$, $\iota_M(1 \otimes F_0 x) = \mathcal{F}_M(\varphi_1^M(1 \otimes x))$. This gives rise to the natural k-linear map

$$M/FM = \operatorname{coker} F_0 \to \operatorname{coker} \mathcal{F}_M$$

induced by the commutative diagram above Lemma 2.2. This is a map between k-vector spaces with the same dimension. In order to show that this map is an isomorphism, we need only check that it is surjective. But this is obvious since the A'-linear composite map

$$A' \otimes_A M \xrightarrow{\iota_M} M_{A'} \to \operatorname{coker} \mathcal{F}_M$$

is surjective, with $\operatorname{coker} \mathcal{F}_M$ annihilated by $\mathfrak{m}$.

Finally, we consider $\mathcal{V}_M$. By definition, $\operatorname{coker} \mathcal{V}_M$ is the quotient of $A' \otimes_A M^{(1)}$ by the A'-submodule consisting of elements of the form

$$\sum_{j=1}^{e} \pi^j \otimes m_j + \sum_{i=0}^{e-1} \pi^i \otimes V_0 n_i,$$

with arbitrary $m_j \in M^{(1)}$ and $n_i \in M$. Since $p = V_0F_0$, this submodule is the same as the submodule of elements of the form

$$1 \otimes V_0\mu + \sum_{i=1}^{e-1} \pi^i \otimes \mu_i,$$

with arbitrary $\mu \in M$, $\mu_i \in M^{(1)}$. It is now clear that $\operatorname{coker} \mathcal{V}_M$ is killed by $\mathfrak{m}$ and that as a vector space over $A'/\mathfrak{m} \simeq k$,

$$\operatorname{coker} \mathcal{V}_M \simeq M^{(1)}/V_0(M) = \operatorname{coker} V_0.$$

This map is easily checked to be an inverse to the natural map arising from the commutative diagram above Lemma 2.2.

Now we check that $\ker \mathcal{V}_M$ is killed by $\mathfrak{m}$ and that the natural k-linear map $\ker V_0 \to \ker \mathcal{V}_M$ is surjective (and therefore is an isomorphism). Choose $(u, w) \in (A' \otimes_A M) \oplus (p^{-1}\mathfrak{m} \otimes_A M^{(1)})$ such that $\mathcal{V}_M(\overline{(u, w)}) = 0$. Writing

$$u = \sum_{i=0}^{e-1} \pi^i \otimes u_i, \quad w = \sum_{j=1}^{e} p^{-1}\pi^j \otimes w_j$$

as usual, the vanishing condition says precisely that

$$\sum_{i=0}^{e-1} \pi^i \otimes V_0u_i + \sum_{j=1}^{e} \pi^j \otimes w_j = 0$$

in $A' \otimes_A M^{(1)}$. Thus, $w_j = -V_0u_j$ for $1 \leq j \leq e-1$ and $V_0(u_0 + F_0\epsilon w_e) = 0$. Using the 'explicit' defining conditions of $M_{A'}$, we readily see that such an element can also be represented by $(u', 0)$ with $V_0u' = 0$. Thus,

$$\ker \mathcal{V}_M = \ker(1 \otimes V_0)/\{\varphi_0^M(u) - F^M(w) \,|\, \varphi_1^M(w) = V^M(u)\},$$

where $1 \otimes V_0 : A' \otimes_A M \to A' \otimes_A M^{(1)}$ is the natural map. The submodule which we are quotienting out by is nothing other than $\ker \iota_M$. Using our explicit desciption above for $\ker \iota_M$, we see that $\ker \mathcal{V}_M$ is killed by $\mathfrak{m}$ and is naturally isomorphic to $\ker V_0$ as a k-vector space in the desired natural way.

■

We're now almost ready to define what a finite Honda system over A' is. Our motivation is Fontaine's classification of p-divisible groups for $e \leq p-1$ as mentioned earlier, together with the arguments we have already seen in the case $e = 1$. First of all, observe that if $L \subset M_{A'}$ is any A'-submodule, where M is a D_k-module, there are natural k-linear maps

$$L/\mathfrak{m}L \to \operatorname{coker} \mathcal{F}_M$$

and

$$L[\mathfrak{m}] \oplus \ker \mathcal{V}_M \to M_{A'}[\mathfrak{m}].$$

Also, we define the A'-linear isomorphism

$$\xi^M = \xi^M_\pi : A' \otimes_A M \simeq \mathfrak{m} \otimes_A M$$

by $\lambda \otimes x \mapsto \pi\lambda \otimes x$. Of course this depends heavily on the choice of π, but if we replace π by *any* other uniformizer, this would only have the effect of composing ξ^M with multiplication by an element of $(A')^\times$ on $\mathfrak{m} \otimes_A M$ and so this would have no effect on the image of an A'-submodule of $A' \otimes_A M$ under ξ^M. For this reason, the role of π here is actually irrelevant to the way in which we will use ξ^M below (though we will use the notation ξ^M_π when it is needed to avoid confusion).

In the arguments when $e = 1$, the essential use of the condition that $V|_L$ is injective was to show that $V(L[p]) \subseteq \ker F$ is an equality. It was *this* condition which was what we needed in the proof of Theorem 1.3. Since $V^M(\xi_M(\iota_M^{-1}(L[\mathfrak{m}])))$ (which does not depend on the choice of π used to define ξ^M!) is one generalization of $V(L[p])$ and inside of $p^{-1}\mathfrak{m} \otimes_A M^{(1)}$ we have

$$V^M(\xi^M(\iota_M^{-1}(L[\mathfrak{m}]))) \subseteq \ker \mathcal{F}_M,$$

we might expect to require this to be an equality. Unfortunately this condition will turn out to be too strong in general, but will cover many cases of interest (e.g., p^n-torsion of a p-divisible group over A'; cf. Theorems 3.3, 3.5, Corollary 4.11).

Before defining $SH^f_{A'}$, we make one final observation. The description of $\ker \mathcal{F}_M$ in the proof of Lemma 2.4 shows that we have a k-linear map

$$\ker \mathcal{F}_M \to \ker(M^{(1)}/V_0 M \xrightarrow{F_0} M/p)$$

given by $1 \otimes w \to w \bmod V_0 M$. It is clear that this map annihilates $V^M(\xi^M(\iota_M^{-1}(L[\mathfrak{m}])))$, so we have a natural k-linear map

$$\ker \mathcal{F}_M / V^M(\xi^M(\iota_M^{-1}(L[\mathfrak{m}]))) \to \ker(M^{(1)}/V_0 M \xrightarrow{F_0} M/p).$$

This will be used in Theorem 3.3.

Definition 2.6. A *finite pre-Honda system over* A' is a triple (L, M, j) with M a D_k-module satisfying $\ell_A(M) < \infty$, L an finite-length A'-module, and $j : L \to M_{A'}$ an A'-linear map. These form an *abelian* category $PSH^f_{A'}$ in an obvious manner (here we implicitly use the exactness assertion in Lemma 2.1, and it is also important here that we do not require j to be injective). When $e < p-1$, we define the category of *finite Honda systems over* A' to be the full subcategory $SH^f_{A'}$ consisting of objects (L, M, j) in $PSH^f_{A'}$ such that the natural k-linear map

$$L/\mathfrak{m}L \to \operatorname{coker} \mathcal{F}_M$$

is an isomorphism and $\mathcal{V}_M \circ j$ is injective (so in particular, j is injective). When $e \le p-1$, we define the category of *unipotent finite Honda systems over* A' to be the full subcategory $SH^{f,u}_{A'}$ in $PSH^f_{A'}$ consisting of triples (L, M, j) in which the action of V on M is nilpotent, $L/\mathfrak{m}L \simeq \operatorname{coker} \mathcal{F}_M$, and $\mathcal{V}_M \circ j$ is injective. The category $SH^{f,c}_{A'}$ of *connected finite Honda systems over* A' is defined similarly, with a nilpotence condition on the F-action.

It is clear that when $e = 1$, the definitions of $SH^f_{A'}$ and $SH^{f,u}_{A'}$ coincide with the ones given previously; we should also mention that the notion of a finite pre-Honda system is introduced primarily to simplify the exposition in certain places, when we wish to discuss certain constructions prior to checking that they make sense within the restricted categories $SH^f_{A'}$ and $SH^{f,u}_{A'}$. Also, when discussing Honda systems, we usually omit reference to the injective map j and regard L as an A'-submodule of $M_{A'}$.

We conclude this section with some observations that will be particularly useful when $e \ge 2$.

Lemma 2.7. *Let (L, M, j) denote an object in $PSH^f_{A'}$ such that $L/\mathfrak{m}L \to \operatorname{coker} \mathcal{F}_M$ is an isomorphism. Then $\mathcal{V}_M \circ j$ is injective if and only if the natural k-linear map*

$$L[\mathfrak{m}] \oplus \ker \mathcal{V}_M \to M_{A'}[\mathfrak{m}]$$

is an isomorphism.

If M is any D_k-module (in particular, we do not require M to have finite A-length) and $2 \le e \le p-1$, then there is a natural k-linear isomorphism

$$\ker V_0 \oplus \ker F_0 \simeq M_{A'}[\mathfrak{m}]$$

taking $\ker V_0$ into $\ker \mathcal{V}_M$.

If $e \le p-1$, $M \hookrightarrow N$ is an injection of D_k-modules, and $\ell_A(M) < \infty$, then the natural A'-linear map

$$M_{A'} \to N_{A'}$$

is injective.

Proof. The last part of the lemma is obvious when $e = 1$. When $2 \le e \le p-1$, it follows easily from the second part of the lemma. Under either case in the first part, j is injective, so we may safely view L there as an A'-submodule of $M_{A'}$. The 'if' direction is obvious, so now assume $\mathcal{V}_M|_L$ is injective. Thus, the map $L[\mathfrak{m}] \oplus \ker \mathcal{V}_M \to M_{A'}[\mathfrak{m}]$ is injective. By Lemma 2.4, the left side has k-dimension equal to $\dim_k \ker F_0 + \dim_k \ker V_0$. When $e = 1$, we have already seen in Step 4 of the proof of Theorem 1.4 that $M_{A'}[\mathfrak{m}] = M[p] \simeq M/p$ has the same k-dimension. It therefore suffices to prove the second part of the lemma.

Consider the natural map $\ker V_0 \oplus \ker F_0 \to M_{A'}$ given by

$$(u, w) \mapsto \overline{(1 \otimes u, p^{-1}\pi^{e-1} \otimes w)}.$$

Note that this requires $e - 1 \geq 1$ in order to make sense. It is trivial to check that the image of this map lies inside of $M_{A'}[\mathfrak{m}]$. We will show that the resulting k-linear map to $M_{A'}[\mathfrak{m}]$ is an isomorphism.

We first will check that the image is all of $M_{A'}[\mathfrak{m}]$. Choose as usual

$$u = \sum_{j=0}^{e-1} \pi^j \otimes u_j \in A' \otimes_A M, \;\; w = \sum_{j=1}^{e} p^{-1}\pi^j \otimes w_j \in p^{-1}\mathfrak{m} \otimes_A M^{(1)}$$

and assume $m = \overline{(u, w)} \in M_{A'}$ is killed by $\mathfrak{m}$. The condition $\pi m = 0$ says that the element

$$(1 \otimes p\epsilon u_{e-1} + \sum_{j=1}^{e-1} \pi^j \otimes u_{j-1}, p^{-1}\pi \otimes p\epsilon w_e + \sum_{j=2}^{e} p^{-1}\pi^j \otimes w_{j-1})$$

in $(A' \otimes_A M) \oplus (p^{-1}\mathfrak{m} \otimes_A M^{(1)})$ is equal to

$$(1 \otimes (p\epsilon x_e - F_0 y_0) + \sum_{j=1}^{e} \pi^j \otimes (x_j - F_0 y_j), 1 \otimes (y_0 - \epsilon V_0 x_e) + \sum_{j=1}^{e-1} p^{-1}\pi^j \otimes (p y_j - V_0 x_j))$$

for suitable $x_j \in M$ and $y_j \in M^{(1)}$. Choosing $y_1, \ldots, y_{e-1} \in M^{(1)}$ and $x_e \in M$, we readily see that we must have $y_0 = \epsilon V_0 x_e + \epsilon w_{e-1}$ and

$$x_j = u_{j-1} + F_0 y_j$$

for $1 \leq j \leq e-1$, with the consistency conditions $w_j = -V_0 u_j$ for $1 \leq j \leq e-2$ (a vacuous condition if $e = 2$) and

$$F_0 w_{e-1} = -p u_{e-1}, \;\; -p\epsilon w_e = V_0 u_0.$$

These last two conditions are independent of each other since $e > 1$. A simple calculation shows that $m = \overline{(1 \otimes u, p^{-1}\pi^{e-1} w)}$, with $u = u_0 + \epsilon F_0 w_e$ and $w = -(w_{e-1} + V_0 u_{e-1})$. Since $V_0 u = 0$ and $F_0 w = 0$, the desired surjectivity is proven.

Now choose $(u, w) \in \ker V_0 \oplus \ker F_0$ which is sent to 0 in $M_{A'}$. Writing out the explicit meaning of this condition, we see that there exist $x_1, \ldots, x_e \in M$ and $y_0, \ldots, y_{e-1} \in M^{(1)}$ such that

$$u = p\epsilon x_e - F_0 y_0, \;\; w = p y_{e-1} - V_0 x_{e-1},$$

with the extra conditions $y_0 = \epsilon V_0 x_e$ and $x_j = F_0 y_j$ for $1 \leq j \leq e-1$. Thus,

$$u = F_0(\epsilon V_0 x_e - y_0) = F_0(0) = 0$$

and

$$w = V_0(F_0 y_{e-1} - x_{e-1}) = V_0(0) = 0.$$

■

3. A Functor on Group Schemes when $e \leq p - 1$

For any G in $\mathcal{FF}_{A'}$, we define $LM_{A'}(G)$ to be the object $(L_{A'}(G), \mathcal{M}(G_k), j)$ in $PSH^f_{A'}$, where $L_{A'}(G)$ is the kernel of the A'-linear map

$$\mathcal{M}(G_k)_{A'} \to CW_{k,A'}(\mathcal{R}_k) \xrightarrow{w'_{\mathcal{R}}} \mathcal{R}_{K'}/\mathfrak{m}\,\mathcal{R},$$

with $\mathcal{R}$ the affine ring of $G_{/A'}$, $CW_{k,A'}(\mathcal{R}_k) = (CW_k(\mathcal{R}_k))_{A'}$, and j the inclusion. The continuous A'-linear map $w'_{\mathcal{R}}$ is a generalization of $w_{\mathcal{R}}$, defined in [7, p. 197], and it is induced by $w_{\mathcal{R}}$ and a natural surjection $A' \otimes_A CW_k(\mathcal{R}_k) \to CW_{k,A'}(\mathcal{R}_k)$. By the last part of Lemma 2.7, we note that we can (and will) view $\mathcal{M}(G_k)_{A'}$ as an A'-submodule of $CW_{k,A'}(\mathcal{R}_k)$. Because $K \otimes_A \mathcal{R} \simeq K' \otimes_{A'} \mathcal{R}$, no confusion should arise from our use of the notation $\mathcal{R}_{K'}$ for what Fontaine writes as $\mathcal{R}_K$ in [7]. Since $e \leq p-1$, we also have $\mathfrak{m}\,\mathcal{R} = P'(\mathcal{R})$ in the notation of [7, Ch IV, §3.1]. Clearly $LM_{A'}$ is an additive contravariant functor from $\mathcal{FF}_{A'}$ to $PSH^f_{A'}$.

For ease of notation, we now fix a choice of G in $\mathcal{FF}_{A'}$, with G in $\mathcal{FF}_{A'}^{f,u}$ or $\mathcal{FF}_{A'}^{f,c}$ if $e(A') = p-1$. Let $L = L_{A'}(G)$ and $M = \mathcal{M}(G_k)$. We begin with a length calculation.

Lemma 3.1. $\ell_{A'}(V^M(\xi^M(\iota_M^{-1}(L[\mathfrak{m}])))) = \ell_{A'}(\iota_M(\iota_M^{-1}(L[\mathfrak{m}]))) \leq \ell_{A'}(L[\mathfrak{m}])$.

Remark 3.2. Note that $V^M \circ \xi^M$ kills $\ker \iota_M$ (see the proof of Lemma 2.4 for an explicit description of $\ker \iota_M$). Thus, there is a surjective A'-linear map from $\iota_M(\iota_M^{-1}(L[\mathfrak{m}]))$ to $V^M(\xi^M(\iota_M^{-1}(L[\mathfrak{m}])))$ given by

$$x \mapsto V^M(\xi^M(y)),$$

where $y \in A' \otimes_A M$ is any element satisfying $\iota_M(y) = x$. This map depends on the choice of π implicit in the definition of $\xi^M = \xi^M_\pi$. The length result we are about to prove implies that this surjection is an isomorphism and when there is a full equality in the lemma, then we have a natural isomorphism $L[\mathfrak{m}] \simeq V^M(\xi^M(\iota_M^{-1}(L[\mathfrak{m}])))$. We'll later see that this full equality holds for $LM_{A'}(G)$ if and only if the right exact sequence of k-vector spaces

$$0 \to M^{(1)}/V_0M \stackrel{F_0}{\to} M/pM \to M/FM \to 0$$

is actually exact.

Proof. Since

$$\ell_{A'}(V^M(\xi^M(\iota_M^{-1}(L[\mathfrak{m}])))) = \ell_{A'}(\xi^M(\iota_M^{-1}(L[\mathfrak{m}]))) - \ell_{A'}((\ker V^M) \cap \xi^M(\iota_M^{-1}(L[\mathfrak{m}]))),$$

but $\ell_{A'}(\xi^M(\iota_M^{-1}(L[\mathfrak{m}]))) = \ell_{A'}(\iota_M^{-1}(L[\mathfrak{m}]))$ is equal to

$$\ell_{A'}(\iota_M(\iota_M^{-1}(L[\mathfrak{m}]))) + \ell_{A'}(\ker \iota_M) = \ell_{A'}(\iota_M(\iota_M^{-1}(L[\mathfrak{m}]))) + (e-1)\ell_A(\ker V)$$

(by Lemma 2.4), it suffices to show

$$\ell_{A'}((\ker V^M) \cap \xi^M(\iota_M^{-1}(L[\mathfrak{m}]))) = (e-1)\ell_A(\ker V).$$

However, $\ker V^M$ is given by

$$\left\{ \sum_{j=1}^{e} \pi^j \otimes u_j \in \mathfrak{m} \otimes_A M \mid \sum_{j=1}^{e} p^{-1}\pi^j \otimes V_0 u_j = 0 \text{ in } p^{-1}\mathfrak{m} \otimes_A M^{(1)} \right\}$$

and since the defining condition says precisely that $V_0 u_j = 0$ for $1 \leq j \leq e$, we see that

$$\ell_{A'}(\ker V^M) = \ell_A(\ker V^M) = e\ell_A(\ker V).$$

We'll now show that $(\ker V^M) \cap \xi^M(\iota_M^{-1}(L[\mathfrak{m}]))$ consists of precisely those elements in $\ker V^M$ for which $u_1 = 0$, which gives what we need. For an element

$$\sum_{j=1}^{e} \pi^j \otimes u_j = \xi^M \left(\sum_{j=0}^{e-1} \pi^j \otimes u_{j+1} \right)$$

in $\ker V^M$, $V_0 u_1 = \cdots = V_0 u_e = 0$. Thus, we want to determine precisely when the element

$$\sum_{j=0}^{e-1} \pi^j \otimes u_{j+1} \in A' \otimes_A M$$

has image in $M_{A'}$ which is $\mathfrak{m}$-torsion and in L.

The $\mathfrak{m}$-torsion condition is *automatically* satsified, since

$$\begin{aligned}\pi \cdot \iota_M\left(\sum_{j=0}^{e-1} \pi^j \otimes u_{j+1}\right) &= \iota_M\left(\sum_{j=1}^{e} \pi^j \otimes u_j\right)\\ &= \iota_M \circ \varphi_0^M\left(\sum_{j=1}^{e} \pi^j \otimes u_j\right)\\ &= \mathcal{F}_M \circ V^M\left(\sum_{j=1}^{e} \pi^j \otimes u_j\right)\\ &= \mathcal{F}_M\left(\sum_{j=1}^{e} p^{-1}\pi^j \otimes V_0 u_j\right)\\ &= 0.\end{aligned}$$

On the other hand, $u_j \in \mathcal{M}(G_k) \subseteq CW_k(\mathcal{R}_k)$ has the form

$$u_j = (\ldots, 0, \ldots, 0, u_{j,0})$$

since $V_0 u_j = 0$, so we easily compute that in $\mathcal{R}_{K'}/\mathfrak{m}\,\mathcal{R}$,

$$w'_{\mathcal{R}} \circ \iota_M\left(\sum_{j=0}^{e-1} \pi^j \otimes u_{j+1}\right) = \sum_{j=0}^{e-1} \pi^j \widehat{u}_{j+1,0} \bmod \mathfrak{m}\,\mathcal{R},$$

where $\widehat{u}_{i,0} \in \mathcal{R}$ is a a lift of $u_{i,0}$. Beware that here and later we abuse notation and do not indicate the presence of the injective A'-linear map $M_{A'} \to CW_{k,A'}(\mathcal{R}_k)$ between $w'_{\mathcal{R}}$ and ι_M. Modulo $\mathfrak{m}\,\mathcal{R} = \pi\,\mathcal{R}$, the right side is represented by $\widehat{u}_{1,0}$ and so vanishes if and only if $u_{1,0} = 0$, which is to say that $u_1 = 0$.

■

The next result nicely explains the failure of the exactness of

$$0 \to M/VM \xrightarrow{F} M/pM \to M/FM \to 0$$

for Dieudonne modules of closed fibers of objects in $\mathcal{FF}_{A'}$ when $e > 1$. Also, the essential calculation in the proof will be needed in the proof of the important Theorem 3.4.

Theorem 3.3. *The inclusion*

$$V^M(\xi^M(\iota_M^{-1}(L[\mathfrak{m}]))) \subseteq \ker \mathcal{F}_M$$

is an equality if and only if the sequence

$$0 \to M^{(1)}/V_0 M \xrightarrow{F_0} M/pM \to M/FM \to 0,$$

which is always right exact, is actually exact. More generally, the 4-term sequence

$$0 \to \ker \mathcal{F}_M/V^M(\xi^M(\iota_M^{-1}(L[\mathfrak{m}]))) \to M^{(1)}/V_0 M \xrightarrow{F_0} M/p \to M/F \to 0$$

is always exact.

Proof. When $e = 1$, we saw in §1 that the theorem is true (in fact, the inclusion is always an equality and the sequence is always exact), so we may assume now that $e > 1$. In a couple of places below it will be crucial that $e - 1 \geq 1$.

Recall from the proof of Lemma 2.4 that

$$\ker \mathcal{F}_M = \left\{1 \otimes w \in p^{-1}\mathfrak{m} \otimes_A M^{(1)} \mid F_0 w = 0\right\}.$$

Our first step is to reformulate when $1 \otimes w \in \ker \mathcal{F}_M$ lies in $V^M(\xi^M(\iota_M^{-1}(L[\mathfrak{m}])))$. More precisely, we claim that this is equivalent to the statement that for our $w \in M^{(1)}$ with $F_0 w = 0$, there exist w' and w'' in M such that $V_0 w' = w$, $V_0 w'' = 0$, and

$$w'_{\mathcal{R}}(\iota_M(\pi^{e-1} \otimes \epsilon^{-1} w' + 1 \otimes w'')) = 0.$$

First assume this latter statement. Then for $1 \otimes w \in \ker \mathcal{F}_M$, we see that

$$\pi^{e-1} \otimes \epsilon^{-1} w' + 1 \otimes w'' \in \iota_M^{-1}(L)$$

and $V^M(\xi^M(\pi^{e-1} \otimes \epsilon^{-1} w' + 1 \otimes w''))$ is equal to

$$\begin{aligned} V^M(\pi^e \otimes \epsilon^{-1} w' + \pi \otimes w'') &= p^{-1}\pi^e \otimes \epsilon^{-1} V_0 w' + p^{-1}\pi \otimes V_0 w'' \\ &= 1 \otimes V_0 w' \\ &= 1 \otimes w, \end{aligned}$$

so $1 \otimes w \in V^M(\xi^M(\iota_M^{-1}(L)))$. But since $pw' = F_0 V_0 w' = F_0 w = 0$,

$$\begin{aligned} \pi \cdot \iota_M(\pi^{e-1} \otimes \epsilon^{-1} w' + 1 \otimes w'') &= \iota_M(\pi^e \otimes \epsilon^{-1} w' + \pi \otimes w'') \\ &= \iota_M(1 \otimes pw') + \iota_M(\pi \otimes w'') \\ &= \iota_M \circ \varphi_0^M(\pi \otimes w'') \\ &= \mathcal{F}_M \circ V^M(\pi \otimes w'') \\ &= \mathcal{F}_M(p^{-1}\pi \otimes V_0 w'') \\ &= 0, \end{aligned}$$

so in fact $1 \otimes w \in V^M(\xi^M(\iota_M^{-1}(L[\mathfrak{m}])))$.

