RAMIFIED DEFORMATION PROBLEMS

BRIAN CONRAD

Introduction

The proof of the semistable Taniyama-Shimura Conjecture by Wiles [22] and Taylor-Wiles [21] uses as its central tool the deformation theory of Galois representations. In [6], Diamond extends these methods, proving that an elliptic curve $E_{/\mathbf{Q}}$ is modular if it is either semistable at 3 and 5 or is just semistable at 3, *provided* that the representation

$$\overline{\rho}_{E,3} : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}(\sqrt{-3})) \to \mathrm{Aut}(E[3](\overline{\mathbf{Q}})) \simeq \mathrm{GL}_2(\mathbf{F}_3)$$

is absolutely irreducible. His proof relies on extending the scope of the deformation-theoretic tools. The remaining obstacle to having an unconditional proof of the Taniyama-Shimura Conjecture is to understand cases which do not satisfy semistability conditions. Examples of such cases are not difficult to find. For example, $E_1 : y^2 = x^3 + 15x - 15$ isn't semistable at 3 or 5, nor are any of its quadratic twists. Also, $E_2 : y^2 = x^3 + 5x$ is semistable at 3, has no semistable quadratic twists at 5, and $\overline{\rho}_{E_2,3}|_{\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}(\sqrt{-3}))}$ is absolutely reducible (since $\mathrm{Gal}(\mathbf{Q}(E_2[3])/\mathbf{Q}(\sqrt{-3})) \simeq \mathbf{Z}/4$). In either of these cases, consider the twist $X(\overline{\rho}_{E_i,3})_{/\mathbf{Q}}$ of $X(3)_{/\mathbf{Q}}$ by the cohomology class arising from

$$\overline{\rho}_{E_i,3} \in \mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}), \mathrm{GL}_2(\mathbf{Z}/3)) \to H^1(\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}), \mathrm{Aut}(X(3)_{/\overline{\mathbf{Q}}})).$$

This twist has connected components which are smooth curves of genus 0 and there is a $\mathbf{Q}$-rational point x_{E_i} corresponding to $E_{i/\mathbf{Q}}$ and the choice of 3-torsion basis implicit in $\overline{\rho}_{E_i,3}$. The component containing x_{E_i} is isomorphic to $\mathbf{P}^1_{\mathbf{Q}}$. Choosing rational points on this component which are 3-adically and 5-adically close to x_{E_i} gives infinitely many non-CM, non-isogenous examples of elliptic curves over $\mathbf{Q}$ violating Diamond's hypotheses.

The aim of this paper is to develop the deformation theory further so that it can be applied to the study of non-semistable cases. Applications of these results to the study of the modularity of elliptic curves over $\mathbf{Q}$ will be explained in [3]. We now outline the role of our deformation theory in this argument (details will be given in [3]). Suppose that $E_{/\mathbf{Q}}$ has semistable reduction at 3. Using results of Diamond, it can be shown that either $\overline{\rho}_{E,5}$ is reducible, in which case $E_{/\mathbf{Q}}$ is modular, or else $\overline{\rho}_{E,5}$ is irreducible and *modular*. Moreover, in this latter case, if $E_{/\mathbf{Q}}$ has potentially ordinary or potentially multiplicative reduction at 5, then $E_{/\mathbf{Q}}$ is modular. In the potentially supersingular case at 5, one can show that, at the expense of replacing $E_{/\mathbf{Q}}$ by a twist, it can be assumed that $E_{/K}$ has good reduction, with $K = \mathbf{Q}_5(5^{1/3})$. Now one is in a position to try to apply Wiles' methods with $p = 5$, and with his 'flat' deformation problem over $\mathbf{Q}_p$ replaced by a 'potentially flat' deformation problem that involves a finite extension $K/\mathbf{Q}_p$ with absolute ramification index $e(K) \leq p - 1$. This deformation problem will be precisely formulated and studied in the present paper.