Conversely, assume $1 \otimes w \in V^M(\xi^M(\iota_M^{-1}(L[\mathfrak{m}])))$, whence

$$1 \otimes w = V^M \circ \xi^M\left(\sum_{j=0}^{e-1} \pi^j \otimes u_j\right),$$

where $u_j \in M$ and

$$\iota_M\left(\sum_{j=0}^{e-1} \pi^j \otimes u_j\right) \in L[\mathfrak{m}].$$

Thus,

$$1 \otimes w = V^M\left(\sum_{j=1}^{e} \pi^j \otimes u_{j-1}\right) = \sum_{j=1}^{e} p^{-1}\pi^j \otimes V_0 u_{j-1},$$

so $w = \epsilon V_0 u_{e-1} = V_0(\epsilon u_{e-1})$ and $V_0 u_j = 0$ for $0 \le j < e-1$. The calculation

$$\begin{aligned}
\pi \cdot \iota_M\left(\sum_{j=0}^{e-1} \pi^j \otimes u_j\right) &= \iota_M\left(\sum_{j=0}^{e-1} \pi^{j+1} \otimes u_j\right)\\
&= \iota_M \circ \varphi_0^M\left(\sum_{j=0}^{e-1} \pi^{j+1} \otimes u_j\right)\\
&= \mathcal{F}_M \circ V^M\left(\sum_{j=0}^{e-1} \pi^{j+1} \otimes u_j\right)\\
&= \mathcal{F}_M\left(\sum_{j=0}^{e-1} p^{-1}\pi^{j+1} \otimes V_0 u_j\right)\\
&= \mathcal{F}_M(p^{-1}\pi^e \otimes V_0 u_{e-1})\\
&= \mathcal{F}_M(1 \otimes \epsilon V_0 u_{e-1})\\
&= \mathcal{F}_M(1 \otimes w)\\
&= 0
\end{aligned}$$

shows that the $\mathfrak{m}$-torsion condition is superfluous, so it remains to see what constraints arise from the condition

$$w'_{\mathcal{R}} \circ \iota_M\left(\sum_{j=0}^{e-1} \pi^j \otimes u_j\right) = 0.$$

If we can show that

$$w'_{\mathcal{R}} \circ \iota_M\left(\sum_{1 \le j < e-1} \pi^j \otimes u_j\right) = 0,$$

then defining $w' = \epsilon u_{e-1}$ and $w'' = u_0$ yields what we want. For $1 \le j < e-1$, we have $u_j = (\dots, 0, \dots, 0, u_{j,0})$ since $V_0 u_j = 0$. Thus, if $\widehat{u}_{j,0} \in \mathcal{R}$ is a lift of $u_{j,0}$, then the element

$$w'_{\mathcal{R}} \circ \iota_M\left(\sum_{1 \le j < e-1} \pi^j \otimes u_j\right) \in \mathcal{R}_{K'}/\mathfrak{m}\,\mathcal{R}$$

is represented by

$$\sum_{1 \le j < e-1} \pi^j \widehat{u}_{j,0} \in \pi\,\mathcal{R} = \mathfrak{m}\,\mathcal{R},$$

thereby giving the desired vanishing.

Now that we have reformulated our main condition, pick $w \in M^{(1)}$ with $F_0 w = 0$. We must determine precisely when we can construct $w', w'' \in M$ with the properties described above.

Identifying M and $M^{(1)}$ as additive groups (via $x \mapsto 1 \otimes x$), we can write $w = (w_{-n}) \in M \subseteq CW_k(\mathcal{R}_k)$, with $w_{-n} \in \mathcal{R}_k$ satisfying $w_{-n}^p = 0$. Our task is to find $\overline{w}'$ and $\overline{w}''$ in $\mathcal{R}_k$ such that the element

$$w' \overset{\text{def}}{=} (\dots, w_{-n+1}, \dots, w_0, \overline{w}') \in CW_k(\mathcal{R}_k)$$

lies in M, as does $w'' \overset{\text{def}}{=} (\dots, 0, \dots, 0, \overline{w}'')$, and moreover

$$w'_{\mathcal{R}} \circ \iota_M(\pi^{e-1} \otimes \epsilon^{-1} w' + 1 \otimes w'') = 0.$$

Let $\widehat{w}_{-n} \in \mathcal{R}$ lift w_{-n} and $\widehat{w}'$, $\widehat{w}'' \in \mathcal{R}$ lift $\overline{w}'$ and $\overline{w}''$ repsectively. The final condition above says

$$\epsilon^{-1}\pi^{e-1}\left(\widehat{w}' + \sum_{n\geq 1} p^{-n}\widehat{w}_{-n+1}^{p^n}\right) + \widehat{w}'' \in \pi\,\mathcal{R}\,.$$

But $e-1 \geq 1$ (!), so $\epsilon^{-1}\pi^{e-1}\widehat{w}' \in \pi\,\mathcal{R}$ and so the above condition is in fact *independent* of $\widehat{w}'$ (and even $\overline{w}'$), being equivalent to

$$\frac{\epsilon^{-1}\pi^{e-1}}{p}\sum_{n\geq 0} p^{-n}(\widehat{w}_{-n}^{p})^{p^n} + \widehat{w}'' \in \pi\,\mathcal{R}\,.$$

Since $\epsilon^{-1}\pi^{e-1}/p = \pi^{-1}$ and

$$p^{-n}(\widehat{w}_{-n}^{p})^{p^n} \in p^{-n}(\pi\,\mathcal{R})^{p^n} = \pi^{p^n - ne}\,\mathcal{R},$$

with $p^n - ne \geq p^n - n(p-1) \geq 2$ for $n \geq 2$ (and even for $n \geq 1$ if $e < p-1$), our condition is equivalent to

$$(p\pi)^{-1}\widehat{w}_{-1}^{p^2} + \pi^{-1}\widehat{w}_0^p + \widehat{w}'' \in \pi\,\mathcal{R}\,.$$

Thus, we are forced to choose $\overline{w}'' \in \mathcal{R}_k$ to be represented by $-((p\pi)^{-1}\widehat{w}_{-1}^{p^2} + \pi^{-1}\widehat{w}_0^p) \in \mathcal{R}$. Let's check that $w'' \in CW_k(\mathcal{R}_k)$ does lie in $M = \mathcal{M}(G_k)$. It is enough to check that

$$\Delta_G(\pi^{-1}\widehat{w}_0^p) \equiv \left(\pi^{-1}\widehat{w}_0^p\right)\otimes 1 + 1\otimes\left(\pi^{-1}\widehat{w}_0^p\right) \bmod \pi(\mathcal{R}\otimes_{A'}\mathcal{R})$$

and

$$\Delta_G((p\pi)^{-1}\widehat{w}_{-1}^{p^2}) \equiv \left((p\pi)^{-1}\widehat{w}_{-1}^{p^2}\right)\otimes 1 + 1\otimes\left((p\pi)^{-1}\widehat{w}_{-1}^{p^2}\right) \bmod \pi(\mathcal{R}\otimes_{A'}\mathcal{R}).$$

Equivalently, we want to show that

$$\Delta_G(\widehat{w}_0)^p \overset{?}{\equiv} \widehat{w}_0^p\otimes 1 + 1\otimes \widehat{w}_0^p \bmod \pi^2(\mathcal{R}\otimes_{A'}\mathcal{R})$$

and

$$\Delta_G(\widehat{w}_{-1})^{p^2} \overset{?}{\equiv} \widehat{w}_{-1}^{p^2}\otimes 1 + 1\otimes \widehat{w}_{-1}^{p^2} \bmod p\pi^2(\mathcal{R}\otimes_{A'}\mathcal{R}).$$

Once we prove the result for $\widehat{w}_0$, we can apply the same argument to $Vw \in M$. It is then straightfoward to keep track of powers of π in order to see that this gives the desired result modulo $p\pi^2$ for $\widehat{w}_{-1}$ (keep in mind that $F_0 w = 0$ forces $\widehat{w}_{-1}^p \in \pi\,\mathcal{R}$). So we now only consider the congruence for $\widehat{w}_0$.

Since $w \in M$, we have that in $\mathcal{R}_k\otimes_k\mathcal{R}_k$,

$$\Delta_{G_k}(w_0) = \lim_{N\to\infty} S_N(w_{-N}\otimes 1,\ldots,w_0\otimes 1; 1\otimes w_{-N},\ldots,1\otimes w_0),$$

whence

$$\Delta_G(\widehat{w}_0) \equiv \lim_{N\to\infty} S_N(\widehat{w}_{-N}\otimes 1,\ldots,\widehat{w}_0\otimes 1; 1\otimes \widehat{w}_{-N},\ldots,1\otimes \widehat{w}_0) \bmod \pi(\mathcal{R}\otimes_{A'}\mathcal{R}).$$

Because $S_N \in \mathbf{Z}[X_{-N},\ldots,X_0;Y_{-N},\ldots,Y_0]$ and $p \in \pi^2\,\mathcal{R}$ ($e > 1$!), we can raise both sides to the pth power so as to obtain

$$\Delta_G(\widehat{w}_0)^p \equiv \lim_{N\to\infty} S_N(\widehat{w}_{-N}^p\otimes 1,\ldots,\widehat{w}_0^p\otimes 1; 1\otimes \widehat{w}_{-N}^p,\ldots,1\otimes \widehat{w}_0^p) \bmod \pi^2(\mathcal{R}\otimes_{A'}\mathcal{R}).$$

Combining the property $\widehat{w}_{-n}^p \in \pi\,\mathcal{R}$ for all $n \geq 0$ with the fact that S_N is equal to $X_0 + Y_0$ plus higher degree terms in the X_{-j} and Y_{-j} for $j > 0$, it follows that

$$S_N(\widehat{w}_{-N}^p\otimes 1,\ldots,\widehat{w}_0^p\otimes 1; 1\otimes \widehat{w}_{-N}^p,\ldots,1\otimes \widehat{w}_0^p) \equiv \widehat{w}_0^p\otimes 1 + 1\otimes \widehat{w}_0^p \bmod \pi^2(\mathcal{R}\otimes_{A'}\mathcal{R})$$

for all $N \geq 1$. Thus, w'' as defined above is necessarily in M.

Therefore, we have shown that $1\otimes w \in \ker \mathcal{F}_M$ lies in the A'-submodule $V^M(\xi^M(\iota_M^{-1}(L[\mathfrak{m}])))$ if and only if *some* $\overline{w}' \in \mathcal{R}_k$ can be chosen so that $w' \in CW_k(\mathcal{R}_k)$ lies in M. That is, w is required to lie in $V_0 M$. This is equivalent to the assertion that the sequence

$$0 \to \ker \mathcal{F}_M / V^M(\xi^M(\iota_M^{-1}(L[\mathfrak{m}]))) \to M^{(1)}/V_0 M \xrightarrow{F} M/pM \to M/FM \to 0$$

is exact.

■

It may be possible to prove Theorem 3.3 purely from the definition of a finite Honda system (once Theorems 3.4 and 3.6 are proven), but it is not clear how to do this.

Theorem 3.4. *(L, M) is an object in $SH^f_{A'}$ when $e < p-1$ and (L, M) is an object in $SH^{f,u}_{A'}$ (resp. $SH^{f,c}_{A'}$) when $e \leq p-1$ and G is unipotent (resp. connected).*

Proof. Without loss of generality, $e \geq 2$. First, we will prove that the natural map

$$L/\mathfrak{m}L \to \operatorname{coker} \mathcal{F}_M$$

is injective, so $\ell_{A'}(L/\mathfrak{m}) \leq \ell_{A'}(\operatorname{coker} \mathcal{F}_M)$. We will then show that the natural map

$$L[\mathfrak{m}] \oplus \ker \mathcal{V}_M \to M_{A'}[\mathfrak{m}]$$

is surjective. By Lemma 2.4 and the second part of Lemma 2.7 (since $e \geq 2$), this surjectivity implies $\ell_{A'}(L/\mathfrak{m}) \geq \ell_{A'}(\operatorname{coker} \mathcal{F}_M)$, so this inequality is forced to be an equality and both maps above are isomorphisms. Using the first part of Lemma 2.7 then finishes the proof. The arguments we use are simply more elaborate versions of the arguments used in the case $e = 1$, except we need to keep track of the powers of π.

Choose $\ell \in L \subseteq M_{A'}$ lying in the image of $\mathcal{F}_M$, so there is an element

$$u = \sum_{j=1}^{e} p^{-1}\pi^j \otimes u_j \in p^{-1}\mathfrak{m} \otimes_A M^{(1)}$$

such that $\mathcal{F}_M(u) = \ell \in L$. Choosing ${u'}_j \in CW_k(\mathcal{R}_k)$ such that $V_0 {u'}_j = u_j$, this says that

$$\sum_{j=1}^{e} \pi^j w_{\mathcal{R}}({u'}_j) = 0$$

in $\mathcal{R}_{K'}/\mathfrak{m}\mathcal{R}$ (here, we have used the isomorphism supplied by [7, Ch IV, §2.7, Prop 2.5], applied to the D_k-module $CW_k(\mathcal{R}_k)$). We need to construct some $\ell' \in L$ such that $\ell = \pi\ell'$. We'll show that we can choose ${u'}_1 \in M$ (that is, $u_1 \in V_0(M)$) and then that this is enough to construct the desired ℓ'.

Let $\widehat{u}'_{i,-n} \in \mathcal{R}$ be a lift of ${u'}_{i,-n}$ ($= u_{i,-n+1}$ if $n \geq 1$), where ${u'}_{i,0} \in \mathcal{R}_k$ can be chosen at random for now. We're given that in $\mathcal{R}_{K'}$,

$$\sum_{j=0}^{e-1} \pi^j \left(\sum_{n=0}^{\infty} p^{-n} (\widehat{u}'_{j+1,-n})^{p^n} \right) \in \mathcal{R},$$

so changing $\widehat{u}'_{1,0}$ modulo $\mathcal{R}$ (i.e., changing ${u'}_{1,0}$), we can even assume that in $\mathcal{R}_{K'}$ we have the essential relation

$$\sum_{j=0}^{e-1} \pi^j \left(\sum_{n=0}^{\infty} p^{-n} (\widehat{u}'_{j+1,-n})^{p^n} \right) = 0.$$

Letting $\mathbf{u'}_i \in \widehat{CW}_A(\mathcal{R})$ denote the covector $(\widehat{u}'_{i,-n})$, the above can be rewritten as

$$\sum_{j=0}^{e-1} \pi^j \widehat{w}_{\mathcal{R}}(\mathbf{u'}_{j+1}) = 0.$$

See [7, Ch II, §5.1, Prop 5.1] (and also [7, Ch II, §5.6, Prop 5.4 Remark]) for a discussion of $\widehat{w}_{\mathcal{R}} : \widehat{CW}_A(\mathcal{R}) \to \mathcal{R}_{K'}$, defined analogously to $w_{\mathcal{R}} : \widehat{CW}_k(\mathcal{R}_k) \to \mathcal{R}_{K'}$. Define

$$\mathcal{L}_{-m}(\mathbf{u'}_i) = \lim_{N\to\infty} S_N(\widehat{u}'_{i,-N-m} \otimes 1, \ldots, \widehat{u}'_{i,-m} \otimes 1; 1 \otimes \widehat{u}'_{i,-N-m}, \ldots, 1 \otimes \widehat{u}'_{i,-m})$$

in $\mathcal{R}$. We first claim that for all $n \geq 1$,

$$\Delta_G(\widehat{u}'_{j,-n})^{p^n} \equiv \mathcal{L}_{-n}(\mathbf{u'}_j)^{p^n} \bmod p^n\pi(\mathcal{R} \otimes_{A'} \mathcal{R}).$$

Fix $n \geq 1$. Since $u_j \in M = \operatorname{Hom}_{\mathrm{gp-sch}_{/k}}(G_k, \widehat{CW}_k)$, we have that in $\mathcal{R}_k \otimes_k \mathcal{R}_k$,

$$\Delta_{G_k}(u_{j,-n+1}) = \lim_{N\to\infty} S_N(u_{j,-N-n+1} \otimes 1, \ldots, u_{j,-n+1}; 1 \otimes u_{j,-N-n+1}, \ldots, 1 \otimes u_{j,-n+1}),$$

which says exactly that

$$\Delta_G(\widehat{u}'_{j,-n}) \equiv \mathcal{L}_{-n}(\mathbf{u'}_j) \bmod \pi(\mathcal{R}\otimes_{A'}\mathcal{R}).$$

Since $\pi^p = \pi\cdot\pi^{p-1} \in p\pi\,\mathcal{R}$, as $e \leq p-1$ (!), we can raise both sides to the pth power in order to get

$$\Delta_G(\widehat{u}'_{j,-n})^p \equiv \mathcal{L}_{-n}(\mathbf{u'}_j)^p \bmod p\pi(\mathcal{R}\otimes_{A'}\mathcal{R}).$$

An easy induction now shows that

$$\Delta_G(\widehat{u}'_{j,-n})^{p^r} \equiv \mathcal{L}_{-n}(\mathbf{u'}_j)^{p^r} \bmod p^r\pi(\mathcal{R}\otimes_{A'}\mathcal{R})$$

for all $r \geq 1$, so taking $r = n$ gives what we claimed above.

This can be conveniently rewritten as

$$p^{-n}\Delta_G(\widehat{u}'_{j,-n})^{p^n} \equiv p^{-n}\mathcal{L}_{-n}(\mathbf{u'}_j)^{p^n} \bmod \pi(\mathcal{R}\otimes_{A'}\mathcal{R}),$$

but be careful to note that the terms in this congruence generally lie in $(\mathcal{R}\otimes_{A'}\mathcal{R})_{K'} \simeq \mathcal{R}_{K'}\otimes_{K'}\mathcal{R}_{K'}$ and not in $\mathcal{R}\otimes_{A'}\mathcal{R}$. Summing over $n \geq 1$, we obtain

$$\sum_{n\geq 1} p^{-n}\Delta_G(\widehat{u}'_{j,-n})^{p^n} \equiv \sum_{n\geq 1} p^{-n}\mathcal{L}_{-n}(\mathbf{u'}_j)^{p^n} \bmod \pi(\mathcal{R}\otimes_{A'}\mathcal{R}).$$

From what we have so far, we may deduce that in $\mathcal{R}_{K'}\otimes_{K'}\mathcal{R}_{K'}$,

$$\begin{aligned}
\sum_{j=0}^{e-1}\pi^j\sum_{n\geq 1}p^{-n}\Delta_G(\widehat{u}'_{j+1,-n})^{p^n} &= \sum_{j=0}^{e-1}\pi^j\sum_{n\geq 1}p^{-n}\Delta_{G_{K'}}(\widehat{u}'_{j+1,-n})^{p^n}\\
&= \Delta_{G_{K'}}\left(\sum_{j=0}^{e-1}\pi^j\sum_{n\geq 1}p^{-n}(\widehat{u}'_{j+1,-n})^{p^n}\right)\\
&= -\Delta_{G_{K'}}\left(\sum_{j=0}^{e-1}\pi^j\widehat{u}'_{j+1,0}\right)\\
&= -\Delta_{G}\left(\sum_{j=0}^{e-1}\pi^j\widehat{u}'_{j+1,0}\right),
\end{aligned}$$

so in fact the element

$$\sum_{j=0}^{e-1}\pi^j\sum_{n\geq 1}p^{-n}\mathcal{L}_{-n}(\mathbf{u'}_j)^{p^n} \in \mathcal{R}_{K'}\otimes_{K'}\mathcal{R}_{K'}$$

lies in $\mathcal{R}\otimes_{A'}\mathcal{R}$ and modulo $\pi(\mathcal{R}\otimes_{A'}\mathcal{R})$ is congruent to

$$-\Delta_G\left(\sum_{j=0}^{e-1}\pi^j\widehat{u}'_{j+1,0}\right).$$

Since *by definition*

$$(\mathcal{L}_{-n}(\mathbf{u'}_j)) = (\widehat{u}'_{j,-n}\otimes 1) + (1\otimes\widehat{u}'_{j,-n})$$

in $\widehat{CW}_A(\mathcal{R}\otimes_{A'}\mathcal{R})$ and $\widehat{w}_{\mathcal{R}}$ is additive, in $\mathcal{R}_{K'}\otimes_{K'}\mathcal{R}_{K'}$ we apply $\widehat{w}_{\mathcal{R}}$ to get

$$\mathcal{L}_0(\mathbf{u'}_j) + \sum_{n\geq 1}p^{-n}\mathcal{L}_{-n}(\mathbf{u'}_j)^{p^n} = \widehat{w}_{\mathcal{R}}(\mathbf{u'}_j)\otimes 1 + 1\otimes\widehat{w}_{\mathcal{R}}(\mathbf{u'}_j).$$

Therefore, modulo $\pi(\mathcal{R} \otimes_{A'} \mathcal{R})$, we have

$$\begin{aligned}
\Delta_G\left(\sum_{j=0}^{e-1} \pi^j \widehat{u}'_{j+1,0}\right) &\equiv -\sum_{j=0}^{e-1} \pi^j \sum_{n\geq 1} p^{-n} \mathcal{L}_{-n}(\mathbf{u'}_{j+1})^{p^n} \\
&\equiv \sum_{j=0}^{e-1} \pi^j \mathcal{L}_0(\mathbf{u'}_j) - \left(\sum_{j=0}^{e-1} \pi^j \widehat{w}_{\mathcal{R}}(\mathbf{u'}_{j+1})\right) \otimes 1 - 1 \otimes \left(\sum_{j=0}^{e-1} \pi^j \widehat{w}_{\mathcal{R}}(\mathbf{u'}_{j+1})\right) \\
&= \sum_{j=0}^{e-1} \pi^j \mathcal{L}_0(\mathbf{u'}_j)
\end{aligned}$$

(recall $\sum \pi^j \widehat{w}_{\mathcal{R}}(\mathbf{u'}_{j+1}) = 0$). Hence,

$$\Delta_G(\widehat{u}'_{1,0}) \equiv \mathcal{L}_0(\mathbf{u'}_1) \bmod \pi(\mathcal{R} \otimes_{A'} \mathcal{R}),$$

which says exactly that $u'_1 \in M$ (since $u'_{1,-j} = u_{1,-j+1}$ for $j \geq 1$ and $u_1 \in M$, so the 0th coordinate of u'_1 is all we need to check).

Now we define $\ell' \in M_{A'}$ and we will show that $\ell' \in L$ and $\pi\ell' = \ell$. In terms of our original explicit description of $M_{A'}$ as a quotient module, define ℓ' to be the element represented by

$$\left(1 \otimes u'_1, \sum_{j=1}^{e-1} p^{-1}\pi^j \otimes u_{j+1}\right).$$

Thus,

$$w'_{\mathcal{R}}(\ell') = w_{\mathcal{R}}(u'_1) + \sum_{j=1}^{e-1} \pi^j w_{\mathcal{R}}(u'_{j+1})$$

is represented by

$$\sum_{j=0}^{e-1} \pi^j \widehat{w}_{\mathcal{R}}(\mathbf{u'}_{j+1}) = 0,$$

so $\ell' \in L$. Also,

$$\begin{aligned}
\pi\ell' &= \overline{(\pi \otimes u'_1, 0)} + \overline{\left(0, \sum_{j=2}^{e} p^{-1}\pi^j \otimes u_j\right)} \\
&= \overline{(0, p^{-1}\pi \otimes V_0 u'_1)} + \overline{\left(0, \sum_{j=2}^{e} p^{-1}\pi^j \otimes u_j\right)} \\
&= \overline{(0, p^{-1}\pi \otimes u_1)} + \overline{\left(0, \sum_{j=2}^{e} p^{-1}\pi^j \otimes u_j\right)} \\
&= \mathcal{F}_M(u),
\end{aligned}$$

which is equal to ℓ. This completes the proof of injectivity of $L/\mathfrak{m} \to \operatorname{coker} \mathcal{F}_M$.

As we explained at the beginning, it remains to prove that the natural k-linear map

$$L[\mathfrak{m}] \oplus \ker \mathcal{V}_M \to M_{A'}[\mathfrak{m}]$$

is surjective. Since $e \geq 2$, the second part of Lemma 2.7 shows that it necessary and sufficient to prove that for $w \in \ker F_0$, there exists $u \in \ker V_0$ such that the element

$$\overline{(1 \otimes u, p^{-1}\pi^{e-1} \otimes w)} \in M_{A'}[\mathfrak{m}]$$

lies in L. We may write $w = (w_{-n})$ in $CW_k(\mathcal{R}_k)$, with $w_{-n} \in \mathcal{R}_k$ satisfying $w_{-n}^p = 0$ for all $n \geq 0$. Choose $u_1, w_1 \in \mathcal{R}_k$ and consider

$$u = (\dots, 0, \dots, 0, u_1), \quad \tilde{w} = (\dots, w_{-n+1}, \dots, w_0, w_1) \in CW_k(\mathcal{R}_k),$$

so $Vu = 0$ and $V\tilde{w} = w$ in $CW_k(\mathcal{R}_k)$. In $CW_{k,A'}(\mathcal{R}_k)$, we have

$$\overline{(1 \otimes u, p^{-1}\pi^{e-1} \otimes w)} = \iota_{CW_k(\mathcal{R}_k)}(1 \otimes u + \pi^{e-1} \otimes \tilde{w}),$$

so

$$w'_{\mathcal{R}}(\overline{(1 \otimes u, p^{-1}\pi^{e-1} \otimes w)}) = \widehat{u}_1 + \pi^{e-1}\left(\sum_{n=0}^{\infty} p^{-n}\widehat{w}_{1-n}^{p^n}\right) \bmod \pi\,\mathcal{R}$$

inside of $\mathcal{R}_{K'}/\mathfrak{m}\,\mathcal{R}$, with $\widehat{u}_1 \in \mathcal{R}$ a lift of u_1. Since $e \geq 2$ and $\widehat{w}_{-m}^p \in \pi\,\mathcal{R}$ for all $m \geq 0$, clearly $\pi^{e-1}p^{-n}\widehat{w}_{1-n}^{p^n} \in \pi\,\mathcal{R}$ for $n \geq 3$ and $n = 0$.

Thus, we are reduced to checking that for

$$u_1 = -\pi^{e-1}(p^{-1}\widehat{w}_0^p + p^{-2}\widehat{w}_{-1}^{p^2}) = -\epsilon^{-1}((p\pi)^{-1}\widehat{w}_{-1}^{p^2} + \pi^{-1}\widehat{w}_0^p) \bmod \pi\,\mathcal{R},$$

we have $u \in M$ (since $e \leq p-1$, the right side does lie in $\mathcal{R}$). Since $e \geq 2$, this is *exactly* the same calculation we did at the end of the proof of Theorem 3.3 (up to the factor of $\epsilon^{-1} \in A'^{\times}$, which can be cancelled at the start).

■

Theorem 3.5. *The sequence*

$$0 \to M/V \xrightarrow{F} M/p \to M/F \to 0$$

is exact if and only if there is equality in Lemma 3.1. *This exactness condition is satisfied when $G \simeq \Gamma[p^n]$ for $\Gamma_{/A'}$ a p-divisible group.*

Proof. Thanks to Theorem 3.3, all we have to verify is the short exact sequence condition when G is the full p^n torsion of a p-divisible group. This is standard: since $M/p \simeq \mathcal{M}(G[p]_k)$, it is enough to pick $\Gamma_{/k}$ a p-divisible group and to check that for $\mathbf{M} = \mathcal{M}(\Gamma)$, the sequence

$$0 \to \mathbf{M}/V \xrightarrow{F} \mathbf{M}/p \to \mathbf{M}/F \to 0$$

is not just right exact but is actually exact. The A-module underlying $\mathbf{M}$ is finite and free with $p = VF$, so F acts *injectively.* Thus, $Fm = pm' = FVm'$ yields $m = Vm'$, as desired.

■

We now come to the essential result.

Theorem 3.6. *$LM_{A'}$ is fully faithful and essentially surjective when $e < p-1$. This is also true for $LM_{A'}^u$ and $LM_{A'}^c$ when $e \leq p-1$.*

Proof. The argument is a generalization of the steps in the proof of Theorem 1.4. As before, when $e = p-1$ we stick with the unipotent case for now, and will return to the connected case at the end. First, let's show that Step 1 holds for any G in $\mathcal{FF}_{A'}$ and any finite flat A'-algebra $\mathcal{S}$. Essentially the same argument works for $e \leq p-1$, since Raynaud's results [17, §3] apply whenever $e \leq p-1$. More precisely, because we are claiming Step 1 goes through for all objects in $\mathcal{FF}_{A'}$ for $e < p-1$ and for all objects in $\mathcal{FF}_{A'}^u$ when $e \leq p-1$, as in the case $e = 1 \leq p-1$ we can reduce the proof of the injectivity of

$$G(\mathcal{S}) \to G_k(\mathcal{S}_k)$$

to the case where A' is strictly Henselian with algebraically closed residue field k and $G_{K'}$ is a simple object in the category of finite commutative K'-group schemes. In this case, we can argue exactly as we did in Step 1 in the proof of Theorem 1.4.

With the analogue of Step 1 pushed through, it is now straightfoward to see that Step 2 makes sense for any G in $\mathcal{FF}_{A'}$, where we use $CW_{k,A'}$ in place of CW_k, $w'_{\mathcal{R}}$ and $w'_{\mathcal{S}}$ in place of $w_{\mathcal{R}}$ and $w_{\mathcal{S}}$ respectively, and we define the functor from finite flat A'-algebras to **Ab** via the formula

$$\underline{G}(\mathcal{S}) = \{\gamma \in G_k(\mathcal{S}_k) \,|\, CW_{k,A'}(\gamma)(L) \subseteq \ker w'_{\mathcal{S}}\}.$$

Via Fontaine's classification of p-divisible groups over A' [7, Ch IV, §5, Prop 5.1(i)], the assertion in Step 3 applies whenever $e \le p-1$, using unipotence conditions and the remark following [7, Ch IV, §4.8, Lemma 4.10] in case $e = p-1$. It is only necessary to make minor notational changes in the $e = 1$ argument ($CW_{k,A'}$ replacing CW_k, etc.).

Next, we prove the analogue of the difficult Step 4. Choose an object (L, M) in $SH^f_{A'}$ if $e < p-1$. If $e = p-1$, choose an object (L, M) in $SH^{f,u}_{A'}$. We will construct an object $G_{(L,M)}$ in $\mathcal{FF}_{A'}$ (resp. in $\mathcal{FF}^u_{A'}$) which is the kernel of an isogeny of p-divisible groups over A' (resp. of unipotent p-divisible groups over A') such that $(L, M) \simeq LM_{A'}(G_{(L,M)})$ in $SH^f_{A'}$ (resp. $(L, M) \simeq LM^u_{A'}(G_{(L,M)})$ in $SH^{f,u}_{A'}$) when $e < p-1$ (resp. when (L, M) lies in $SH^{f,u}_{A'}$).

As in the $e = 1$ argument, we can construct an exact sequence of D_k-modules

$$0 \to M_2 \xrightarrow{i} M_1 \xrightarrow{\mathcal{P}} M \to 0$$

with the M_i free of finite rank over A, so $M_i \simeq \mathcal{M}(\overline{\Gamma}_i)$ for $\overline{\Gamma}_i$ a p-divisible group over k. If V acts in a nilpotent manner on M, we can choose the $\overline{\Gamma}_i$ to be unipotent p-divisible groups. Note that the sequence of A'-modules

$$0 \to (M_2)_{A'} \xrightarrow{i'} (M_1)_{A'} \xrightarrow{\mathcal{P}'} M_{A'} \to 0$$

is not just right exact [7, Ch IV, §2, Prop 2.4], but actually exact. This is simply because by the remark in [7, Ch IV, §2.3], we have a *canonical* isomorphism of A'-modules

$$A' \otimes_A N + p^{-1}\mathfrak{m} \otimes_A FN \simeq N_{A'}$$

whenever N is free of finite rank as an A-module (and the left side is viewed as a sum inside of $K' \otimes_A N$). For notational ease, we now adopt Fontaine's notation $X_{A'}[1] = p^{-1}\mathfrak{m} \otimes_A X^{(1)}$ for a D_k-module X [7, Ch IV, §2.4ff]. The natural map $N_{A'}[1] \to N_{A'}$ of A'-modules is injective and via the above isomorphism is identified with the submodule $p^{-1}\mathfrak{m} \otimes_A FN$, so we can safely write $N_{A'}/N_{A'}[1]$ in place of $\operatorname{coker} \mathcal{F}_N$ if we prefer (for such N). Also, recall [7, Ch IV, §2.5, Cor 1] that there is even a canonical k-linear isomorphism

$$N/FN \simeq N_{A'}/N_{A'}[1].$$

This is analogous to the isomorphism $\operatorname{coker} F_0 \simeq \operatorname{coker} \mathcal{F}_M$ in Lemma 2.4.

What we will now do is construct A'-submodules $\mathcal{L}_i \hookrightarrow (M_i)_{A'}$ such that the natural k-linear maps

$$\mathcal{L}_i/\mathfrak{m}\mathcal{L}_i \to (M_i)_{A'}/(M_i)_{A'}[1] \simeq \operatorname{coker} \mathcal{F}_{M_i}$$

are isomorphisms, $(M_2)_{A'} \hookrightarrow (M_1)_{A'}$ takes $\mathcal{L}_2$ over into $\mathcal{L}_1$, and the image of $\mathcal{L}_1$ under $(M_1)_{A'} \twoheadrightarrow M_{A'}$ is precisely L. Once these A'-modules $\mathcal{L}_1$ and $\mathcal{L}_2$ are constructed, the rest of the argument is exactly like that in Step 4 in the case $e = 1$, with minor changes in notation.

We construct $\mathcal{L}_1$ as in the case $e = 1$. That is, we can either use the isomorphism $\operatorname{coker} F_0 \simeq \operatorname{coker} \mathcal{F}_M$ in Lemma 2.4 and its analogue above for M_1 and M_2 in order to literally use the $e = 1$ construction word-for-word, or alternatively (which amounts to the same thing) we choose

$$\overline{e}_1, \ldots, \overline{e}_r \in (M_1)_{A'}/(M_1)_{A'}[1] \simeq \operatorname{coker} \mathcal{F}_{M_1}$$

giving a basis for the image of $(M_2)_{A'}/(M_2)_{A'}[1]$, with representatives $e_i \in (M_2)_{A'} \subseteq (M_1)_{A'}$. Let $\overline{e}_{r+1}, \ldots, \overline{e}_n$ extend this to a full k-basis of $(M_1)_{A'}/(M_1)_{A'}[1] = \operatorname{coker} \mathcal{F}_{M_1}$, so the images of $\overline{e}_{r+1}, \ldots, \overline{e}_n$ in $M_{A'}/M_{A'}[1]$ give a k-basis of

$$\operatorname{coker} \mathcal{F}_M \xleftarrow{\sim} L/\mathfrak{m}L.$$

Therefore we may (and do) choose representatives $e_{r+1}, \ldots, e_n \in (M_1)_{A'}$ so that their images in $M_{A'}$ under $\mathcal{P}'$ lie in L and constitute a minimal A'-basis of L. Define $\mathcal{L}_1 = \sum A' e_i$.

The natural map
$$\mathcal{L}_1/\mathfrak{m}\mathcal{L}_1 \to \operatorname{coker} \mathcal{F}_{M_1}$$
is clearly an isomorphism and the composite map of A'-modules
$$\mathcal{L}_1 \hookrightarrow (M_1)_{A'} \twoheadrightarrow M_{A'}$$
has image precisely L.

In order to construct $\mathcal{L}_2$ as in the case $e = 1$, the only issue is to check that any $x \in ((M_1)_{A'}[1]) \cap (M_2)_{A'}$ can be represented in $(M_2)_{A'}/(M_2)_{A'}[1]$ by an element of $\mathcal{L}_1 \cap (M_2)_{A'}$. Then the construction of $\mathcal{L}_2$ will go through as desired. At this point, we can (and will) assume $e > 1$.

We have the exact sequence of A'-modules
$$0 \to A' \otimes_A M_2 + p^{-1}\mathfrak{m} \otimes FM_2 \xrightarrow{i'} A' \otimes_A M_1 + p^{-1}\mathfrak{m} \otimes FM_1 \xrightarrow{\mathcal{P}'} M_{A'} \to 0$$
with i' the 'inclusion' map and (using $FM_1 = F_0 M_1^{(1)}$)
$$\mathcal{P}' : \lambda \otimes m + \mu \otimes F_0 m' \mapsto \overline{(\lambda \otimes \mathcal{P}(m), \mu \otimes \mathcal{P}(m'))}.$$
Also, note that since $e > 1$, we have (in obvious notation) the A-module decomposition
$$(M_i)_{A'} = A' \otimes_A M_i + p^{-1}\mathfrak{m} \otimes_A FM_i = (1 \otimes M_i) \oplus (p^{-1}\pi \otimes FM_i) \oplus \cdots \oplus (p^{-1}\pi^{e-1} \otimes FM_i).$$
We can suppose without loss of generality that $x \in A' \otimes_A M_2$ and by hypothesis x (or rather, $i'(x)$) lies in $p^{-1}\mathfrak{m} \otimes_A FM_1$, which says
$$i'(x) = 1 \otimes F_0 m + \sum_{j=1}^{e-1} \pi^j \otimes m_j,$$
with $m_j \in M_2$ and $m \in M_1^{(1)}$, $F_0 m \in M_2$. For $1 \le j \le e-1$, we have
$$\pi^j \otimes m_j = p^{-1}\pi^j \otimes pm_j \in (M_2)_{A'}[1],$$
so by altering x, we can assume without loss of generality that $m_1 = \cdots = m_{e-1} = 0$, which is to say
$$i'(x) = 1 \otimes F_0 m,$$
where $m \in M_1^{(1)}$ and $F_0 m \in M_2$. Since $\mathcal{P}'(i'(x)) = 0$, we see that the element $1 \otimes \mathcal{P}(m) \in M_{A'}[1]$ maps to 0 in $M_{A'}$, which is to say that it lies in $\ker \mathcal{F}_M$.

Consider the isomorphism
$$\psi^M = \psi^M_\pi : p^{-1}\mathfrak{m} \otimes_A M^{(1)} \simeq A' \otimes_A M^{(1)}$$
given by $\psi^M(a \otimes n) = \pi^{e-1} a \otimes n$. If we combine the isomorphisms
$$\ker V_0 \oplus \ker F_0 \simeq M_{A'}[\mathfrak{m}]$$
and
$$\ker \mathcal{V}_M \oplus L[\mathfrak{m}] \simeq M_{A'}[\mathfrak{m}],$$
we compute that $\mathcal{V}_M(L[\mathfrak{m}]) = \mathcal{V}_M(M_{A'}[\mathfrak{m}]) = \psi^M(\ker \mathcal{F}_M)$. Thus, there exists some $x \in L[\mathfrak{m}]$ such that
$$\pi^{e-1} \otimes \mathcal{P}(m) = \mathcal{V}_M(x).$$
By the second part of Lemma 2.7, we can write $x = \overline{(1 \otimes v, p^{-1}\pi^{e-1} \otimes w)}$ with $v \in \ker V_0$ and $w \in \ker F_0$. Since $\mathcal{V}_M(x) = \pi^{e-1} \otimes w$, it follows that $w = \mathcal{P}(m)$. Therefore we get a critical link between m and L, namely the element
$$\overline{(1 \otimes v, p^{-1}\pi^{e-1} \otimes \mathcal{P}(m))} \in M_{A'}$$
actually lies in $L[\mathfrak{m}]$, with $v \in \ker V_0$.

By construction, $(M_1)_{A'} \twoheadrightarrow M_{A'}$ takes $\mathcal{L}_1$ *onto* L, so there exists an $\ell_1 \in \mathcal{L}_1$ such that
$$\mathcal{P}'(\ell_1) = \overline{(1 \otimes v, p^{-1}\pi^{e-1} \otimes \mathcal{P}(m))}$$

in $M_{A'}$. Inside of $(M_1)_{A'} = A' \otimes_A M_1 + p^{-1}\mathfrak{m} \otimes FM_1$, we can write (using $FM_1 = F_0 M_1^{(1)}$)

$$\ell_1 = 1 \otimes y + \sum_{r=1}^{e-1} p^{-1}\pi^r \otimes F_0 z_r,$$

so

$$\mathcal{P}'(\ell_1) = \overline{\left(1 \otimes \mathcal{P}(y), \sum_{r=1}^{e-1} p^{-1}\pi^r \otimes \mathcal{P}(z_r)\right)}.$$

Comparing our two formulas for $\mathcal{P}'(\ell_1)$, there exist $u \in \mathfrak{m} \otimes_A M$ and $w \in A' \otimes_A M^{(1)}$ such that

$$\left(1 \otimes (\mathcal{P}(y) - v), \sum_{r=1}^{e-2} p^{-1}\pi^r \otimes \mathcal{P}(z_r) + p^{-1}\pi^{e-1} \otimes \mathcal{P}(z_{e-1} - m)\right) = (\varphi_0^M(u) - F^M(w), \varphi_1^M(w) - V^M(u)).$$

However, in $M_{A'}[1]$ we have

$$\begin{aligned} \pi \cdot (\varphi_1^M(w) - V^M(u)) + V^M(\xi^M(\varphi_0^M(u) - F^M(w))) &= \pi\varphi_1^M(w) - V^M\xi^M(F^M(w)) \\ &= 0, \end{aligned}$$

and so in $M_{A'}[1]$,

$$\begin{aligned} 0 &= \sum_{r=1}^{e-2} p^{-1}\pi^{r+1} \otimes \mathcal{P}(z_r) + \big(p^{-1}\pi^e \otimes \mathcal{P}(z_{e-1} - m) + p^{-1}\pi \otimes V_0(\mathcal{P}(y) - v)\big) \\ &= \sum_{r=1}^{e-2} p^{-1}\pi^{r+1} \otimes \mathcal{P}(z_r) + p^{-1}\pi^e \otimes \mathcal{P}(z_{e-1} - m) + p^{-1}\pi \otimes V_0(\mathcal{P}(y)), \end{aligned}$$

since $v \in \ker V_0$.

Thus, the elements $\epsilon \otimes m = p^{-1}\pi^e \otimes m$ and $p^{-1}\pi \otimes V_0 y + \sum_{r=1}^{e-1} p^{-1}\pi^{r+1} \otimes z_r$ in $(M_1)_{A'}[1]$ have the same image in $M_{A'}[1]$ under $\mathcal{P}'$. Now the sequence of A'-modules

$$0 \to (M_2)_{A'}[1] \to (M_1)_{A'}[1] \to M_{A'}[1] \to 0$$

is the same as

$$0 \to p^{-1}\mathfrak{m} \otimes_A M_2^{(1)} \to p^{-1}\mathfrak{m} \otimes_A M_1^{(1)} \to p^{-1}\mathfrak{m} \otimes_A M^{(1)} \to 0,$$

which is exact since $N \rightsquigarrow N^{(1)}$ is exact from the category of A-modules to itself and $p^{-1}\mathfrak{m}$ is a flat A-module.

Therefore, the elements $\epsilon \otimes m$ and $p^{-1}\pi \otimes V_0 y + \sum_{r=1}^{e-1} p^{-1}\pi^{r+1} \otimes z_r$ in $(M_1)_{A'}[1]$ differ by an element of $(M_2)_{A'}[1]$, so $\epsilon i'(x) = \epsilon \otimes F_0 m$ differs from

$$\begin{aligned} p^{-1}\pi \otimes F_0 V_0 y + \sum_{r=1}^{e-1} p^{-1}\pi^{r+1} \otimes F z_r &= \pi \otimes y + \sum_{r=1}^{e-1} p^{-1}\pi^{r+1} \otimes F z_r \\ &= \pi\ell_1 \end{aligned}$$

by an element of $(M_2)_{A'}[1]$. In particular, $\pi\ell_1$ lies in $(M_2)_{A'}$ inside of $(M_1)_{A'}$. But $\pi\ell_1 \in \mathcal{L}_1$, so $\epsilon^{-1}\pi\ell_1 \in \mathcal{L}_1 \cap (M_2)_{A'}$ is the desired element which represents $x \in (M_2)_{A'}$ in $(M_2)_{A'}/(M_2)_{A'}[1]$. Note that since $\mathcal{L}_1/\mathfrak{m}\mathcal{L}_1 \simeq \operatorname{coker} \mathcal{F}_{M_1}$ by construction of $\mathcal{L}_1$, the image of x in $\mathcal{L}_1$ must a priori lie in $\mathfrak{m}\mathcal{L}_1 = \pi\mathcal{L}_1$. Thus, the presence of π in the above representative $\epsilon^{-1}\pi\ell_1$ for x is not unexpected.

The argument for Step 5 goes through exactly as in the case $e = 1$.

When $e = p - 1$ and we consider connected objects, the modifications to the above argument exactly parallel the changes needed for the connected case with $p = 2$ in the proof of Theorem 1.4. Note that in order to handle the variant on $w_{\mathcal{S}}$ which will arise, the inequality $p^n - ne \geq 0$ will arise for all $n \geq 1$, and this is satisfied for $e \leq p - 1$.

■

Corollary 3.7. *The additive functor $\mathcal{FF}_{A'} \to \mathcal{FF}_k$ given by $G \rightsquigarrow G_k$ is faithful when $e < p - 1$. The analogous additive functors $\mathcal{FF}^u_{A'} \to \mathcal{FF}^u_k$ and $\mathcal{FF}^c_{A'} \to \mathcal{FF}^c_k$ are faithful when $e \leq p - 1$.*

Proof. A morphism of finite Honda systems $(L_1, M_1) \to (L_2, M_2)$ vanishes if and only if the associated map $M_1 \to M_2$ vanishes. ∎

4. Classification of Group Schemes when $e \le p-1$

We begin by recalling a result due to Raynaud, extending Corollary 1.5.

Lemma 4.1. (*Raynaud*) *If $e < p-1$, the category $\mathfrak{FF}_{A'}$ is stable under formation of scheme-theoretic kernels and is an abelian category. A morphism is a kernel if and only if it is a closed immersion and is a cokernel if and only if it is faithfully flat. The formation of the cokernel of a closed immersion is as usual. The same assertions holds for $\mathfrak{FF}^u_{A'}$ and $\mathfrak{FF}^c_{A'}$ if $e \le p-1$.*

The functor $G \rightsquigarrow G_{K'}$ which associates to every object of $\mathfrak{FF}_{A'}$ its K'-group scheme generic fiber is a fully faithful exact functor when $e < p-1$. The same is true on $\mathfrak{FF}^u_{A'}$ when $e \le p-1$.

A sequence $G' \to G \to G''$ in $\mathfrak{F}_{A'}$ for $e < p-1$ (resp. in $\mathfrak{FF}^c_{A'}$, $\mathfrak{FF}^u_{A'}$ for $e = p-1$) is exact if and only if the closed fiber sequence is exact if and only if the generic fiber sequence is exact.

Remark 4.2. The analogue of Theorem 1.9 also carries over to the $e \le p-1$ setting by the same arguments which we used in the $e = 1$ case.

Proof. The second part follows from the first part, just as in the way we deduced Corollary 1.6 from Corollary 1.5 earlier.

Now we consider the first part. When $e < p-1$, this is essentially [17, Cor 3.3.6(1)], together with the fact that a closed subgroup scheme and a quotient of a unipotent object is again unipotent (as this can be detected on the closed fiber, where it follows from Cartier duality and the canonical splitting of the closed fiber connected-étale sequence).

When $e = p-1$ and we consider only unipotent objects, the proof of [17, Cor 3.3.6(1)] still goes through, since we may use [17, Prop 3.3.2(3)] to carry over [17, Thm 3.3.3] to the present setting. The connected case then follows by the exactness of Cartier duality.

Since passage to the generic fiber is an exact functor and all of our categories are abelian, the final part of the assertion comes down to the statement that a morphism $f : G_1 \to G_2$ is an isomorphism (resp. 0) if and only if this is true on the closed fiber if and only if this is true on the generic fiber. For the generic fiber, use full faithfulness of $G \rightsquigarrow G_{K'}$. For the closed fiber, the vanishing part follows from faithfulness of passage to the closed fibers, while the isomorphism part follows from Nakayama's Lemma and flatness. ∎

Now that we know $LM_{A'}$ and $LM^u_{A'}$ are fully faithful and essentially surjective, it follows from Lemma 4.1 that $SH^f_{A'}$ is an abelian category when $e < p-1$ and $SH^{f,u}_{A'}$, $SH^{f,c}_{A'}$ are abelian categories when $e \le p-1$. Of course, $SH^f_{A'}$, $SH^{f,u}_{A'}$, and $SH^{f,c}_{A'}$ are full subcategories of the abelian category $PSH^f_{A'}$, so there are obvious candidates for what kernels and cokernels should be. More precisely, it is reasonable to expect that the composite functors $\mathfrak{FF}_{A'} \to PSH^f_{A'}$ and $\mathfrak{FF}^u_{A'}, \mathfrak{FF}^c_{A'} \to PSH^f_{A'}$ (for $e < p-1$ and $e \le p-1$ respectively) are exact. We now prove that this is indeed the case.

Theorem 4.3. *When $e < p-1$, the functor $\mathfrak{FF}_{A'} \to PSH^f_{A'}$ is exact. When $e \le p-1$, the functors $\mathfrak{FF}^c_{A'}, \mathfrak{FF}^u_{A'} \to PSH^f_{A'}$ are exact. More precisely, if*

$$\varphi : (L_1, M_1) \to (L_2, M_2)$$

is a morphism in $SH^f_{A'}$ with $e < p-1$ (resp. is a morphism in $SH^{f,c}_{A'}$, $SH^{f,u}_{A'}$ with $e \le p-1$), then $\ker\varphi = (L', M')$ and $\operatorname{coker}\varphi = (L'', M'')$ satisfy

$$M' = \ker(M_1 \to M_2), \;\; M'' = \operatorname{coker}(M_1 \to M_2)$$

and

$$L' = (M')_{A'} \cap L_1, \;\; L'' = \operatorname{image}(L_2 \hookrightarrow (M_2)_{A'} \twoheadrightarrow (M'')_{A'}),$$

and the natural map $\operatorname{coker}(L_1 \to L_2) \twoheadrightarrow L''$ is an isomorphism.

Proof. We give the argument in the case $e < p-1$. When $e \leq p-1$ and we impose unipotence or connectedness conditions, the argument is proceeds in exactly the same way.

Let G_i be an object in $\mathcal{FF}_{A'}$ such that $LM_{A'}(G_i) \simeq (L_i, M_i)$, so $\varphi = LM_{A'}(f)$ for $f : G_2 \to G_1$ a morphism in the category $\mathcal{FF}_{A'}$.

Define $(L', M') = LM_{A'}(\operatorname{coker} f)$ and $(L'', M'') = LM_{A'}(\ker f)$ to be the respective images under $LM_{A'}$ of the cokernel and kernel of the corresponding morphism f in $\mathcal{FF}_{A'}$. It is easy to see that M' and M'' are as claimed (on the group scheme side, one simply notes that passage to the closed fiber commutes with formation of short exact sequences, and then one applies the *exact* contravariant Dieudonné-module functor to everything). Let's (temporarily) define $\mathcal{L}' = (M')_{A'} \cap L_1 = \ker(L_1 \to L_2)$ and also

$$\mathcal{L}'' = \operatorname{image}(L_2 \hookrightarrow (M_2)_{A'} \twoheadrightarrow (M'')_{A'}),$$

so $L' \subseteq \mathcal{L}'$ and $\mathcal{L}'' \subseteq L''$. We must prove that these inclusions of A'-modules are equalities and that $\mathcal{L}''$ is the cokernel of $L_1 \to L_2$.

For the assertion about $\ker \varphi = (L', M')$, clearly we can (and will) assume that f is a monomorphism. Since monomorphisms in $\mathcal{FF}_{A'}$ are the same thing as closed immersions of group schemes, we see that the group scheme G_1/G_2 makes sense in $\mathcal{FF}_{A'}$ and there is a natural $PSH^f_{A'}$-morphism $\ker(\varphi) = LM_{A'}(G_1/G_2) \to (\mathcal{L}', M')$ which is an isomorphism on the Dieudonné module part. We wish to show that this map must be an isomorphism in $PSH^f_{A'}$. If we let $\mathcal{R}_i$ denote the affine ring of G_i and let $\mathcal{R}$ denote the affine ring of G_1/G_2, then the map of A'-algebras $\mathcal{R} \to \mathcal{R}_1$ is not only injective but is also *faithfully flat*. Therefore, $\mathfrak{m}\,\mathcal{R} = \mathcal{R} \cap \mathfrak{m}\,\mathcal{R}_1$ [13, Thm 7.5(*ii*)], so

$$\mathcal{R}_{K'}/\mathfrak{m}\,\mathcal{R} \to (\mathcal{R}_1)_{K'}/\mathfrak{m}\,\mathcal{R}_1$$

is *injective*. Combining this with the injectivity of $(M')_{A'} \to (M_1)_{A'}$ (see Lemma 2.1), it follows easily from the commutative diagram

$$\begin{array}{ccc}
(M')_{A'} & \hookrightarrow & (M_1)_{A'} \\
\big\downarrow & & \big\downarrow \\
CW_{k,A'}(\mathcal{R}_k) & \longrightarrow & CW_{k,A'}((\mathcal{R}_1)_k) \\
\big\downarrow & & \big\downarrow \\
\mathcal{R}_{K'}/\mathfrak{m}\,\mathcal{R} & \hookrightarrow & (\mathcal{R}_1)_{K'}/\mathfrak{m}\,\mathcal{R}_1
\end{array}$$

that $L' = L_{A'}(G_1/G_2)$ is given by

$$L' = \mathcal{M}((G_1/G_2)_k)_{A'} \cap L_{A'}(G_1) = (M')_{A'} \cap \mathcal{L}_1 = \mathcal{L}'.$$

It remains to check that cokernels are what we think they are; that is, $\mathcal{L}'' = L''$ and $L_1 \to L_2 \twoheadrightarrow \mathcal{L}''$ is exact at L_2. Since the k-linear map $L_2/\mathfrak{m}L_2 \to \operatorname{coker} \mathcal{F}_{M_2}$ is an isomorphism, we at least see that the k-linear map

$$\mathcal{L}''/\mathfrak{m}\mathcal{L}'' \to \operatorname{coker} \mathcal{F}_{M''}$$

is surjective. However, this factors through the (abstract) k-linear map

$$L''/\mathfrak{m}L'' \to \operatorname{coker} \mathcal{F}_{M''}$$

which is an isomorphism, so the map

$$\mathcal{L}''/\mathfrak{m}\mathcal{L}'' \to L''/\mathfrak{m}L''$$

induced by the inclusion $\mathcal{L}'' \subseteq L''$ is surjective. By Nakayama's Lemma, we conclude $\mathcal{L}'' = L''$.

Finally, we check that $L_1 \to L_2 \twoheadrightarrow \mathcal{L}''$ is exact at L_2. Since we have already proven that $\mathcal{L}'' = L''$ always holds, we may reduce to the case in which $f : G_2 \to G_1$ is an epimorphism, so $M_1 \to M_2$ is injective and $\mathcal{R}_1 \to \mathcal{R}_2$ is faithfully flat. Our assertion amounts to the claim that $L_2 \cap (M_1)_{A'} = L_1$, but this follows from the same commutative diagram argument which we used above.

■

It is clear that if $e < p-1$ and G is in $\mathcal{FF}_{A'}$, then we can define $\underline{G}$ in the obvious manner as a functor from p-adic A'-rings to **Ab** in a manner analogous to the earlier definition for $e = 1$ in Step 2 of the proof of Theorem 1.4. The natural transformation $G \to \underline{G}$ of functors on p-adic A'-rings (not just finite flat A'-algebras) is an isomorphism. The same statement holds if $e = p-1$ and we require G to be unipotent. The proofs in both cases are essentially the same as in the case $e = 1$, except that we use the general formulation of Fontaine's classification of p-divisible groups (i.e., when $e \leq p-1$) rather than the formulation in the special case $e = 1 \leq p-1$. In particular, for $e < p-1$ and G in $\mathcal{FF}_{A'}$ (resp. for $e = p-1$ and G in $\mathcal{FF}^u_{A'}$), we can intrinsically recover from $LM_{A'}(G)$ (resp. from $LM^u_{A'}(G)$) the *group functor* $G \simeq \underline{G}$ on finite flat A'-algebras. In fact, with a choice of algebraic closure $\overline{K}$ of K we can *functorially* recover the group *scheme* G; cf. Remark for Lemma 4.1. When $e = p-1$ and we restrict attention to connected objects, we have a similar result, though the definition of $\underline{G}$ needs to be modified in order to account for the different formulation of Fontaine's classification of connected p-divisible groups in this case (just like for $p = 2$ earlier). In case $e < p-1$ and we look at connected objects, there is a natural map between the two definitions of $\underline{G}$, compatible with the isomorphisms of each with G, so these functors are all naturally identified. Similarly, if $e = p-1$ and we consider G which are simultaneously unipotent and connected, the two definitions of $\underline{G}$ are naturally isomorphic.

Note that by the second part of Lemma 4.1, we can view $\mathcal{FF}_{A'}$ as a (very mysterious) full abelian subcategory of the abelian category of commutative finite K'-group schemes of p-power order when $e < p-1$, and similarly for $\mathcal{FF}^u_{A'}$, $\mathcal{FF}^c_{A'}$ when $e \leq p-1$. If we are given some finite commutative K'-group scheme with p-power order and know that it is the generic fiber of some G in $\mathcal{FF}_{A'}$ with $e < p-1$ (or in $\mathcal{FF}^u_{A'}$, $\mathcal{FF}^c_{A'}$ with $e = p-1$), then G is unique up to canonical isomorphism and we can readily read off a small amount of information about G in a special case (the argument is the same as the one needed to justify [9, Rem 3.4]):

Theorem 4.4. *Assume that K' has residue field $k = \mathbf{F}_p$ (i.e., K' is a finite totally ramified extension of $\mathbf{Q}_p$). Let $\rho : \mathrm{Gal}(\overline{K'}/K') \to \mathrm{Aut}(\mathbf{M})$ be the continuous representation associated to the generic fiber of an object G in $\mathcal{FF}_{A'}$, with G unipotent or connected if $e = p-1$. Assume $\mathbf{M} = G(\overline{K}')$ has the structure of a finite-length $\mathcal{O}$-module, compatible with the Galois action, where $\mathcal{O}$ is a complete mixed characteristic discrete valuation ring with a finite residue field $\mathbf{F}$ having characteristic p. Prolong the $\mathcal{O}$-action on $G_{K'}$ to one on G (by Lemma 4.1). Then there is a non-canonical isomorphism of $\mathcal{O}$-modules*

$$\mathcal{M}(G_k) \simeq \mathbf{M}.$$

Proof. Since $\mathcal{M}(G_k)$ and $\mathbf{M}$ are both finite-length $\mathcal{O}$-modules, in order to show that they are isomorphic it suffices to show that they have the same invariant factors. The invariant factors of a finite-length $\mathcal{O}$-module N are determined by the invariant factors of $\pi_{\mathcal{O}} N$, together with the values of $\ell_{\mathcal{O}}(\pi_{\mathcal{O}} N)$ and $\ell_{\mathcal{O}}(N)$.

If we let $\pi_{\mathcal{O}} G$ denote the 'image' of the morphism $\pi_{\mathcal{O}} : G \to G$ in the abelian category $\mathcal{FF}_{A'}$ when $e < p-1$ (resp. in the abelian categories $\mathcal{FF}^u_{A'}$ or $\mathcal{FF}^c_{A'}$ when $e = p-1$), then $\pi_{\mathcal{O}}\mathbf{M} = (\pi_{\mathcal{O}} G)(\overline{K'})$ and so for $q = |\mathbf{F}|$, the order of $\pi_{\mathcal{O}} G$ is $q^{\ell_{\mathcal{O}}(\pi_{\mathcal{O}}\mathbf{M})}$, which is also equal to the order of $(\pi_{\mathcal{O}} G)_k$. But since $k = \mathbf{F}_p$, this order is equal to the cardinality of $\mathcal{M}((\pi_{\mathcal{O}} G)_k)$ (cf. [7, Ch III, Prop 3.4(i), Prop 4.5(i)]), which is equal to $q^{\ell_{\mathcal{O}}(\mathcal{M}((\pi_{\mathcal{O}} G)_k))}$. In a similar manner, we have $\ell_{\mathcal{O}}(\mathbf{M}) = \ell_{\mathcal{O}}(\mathcal{M}(G_k))$. Since $\mathcal{M}((\pi_{\mathcal{O}} G)_k) \simeq \pi_{\mathcal{O}}\, \mathcal{M}(G_k)$ by standard exactness arguments, it remains to verify that the finite-length $\mathcal{O}$-modules $\pi_{\mathcal{O}}\, \mathcal{M}(G_k) \simeq \mathcal{M}((\pi_{\mathcal{O}} G)_k)$ and $\pi_{\mathcal{O}}\mathbf{M} \simeq (\pi_{\mathcal{O}} G)(\overline{K'})$ have the same invariant factors. That is, we can work with $\pi_{\mathcal{O}} G$ in place of G. However, $\pi_{\mathcal{O}} G$ is a proper closed subgroupscheme of G unless G is trivial, so we are reduced to the case where G is trivial, which is itself a trivial case. ∎

Some other constructions on $\mathcal{FF}_{A'}$ which we wish to translate into the language of finite Honda systems are Cartier duality and base change. Let us first consider Cartier duality.

If M is a D_k-module with finite A-length, we define $M^* = \mathrm{Hom}_A(M, K/A)$ as an A-module and $F(\psi) : m \mapsto \sigma^{-1}(\psi(V(m))$, $V(\psi) : m \mapsto \sigma(\psi(F(m)))$. There is a natural D_k-module isomorphism $M \simeq M^{**}$ as usual. For G in $\mathcal{FF}_k$ with Cartier dual $\widehat{G}$, Fontaine constructs in [7, Ch III, §5.3, Cor 2] an isomorphism $\mathcal{M}(\widehat{G}) \simeq \mathcal{M}(G)^*$, natural in G.

We have not been able to fully justify a formulation of Cartier duality in terms of finite Honda systems, but there is a reasonable candidate which we now describe. Let M be a D_k-module with finite A-length.

We will construct a symmetric pairing

$$M_{A'} \otimes_{A'} (M^*)_{A'} \to K'/p^{-1}\mathfrak{m}A',$$

so we begin with a pairing

$$\Big((A' \otimes_A M) \oplus (p^{-1}\mathfrak{m} \otimes_A M^{(1)})\Big) \otimes_{A'} \Big((A' \otimes_A M^*) \oplus (p^{-1}\mathfrak{m} \otimes_A (M^*)^{(1)})\Big) \to K'/p^{-1}\mathfrak{m}A'$$

defined by

$$(\lambda \otimes x, p^{-1}\mu \otimes y) \otimes (\alpha \otimes \varphi, p^{-1}\beta \otimes \psi) \mapsto \alpha(\lambda \cdot \varphi(x) + p^{-1}\mu \cdot \varphi(F_0(y))) + p^{-1}\beta(\mu \cdot \psi(y) + \lambda \cdot \psi(V_0 x))$$

(here we have implicitly used a canonical isomorphism $(M^*)^{(1)} \simeq (M^{(1)})^*$). It is straightfoward to check that we can pass to quotients and get a well-defined symmetric pairing between $M_{A'}$ and $(M^*)_{A'}$ as desired.

In order to check that this is non-degenerate, we want to verify that the map

$$e_M : M_{A'} \to \mathrm{Hom}_{A'}((M^*)_{A'}, K'/p^{-1}\mathfrak{m}A')$$

is an isomorphism. Applying $\otimes_A W(\overline{k})$, we may assume (with a little compatibility checking) that k is algebraically closed. Also, by functoriality and exactness, we may assume that M is a simple object, so $M = k$ with either $F = V = 0$ or $F = 0$, $V = \sigma^{-1}$ or $V = 0$, $F = \sigma$. By length comparsions, it is enough to check that e_M is injective. This is easy.

Given a finite Honda system (L, M) (connected *and* unipotent if $e = p - 1$), we should define the dual Honda system (L^*, M^*), with $L^* \subseteq (M^*)_{A'}$ the annihilator of $L \subseteq M_{A'}$ under the above pairing. If $(L, M) = LM_{A'}(G)$, then Fontaine's duality pairing between $\mathcal{M}(G_k)$ and $\mathcal{M}((\widehat{G})_k) = \mathcal{M}(\widehat{G_k})$ gives rise to an isomorphism $\mathcal{M}(\widehat{G}_k)_{A'} \simeq (\mathcal{M}(G_k)^*)_{A'}$, and the essential claim is that this takes $\mathcal{L}_{A'}(\widehat{G})$ over to L^*. We do not see how to prove this, though clearly it is enough (by a duality and length argument) to show that $\mathcal{L}_{A'}(\widehat{G})$ lands inside of L^*.

Now let us consider base change, which can be useful for descent considerations (as we will see in the proof of Theorem 5.2). In this case, we *can* prove things. We first consider the simpler case of what we will call *pseudo-étale* base change. Let $(\mathcal{A}', \mathfrak{n})$ be a mixed characteristic complete discrete valuation ring with residue field κ perfect of characteristic p. Define $\mathcal{A} = W(\kappa)$ and suppose we are given a map of rings $h : A' \to \mathcal{A}'$, necessarily local and faithfully flat, such that $h(\mathfrak{m})\mathcal{A}' = \mathfrak{n}$. In particular, $e(\mathcal{A}') = e(A') = e$. We let $\overline{h} : k \hookrightarrow \kappa$ denote the induced map on the residue fields. When the above hypotheses are met, we say that h is *pseudo-étale* (note that we allow $\overline{h}$ to be a non-algebraic extension).

Fix such an h and choose G in $\mathcal{FF}_{A'}$ (unipotent or connected if $e = p - 1$), so $G \times_{A'} \mathcal{A}'$ trivially lies in $\mathcal{FF}_{\mathcal{A}'}$ (and is unipotent or connected if $e = p - 1$). We wish to explicitly define a 'base change' functor

$$\mathbf{B}_h : PSH^f_{A'} \to PSH^f_{\mathcal{A}'}$$

which takes $SH^f_{A'}$ over into $SH^f_{\mathcal{A}'}$ for $e < p - 1$ and likewise for unipotent and connected Honda systems when $e \le p - 1$. When $e < p - 1$ we want to have

$$\mathbf{B}_h \circ LM_{A'} \simeq LM_{\mathcal{A}'} \circ B_h,$$

where $B_h : \mathcal{FF}_{A'} \to \mathcal{FF}_{\mathcal{A}'}$ is the usual base change functor. We also want a similar statement in the unipotent and connected settings when $e \le p - 1$. Later, we will carry this out without a pseudo-étale hypothesis.

We begin with a few preliminary definitions.

Definition 4.5. For a D_k-module M and any perfect extension $\overline{h} : k \to \kappa$, define $M_{\overline{h}} = \mathcal{A} \otimes_A M$ as an $\mathcal{A}$-module (using $W(\overline{h}) : A \to \mathcal{A} = W(\kappa)$) and define

$$F_{M_{\overline{h}}}(\lambda \otimes x) = \sigma(\lambda) \otimes F_M(x), \quad V_{M_{\overline{h}}}(\lambda \otimes x) = \sigma^{-1}(\lambda) \otimes V_M(x),$$

so $M_{\overline{h}}$ is a D_κ-module. For (L, M, j) in $PSH^f_{A'}$ and $h : A' \to \mathcal{A}'$ a pseudo-étale extension as above, define $L_h = \mathcal{A}' \otimes_{A'} L$.

It is obvious, by the way, that there are natural $\mathcal{A}$-module isomorphisms $(M^{(j)})_{\overline{h}} \simeq (M_{\overline{h}})^{(j)}$ compatible with the F and V maps, so we may unambiguously write $M^{(j)}_{\overline{h}}$.

Theorem 4.6. *For a pseudo-étale extension $h : A' \to \mathcal{A}'$, there is a functorial isomorphism of $\mathcal{A}'$-modules*

$$\mathcal{A}' \otimes_{A'} (M_{A'}) \simeq (M_{\overline{h}})_{\mathcal{A}'}$$

and a natural $\mathcal{A}'$-module map $j_h : L_h \to (M_{\overline{h}})_{\mathcal{A}'}$, with j_h injective if and only if j is injective. When $e < p-1$, the object $(L_h, M_{\overline{h}}, j_h)$ in $PSH^f_{\mathcal{A}'}$ lies in $SH^f_{\mathcal{A}'}$ if and only if (L, M, j) lies in $SH^f_{A'}$, and similarly for unipotent and connected Honda systems when $e \le p-1$. The additive covariant functor

$$\mathbf{B}_h : PSH^f_{A'} \to PSH^f_{\mathcal{A}'}$$

defined by $(L, M, j) \rightsquigarrow (L_h, M_{\overline{h}}, j_h)$ is exact and satisfies $\mathbf{B}_h \circ LM_{A'} \simeq LM_{\mathcal{A}'} \circ B_h$ when $e < p-1$ and satisfies $\mathbf{B}_h \circ LM^u_{A'} \simeq LM^u_{\mathcal{A}'} \circ B^u_h$, $\mathbf{B}_h \circ LM^c_{A'} \simeq LM^c_{\mathcal{A}'} \circ B^c_h$, when $e \le p-1$ (with B^u_h, B^c_h the restrictions of B_h to the categories of unipotent and connected objects respectively).

Proof. Trivially $\ell_{\mathcal{A}}(M_{\overline{h}}) = \ell_A(M) < \infty$. Also, since h is pseudo-étale, $\mathcal{A}' \otimes_{A'} \mathfrak{m} \to \mathfrak{n}$ is an *isomorphism*, so there is an obvious $\mathcal{A}'$-module isomorphism

$$\mathcal{A}' \otimes_{A'} ((A' \otimes_A M) \oplus (p^{-1}\mathfrak{m} \otimes_A M^{(1)})) \simeq (\mathcal{A}' \otimes_{\mathcal{A}} M_{\overline{h}}) \oplus (p^{-1}\mathfrak{n} \otimes_{\mathcal{A}} M^{(1)}_{\overline{h}}).$$

Since $\mathcal{A}'$ is A'-flat, we can pass to the quotient to get an $\mathcal{A}'$-module map

$$\mathcal{A}' \otimes_{A'} (M_{A'}) \to (M_{\overline{h}})_{\mathcal{A}'}$$

which is certainly surjective. However, both sides have the same $\mathcal{A}'$-length (namely, $e\ell_A(M)$), so this is an isomorphism, visibly functorial in M. The definition of j_h and the claim about its injectivity are obvious.

The above isomorphism is compatible with the isomorphism $\mathcal{A}' \otimes_{A'} (M_{A'}[1]) \simeq (M_{\overline{h}})_{\mathcal{A}'}[1]$ and this enables us to identify $\mathcal{F}_{M_{\overline{h}}}$ with $\mathrm{id}_{\mathcal{A}'} \otimes \mathcal{F}_M$. In this way, the κ-linear map

$$L_h/\mathfrak{n}L_h \to \operatorname{coker} \mathcal{F}_{M_{\overline{h}}}$$

is the same as applying the base extension $\overline{h}$ to the k-linear map

$$L/\mathfrak{m}L \to \operatorname{coker} \mathcal{F}_M.$$

Also, via the $\mathcal{A}'$-linear isomorphism

$$\mathcal{A}' \otimes_{A'} (A' \otimes_A M^{(1)}) \simeq \mathcal{A}' \otimes_{\mathcal{A}} M^{(1)}_{\overline{h}}$$

we may identify $\mathcal{V}_{M_{\overline{h}}} \circ j_h$ with the base change by h of $\mathcal{V}_M \circ j$. Since h and $\overline{h}$ are faithfully flat, we have proven that when $e < p-1$, $(L_h, M_{\overline{h}}, j_h)$ is an object in $SH^f_{\mathcal{A}'}$ if and only if (L, M, j) is an object in $SH^f_{A'}$, and likewise for unipotent and connected Honda systems when $e \le p-1$.

We now must check that the functor $(L, M) \rightsquigarrow (L_h, M_{\overline{h}})$ on Honda systems is compatible with pseudo-étale base change on the group scheme side. We give the argument in the general case when $e < p-1$. The argument for $e \le p-1$ with unipotence or connectedness hypotheses is essentially the same.

Let G in $\mathcal{FF}_{A'}$ have affine ring $\mathcal{R}$ and let $\mathcal{G} = G \times_{A'} \mathcal{A}'$ have affine ring $\mathcal{S}$. There's a natural map of D_κ-modules

$$\mathcal{A} \otimes_A CW_k(\mathcal{R}_k) \to CW_\kappa(\mathcal{S}_\kappa)$$

This map clearly gives rise to a map of D_κ-modules with finite $\mathcal{A}$-length

$$\mathcal{A} \otimes_A \mathcal{M}(G_k) \to \mathcal{M}(\mathcal{G}_\kappa)$$

and this is an isomorphism for κ/k finite, by [7, Ch III, §2.2, Prop 2.2(i)]. In fact, as Oda explains in [14, Cor 3.16], this remains true without a finiteness assumption on $[\kappa : k]$, and so permits us to identify $M_{\overline{h}}$ with $\mathcal{M}(\mathcal{G}_\kappa)$.

Since Oda's definition of $\mathcal{M}$ is not quite the same as Fontaine's, for the convenience of the reader we now briefly explain how to directly deduce the fact that for H any object in $\mathcal{FF}_k$, $\mathcal{A} \otimes_A \mathcal{M}(H) \to \mathcal{M}(H_{/\kappa})$ is an isomorphism, granting this when κ/k is a finite extension. Without loss of generality, we may assume κ is algebraically closed. We can always replace k by a suitable finite extension inside of κ (due to the result in the case of finite extensions). Since we may also begin by assuming H is a simple object in $\mathcal{FF}_k$, passing to a finite extension of k and using compatibility with respect to formation of products reduces us to the case in which H is either α_p, μ_p, or $\underline{\mathbf{Z}/p}$. It then remains to check that the κ-linear map $\kappa \otimes_k \mathcal{M}(H) \to \mathcal{M}(H_{/\kappa})$ between 1-dimensional spaces is non-zero. But $\mathcal{M}(H) \to \mathcal{M}(H_{/\kappa})$ is visibly injective.

Next, note that our above constructions show that there is always a natural (surjective) map of $\mathcal{A}'$-modules

$$\mathcal{A}' \otimes_{A'} (N_{A'}) \to (N_{\overline{h}})_{\mathcal{A}'}$$

for *any* D_k-module N, regardless of whether or not $\ell_A(N)$ is finite. By [7, Ch IV, §2.6, Prop 2.5], this map is an isomorphism when $N = CW_k(\mathcal{R}_k)$. Since there is also a canonical isomorphism of $\mathcal{A}'$-modules

$$\mathcal{A}' \otimes_{A'} (\mathcal{R}_{K'}/\mathfrak{m}\,\mathcal{R}) \simeq \mathcal{S}_{\mathcal{K}'}/\mathfrak{n}\mathcal{S},$$

where $\mathcal{K}'$ is the fraction field of $\mathcal{A}'$, it follows that the isomorphism $(M_{\overline{h}})_{\mathcal{A}'} \simeq \mathcal{M}(\mathcal{G}_\kappa)_{\mathcal{A}'}$ takes L_h over to $L_{\mathcal{A}'}(\mathcal{G})$.

In other words, we have constructed an isomorphism in $PSH^f_{\mathcal{A}'}$

$$(L_h, M_{\overline{h}}) \simeq LM_{\mathcal{A}'}(G \times_{A'} \mathcal{A}')$$

functorial in G. Since $\mathbf{B}_h$ is trivially additive, covariant, and exact, we're done.

■

Now consider $h : A' \to \mathcal{A}'$ which is a totally ramified finite extension and let $\mathfrak{n}$ be the maximal ideal of $\mathcal{A}'$. Choose a uniformizer Π of $\mathcal{A}'$ so that $\Pi^{e(\mathcal{A}')} = p\varepsilon$ for some $\varepsilon \in A^\times$. We assume of course that $e(\mathcal{A}') \leq p-1$.

Fix G in $\mathcal{FF}_{A'}$ if $e(\mathcal{A}') < p-1$ (resp. in $\mathcal{FF}^u_{A'}$ or $\mathcal{FF}^c_{A'}$) if $e(\mathcal{A}') = p-1$) and let $(L, M) = LM_{A'}(G)$ (resp. $LM^u_{A'}(G)$, $LM^c_{A'}(G)$). Note that A' and $\mathcal{A}'$ have the same residue field and $\mathcal{G} = G \times_{A'} \mathcal{A}'$ has the same closed fiber as G and $\mathcal{G}$ is unipotent if G is. Thus, we can write $LM_{\mathcal{A}'}(\mathcal{G}) = (\mathcal{L}, M)$ if $e(\mathcal{A}') < p-1$ (resp. $LM^u_{\mathcal{A}'}(\mathcal{G})$ or $LM^c_{\mathcal{A}'}(\mathcal{G}) = (\mathcal{L}, M)$ if $e(\mathcal{A}') = p-1$), with $\mathcal{L} = L_{\mathcal{A}'}(\mathcal{G}) \subseteq M_{\mathcal{A}'}$. We wish to describe $\mathcal{L}$ in terms of L and M, in a manner which is functorial in G.

There's certainly a natural A'-module map $J : M_{A'} \to M_{\mathcal{A}'}$, so there is an $\mathcal{A}'$-module map

$$J_L : \mathcal{A}' \otimes_{A'} L \to M_{\mathcal{A}'}.$$

Lemma 4.7. *The image of J_L is $\mathcal{L}$ and the induced map of $\mathcal{A}'$-modules*

$$\mathcal{A}' \otimes_{A'} L \to \mathcal{L}$$

is an isomorphism.

Proof. Let $\mathcal{R}$ and $\mathcal{S}$ be the affine rings of G and $\mathcal{G}$ respectively. Since $A/\mathfrak{m} \simeq \mathcal{A}'/\mathfrak{n}$, the natural maps $\mathcal{R}/\mathfrak{m} \to \mathcal{S}/\mathfrak{n}$ and $\mathcal{R}_{K'}/\mathfrak{m}\,\mathcal{R} \to \mathcal{S}_{\mathcal{K}'}/\mathfrak{n}\mathcal{S}$ are isomorphisms and so are injective. Thus, the image of J_L lies in $\mathcal{L}$, thanks to the commutative diagram

$$\begin{array}{ccc}
M_{A'} & \longrightarrow & M_{\mathcal{A}'} \\
\downarrow & & \downarrow \\
CW_{k,A'}(\mathcal{R}_k) & \longrightarrow & CW_{k,\mathcal{A}'}(\mathcal{S}_k) \\
\downarrow & & \downarrow \\
\mathcal{R}_{K'}/\mathfrak{m}\,\mathcal{R} & \hookrightarrow & \mathcal{S}_{\mathcal{K}'}/\mathfrak{n}\mathcal{S}
\end{array}$$

We'll show now that the map

$$\alpha_L : \mathcal{A}' \otimes_{A'} L \to \mathcal{L}$$

is an isomorphism modulo $\mathfrak{n}$ and so therefore is surjective.

As k-modules we have $(\mathcal{A}' \otimes_{A'} L)/\mathfrak{n} \simeq L/\mathfrak{m}$, so α_L mod $\mathfrak{n}$ is the top row in the commutative diagram of k-vector spaces

$$\begin{array}{ccc}
L/\mathfrak{m} & \longrightarrow & \mathcal{L}/\mathfrak{n} \\
\simeq\big\downarrow & & \big\downarrow\simeq \\
\operatorname{coker} \mathcal{F}_{M,A'} & \longrightarrow & \operatorname{coker} \mathcal{F}_{M,\mathcal{A}'} \\
\simeq\big\uparrow & & \big\uparrow\simeq \\
M/FM & = & M/FM
\end{array}$$

and so α_L mod $\mathfrak{n}$ is an isomorphism.

Now we prove that $\mathcal{A}' \otimes_{A'} L \twoheadrightarrow \mathcal{L}$ is injective. It suffices to prove injectivity on $\mathfrak{n}$-torsion. Note that the map

$$p^{-1}\mathfrak{m} \otimes_A M^{(1)} \to p^{-1}\mathfrak{n} \otimes_A M^{(1)}$$

induced by the inclusion $p^{-1}\mathfrak{m} \hookrightarrow p^{-1}\mathfrak{n}$ gives rise to a k-linear map

$$\ker \mathcal{F}_{M,A'} \to \ker \mathcal{F}_{M,\mathcal{A}'}$$

which is an *isomorphism*, thanks to the explicit kernel formulas in the proof of Lemma 2.4.

Using Theorem 3.4 and isomorphisms ψ_π^M and ψ_Π^M introduced in the proof of full faithfulness in Theorem 3.6, we have the identifications of k-vector spaces

$$L[\mathfrak{m}] \simeq \mathcal{V}_{M,A'}(L[\mathfrak{m}]) = \psi_\pi^M(\ker \mathcal{F}_{M,A'}) \xleftarrow{\sim} \ker \mathcal{F}_{M,A'}$$

and

$$\mathcal{L}[\mathfrak{n}] \simeq \mathcal{V}_{M,\mathcal{A}'}(\mathcal{L}[\mathfrak{n}]) = \psi_\Pi^M(\ker \mathcal{F}_{M,\mathcal{A}'}) \xleftarrow{\sim} \ker \mathcal{F}_{M,\mathcal{A}'}.$$

Combining this with the k-vector space isomorphism

$$I_L : L[\mathfrak{m}] \simeq (\mathcal{A}' \otimes_{A'} L)[\mathfrak{n}]$$

given by $x \mapsto (\pi\varepsilon)(\Pi\epsilon)^{-1} \otimes x$, it looks like we should have the desired injection on the $\mathfrak{n}$-torsion. In order to justify this, we need only check that the diagram of k-vector spaces

$$\begin{array}{ccccc}
L[\mathfrak{m}] & \xrightarrow{I_L} & (\mathcal{A}' \otimes_{A'} L)[\mathfrak{n}] & \longrightarrow & \mathcal{L}[\mathfrak{n}] \\
\simeq \downarrow & & & & \downarrow \simeq \\
\mathcal{V}_{M,A'}(L[\mathfrak{m}]) & & & & \mathcal{V}_{M,\mathcal{A}'}(\mathcal{L}[\mathfrak{n}]) \\
\simeq \uparrow & & & & \uparrow \simeq \\
\ker \mathcal{F}_{M,A'} & & \xrightarrow{\sim} & & \ker \mathcal{F}_{M,\mathcal{A}'}
\end{array}$$

commutes. The careful reader will observe that although the map I_L depends on the choices of π and Π, the bottom maps in the left and right columns depend on the choices of π and Π respectively (via ψ_π^M and ψ_Π^M), so it is not a priori unreasonable to expect that the above diagram commutes.

Let's check the commutativity. By Lemma 2.7, we may write an element of $\ell \in L[\mathfrak{m}]$ in the form $\ell = \overline{(1 \otimes u, p^{-1}\pi^{e(A')-1} \otimes w)}$, with $u \in M$ and $w \in M^{(1)}$ satisfying $V_0 u = 0$ and $F_0 w = 0$. The map down to $\mathcal{V}_{M,A'}(L[\mathfrak{m}]) \subseteq A' \otimes_A M^{(1)}$ sends ℓ to $\pi^{e(A')-1} \otimes w$. Note that this is *independent* of u. If we go across the top row and down to $\mathcal{V}_{M,\mathcal{A}'}(\mathcal{L}[\mathfrak{n}])$, we obtain the element $\Pi^{e(\mathcal{A}')-1} \otimes w \in \mathcal{A}' \otimes_A M^{(1)}$. Here we have used the 'independence of u' remark and the easy identity

$$(\pi\varepsilon)(\Pi\epsilon)^{-1}\pi^{e(A')-1} = \Pi^{e(\mathcal{A}')-1}.$$

Appending the natural isomorphisms $\ker F_0 \simeq \ker \mathcal{F}_{M,A'}$ and $\ker F_0 \simeq \ker \mathcal{F}_{M,\mathcal{A}'}$ (from Lemma 2.4) to the bottom of the diagram and considering the element $w \in \ker F_0$, the commutativity follows.

■

We are now in a position to define a base change functor without a pseudo-étale hypothesis. Let $h : A' \to \mathcal{A}'$ be a ring extension which induces an extension $\overline{h} : k \to \kappa$ on (perfect!) residue fields. For an object (L, M, j) in $PSH^f_{A'}$, we define the object $(L, M, j)_h = (L_h, M_{\overline{h}}, j_h)$ in $PSH^f_{\mathcal{A}'}$ by using the definition of $M_{\overline{h}}$ as given earlier and j_h maps $L_h \stackrel{\text{def}}{=} \mathcal{A}' \otimes_{A'} L$ to $\left(M_{\overline{h}}\right)_{\mathcal{A}'}$ as an $\mathcal{A}'$-submodule in the following manner: there is a natural A-linear map $M \to M_{\overline{h}} = \mathcal{A} \otimes_A M$ (where $\mathcal{A} = W(\kappa)$) which induces an A'-linear map $j_M : M_{A'} \to \left(M_{\overline{h}}\right)_{\mathcal{A}'}$. There is a natural map $j_h : L_h \to (M_{\overline{h}})_{\mathcal{A}'}$ defined using $j : L \to M_{A'}$ and j_M. When $e(\mathcal{A}') < p - 1$ and (L, M, j) is in $SH^f_{A'}$, then j_h is injective and $(L, M, j)_h$ is in $SH^f_{\mathcal{A}'}$ by Lemma 4.7. If $e(\mathcal{A}') \le p - 1$ and (L, M, j) is in $SH^{f,u}_{A'}$, then we get the same assertion using $SH^{f,u}_{\mathcal{A}'}$, and likewise in the connected case.

The construction of $\mathbf{B}_h$ in the pseudo-étale case is extended by the following theorem, whose proof is clear in view of what we have already done.

Theorem 4.8. *Suppose $e(A') < p-1$. For h as above, (L,M) in $SH^f_{A'}$, $(L,M)_h$ lies in $SH^f_{A'}$. The additive covariant functor*

$$\mathbf{B}_h : SH^f_{A'} \to SH^f_{A'}$$

given by $(L,M) \rightsquigarrow (L,M)_h$ is exact and satisfies $\mathbf{B}_h \circ LM_{A'} \simeq LM_{A'} \circ B_h$, where

$$B_h : \mathfrak{FF}_{A'} \to \mathfrak{FF}_{A'}$$

is the usual base change functor.

If $h_1 : A'_1 \to A'_2$ and $h_2 : A'_2 \to A'_3$ are two such base changes, then there are natural isomorphisms

$$\alpha_{h_1,h_2} : \mathbf{B}_{h_1} \circ \mathbf{B}_{h_2} \simeq \mathbf{B}_{h_1 \circ h_2}$$

which satisfy the 'triple overlap' compatibility; that is, the natural transformations

$$\alpha_{h_1,h_2} \circ \mathbf{B}_{h_3} \circ \alpha_{h_1 \circ h_2, h_3} : \mathbf{B}_{(h_1 \circ h_2) \circ h_3} \to (\mathbf{B}_{h_1} \circ \mathbf{B}_{h_2}) \circ \mathbf{B}_{h_3}$$

and

$$\mathbf{B}_{h_1} \circ \alpha_{h_2,h_3} \circ \alpha_{h_1, h_2 \circ h_3} : \mathbf{B}_{h_1 \circ (h_2 \circ h_3)} \to \mathbf{B}_{h_1} \circ (\mathbf{B}_{h_2} \circ \mathbf{B}_{h_3})$$

are equal.

If we relax the ramification to merely not exceed $p-1$, then the same assertions are true for the full subcategories of unipotent group schemes and unipotent Honda systems, as well as for the full subcategories of connected objects.

For any morphism $\varphi : (L_1, M_1) \to (L_2, M_2)$ in $PSH^f_{A'}$, we shall let φ_h denote the induced morphism $\mathbf{B}_h(\varphi) : (L_1,M_1)_h \to (L_2,M_2)_h$ in $PSH^f_{A'}$. This notation will be used throughout §5.

Now we prove some facts concerning finite Honda systems which are quite critical in applications of the present work to the deformation theory of Galois representations.

Theorem 4.9. *When $e < p-1$ and $X_i = (L_i, M_i)$ are two p-torsion objects in $SH^f_{A'}$ for which the sequences*

$$0 \to M_i/VM_i \xrightarrow{F} M_i/p = M_i \to M_i/FM_i \to 0$$

are exact, any p-torsion *object X in $PSH^f_{A'}$ which is an extension of X_2 by X_1 in $PSH^f_{A'}$ necessarily is an object in $SH^f_{A'}$. If $e \le p-1$, the same is true with $SH^{f,u}_{A'}$ or $SH^{f,c}_{A'}$ replacing $SH^f_{A'}$.*

If $e < p-1$, (L,M,j) is an object in $PSH^f_{A'}$, and $M \simeq (A/p^n)^{\oplus r}$ as an A-module, then (L,M,j) lies in $SH^f_{A'}$ if and only if the object $(L[p], M[p], j_p)$ in $PSH^f_{A'}$ lives in $SH^f_{A'}$ (with j_p the map naturally induced by j on p-torsion) and $L/p \to M_{A'}/p$ is injective. If $e \le p-1$, then the same assertion is true with $SH^{f,u}_{A'}$ or $SH^{f,c}_{A'}$ replacing $SH^f_{A'}$.

Remark 4.10. Note that the injectivity of $L/p \to M_{A'}/p$ holds if L is an A'-module direct summand of $M_{A'}$. This is the case in the application of this result to studying the deformation theory of Galois representations.

Proof. Note that for any $X = (L_X, M_X, j_X)$ as in the first part, j_X is necessarily injective. Also, for (L,M,j) as in the second part, j is clearly injective if and only if j_p is injective. Thus, throughout we may assume that all j-maps are injective and we therefore omit reference to them in what follows.

We now prove 'if' in the second part of the theorem ('only if' is clear). Since $\mathfrak{m}$-torsion lies inside of p-torsion, certainly

$$L[\mathfrak{m}] \oplus \ker \mathcal{V}_M \to M_{A'}[\mathfrak{m}]$$

is an isomorphism. It remains (for the second part of the theorem) to check that $L/\mathfrak{m} \to \operatorname{coker} \mathcal{F}_M$ is an isomorphism.

The D_k-module isomorphism $M/p \simeq M[p]$ induces an A'-linear isomorphism $(M_{A'})/p = (M/p)_{A'} \simeq (M[p])_{A'}$ and by the injectivity hypothesis, we have an *injection* $L/p \hookrightarrow (M[p])_{A'} \simeq M_{A'}[p]$ with the image landing inside of $L[p]$. An A'-length calculation shows that this is an isomorphism onto $L[p]$. Using $L/\mathfrak{m} \simeq (L/p)/\mathfrak{m}$, we get a commutative diagram of k-vector spaces

$$\begin{array}{ccccc} L/\mathfrak{m} & \longrightarrow & \operatorname{coker} \mathcal{F}_M & \overset{\sim}{\longleftarrow} & M/F \\ \simeq\downarrow & & \downarrow & & \downarrow\simeq \\ (L[p])/\mathfrak{m} & \overset{\sim}{\longrightarrow} & \operatorname{coker} \mathcal{F}_{M[p]} & \overset{\sim}{\longleftarrow} & M[p]/F \end{array}$$

so the left arrow in the top row is an isomorphism.

Now consider the first part of the theorem. The commutative diagram of k-vector spaces

$$\begin{array}{ccccccc} L_1/\mathfrak{m} & \longrightarrow & L_X/\mathfrak{m} & \longrightarrow & L_2/\mathfrak{m} & \longrightarrow & 0 \\ \simeq\downarrow & & \downarrow & & \downarrow\simeq & & \\ \operatorname{coker}\mathcal{F}_{M_1} & \longrightarrow & \operatorname{coker}\mathcal{F}_{M_X} & \longrightarrow & \operatorname{coker}\mathcal{F}_{M_2} & \longrightarrow & 0 \\ \simeq\uparrow & & \simeq\uparrow & & \uparrow\simeq & & \\ M_1/F & \longrightarrow & M_X/F & \longrightarrow & M_2/F & \longrightarrow & 0 \end{array}$$

has an exact bottom row, so easily the middle row is also exact. Since the top row is exact as well, we can conclude that the map

$$L_X/\mathfrak{m} \to \operatorname{coker}\mathcal{F}_{M_X}$$

is surjective. If $M_1/F \to M_X/F$ is injective, then it is easy to see that the left maps in each row above are injective, from which the injectivity of

$$L_X/\mathfrak{m} \to \operatorname{coker}\mathcal{F}_{M_X}$$

would follow.

In order to prove that $M_1/F \to M_X/F$ is injective, we will make essential use of our p-torsion hypothesis. More precisely, since $M_i = M_i/p$ and $M_X = M_X/p$, we have the following commutative diagram with exact rows and columns:

$$\begin{array}{ccccccccc} & & 0 & & & & 0 & & \\ & & \downarrow & & & & \downarrow & & \\ & & M_1/V & \longrightarrow & M_X/V & \longrightarrow & M_2/V & \longrightarrow & 0 \\ & & F\downarrow & & F\downarrow & & F\downarrow & & \\ 0 & \longrightarrow & M_1 & \longrightarrow & M_X & \longrightarrow & M_2 & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & M_1/F & \longrightarrow & M_X/F & \longrightarrow & M_2/F & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & 0 & & 0 & & 0 & & \end{array}$$

(the main point is the injectivity of $M_1 = M_1/p \to M_X/p = M_X$). From this diagram we see that the map $F : M_X/V \to M_X/p = M_X$ is injective, and also we see that the rows all form short exact sequences if we fill in the missing 0's on the left. In particular, $M_1/F \to M_X/F$ is injective.

Since it is obvious that $\mathcal{V}_{M_X} \circ j_X$ is injective, we are done.

■

We also have the following result concerning objects killed by p; this can be useful when lifting certain finite group schemes from characteristic p to characteristic 0 (cf. proof of Theorem 3.5).

Corollary 4.11. *Let (L, M, j) be an object in $PSH^f_{A'}$ which is killed by p and has the properties that j is injective,*

$$L/\mathfrak{m} \to \operatorname{coker}\mathcal{F}_M$$

is an isomorphism, and

$$0 \to M/V \xrightarrow{F} M/p = M \to M/F \to 0$$

is an exact sequence. If $e = p-1$, then assume that V (resp. F) acts in a nilpotent manner on M. Then (L, M, j) lies in $SH^f_{A'}$ if $e < p-1$ and it lies in $SH^{f,u}_{A'}$ (resp. $SH^{f,c}_{A'}$) if $e = p-1$.

More precisely, if $e < p-1$ then $LM_{A'}$ induces an anti-equivalence of categories between the full subcategory of p-torsion objects G in $\mathcal{FF}_{A'}$ for which the sequence

$$0 \to \mathcal{M}(G_k)/V \xrightarrow{F} \mathcal{M}(G_k)/p = \mathcal{M}(G_k) \to \mathcal{M}(G_k)/F \to 0$$

is exact and the full subcategory of p-torsion objects (L, M, j) in $PSH^f_{A'}$ for which $L/\mathfrak{m} \to \operatorname{coker} \mathcal{F}_M$ is an isomorphism, j is injective, and the sequence

$$0 \to M/V \xrightarrow{F} M/p = M \to M/F \to 0$$

is exact. If $e = p-1$, the same statement is true for the corresponding categories consisting of unipotent objects killed by p, and likewise with the categories of connected objects.

Proof. If $e = 1$, then since $FM \subseteq \ker V$, the hypotheses imply that $L[p] \oplus \ker V = L \oplus \ker V$ surjects onto $M = M/p$, with both sides having the same A-length. This settles the $e = 1$ case.

Now we suppose $e \geq 2$. We begin by proving that the inclusion

$$V^M(\xi^M(\iota_M^{-1}(L[\mathfrak{m}]))) \subseteq \ker \mathcal{F}_M$$

is an equality. Since $pM = 0$ and the sequence

$$0 \to M/V \xrightarrow{F} M \to M/F \to 0$$

is exact, we have

$$\ker \mathcal{F}_M = \{1 \otimes V_0 x | x \in M\} \subseteq p^{-1}\mathfrak{m} \otimes_A (M)^{(1)}.$$

Pick any $x \in M$. The isomorphism $L/\mathfrak{m} \simeq \operatorname{coker} \mathcal{F}_M$ shows that we can write

$$\iota_M(1 \otimes x) = \ell + \mathcal{F}_M(u),$$

where $\ell \in L$ and $u \in (M)_{A'}[1] = p^{-1}\mathfrak{m} \otimes_A (M)^{(1)}$. Since p kills M, so p also kills $(M)_{A'}$, we see that multiplication by π^{e-1} on $(M)_{A'}$ has its image inside the $\mathfrak{m}$-torsion submodule $(M)_{A'}[\mathfrak{m}]$, so

$$\iota_M(\pi^{e-1} \otimes x) = \pi^{e-1}\ell + \mathcal{F}_M(\pi^{e-1}u),$$

with $\pi^{e-1}\ell \in L \cap ((M)_{A'}[\mathfrak{m}]) = L[\mathfrak{m}]$ and, for $u = \sum_{j=1}^{e} p^{-1}\pi^j \otimes u_j$,

$$\begin{aligned} \pi^{e-1}u &= 1 \otimes \epsilon u_1 + \sum_{j=2}^{e} p^{-1}\pi^{j+e-1} \otimes u_j \\ &= 1 \otimes \epsilon u_1 + \sum_{j=2}^{e} p^{-1}\epsilon\pi^{j-1} \otimes p u_j \\ &= 1 \otimes \epsilon u_1. \end{aligned}$$

Thus,

$$\iota_M(\pi^{e-1} \otimes x) = \ell' - \epsilon \cdot \mathcal{F}_M(1 \otimes z),$$

where $\ell' \in L[\mathfrak{m}]$ and $z = -u_1 \in (M)^{(1)}$.

Since $\mathcal{F}_M(1 \otimes z) = \mathcal{F}_M(\varphi_1^M(1 \otimes z)) = \iota_M \circ F^M(1 \otimes z) = \iota_M(1 \otimes F_0 z)$, we have that for all $x \in M$, there exists $z \in (M)^{(1)}$ such that

$$\iota_M(1 \otimes F_0 z + \pi^{e-1} \otimes \epsilon^{-1}x) \in L[\mathfrak{m}].$$

Combining this with

$$\begin{aligned} V^M(\xi^M(1 \otimes F_0 z + \pi^{e-1} \otimes \epsilon^{-1}x) &= V^M(\pi \otimes F_0 z + p \otimes x) \\ &= p^{-1}\pi \otimes V_0 F_0 z + 1 \otimes V_0 x \\ &= 1 \otimes V_0 x \end{aligned}$$

($V_0 F_0 = p$ kills $(M)^{(1)}$!), we have shown that $\ker \mathcal{F}_M \subseteq V^M(\xi^M(\iota_M^{-1}(L[\mathfrak{m}])))$, the reverse of the usual inclusion.

We will now use the equality

$$\ker \mathcal{F}_M = V^M(\xi^M(\iota_M^{-1}(L[\mathfrak{m}])))$$

in order to *directly* prove that (L, M) arises from $\mathcal{FF}_{A'}$ (and from $\mathcal{FF}^u_{A'}$ (resp. $\mathcal{FF}^c_{A'}$) if V (resp. F) is nilpotent on M) and so (L, M) lies in $SH^f_{A'}$ when $e < p-1$ and in $SH^{f,u}_{A'}$ when V is nilpotent on M and in $SH^{f,c}_{A'}$ when F is nilpotent on M. At this point, we will *not* require the p-torsion condition anymore. The argument is simply a modification of the proof of essential surjectivity in Step 4 of the proof of Theorem 3.6 in the case $e \geq 2$. More precisely, we construct M_1, M_2, and $\mathcal{L}_1$ in exactly the same way. As for the construction of $\mathcal{L}_2$, that also reduces in the same manner to the consideration of whether $x \in ((M_1)_{A'}[1]) \cap (M_2)_{A'}$ can be represented in $(M_2)_{A'}/(M_2)_{A'}[1]$ by an element of $\mathcal{L}_1 \cap (M_2)_{A'}$. It is at the stage where we invoke $\mathcal{V}_M(L[\mathfrak{m}]) \simeq \psi_\pi^M(\ker \mathcal{F}_M)$ in Step 4 that the argument needs to be slightly altered.

Using the same notation as in the proof of Theorem 3.6, we use the expression above for $\ker \mathcal{F}_M$ in order to write

$$1 \otimes \mathcal{P}(m) = \sum_{j=1}^{e} p^{-1}\pi^j \otimes V_0 n_j$$

in $(M)_{A'}[1]$, where the element

$$\sum_{j=0}^{e-1} \pi^j \otimes n_{j+1} \in A' \otimes_A M$$

has image in $(M)_{A'}$ that lies in L. Recalling the general formula for $\ker \iota_N$ for any D_k-module N (see Lemma 2.7), a simple calculation shows that we may suppose without loss of generality that $n_i = 0$ for $1 < i < e$. Clearly $V_0 n_1 = 0$ and $V_0 n_e = \epsilon^{-1}\,\mathcal{P}(m)$.

By construction, $(M_1)_{A'} \twoheadrightarrow (M)_{A'}$ takes $\mathcal{L}_1$ *onto* L, so there exists an $\ell_1 \in \mathcal{L}_1$ such that

$$\mathcal{P}'(\ell_1) = \overline{(1 \otimes n_1 + \pi^{e-1} \otimes n_e, 0)}$$

in $M_{A'}$. Now inside of $(M_1)_{A'} = A' \otimes_A M_1 + p^{-1}\mathfrak{m} \otimes FM_1$, we can write

$$\ell_1 = 1 \otimes y - \sum_{r=1}^{e-1} p^{-1}\pi^r \otimes Fz_r,$$

so

$$\mathcal{P}'(\ell_1) = \overline{\left(1 \otimes \mathcal{P}(y), \sum_{r=1}^{e-1} p^{-1}\pi^r \otimes \mathcal{P}(z_r)\right)}.$$

Consequently, there exist $u \in \mathfrak{m} \otimes_A M$ and $w \in A' \otimes_A (M)^{(1)}$ such that

$$\left(1 \otimes \mathcal{P}(y) - 1 \otimes n_1 - \pi^{e-1} \otimes n_e, \sum_{r=1}^{e-1} p^{-1}\pi^r \otimes \mathcal{P}(z_r)\right) = (\varphi_0^M(u) - F^M(w), \varphi_1^M(w) - V^M(u)).$$

However, in $(M)_{A'}[1]$ we have

$$\begin{aligned} \pi \cdot (\varphi_1^M(w) - V^M(u)) + V^M(\xi^M(\varphi_0^M(u) - F^M(w))) &= \pi\varphi_1^M(w) - V^M\xi^M(F^M(w)) \\ &= 0, \end{aligned}$$

and so in $(M)_{A'}[1]$,

$$\begin{aligned} 0 &= \sum_{r=1}^{e-1} p^{-1}\pi^{r+1} \otimes \mathcal{P}(z_r) + V^M\left(\pi \otimes \mathcal{P}(y) - \pi \otimes n_1 - \pi^e \otimes n_e\right) \\ &= \sum_{r=1}^{e-1} p^{-1}\pi^{r+1} \otimes \mathcal{P}(z_r) + p^{-1}\pi \otimes V_0\,\mathcal{P}(y) - p^{-1}\pi \otimes V_0 n_1 - \epsilon \otimes V_0 n_e. \end{aligned}$$

Recall that $V_0 n_e = \epsilon^{-1}\,\mathcal{P}(m)$ and $V_0 n_1 = 0$, so the elements $1 \otimes m$ and $p^{-1}\pi \otimes V_0 y + \sum_{r=1}^{e-1} p^{-1}\pi^{r+1} \otimes z_r$ in $(M_1)_{A'}[1]$ have the same image in $(M)_{A'}[1]$ under $\mathcal{P}'$. Now the sequence of A'-modules

$$0 \to (M_2)_{A'}[1] \to (M_1)_{A'}[1] \to (M)_{A'}[1] \to 0$$

is the same as

$$0 \to p^{-1}\mathfrak{m} \otimes_A M_2^{(1)} \to p^{-1}\mathfrak{m} \otimes_A M_1^{(1)} \to p^{-1}\mathfrak{m} \otimes_A (M)^{(1)} \to 0,$$

which is exact since $N \rightsquigarrow N^{(1)}$ is exact from the category of A-modules to itself and $p^{-1}\mathfrak{m}$ is a flat A-module.

Therefore, the elements $1 \otimes m$ and $p^{-1}\pi \otimes V_0 y - \sum_{r=1}^{e-1} p^{-1}\pi^{r+1} \otimes z_r$ in $(M_1)_{A'}[1]$ differ by an element of $(M_2)_{A'}[1]$, so $i'(x) = 1 \otimes F_0 m$ differs from

$$\begin{aligned} p^{-1}\pi \otimes F_0 V_0 y - \sum_{r=1}^{e-1} p^{-1}\pi^{r+1} \otimes F_0 z_r &= \pi \otimes y - \sum_{r=1}^{e-1} p^{-1}\pi^{r+1} \otimes F_0 z_r \\ &= \pi \ell_1 \end{aligned}$$

by an element of $(M_2)_{A'}[1]$. In particular, $\pi\ell_1$ lies in $(M_2)_{A'}$ inside of $(M_1)_{A'}$. But $\pi\ell_1 \in \mathcal{L}_1$, so this is exactly what we wanted to prove.

∎

The above two results show that when analyzing certain p-torsion group schemes over A', we have the technical freedom to work within $PSH^f_{A'}$ without straying outside of the essential image of $LM_{A'}$. It is precisely this sort of technical freedom which one needs in [4], since checking *explicitly* whether an object constructed in $PSH^f_{A'}$ actually lies in $SH^f_{A'}$ or $SH^{f,u}_{A'}$ or $SH^{f,c}_{A'}$ can be very cumbersome.

For later use, it will be convenient to state a key lemma which we did not bother to state explicitly in the $e = 1$ case, but which was essentially proven in the course of the arguments in §1.

Lemma 4.12. *Assume $e < p-1$. Let $\Gamma_1 \to \Gamma_2$ be an isogeny of d-dimensional p-divisible groups over A' with kernel G, so G is in $\mathcal{FF}_{A'}$. Let $(\mathcal{L}_i, M_i) = LM_{A'}(\Gamma_i)$ in $H^d_{A'}$. Define the D_k-module $M = \operatorname{coker}(M_2 \hookrightarrow M_1)$ and define the A'-module*

$$L = \operatorname{image}(\mathcal{L}_1 \to (M_1)_{A'} \twoheadrightarrow M_{A'}).$$

Under the natural isomorphism of D_k-modules $M \simeq \mathcal{M}(G_k)$, the induced map of A'-modules $M_{A'} \simeq \mathcal{M}(G_k)_{A'}$ takes L isomorphically over to $L_{A'}(G)$, so (L, M) in $PSH^f_{A'}$ actually lies in $SH^f_{A'}$. The isomorphism $(L, M) \simeq LM_{A'}(G)$ depends functorially (in an obvious manner) on the given isogeny of p-divisible groups $\Gamma_1 \to \Gamma_2$ and is compatible with base change (preserving the '$e < p-1$' condition).

In particular, if Γ is a p-divisible group over A' with $(\mathcal{L}, M) = LM_{A'}(\Gamma)$, then $\mathcal{L}$ is an A'-module direct summand of $M_{A'}$ and there are natural injections of A'-modules $\mathcal{L}/p^n \hookrightarrow (M/p^n)_{A'}$ and isomorphisms in $PSH^f_{A'}$ (even in $SH^f_{A'}$)

$$LM_{A'}(\Gamma[p^n]) \simeq (\mathcal{L}/p^n, M/p^n)$$

which are compatible with change in n, as well as base change, and are functorial in Γ.

If we impose unipotence conditions on all group objects, the same statements are true with $e \le p-1$, and likewise with connectedness conditions.

Proof. First assume $e < p-1$. As we explained near the end of the proof of Theorem 3.4, $M_{A'} \simeq \mathcal{M}(G_k)_{A'}$ takes L over into $L_{A'}(G)$ and moreover $L \simeq L_{A'}(G)$. The functoriality properties of $(L, M) \simeq LM_{A'}(G)$ are clear from the construction. The special case of p-power torsion of a p-divisible group is clear; the only point of interest is that $\mathcal{L}/p^n \to (M/p^n)_{A'} \simeq M_{A'}/p^n$ is injective because $\mathcal{L}$ is an A'-module direct summand of $M_{A'}$. This direct summand property holds because the composite map

$$\mathcal{L}/\mathfrak{m} \to M_{A'}/\mathfrak{m} \to \operatorname{coker} \mathcal{F}_M$$

is a k-linear isomorphism [7, Ch IV, §4, Prop 4.2(i)], so the inclusion $\mathcal{L} \hookrightarrow M_{A'}$ is injective modulo $\mathfrak{m}$. Since $M_{A'}$ is a finite free A'-module [7, Ch IV, §2.3 Remark], this implies that $\mathcal{L}$ is an A'-module direct summand of $M_{A'}$.

If $e \le p-1$, using $LM^u_{A'}$ or $LM^c_{A'}$ in place of $LM_{A'}$ permits the same arguments to go through with unipotence or connectedness conditions.

∎

5. Descent Formalism and Abelian Varieties

As an application of our study of base change for finite Honda systems, we will prove an interesting theorem on good reduction of certain abelian varieties.

To start off, let's quickly review the formalism of Galois descent in our situation (see [1, §6.2] for further details). Let $\mathcal{K}'$ be a finite *Galois* extension of the fraction field K' of A' with $e(\mathcal{K}') \leq p-1$, and let $(\mathcal{A}', \mathfrak{n})$ denote the valuation ring of $\mathcal{K}'$, as usual. The descent data on a $\mathcal{K}'$-group scheme $\mathcal{G}$ which encodes the fact that it arises as the base extension of a specified *group scheme* over K' is a collection of commutative diagrams of schemes

$$\begin{array}{ccc} \mathcal{G} & \xrightarrow{\gamma_{\mathcal{G}}} & \mathcal{G} \\ \downarrow & & \downarrow \\ \operatorname{Spec} \mathcal{K}' & \xrightarrow{\gamma^*} & \operatorname{Spec} \mathcal{K}' \end{array}$$

for all $\gamma \in \operatorname{Gal}(\mathcal{K}'/K')$, with $\gamma_{\mathcal{G}} \circ \widetilde{\gamma}_{\mathcal{G}} = (\widetilde{\gamma} \circ \gamma)_{\mathcal{G}}$, $(\mathrm{id}_{\mathcal{K}'})_{\mathcal{G}} = \mathrm{id}_{\mathcal{G}}$, and each $\gamma_{\mathcal{G}}$ must be compatible (over the action of γ on the base) with the *group scheme* structure morphisms for $\mathcal{G}$ over $\mathcal{K}'$. Of course, in a situation as affine as this one, Galois descent data is always effective. Also, note that using $\gamma = \widetilde{\gamma} = \mathrm{id}_{\mathcal{K}'}$ yields $(\mathrm{id}_{\mathcal{K}'})_{\mathcal{G}} = \mathrm{id}_{\mathcal{G}}$ as a consequence of the other conditions if we axiomatize the fact that each $\gamma_{\mathcal{G}}$ is an *isomorphism* of schemes.

A more convenient way to say all of this is that if we let $\mathcal{G}_\gamma$ denote the base-extended $\mathcal{K}'$-group scheme

$$\mathcal{G}_\gamma = \mathcal{G} \times_{\operatorname{Spec} \mathcal{K}'} \operatorname{Spec} \mathcal{K}',$$

using $\gamma^* : \operatorname{Spec} \mathcal{K}' \simeq \operatorname{Spec} \mathcal{K}'$, then we require the existence of isomorphisms of $\mathcal{K}'$*-group schemes* $\gamma_{\mathcal{G}} : \mathcal{G} \to \mathcal{G}_\gamma$ such that for all $\gamma, \widetilde{\gamma} \in \operatorname{Gal}(\mathcal{K}'/K')$,

$$(\gamma_{\mathcal{G}})_{\widetilde{\gamma}} \circ \widetilde{\gamma}_{\mathcal{G}} = (\widetilde{\gamma} \circ \gamma)_{\mathcal{G}}.$$

Here, for any morphism of $\mathcal{K}'$-schemes $f : X \to Y$ we denote by f_γ the morphism $X_\gamma \to Y_\gamma$ induced via base extension by γ^*; note that in the above we have implicitly used the natural isomorphism $(X_\gamma)_{\widetilde{\gamma}} \simeq X_{\widetilde{\gamma} \circ \gamma}$.

Now make the further assumption that $\mathcal{G}$ is the generic fiber of an object $\mathcal{G}_0$ in $\mathcal{FF}_{A'}$, with $\mathcal{G}_0$ unipotent or connected if $e(\mathcal{K}') = p-1$. By the final part of Lemma 4.1, the above data on $\mathcal{G}$ is *equivalent* to corresponding data on $\mathcal{G}_0$. Here, we use the usual action of $\operatorname{Gal}(\mathcal{K}'/K')$ on $\mathcal{A}'$ and we replace '$\mathcal{K}'$-group scheme' by '$\mathcal{A}'$-group scheme' (note that in Lemma 4.1 we only have full faithfulness with respect to morphisms of group schemes, not just of schemes, over the base). Of course, in the category of $\mathcal{A}'$-schemes this generally does not constitute descent data down to A', since the cover $\operatorname{Spec} \mathcal{A}' \to \operatorname{Spec} A'$ is typically far from Galois.

Since an automorphism $\gamma : \mathcal{A}' \to \mathcal{A}'$ is trivially pseudo-étale, Theorem 4.6 enables us to reformulate all of this intrinsically in the category $PSH^f_{\mathcal{A}'}$. We state this more formally as a definition. Note that the contravariance of $LM_{\mathcal{A}'}$, $LM^c_{\mathcal{A}'}$, and $LM^u_{\mathcal{A}'}$ will cancel out the contravariance of Spec implicit in the descriptions of the action of $\operatorname{Gal}(\mathcal{K}'/K')$ above, leaving us with a more psychologically pleasing left action of $\operatorname{Gal}(\mathcal{K}'/K')$ rather than a right action.

Definition 5.1. For an object (L, M, j) in $PSH^f_{\mathcal{A}'}$, *descent data* $\mathcal{D}$ *on* (L, M, j) (*relative to* $A' \to \mathcal{A}'$) is a collection of $PSH^f_{\mathcal{A}'}$-isomorphisms

$$[\gamma]_{\mathcal{D}} : (L, M, j)_\gamma \xrightarrow{\sim} (L, M, j),$$

for all $\gamma \in \operatorname{Gal}(\mathcal{K}'/K')$, such that $[\gamma_1]_{\mathcal{D}} \circ ([\gamma_2]_{\mathcal{D}})_{\gamma_1} = [\gamma_1 \circ \gamma_2]_{\mathcal{D}}$.

If one were interested in generalizing the considerations of Ramakrishna [16] to study a local deformation problem analogous to the one in [10] (suitably modified to force the p-divisible group to arise over an extension with $e \leq p-1$), a natural thing to study would be the abelian category $DPSH^f_{\mathcal{A}'}$ whose objects consist of pairs $((L, M, j), \mathcal{D})$ with (L, M, j) an object in $PSH^f_{\mathcal{A}'}$ and $\mathcal{D}$ a descent data on (L, M, j) (relative to $A' \to \mathcal{A}'$, even though we omit mention of A' in the notation); we define a morphism

$$((L_1, M_1, j_1), \mathcal{D}_1) \to ((L_2, M_2, j_2), \mathcal{D}_2)$$

to be a morphism $\varphi : (L_1, M_1, j_1) \to (L_2, M_2, j_2)$ compatible with the descent data (i.e., $\varphi \circ [\gamma]_{\mathcal{D}_1} = [\gamma]_{\mathcal{D}_2} \circ \varphi_\gamma$ for all $\gamma \in \mathrm{Gal}(\mathcal{K}'/K')$). Full abelian subcategories $DSH^f_{A'}$ (when $e(\mathcal{K}') < p-1$) and $DSH^{f,u}_{A'}$, $DSH^{f,u}_{A'}$ can be defined in the obvious manner, but we don't have any need for them, essentially because of Theorem 4.9. When considering the computation of Ext^1's along the lines of argument as in [16], one is also led to consider the full abelian subcategory $\widetilde{DPSH}^f_{A'}$ consisting of p-torsion objects. It is trivial to check that the forgetful functors $\widetilde{DPSH}^f_{A'} \to DPSH^f_{A'}$ and $DPSH^f_{A'} \to PSH^f_{A'}$ are exact. This is used in [4].

We'll now use the descent formalism in order to prove a 'good reduction' theorem for certain abelian varieties. First, let's formulate a theorem about p-divisible groups which will be the means by which we study good reduction of abelian varieties.

Theorem 5.2. *Let $\mathcal{K}'$ be a finite (not necessarily Galois!) extension of K', with valuation ring $\mathcal{A}'$ and $e(\mathcal{K}') \le p-1$. Let $\Gamma_{K'}$ be a p-divisible group over K' and assume that there exists a p-divisible group Γ' over $\mathcal{A}'$ such that*

$$\Gamma_{K'} \times_{K'} \mathcal{K}' \simeq \Gamma' \times_{\mathcal{A}'} \mathcal{K}'$$

as p-divisible groups over $\mathcal{K}'$. Suppose that $\Gamma_{K'}[p] \simeq G \times_{A'} K'$ as K'-group schemes for some G in $\mathfrak{FF}_{A'}$. If $e(\mathcal{K}') = p-1$, then also assume G and Γ' are both unipotent or both connected (the latter condition being equivalent to the unipotence/connectedness of $\Gamma'[p]$). Then there exists a p-divisible group Γ over A' such that $\Gamma_{K'} \simeq \Gamma \times_{A'} K'$, with Γ unipotent/connected if Γ' and G are unipotent/connected.

Before proving Theorem 5.2, let's explain how it is used to prove the following result:

Theorem 5.3. *With K' and $\mathcal{K}'$ as in Theorem 5.2, let $X_{/K'}$ be an abelian variety such that X acquires good reduction over $\mathcal{K}'$. Also, suppose that $X[p] \simeq G \times_{A'} K'$ for some G in $\mathfrak{FF}_{A'}$. If $e(\mathcal{K}') = p-1$, then assume that either G is unipotent and the Néron model of $X \times_{K'} \mathcal{K}'$ over $\mathcal{A}'$ has unipotent p-torsion, or that these finite flat group schemes are connected. Then X has good reduction over K'.*

Proof. Define $\Gamma_{K'}$ to be the p-divisible group associated to $X_{/K'}$, so $\Gamma_{K'} \times_{K'} \mathcal{K}' \simeq \Gamma' \times_{\mathcal{A}'} \mathcal{K}'$, where Γ' is the p-divisible group of the Néron model of $X \times_{K'} \mathcal{K}'$ over $\mathcal{A}'$. If $e(\mathcal{K}') = p-1$, our p-torsion hypothesis on the Néron model implies that Γ' is unipotent or connected. Theorem 5.2 ensures that $\Gamma_{K'} \simeq \Gamma \times_{A'} K'$ for some p-divisible group Γ over A'. By a theorem of Grothendieck [11, Cor 5.10], this implies that $X_{/K'}$ has good reduction.

We should stress that [11, Cor 5.10] is *much* stronger than what we actually need. All we need is the fact that if R is a henselian discrete valuation ring with a characteristic 0 fraction field K and with residue characteristic p, and X is an abelian variety over K which acquires good reduction over a finite extension of K, then X has good reduction over K if and only if the p-divisible group of X has good reduction over K. The proof of this fact can be extracted from the end of the proof of [11, Cor 5.10], requiring just the usual Néron-Ogg-Shafarevich criterion and none of the theory of semi-stable reduction for abelian schemes.

For the convenience of the reader, we explain in more detail the relevant part of Grothendieck's argument (phrased in a self-contained manner which bypasses semi-stability considerations). Let K'/K be a finite extension over which $X' = X \times_K K'$ acquires good reduction and let $\Gamma_{/R}$ be a p-divisible group equipped with an isomorphism $\Gamma_{/K} \simeq T_p(X)$ of p-divisible groups over K. We want to show that $X_{/K}$ has good reduction. Since the Néron model is of formation compatible with passage to the strict henselization of the base (either by [1, 7.2/2] or the actual construction), we can assume that R is strictly henselian, and then that K'/K is Galois with Galois group G. Let R' denote the valuation ring of K', and let k'/k denote the (finite, purely inseparable) extension of residue fields. Let $\mathcal{X}'_{/R'}$ denote the (proper) Néron model of $X'_{/K'}$.

Pick a prime $\ell \ne p$. Since the ℓ-adic Tate module $T_\ell(X')$ is a constant ℓ-divisible group (as it is the generic fiber of an ℓ-divisible group $T_\ell(\mathcal{X}')$ over the strictly henselian R'), there is a natural action of G on $T_\ell(X)$ via the 'geometric points' (which all arise over K'). We need to prove this action is trivial. Equivalently, for each n we have an action of G on $X'[\ell^n](K')$ defined by

$$g(x) = (1 \times g^{-1})^* \circ x \circ g^*,$$

where $g^* : \mathrm{Spec}(K') \to \mathrm{Spec}(K')$ and $(1 \times g^{-1})^* : X' = X \times_K K' \to X'$ are the natural maps, and we want to prove this action is trivial.

Letting $(\cdot)_g$ denote base change by the automorphism g^* (on either $\mathrm{Spec}(K')$ or $\mathrm{Spec}(R')$), the isomorphisms $X' \simeq X'_{g^{-1}}$ over g^* extend to isomorphisms $[g] : \mathcal{X}' \simeq \mathcal{X}'_{g^{-1}}$. Since k'/k is a purely inseparable extension, so $\mathrm{Aut}(k'/k)$ is trivial, passing to the closed fiber gives k'-automorphisms $\overline{[g]} : \overline{\mathcal{X}'} \simeq \overline{\mathcal{X}'}$. The Néron property of $\mathcal{X}'$ and the strict henselianity of R' give identifications

$$X'[\ell^n](K') = \mathcal{X}'[\ell^n](R') = \overline{\mathcal{X}'}[\ell^n](k')$$

under which the action of G on the left side translates into the induced action by the $\overline{[g]}$'s on the right side. Thus, it is enough to prove that for each $g \in G$, the automorphism $\overline{[g]}$ of the abelian variety $\overline{\mathcal{X}'}_{/k'}$ is the identity. This assertion does not have anything to do with ℓ and can be checked by looking at the action on the p-divisible group of $\overline{\mathcal{X}'}_{/k'}$. Thus, it is enough to prove that the p-divisible group maps

$$T_p([g]) : T_p(\mathcal{X}') \to T_p(\mathcal{X}'_{g^{-1}}) \simeq T_p(\mathcal{X}')_{g^{-1}}$$

(over $g^* : \mathrm{Spec}(R') \simeq \mathrm{Spec}(R')$) induce the identity on the closed fiber.

Now $\Gamma \times_R K \simeq T_p(X)$ enters the picture. Base changing to K', we get an isomorphism of p-divisible groups over K'

$$(\Gamma \times_R R') \times_{R'} K' \simeq T_p(\mathcal{X}') \times_{R'} K'$$

compatibly with the isomorphisms on each side with G-twists (with the ones on the right coming from the $T_p([g])$'s), so by Tate's theorem [19, Thm 4] we obtain an isomorphism of p-divisible groups $i : \Gamma \times_R R' \simeq T_p(\mathcal{X}')$ over R' such that the diagrams

$$\begin{array}{ccc} \Gamma \times_R R' & \stackrel{i}{\to} & T_p(\mathcal{X}') \\ \downarrow & & \downarrow [g] \\ (\Gamma \times_R R')_{g^{-1}} & \stackrel{(g^{-1})^*(i)}{\to} & T_p(\mathcal{X}')_{g^{-1}} \end{array}$$

commute. Passing to the closed fiber and noting that the left side reduces to the identity and the two rows reduce to the same map, it follows that the right side always reduces to the identity, as desired.

■

The unipotence/connectedness condition on the p-torsion of the Néron model is satisfied when $X_{/K'}$ is an elliptic curve with potentially supersingular reduction. This was the source of the original motivation for proving Theorem 5.2. More precisely, the theory of finite Honda systems can be used to study the deformation theory of Galois representations, and in particular the problem of classifying Galois representations of $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ which 'come from finite flat group schemes' over K' (or $\mathcal{K}'$). In [4] this is carried out, and one gets universal deformation rings $R_{K'}$ and $R_{\mathcal{K}'}$, together with a natural map $R_{K'} \to R_{\mathcal{K}'}$. This map turns out (by computational observation) to be an isomorphism. An 'explanation' for this isomorphism is provided by Theorem 5.2.

With the application to abelian varieties settled, we now carry out the computations:

Proof. (of Theorem 5.2) Note that Galois descent for schemes carries over to p-divisible groups because of the way in which they are built up out of genuine (i.e., non-formal) group schemes. This will be implicit in our use of descent below.

We can certainly replace K' by the maximal unramified extension of it within $\mathcal{K}'$, by Galois descent of (group) schemes, so we may (and will) assume that $\mathcal{K}'/K'$ is a *totally ramified* finite extension. In particular, the residue field $\mathcal{A}'/\mathfrak{n}$ can be identified with k. Also, note that as $\mathcal{K}'$-group schemes,

$$\Gamma'[p] \times_{A'} \mathcal{K}' \simeq \Gamma_{K'}[p] \times_{K'} \mathcal{K}' \simeq G \times_{A'} \mathcal{K}' \simeq (G \times_{A'} \mathcal{A}') \times_{\mathcal{A}'} \mathcal{K}',$$

so by Lemma 4.1 it follows that $\Gamma'[p] \simeq G \times_{A'} \mathcal{A}'$. This will be used below. We also emphasize that we *fix* a choice of isomorphism $\Gamma_{K'}[p] \simeq G \times_{A'} K'$ for the purposes of our constructions below. In what follows, we will consider only the case $e(\mathcal{K}') < p-1$. When $e(\mathcal{K}') = p-1$ and there are unipotence or connectedness conditions, the arguments go through with only minor notational changes (e.g., $LM^u_{\mathcal{A}'}$ in place of $LM_{\mathcal{A}'}$, etc.).

Let $LM_{\mathcal{A}'}(\Gamma') = (L', M')$ in $H^d_{\mathcal{A}'}$. As was noted in the second half of Lemma 4.12, we have

$$LM_{\mathcal{A}'}(\Gamma'[p^n]) \simeq (L'/p^n, M'/p^n),$$

with this isomorphism functorial in Γ' and compatible with change in n and base change as in §4. We will need to use these isomorphisms below in the case when the base is the valuation ring $\mathcal{A}''$ of the Galois closure $\mathcal{K}''$ of $\mathcal{K}'$ over K'. Note that since $\mathcal{K}'/K'$ is a totally ramified extension of degree $e \stackrel{\text{def}}{=} e(\mathcal{K}'/K')$ prime to p, we have $\mathcal{K}'' = \mathcal{K}'(\zeta_e)$ and so $e(\mathcal{K}'') = e(\mathcal{K}')$. This is the main reason it was important to reduce to the case in which $\mathcal{K}'/K'$ is totally ramified.

Since $\Gamma'[p] \simeq G \times_{A'} \mathcal{A}'$, we see that $\Gamma'[p]_k \simeq G_k$ (recall $k \simeq \mathcal{A}'/\mathfrak{n}$). Thus, $\mathcal{M}(G_k) \simeq \mathcal{M}(\Gamma'[p]_k) \simeq M'/p$. There is an A'-submodule $\overline{L} \subseteq (M'/p)_{A'}$ such that

$$LM_{A'}(G) \simeq (\overline{L}, M'/p)$$

and the results in §4 enable us to relate $\overline{L}$ and L'/p. In fact, since $A' \to \mathcal{A}'$ is a totally ramified finite extension, Lemma 4.5 and the isomorphism $G \times_{A'} \mathcal{A}' \simeq \Gamma'[p]$ imply that the natural map $\mathcal{A}' \otimes_{A'} ({M'}_{A'}) \to {M'}_{\mathcal{A}'}$ of $\mathcal{A}'$-modules induces an $\mathcal{A}'$-linear isomorphism

$$\mathcal{A}' \otimes_{A'} \overline{L} \simeq L'/p.$$

Now choose an A'-module direct summand $L \subseteq {M'}_{A'}$ such that $L/p \hookrightarrow {M'}_{A'}/p \simeq (M'/p)_{A'}$ has image $\overline{L}$. We make the crucial claim that we can choose $L \subseteq {M'}_{A'} \subseteq {M'}_{\mathcal{A}'}$ to lie inside of L' (recall that ${M'}_{A'} \to {M'}_{\mathcal{A}'}$ is injective, as it is compatible with

$$K' \otimes_{A'} ({M'}_{A'}) \simeq K' \otimes_A M' \hookrightarrow \mathcal{K}' \otimes_A M' \simeq \mathcal{K}' \otimes_{\mathcal{A}'} ({M'}_{\mathcal{A}'}),$$

by [7, Ch IV, §2.3, Prop 2.1]).

The construction of such an L will require a long argument. First of all, consider the commutative diagram

$$\begin{array}{ccc}
(M'/p)_{A'} & \to & (M'/p)_{\mathcal{A}'} \\
\downarrow & & \downarrow \\
CW_{k,A'}(\mathcal{R}_k) & \longrightarrow & CW_{k,\mathcal{A}'}(\mathcal{S}_k) \\
{\scriptstyle {w'}_{\mathcal{R}}}\downarrow & & \downarrow{\scriptstyle {w'}_{\mathcal{S}}} \\
\mathcal{R}_{K'}/\mathfrak{m}\mathcal{R} & \longrightarrow & \mathcal{S}_{\mathcal{K}'}/\mathfrak{n}\mathcal{S}
\end{array}$$

with $\mathcal{S} = \mathcal{A}' \otimes_{A'} \mathcal{R}$ the affine ring of $G \times_{A'} \mathcal{A}'$. The bottom row is an injection, as we noted at the beginning of the proof of Lemma 4.5. Recalling that $LM_{\mathcal{A}'}(\Gamma'[p]) \simeq (L'/p, M'/p)$, this diagram enables us to conclude that kernel $\overline{L} \subseteq (M'/p)_{A'}$ of the left column contains $(L' \cap ({M'}_{A'}))/p \hookrightarrow {M'}_{A'}/p \simeq (M'/p)_{A'}$. Here, the intersection uses the fact mentioned earlier that the natural map ${M'}_{A'} \to {M'}_{\mathcal{A}'}$ is an A'-linear injection, as it is compatible with the injection $K' \otimes_A M' \to \mathcal{K}' \otimes_A M'$. Also, the map $(L' \cap (M')_{A'})/p \to {M'}_{A'}/p$ is injective because $L' \cap ({M'}_{A'})$ is an A'-module direct summand of ${M'}_{A'}$. In order to justify this direct summand property, it is enough to show that L' is an $\mathcal{A}'$-module direct summand of ${M'}_{\mathcal{A}'} \supseteq {M'}_{A'}$. Since ${M'}_{\mathcal{A}'}$ is a finite free $\mathcal{A}'$-module, it suffices to check that $L'/\mathfrak{n} \to {M'}_{\mathcal{A}'}/\mathfrak{n}$ is injective. But this is clear, since we have an isomorphism via $L'/\mathfrak{n} \simeq {M'}_{\mathcal{A}'}/{M'}_{\mathcal{A}'}[1]$, with the latter a quotient of ${M'}_{\mathcal{A}'}/\mathfrak{n}$.

We will show that the inclusion

$$(L' \cap ({M'}_{A'}))/p \subseteq \overline{L}$$

of A'-submodules of $(M'/p)_{A'}$ is an equality. This will finish the proof, by taking $L \stackrel{\text{def}}{=} L' \cap (M'_{A'})$. Note that at this point it is not even clear that $L' \cap ({M'}_{A'})$ would ever be *non-zero* (for $e(\mathcal{K}') > 1$). Proving that the above inclusion is an equality is something that can be checked after making a faithfully flat base extension, so we will show that

$$\mathcal{A}' \otimes_{A'} ((L' \cap ({M'}_{A'})/p)) \hookrightarrow \mathcal{A}' \otimes_{A'} \overline{L}$$

is an isomorphism. Recall from our discussion of totally ramified base change in §4 that the natural $\mathcal{A}'$-linear map from $\mathcal{A}' \otimes_{A'} \overline{L}$ to $(M'/p)_{\mathcal{A}'}$ is *injective* with image L'/p (since $G \times_{A'} \mathcal{A}' \simeq \Gamma'[p]$!), so what we wish to prove is equivalent to showing that $(L' \cap ({M'}_{A'}))/p$ and $\overline{L}$ have images in $(M'/p)_{\mathcal{A}'}$ (via $(M'/p)_{A'} \to (M'/p)_{\mathcal{A}'}$)

with the same $\mathcal{A}'$-linear span. Since the $\mathcal{A}'$-linear span of the image of $\overline{L}$ is precisely L'/p, it is sufficient to prove that the $\mathcal{A}'$-linear map

$$\mathcal{A}' \otimes_{A'} (L' \cap (M'_{A'})) \hookrightarrow L'$$

is an isomorphism.

The first thing we will show is that the above injection remains injective modulo $\mathfrak{n}$, so $\mathcal{A}' \otimes_{A'} (L' \cap (M'_{A'}))$ is at least an $\mathcal{A}'$-module direct summand of L'. Well, modulo $\mathfrak{n}$ the map is $(L' \cap (M'_{A'}))/\mathfrak{m} \to L'/\mathfrak{n}$ and this fits into the commutative (!) diagram

$$\begin{array}{ccccc} (L' \cap (M'_{A'}))/\mathfrak{m} & \longrightarrow & L'/\mathfrak{n} & \xrightarrow{\sim} & M'_{\mathcal{A}'}/M'_{\mathcal{A}'}[1] \\ \big\downarrow & & & & \big\uparrow \simeq \\ \overline{L}/\mathfrak{m} & \xrightarrow{\sim} & \operatorname{coker} \mathcal{F}_{M'/p, A'} & \xleftarrow{\sim} & M'/FM' \end{array}$$

so if the left column is injective, then the map $(L' \cap (M'_{A'}))/\mathfrak{m} \to L'/\mathfrak{n}$ is injective also, as desired. The injectivity of the left column says exactly that $(L' \cap (M'_{A'}))/p \subseteq \overline{L}$ is an A'-module direct summand; in order to prove this latter condition, it suffices to prove that that $(L' \cap (M'_{A'}))/p \subseteq (M'/p)_{A'} \simeq M'_{A'}/p$ is an A'-module direct summand. But as we noted above, $L' \cap (M'_{A'})$ is an A'-module direct summand of $M'_{A'}$, so just reduce modulo p.

Since the inclusion $\mathcal{A}' \otimes_{A'} (L' \cap (M'_{A'})) \hookrightarrow L'$ has been proven to be an isomorphism onto an $\mathcal{A}'$-module direct summand, in order to prove that this submodule actually fills up all of L', it is enough to check that we have an isomorphism after passing to the generic fiber, which is to say that we want to show

$$\mathcal{K}' \otimes_{A'} (L' \cap (M'_{A'})) \stackrel{?}{=} \mathcal{K}' \otimes_{\mathcal{A}'} L'$$

inside of $\mathcal{K}' \otimes_{A'} (M'_{A'}) = \mathcal{K}' \otimes_{\mathcal{A}'} (M'_{\mathcal{A}'})$. If $\mathcal{K}' \otimes_{\mathcal{A}'} L' \subseteq \mathcal{K}' \otimes_{\mathcal{A}'} (M'_{\mathcal{A}'}) \simeq \mathcal{K}' \otimes_{K'} (K' \otimes_{A'} (M'_{A'}))$ is a K'-*rational subspace* (i.e., of the form $\mathcal{K}' \otimes_{K'} V$ for some K'-subspace V of $K' \otimes_{A'} (M'_{A'}) \simeq K' \otimes_A M'$), then

$$\begin{aligned} \mathcal{K}' \otimes_{\mathcal{A}'} L' &= \mathcal{K}' \otimes_{K'} \left((\mathcal{K}' \otimes_{\mathcal{A}'} L') \cap (K' \otimes_{A'} (M'_{A'})) \right) \\ &= \mathcal{K}' \otimes_{K'} (K' \otimes_{A'} (L' \cap (M'_{A'}))) \\ &= \mathcal{K}' \otimes_{A'} (L' \cap (M'_{A'})), \end{aligned}$$

as desired. Clearly it even suffices to prove that the $\mathcal{K}''$-subspace

$$\mathcal{K}'' \otimes_{\mathcal{A}'} L' \subseteq \mathcal{K}'' \otimes_{\mathcal{A}'} (M'_{\mathcal{A}'})$$

is a K'-rational subspace, with $\mathcal{K}''$ the Galois closure of $\mathcal{K}'$ over K'. Note that $\mathcal{K}'' = \mathcal{K}'(\zeta_{e_0})$, where $e_0 \stackrel{\text{def}}{=} e(\mathcal{K}'/K')$, so the inclusion of valuation rings $\mathcal{A}' \to \mathcal{A}''$ is a finite *étale* extension and $\mathcal{A}''$ has $A[\zeta_{e_0}]$ as its maximal unramified subring (i.e, this is the Witt ring of the perfect residue field $k(\zeta_{e_0})$ of $\mathcal{A}''$ and $A = W(k)$ as usual). This will permit us to apply our previous base change formalism (after passing to an inverse limit).

The idea behind the proof that $\mathcal{K}'' \otimes_{\mathcal{A}'} L' \subseteq \mathcal{K}'' \otimes_{\mathcal{A}'} M'_{\mathcal{A}'} = \mathcal{K}'' \otimes_{K'} (K' \otimes_{A'} (M'_{A'}))$ is K'-rational is that $(L', M') = LM_{\mathcal{A}'}(\Gamma')$ where $\Gamma' \times_{\mathcal{A}'} \mathcal{K}' \simeq \Gamma_{K'} \times_{K'} \mathcal{K}'$. This latter isomorphism base extends to the isomorphism $\Gamma' \times_{\mathcal{A}'} \mathcal{K}'' \simeq \Gamma_{K'} \times_{K'} \mathcal{K}''$ and we now ought to be able to transfer Galois descent formalism of $\mathrm{Gal}(\mathcal{K}''/K')$ from the right side to the left side.

More precisely, we note that for $L'' = \mathcal{A}'' \otimes_{\mathcal{A}'} L'$ and $M'' = A[\zeta_{e_0}] \otimes_A M'$,

$$LM_{\mathcal{A}''}(\Gamma' \times_{\mathcal{A}'} \mathcal{A}'') \simeq (L'', M'').$$

To see this, simply consider the analogous assertion for the p^n-torsion via Theorem 4.6 and pass to the inverse limit, using the fact that the natural $\mathcal{A}''$-module map

$$M''_{\mathcal{A}''} \to \varprojlim ((M''/p^n)_{\mathcal{A}''})$$

is an isomorphism, thanks to $(M''_{\mathcal{A}''})/p^n \simeq (M''/p^n)_{\mathcal{A}''}$. Since $\Gamma'' \stackrel{\text{def}}{=} \Gamma' \times_{\mathcal{A}'} \mathcal{A}''$ has generic fiber isomorphic to $\Gamma_{K'} \times_{K'} \mathcal{K}''$, for each $\gamma \in \mathrm{Gal}(\mathcal{K}''/K')$ we have a morphism of p-divisible groups over $\mathcal{K}''$

$$[\gamma] : \Gamma'' \times_{\mathcal{A}''} \mathcal{K}'' \to (\Gamma'' \times_{\mathcal{A}''} \mathcal{K}'')_\gamma \simeq \Gamma''_\gamma \times_{\mathcal{A}''} \mathcal{K}''$$

satisfying $[\mathrm{id}_{\mathcal{K}''}] = \mathrm{id}_{\Gamma'' \times_{\mathcal{A}''} \mathcal{K}''}$ and $[\gamma]_{\widetilde{\gamma}} \circ [\widetilde{\gamma}] = [\widetilde{\gamma} \circ \gamma]$ for all γ, $\widetilde{\gamma} \in \mathrm{Gal}(\mathcal{K}''/K')$.

By Tate's full faithfulness theorem for p-divisible groups [19, Thm 4], or even just by repeated applications of Lemma 4.1 (since $e(\mathcal{K}'') = e(\mathcal{K}')$), we get the same formalism canonically over $\mathcal{A}''$. We will use this formalism to show that for each $\gamma \in \mathrm{Gal}(\mathcal{K}''/K')$, the $\mathcal{K}''$-semilinear map

$$\gamma \otimes 1 : \mathcal{K}'' \otimes_{\mathcal{A}'} (M'_{\mathcal{A}'}) \to \mathcal{K}'' \otimes_{\mathcal{A}'} (M'_{\mathcal{A}'})$$

takes the subspace $\mathcal{K}'' \otimes_{\mathcal{A}'} L'$ to itself. The classical formulation of Galois descent (i.e., the normal basis theorem) then would yield that $\mathcal{K}'' \otimes_{\mathcal{A}'} L'$ is K'-rational, as desired.

To start off, define L''_γ and $M''_{\overline{\gamma}}$ to be the base extensions of L'' and M'' by the respective base changes $\gamma : \mathcal{A}'' \to \mathcal{A}''$ and $\overline{\gamma} : A[\zeta_{e_0}] \to A[\zeta_{e_0}]$. Passing to the inverse limit on our discussion in §4 gives rise to the natural $\mathcal{A}''$-module isomorphism

$$j_\gamma : \mathcal{A}'' \otimes_{\mathcal{A}''} (M''_{\mathcal{A}''}) \simeq (M''_{\overline{\gamma}})_{\mathcal{A}''},$$

where on the left side we use $\gamma : \mathcal{A}'' \to \mathcal{A}''$. A simple 'passage to the inverse limit' argument based on Theorem 4.6 also shows that

$$LM_{\mathcal{A}''}(\Gamma''_\gamma) \simeq (L''_\gamma, M''_{\overline{\gamma}}),$$

where we use j_γ to embed L''_γ as an $\mathcal{A}''$-submodule of $(M''_{\overline{\gamma}})_{\mathcal{A}''}$.

The 'Galois descent' formalism over $\mathcal{A}''$ translates into $D_{k(\zeta_{e_0})}$-module maps

$$[\gamma] : M''_{\overline{\gamma}} \to M''$$

for all $\gamma \in \mathrm{Gal}(\mathcal{K}''/K')$, such that $[\gamma]_{\mathcal{A}''}$ takes L''_γ over into L'' (!) and

$$[\gamma_1] \circ [\gamma_2]_{\overline{\gamma_1}} = [\gamma_1 \circ \gamma_2].$$

Consider the γ-semilinear map of $\mathcal{A}''$-modules

$$M''_{\mathcal{A}''} \to \mathcal{A}'' \otimes_{\mathcal{A}''} (M''_{\mathcal{A}''}) \xrightarrow{[\gamma]_{\mathcal{A}''} \circ j_\gamma} M''_{\mathcal{A}''}$$

given by $m \mapsto [\gamma]_{\mathcal{A}''} \circ j_\gamma(1 \otimes m)$ (of course, the base change $\mathcal{A}'' \to \mathcal{A}''$ implicit in the tensor product is the one induced by γ). Since the map $M''_{\mathcal{A}''} \to \mathcal{A}'' \otimes_{\mathcal{A}''} (M''_{\mathcal{A}''})$ used above takes L'' over to $j_\gamma^{-1}(L''_\gamma)$ (by definition!), we see that the composite γ-semilinear map takes L'' over to itself. Therefore, as long as this map fixes every element of the natural copy of $M'_{\mathcal{A}'}$ sitting inside of $M''_{\mathcal{A}''}$, it follows that the induced semilinear map on $\mathcal{K}'' \otimes_{\mathcal{A}''} (M''_{\mathcal{A}''}) = \mathcal{K}'' \otimes_{\mathcal{A}'} (M'_{\mathcal{A}'})$ is exactly $\gamma \otimes 1$. In other words, $\gamma \otimes 1$ takes $\mathcal{K}'' \otimes_{\mathcal{A}''} L''$ over into itself, which is *exactly* what we had promised to show.

It remains (for the construction of L inside of L') to check that $M'_{\mathcal{A}'}$ is fixed in the manner just described. Since we have an inclusion of subsets of $M''_{\mathcal{A}''}$ given by

$$M' \subseteq M'' \subseteq M''_{\mathcal{A}''}$$

in the obvious way, it is in fact enough to consider the $A[\zeta_{e_0}]$-linear map

$$[\gamma] : M''_{\overline{\gamma}} \to M''$$

and to show that this takes $1 \otimes m$ to m for every $m \in M' \hookrightarrow M''$. We can rewrite this as a $\overline{\gamma}$-semilinear map of $A[\zeta_{e_0}]$-modules

$$A[\zeta_{e_0}] \otimes_A M' \to A[\zeta_{e_0}] \otimes_A M'$$

and we want to show that for all $m \in M'$, the element $1 \otimes m$ is fixed by this map. That is, the (abstract) semilinear action of $\mathrm{Gal}(K'(\zeta_{e_0})/K') \simeq \mathrm{Gal}(K(\zeta_{e_0})/K) \simeq \mathrm{Gal}(k(\zeta_{e_0})/k)$ on $A[\zeta_{e_0}] \otimes_A M'$ arising from the above generic fiber descent formalism should fix M' and so should be the obvious action.

By [7, Ch II, §2.2], this 'obvious' action is precisely what we get if we use the functor $\mathcal{M}$ to translate the canonical Galois descent data for $(\Gamma'_k) \times_k k(\zeta_{e_0})$ down to Γ'_k into the language of of Dieudonné modules (much like in the discussion at the beginning of this section). The prolonged 'Galois descent data' formalism of $\mathrm{Gal}(\mathcal{K}''/K')$ on $\Gamma' \times_{\mathcal{A}'} \mathcal{A}''$ induces (abstract) 'Galois descent data' formalism of $\mathrm{Gal}(K'(\zeta_{e_0})/K') \simeq \mathrm{Gal}(k(\zeta_{e_0})/k)$ on the closed fiber; we must verify that this is exactly the usual Galois descent data on this closed fiber. The key point will be that the projection $\mathrm{Gal}(\mathcal{K}''/K') \twoheadrightarrow \mathrm{Gal}(K'(\zeta_{e_0})/K')$ has a section, namely the inverse to the natural isomorphism $\mathrm{Gal}(\mathcal{K}''/\mathcal{K}') \simeq \mathrm{Gal}(K'(\zeta_{e_0})/K')$ which arises from the linear disjointness of $\mathcal{K}'$ and $K'(\zeta_{e_0})$ over K'.

Since $\Gamma' \times_{A'} \mathcal{K}' \simeq \Gamma_{K'} \times_{K'} \mathcal{K}'$ as p-divisible groups over $\mathcal{K}'$, we are reduced to showing that if we begin with the canonical Galois descent data for $\left(\Gamma' \times_{\mathcal{A}'} \mathcal{K}'\right) \times_{\mathcal{K}'} \mathcal{K}''$ down to $\Gamma' \times_{\mathcal{A}'} \mathcal{K}'$ and 'formally' prolong it to the entire p-divisible group $\Gamma' \times_{\mathcal{A}'} \mathcal{A}''$ (by Tate's theorem or Lemma 4.1), then the induced formalism over the closed fiber is exactly the canonical Galois descent data for $(\Gamma' \times_{\mathcal{A}'} k) \times_k k(\zeta_{e_0})$ down to $\Gamma' \times_{\mathcal{A}'} k = \Gamma'_k$. However, this assertion is a direct consequence of the way in which Galois descent of fields is realized as faithfully flat descent and the fact that $\mathcal{A}' \to \mathcal{A}''$ is a *Galois* extension of discrete valuation rings (see [1, §6.2, Example B] for more details). This completes the construction of the desired $L \subseteq M'_{A'} \subseteq M'_{\mathcal{A}'}$ lying inside of L'.

Let us see how such an L enables us to construct Γ of the desired sort. The commutative diagram

$$\begin{array}{ccccc} L/\mathfrak{m} & \longrightarrow & M'_{\mathcal{A}'}/M'_{\mathcal{A}'}[1] & \overset{\sim}{\longleftarrow} & M'/FM' \\ \big\downarrow & & & & \big\downarrow \simeq \\ \overline{L}/\mathfrak{m} & \overset{\sim}{\longrightarrow} & \operatorname{coker} \mathcal{F}_{M'/p,A'} & \overset{\sim}{\longleftarrow} & (M'/p)/F(M'/p) \end{array}$$

shows that (L, M') lies in $H^d_{A'}$, so $(L, M') \simeq LM_{A'}(\Gamma)$ for a p-divisible group Γ over A'. Certainly the $\mathcal{A}'$-submodule

$$L_{\mathcal{A}'}(\Gamma \times_{A'} \mathcal{A}') \hookrightarrow M'_{\mathcal{A}'} \subseteq \mathcal{K}' \otimes_A M'$$

contains $L = L_{A'}(\Gamma)$. Thus, $\mathcal{A}' \otimes_{A'} L$ lies inside of $L_{\mathcal{A}'}(\Gamma \times_{A'} \mathcal{A}')$. Modulo $\mathfrak{n}$, however, this inclusion is precisely the top row in the commutative diagram

$$\begin{array}{ccc} L/\mathfrak{m} & \longrightarrow & L_{\mathcal{A}'}(\Gamma \times_{A'} \mathcal{A}')/\mathfrak{n} \\ \simeq \big\downarrow & & \big\downarrow \simeq \\ M'_{\mathcal{A}'}/M'_{\mathcal{A}'}[1] & & M'_{\mathcal{A}'}/M'_{\mathcal{A}'}[1] \\ \simeq \big\uparrow & & \big\uparrow \simeq \\ M'/FM' & = & M'/FM' \end{array}$$

so $\mathcal{A}' \otimes_{A'} L = L_{\mathcal{A}'}(\Gamma \times_{A'} \mathcal{A}')$ inside of $\mathcal{K}' \otimes_A M'$. Since we are assuming that L lies inside of L', so $\mathcal{A}' \otimes_{A'} L \subseteq L'$, the commutative diagram

$$\begin{array}{ccc} (\mathcal{A}' \otimes_{A'} L)/\mathfrak{n} & \longrightarrow & L'/\mathfrak{n} \\ \simeq \big\downarrow & & \big\downarrow \simeq \\ M'_{\mathcal{A}'}/M'_{\mathcal{A}'}[1] & = & M'_{\mathcal{A}'}/M'_{\mathcal{A}'}[1] \end{array}$$

forces $\mathcal{A}' \otimes_{A'} L = L'$. Therefore, $LM_{\mathcal{A}'}(\Gamma') = (L', M') = (\mathcal{A}' \otimes_{A'} L, M')$ is isomorphic to $LM_{\mathcal{A}'}(\Gamma \times_{A'} \mathcal{A}')$, from which we get an isomorphism of formal $\mathcal{A}'$-group schemes $\Gamma \times_{A'} \mathcal{A}' \simeq \Gamma'$.

Passing to the generic fiber, we get an isomorphism of p-divisible groups over $\mathcal{K}'$

$$(\Gamma \times_{A'} K') \times_{K'} \mathcal{K}' \simeq \Gamma' \times_{\mathcal{A}'} \mathcal{K}' \simeq \Gamma_{K'} \times_{K'} \mathcal{K}' .$$

Recall that by hypothesis, $\Gamma_{K'}[p] \simeq G \times_{A'} K'$ for some G in $\mathcal{FF}_{A'}$ and Γ is *defined* so that

$$LM_{A'}(\Gamma[p]) \simeq (L/p, M'/p) = (\overline{L}, M'/p) \simeq LM_{A'}(G),$$

so $G \simeq \Gamma[p]$. On the generic fiber this gives $\Gamma_{K'}[p] \simeq \Gamma[p] \times_{A'} K'$. Hence, $\Gamma \times_{A'} K'$ and $\Gamma_{K'}$ are two p-divisible groups over K' which become isomorphic over $\mathcal{K}'$ and have p-torsion subgroups which are isomorphic over K'.

Since $\Gamma_{K'}$ and $\Gamma \times_{A'} K'$ have the same height h (as this can be computed after base extension to $\mathcal{K}'$), upon fixing a choice of algebraic closure $\overline{K'}$ of K' and a K'-embedding $\mathcal{K}' \hookrightarrow \overline{K'}$, we may view $\Gamma_{K'}$ and $\Gamma \times_{A'} K'$ as continuous Galois representations

$$\rho_i : \mathrm{Gal}(\overline{K'}/K') \to \mathrm{GL}_h(\mathbf{Z}_p)$$

$(i = 1, 2)$ such that $\rho_1|_{\mathrm{Gal}(\overline{K'}/\mathcal{K}')} \simeq \rho_2|_{\mathrm{Gal}(\overline{K'}/\mathcal{K}')}$ and for $\overline{\rho}_i \overset{\mathrm{def}}{=} \rho_i \bmod p$, there is an isomorphism $\overline{\rho}_1 \simeq \overline{\rho}_2$. In fact, we claim that the *same* matrix $\mu \in \mathrm{GL}_h(\mathbf{Z}_p)$ can be used to conjugate $\rho_1|_{\mathrm{Gal}(\overline{K'}/\mathcal{K}')}$ into $\rho_2|_{\mathrm{Gal}(\overline{K'}/\mathcal{K}')}$ and $\overline{\rho}_1$ into $\overline{\rho}_2$. Such a conjugation by μ gives a 'compatible' choice of bases and so would allow us to assume that $\rho_1|_{\mathrm{Gal}(\overline{K'}/\mathcal{K}')}$ and $\rho_2|_{\mathrm{Gal}(\overline{K'}/\mathcal{K}')}$ are literally *equal*, as are $\overline{\rho}_1$ and $\overline{\rho}_2$. Lemma 5.4 then would yield $\rho_1 \simeq \rho_2$, so

$$\Gamma_{K'} \simeq \Gamma \times_{A'} K',$$

which is what we wanted to prove.

The rigorous justification of the existence of μ is based on giving a more canonical description of the meaning of the existence of μ. Consider the isomorphism

$$(\Gamma \times_{A'} K') \times_{K'} \mathcal{K}' \simeq \Gamma_{K'} \times_{K'} \mathcal{K}'$$

from above. This induces an isomorphism of $\mathcal{K}'$-group schemes

$$\varphi_1 : (\Gamma[p] \times_{A'} K') \times_{K'} \mathcal{K}' \simeq \Gamma_{K'}[p] \times_{K'} \mathcal{K}' \simeq (G \times_{A'} K') \times_{K'} \mathcal{K}',$$

the latter isomorphism being induced by the base extension $K' \to \mathcal{K}'$. However, by using the isomorphism $G \simeq \Gamma[p]$ obtained at the end of the above lengthy construction of L, the base extension $A' \to \mathcal{K}'$ gives rise to an isomorphism

$$\varphi_2 : (\Gamma[p] \times_{A'} K') \times_{K'} \mathcal{K}' \simeq (G \times_{A'} K') \times_{K'} \mathcal{K}'.$$

The existence of μ is precisely the assertion that $\varphi_1 = \varphi_2$.

These maps φ_1, φ_2 lift to isomorphisms of the corresponding $\mathcal{A}'$-group schemes, so by the faithfulness of passage to the closed fiber (Corollary 3.7) it suffices to check that the induced maps on the closed fibers coincide. Since $A' \to \mathcal{A}'$ induces an isomorphism on the residue fields, we have two (abstract) isomorphisms

$$\mathcal{M}(G_k) \simeq \mathcal{M}(\Gamma[p]_k)$$

which we must prove are the same. From $\Gamma'[p] \simeq G \times_{A'} \mathcal{A}'$ we get $\mathcal{M}(G_k) \simeq \mathcal{M}(\Gamma'[p]_k) \simeq M'/p$; an isomorphism $M' \simeq \mathcal{M}(\Gamma_k)$ is furnished by the *definition* of Γ, so we have also an isomorphism $M'/p \simeq \mathcal{M}(\Gamma[p]_k)$. The composite isomorphism $\mathcal{M}(G_k) \simeq \mathcal{M}(\Gamma[p]_k)$ is precisely the map induced from φ_1. Now consider the isomorphism $\Gamma[p] \simeq G$ constructed above via Honda systems (actually, it is the inverse that we constructed). On the level of closed fibers, it is obvious that we have *exactly* the same map on the Dieudonné modules as was just described. Hence, φ_1 and φ_2 do indeed coincide. ∎

We now prove the lemma which was critical in the above proof.

Lemma 5.4. *Let G be a profinite group and H an open normal subgroup of index prime to p, with p a prime. Let $\rho_i : G \to \mathrm{GL}_n(\mathbf{Z}_p)$ be two continuous representations for which $\rho_1|_H = \rho_2|_H$ and $\overline{\rho}_1 = \overline{\rho}_2$, where $\overline{\rho}_i$ is the residual representation $\rho_i \bmod p$. Then $\rho_1 \simeq \rho_2$.*

Proof. Let ρ denote the common restriction of ρ_1 and ρ_2 to H. Define $f(g) = \rho_1(g)\rho_2(g)^{-1}$. It is easy to check that this is a function from the group G/H to the group

$$K_n = \ker(\mathrm{GL}_n(\mathbf{Z}_p) \to \mathrm{GL}_n(\mathbf{F}_p)).$$

Moreover, given that ρ_2 is a representation, the condition that ρ_1 is a representation is equivalent to the condition

$$f(g_1 g_2) = f(g_1) \cdot \rho_2(g_1) f(g_2) \rho_2(g_1)^{-1}.$$

In particular, if we take $g_1 = h$ to be any element of H and $g_2 = g$ to be any element of G, then

$$f(g) = f(hg) = \rho(h) f(g) \rho(h)^{-1},$$

so f takes its values in the subgroup K_n^H of invariants under $\rho = \rho_2|_H$. Note that this is a closed subgroup of K_n and so is a pro-p group with a G/H-stable solvability series (using the conjugation action of ρ_2).

Since the abelian higher cohomology of G/H on abelian p-groups always vanishes, the standard short exact sequence arguments and compactness of K_n^H show that $H^1(G/H, K_n^H)$ is the trivial pointed set (here, we are using continuous non-abelian cohomology). Hence, there exists $x \in K_n^H$ such that

$$f(g) = x^{-1} \rho_2(g) x \rho_2(g)^{-1}.$$

In other words, $x \in \mathrm{GL}_n(\mathbf{Z}_p)$ conjugates ρ_2 into ρ_1, so we have the desired isomorphism. ∎

We conclude by mentioning a question raised by Nicholas Katz. Fix a prime p. Choose a local field K with characteristic 0 and having a valuation ring with a perfect characteristic p residue field. Let K'/K be a finite extension. Consider an abelian variety $A_{/K}$ such that $A_{/K'}$ has good reduction. For a positive integer n, say that $A[p^n]$ has *good reduction over* K if there is a finite flat $\mathcal{O}_K$-group scheme G and a K-group scheme isomorphism $A[p^n] \simeq G \times_{\mathcal{O}_K} K$. Does there exist an explicit strictly increasing sequence of positive integers $e(1,p) < e(2,p) < \cdots < e(n,p) < \ldots$ so that if (for some n) $e(K') < e(n,p)$ and $A[p^n]$ has good reduction over K, then A has good reduction over K? Intuitively, if K'/K is fixed, there should be a p-power torsion level depending only on $e(K')$ so that detecting good reduction for an abelian variety over K is equivalent to good reduction over K' and good reduction for a suitable torsion level over K. We showed above that one should take $e(1,p) = p - 1$. The existence of a sequence $\{e(n,p)\}$ would be a nice complement to [11, Cor 5.10].

Appendix A

In this appendix, we would like to clarify an important point in the proof of Fontaine's classification of smooth p-formal group schemes over A', where $e(A') < p - 1$ (or $e(A') \leq p - 1$ if we restrict attention to connected or unipotent objects). The point of interest arises on [7, p. 180], where one has a system of equations

$$c + Ax + Bx^p = 0,$$

where x is an unknown vector with n entries in an $\mathbf{F}_p$-algebra S, c is a given vector in S^n, A is an invertible n by n matrix over S, B is a nilpotent n by n matrix over S, and x^p denotes the vector obtained from x by raising the entries to the pth power. It is asserted that such a system of equations admits a unique solution. In this level of generality, the claim is not quite true, because the matrix $A^{-1}B$ might not be nilpotent. We would like to explain why this does not cause problems. More precisely, we will show that in the particular setting considered in [7], the matrix $A^{-1}B$ is actually nilpotent and that this suffices to get existence and uniqueness of solutions. Since this is just a technicality that is only of interest to someone reading [7], we take the liberty here of using the notation in [7] without comment (it would be too much of a digression to recall here all of the notation we need).

For a 'bad' example, consider the hypothetical possibility that $\alpha_1^c = X_1 + X_2 + (1/p)X_2^p$, $\alpha_2^c = X_1$, $x_2^0 \equiv 0 \bmod p$, and x_1^0 is allowed to be anything. We then get the simultaneous equations

$$y_1 + y_2 + y_2^p + \gamma_1 = 0, \quad y_1 + \gamma_2 = 0.$$

If $\gamma_1 = \gamma_2 = 0$, then $(0,1)$ and $(0,0)$ are both solutions. If $\gamma_1 = 1$, $\gamma_2 = 0$, then we need to solve the equation $T^p - T + 1$, which has no solution if our characteristic p ring is $\mathbf{F}_p$. We need to make fuller use of our group scheme setting in order to rule out examples of this type. The key fact is:

Theorem A.1. *There is a matrix identity*

$$\left(\frac{\partial \alpha_i^c}{\partial X_\ell}\right)^{-1}\left(\frac{\partial^p \alpha_i^c}{\partial X_j^p}\right) \equiv -\left(\left(\frac{\partial V(X_\ell)}{\partial X_j}\right)^p\right) \bmod \widehat{\mathfrak{m}},$$

where the right side is the negative of the matrix obtained by taking the (semi-linear) matrix of V with respect to the k-basis $\{X_i\}$ of the $k[V]$-module $\mathfrak{m}/\mathfrak{m}^2 \simeq \underline{M}/F\underline{M} = \underline{M}^c/F\underline{M}^c$ and raising the entries to the pth power.

Granting this, we can choose coordinates X_i so that the matrix of the nilpotent V on $\mathfrak{m}/\mathfrak{m}^2$ with respect to the basis $\{X_i\}$ has all entries 0, except for some lower diagonal $(i, i+1)$ entries which might equal 1. It would then remain to prove:

Lemma A.2. *Let S be an $\mathbf{F}_p$-algebra, $c \in S^n$, $N = (\nu_{ij})$ an n by n matrix with ν_{ij} nilpotent for $j \neq i+1$. Then the vector equation*

$$x = c + Nx^p$$

has a unique solution $x \in S^n$ (here, as above, $x^p \in S^n$ denotes the vector obtained by raising the entries in x to the pth power).

Proof. By standard limit arguments, we may assume S is a localization of a finite type $\mathbf{F}_p$-algebra. Uniqueness can then be checked over the completion, and once we have uniqueness in general, existence can be obtained by descent from the completion. Thus, we may assume that S is a complete local noetherian $\mathbf{F}_p$-algebra with a *finite* residue field k, in which case it is enough to work over the artinian quotients of S. That is, we may assume S is a *finite* local $\mathbf{F}_p$-algebra. We want to show that the map of sets

$$\varphi : S^n \to S^n$$

given by $x \mapsto x - Nx^p$ is a bijection. Since S is a finite set, it suffices to check injectivity. Since φ is additive, it is enough to check that $x = Nx^p$ implies $x = 0$. If $x \equiv 0 \bmod \mathfrak{m}_S$, we can iterate, so it is enough to pass to $S/\mathfrak{m}_S$. That is, we may assume S is a *field* and $N = (\nu_{ij})$ is a lower diagonal matrix. Any product of $n+1$ such matrices is 0, so $x = Nx^p = N \cdot \dots \cdot N^{(p^n)} x^{p^{n+1}} = 0$, where $N^{(p^r)} = (\nu_{ij}^{p^r})$. ■

Now we prove Theorem A.1

Proof. The key input from the theory of formal group schemes is [7, Ch III, Prop 3.1], which gives $a^c_{-1,i} = V(a^c_{0,i})$. Since $R^c = k[\![X_1, \dots, X_n]\!]$, we have a σ^{-1}-linear ring map $V : k[\![X_1, \dots, X_n]\!] \to k[\![X_1, \dots, X_n]\!]$ (where σ denotes absolute Frobenius on k) and by the Chain Rule we compute that for $f \in k[\![X_1, \dots, X_n]\!]$,

$$\frac{\partial}{\partial X_j}(V(f)) = \sum_\ell \sigma^{-1}\left(\frac{\partial f}{\partial X_\ell}\,|_{(\sigma(V(X_1)),\dots,\sigma(V(X_n)))}\right) \cdot \frac{\partial V(X_\ell)}{\partial X_j}.$$

Thus,

$$\frac{\partial a^c_{-1,i}}{\partial X_j} = \sum_\ell \sigma^{-1}\left(\frac{\partial a^c_{0,i}}{\partial X_\ell}\,|_{(\sigma(V(X_1)),\dots,\sigma(V(X_n)))}\right) \cdot \frac{\partial V(X_\ell)}{\partial X_j}.$$

This yields

$$\begin{aligned}
\frac{\partial^p \alpha^c_i}{\partial X_j^p} &\equiv (p-1)!\left(\frac{\partial a^c_{-1,i}}{\partial X_j}\right)^p \bmod \widehat{\mathfrak{m}} \\
&\equiv -\sum_\ell \sigma^{-1}\left(\frac{\partial a_{0,i}}{\partial X_\ell}\,|_0\right)^p \left(\frac{\partial V(X_\ell)}{\partial X_j}\,|_0\right)^p \bmod \widehat{\mathfrak{m}} \\
&\equiv -\sum_\ell \frac{\partial \alpha^c_i}{\partial X_\ell}\,|_0 \cdot \left(\frac{\partial V(X_\ell)}{\partial X_j}\,|_0\right)^p \bmod \widehat{\mathfrak{m}}.
\end{aligned}$$

Therefore, we get the matrix identity asserted in the statement of the theorem. ■

We conclude by noting that the existence and uniqueness assertion for the system of equations on [7, p. 183] is a special case of the general claim that for any $\mathbf{F}_p$-algebra S, any n by n matrix A with entries in S, and $\gamma \in S^n$ any vector with nilpotent entries, the vector equation

$$\gamma + x + Ax^p = 0$$

has a unique solution in S^n with nilpotent entries. The proof proceeds exactly like the proof in the Lemma A.2, via reduction to the case in which S is a finite local $\mathbf{F}_p$-algebra, and we then want to show that the additive map $S^n \to S^n$ given by $x \mapsto x + Ax^p$ induces a bijection on vectors with nilpotent entries. The map certainly sends 'nilpotent' vectors to 'nilpotent' vectors, so by a counting argument it is enough to check that if $x + Ax^p = 0$ and x has nilpotent entries, then $x = 0$. But this is clear.

References

[1] S. Bosch, W. Lütkebohmert, M. Raynaud, *Néron models*, Springer-Verlag, 1980.
[2] C. Breuil, *Schémas en roupes sur un anneau de valuation discrète complet très ramifié*, preprint.
[3] C. Breuil, B. Conrad, F. Diamond, R. Taylor, *On the modularity of elliptic curves over* $\mathbf{Q}$, in preparation.
[4] B. Conrad, *Ramified deformation problems*, Duke Mathematical Journal (3) **97** (1999), pp. 439–511.
[5] B. Conrad, F. Diamond, R. Taylor, *Modularity of certain potentially Barsotti-Tate Galois representations*, Journal of the American Math. Society (2) **12** (1999), pp. 521–567.
[6] F. Diamond, *On Deformation Rings and Hecke Rings*, Annals of Mathematics (1) **144** (1996), pp. 137-166.
[7] J.-M. Fontaine, *Groupes p-divisible sur les corps locaux*, Astérisque 47-48, Soc. Math. de France, 1977.
[8] J.-M. Fontaine, *Groupes finis commutatifs sur les vecteurs de Witt*, C.R. Acad. Sci. **280** (1975), pp. 1423-1425.
[9] J.-M. Fontaine, G. Laffaille, *Construction de représentations p-adiques*, Ann. Sci. E.N.S. (1982), pp. 547-608.
[10] J.-M. Fontaine, B. Mazur, *Geometric Galois Representations* in Conference on Elliptic Curves and Modular Forms (Hong Kong), International Press, 1995.
[11] A. Grothendieck, *Séminaire de Géométrie Algébrique* 7, Exposé IX.
[12] H. Kowalsky, *Topological Spaces*, Birkhäuser, 1961.
[13] H. Matsumura, *Commutative Ring Theory*, Cambridge Univ. Press, 1986.
[14] T. Oda, *The first deRham Cohomology group and Dieudonné modules*, Ann. Sci. E.N.S., 5e série, t.2, 1969, 63-135.
[15] F. Oort, J. Tate, *Group Schemes of Prime Order*, Ann. Sci. E.N.S. (1970), pp. 1-21.
[16] R. Ramakrishna, *On a Variation of Mazur's Deformation Functor*, Compositio Math. (3) **87** (1993), pp. 269-286.
[17] M. Raynaud, *Schémas en groupes de type* $(p, p, \dots, p)$, Bull. Soc. Math. France **102** (1974), pp. 241-280.
[18] J. Roubaud, *Schémas en groupes finis sur un anneau de valuation discrète et systèmes de Honda associés*, Publ. Math. d'Orsay, Univ. de Paris-Sud, 91-01.
[19] J. Tate, *p-divisible groups* in Proceedings of a Conference on Local Fields (Driebergen), pp. 158-183, 1966.

Department of Mathematics, Harvard University, Cambridge, MA 02138, USA
E-mail address: `bconrad@math.harvard.edu`