We now give the setting for our main deformation-theoretic result. Consider a continuous representation $\overline{\rho} : \mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p) \to \mathrm{GL}_2(k)$, with k a finite field of characteristic p. We make *no* hypotheses on $\det \overline{\rho}|_{I_p}$, nor do we make any semisimplicity or irreducibility hypotheses. Fix a finite extension $K/\mathbf{Q}_p$ inside of $\overline{\mathbf{Q}}_p$ for which $e(K) \leq p - 1$ and assume that the restricted representation $\overline{\rho}|_{\mathrm{Gal}(\overline{\mathbf{Q}}_p/K)}$ is the generic fiber of a finite flat $\mathcal{O}_K$-group scheme G for which G and the Cartier dual $\widehat{G}$ are *both* connected. Letting M denote the Dieudonne module of the closed fiber of G, we assume that the sequence of groups

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

This research was partially supported by a DoD grant.

is *exact* (this holds when G is the p-torsion of a p-divisible group over $\mathcal{O}_K$). The motivating example is when $k = \mathbf{F}_p$ and $\overline{\rho}$ is the p-torsion representation arising from an elliptic curve $E_{/\mathbf{Q}_p}$ with supersingular reduction over K.

Our first main result is the classification of all $\overline{\rho}$ which can arise. There is a slight technicality in the description of the reducible cases, so we first set up some notation. For $x \in k^\times$, let $\eta_x : \mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p) \to k^\times$ be the unique continuous unramified character sending arithmetic Frobenius to x. For $a, b \in k^\times$ and *distinct* $n, m \in \mathbf{Z}/(p-1)$, consider *non-semisimple* representations of the form

$$\begin{pmatrix} \eta_a \omega^m & * \\ 0 & \eta_b \omega^n \end{pmatrix}.$$

By using a k-linear analogue of Tate duality and the relation between H^1 and Ext^1, we see that as long as $m \neq n+1$ or $a \neq b$, there is exactly one such representation (up to isomorphism), which we denote by $\overline{\rho}_{a,b,m,n}$. When $m = n+1$ and $a = b$, there are exactly $|k|$ such representations, up to $k[D_p]$-module isomorphism. The classification of possible $\overline{\rho}$ is given by:

Theorem *All $\overline{\rho}$ are either absolutely irreducible or are reducible with a trivial centralizer (i.e., $\mathrm{End}_{k[D_p]}(\overline{\rho}) = k$), with the latter case only possible when e does not divide $p-1$. The complete list of $\overline{\rho}$ is as follows:*
(i) $\overline{\rho}|_{I_p} \otimes_k \overline{k} \simeq \psi^m \oplus \psi^{mp}$, where $em \equiv e \bmod p^2-1$ and $\psi : I_p \to \mathbf{F}_{p^2}^\times \subseteq \overline{k}^\times$ is a fundamental character of level 2. These cases are absolutely irreducible.
(ii) Choose $n \in \mathbf{Z}/(p-1)$ satisfying $ne \equiv i+1 \bmod p-1$ with $0 \le i \le e-2$ (so $e \ge 2$). Assume $e|(i+1)(p+1)$ and define $m = n+1-(i+1)(p+1)/e \bmod p-1$ (so $me = e-(i+1) \bmod p-1$ and $m \neq n$). Note that $m = n+1$ if and only if $e = (p+1)/2$, $n = (p-1)/2 \bmod p-1$, $p \equiv 1 \bmod 4$. The reducible $\overline{\rho}$ which occur are precisely the representations $\overline{\rho}_{a,b,m,n}$ for aribitrary $a, b \in k^\times$ and for m, n as above with $m \neq n+1$ or $a \neq b$, together with the unramified k-twists of a certain non-semisimple $\mathbf{F}_p$-representation of the form

$$\overline{\rho} \simeq \begin{pmatrix} \omega^{(p+1)/2} & * \\ 0 & \omega^{(p-1)/2} \end{pmatrix}$$

when $p \equiv 1 \bmod 4$, $e = (p+1)/2$.

We don't have a more explicit description of the 'exceptional' reducible case when $p \equiv 1 \bmod 4$, $e = (p+1)/2$.

Fix a mixed characteristic complete discrete valuation ring $\mathcal{O}$ with residue field k (i.e., we are given a ring extension $W(k) \to \mathcal{O}$ which is finite and totally ramified). Consider deformations $\rho : \mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p) \to \mathrm{GL}_2(R)$ of $\overline{\rho}$, with $(R, \mathfrak{m}_R)$ a complete local noetherian $\mathcal{O}$-algebra with residue field k. We say that ρ is $\mathcal{O}_K$*-flat* if for all $n \geq 1$, each finite quotient $\rho|_{\mathrm{Gal}(\overline{\mathbf{Q}}_p/K)} \bmod \mathfrak{m}_R^n$ is the generic fiber of a finite flat $\mathcal{O}_K$-group scheme (we'll check that these $\mathcal{O}_K$-group schemes are necessarily connected with a connected dual and are canonically unique). Since $\overline{\rho}$ has a trivial centralizer, there is a universal $\mathcal{O}_K$-flat deformation $\overline{\rho}^{\mathrm{univ}} : \mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p) \to \mathrm{GL}_2(R_K^{\mathrm{univ}}(\overline{\rho}))$. Our second main result is:

Theorem *There is an abstract isomorphism of $\mathcal{O}$-algebras*

$$R_K^{\mathrm{univ}}(\overline{\rho}) \simeq \mathcal{O}[\![T_1, T_2]\!].$$

The central technical tool in our proofs is a generalization to the ramified case of Fontaine's 'module-theoretic' description [8] of finite flat group schemes in the unramified case; more precisely, we need a generalization which applies in the case $e \le p-1$. We have worked out such a generalization, and the details of this theory can be found in [2]. This is quite critical. Keep in mind that in the motivating example from elliptic curves over $\mathbf{Q}$, we have $e = 3$, $p = 5$.

The determination of the universal deformation ring generalizes an earlier theorem of Ramakrishna [15], who studied the case $e = 1$ and odd p. It is interesting to note that the arguments in [15] for irreducible $\overline{\rho}$ work when $p = 2$, since Fontaine has results for $p = 2$ analogous to the results for odd p that Ramakrishna invoked. Ramakrishna also considers $e = 1$ cases without connectedness hypotheses on the group schemes. Our methods should carry over to such cases as long as $e < p-1$, but we have not carried this out and so do not know what the results are in these other cases. The method for determining the universal deformation ring by 'counting points' is based on the method used by Ramakrishna.

One application we give of the 'abstract' structure of the universal deformation ring is the following: the determinant character $\det \overline{\rho}^{\mathrm{univ}}$ restricts to $\epsilon|_{I_K}$ on I_K. Also, for a continuous character $\chi : D_p \to \mathcal{O}^\times$ with $\chi \bmod \mathfrak{m}_{\mathcal{O}} = \det \overline{\rho}$ and $\chi|_{I_K} = \epsilon|_{I_K}$, suppose we consider only deformations $\rho : \mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p) \to \mathrm{GL}_2(R)$ for which $\det \rho : D_p \to R^\times$ is equal to χ. Then this restricted functor is representable, with universal deformation ring abstractly isomorphic to $\mathcal{O}[\![T]\!]$. The critical technical input here is Fontaine's work on representations coming from p-divisible groups (this is needed particularly in cases when $\overline{\rho}$ does not admit an unramified $\overline{k}$-twist with field of definition $\mathbf{F}_p$, since these cases cannot be reduced to the case $\mathcal{O} = \mathbf{Z}_p$).

I am grateful to F. Diamond and R. Taylor for encouragement to make some results more explicit, and to R. Ramakrishna and J.-M. Fontaine for proving the foundational results needed in the theory of 'flat' deformations of Galois representations. Most importantly, I would like to thank my advisor Andrew Wiles for proving Fermat's Last Theorem and thereby giving me an opportunity to work on some very exciting mathematics.

Notation For every prime p, we fix an algebraic closure $\overline{\mathbf{Q}}_p$ of $\mathbf{Q}_p$, with $\overline{\mathbf{F}}_p$ the residue field of the valuation ring, and we let D_p denote the topological group $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ and let I_p denote the inertia subgroup (so $D_p/I_p \simeq \widehat{\mathbf{Z}}$). For K a finite extension of $\mathbf{Q}_p$ inside of $\overline{\mathbf{Q}}_p$, I_K denotes the inertia subgroup of $G_K \overset{\mathrm{def}}{=} \mathrm{Gal}(\overline{\mathbf{Q}}_p/K) \subseteq D_p$. We adopt the notation $\mathbf{Q}_{p^n}$ for the unique unramified extension of $\mathbf{Q}_p$ of degree n inside of $\overline{\mathbf{Q}}_p$, with $D_{p^n} = G_{\mathbf{Q}_{p^n}}$ the corresponding open subgroup of D_p. We let $\mathrm{Frob}_{p^n} \in D_{p^n}$ denote any element whose image in $\mathrm{Aut}(\overline{\mathbf{F}}_p)$ is $x \mapsto x^{p^n}$. The completion of $\overline{\mathbf{Q}}_p$ is denoted $\mathbf{C}_p$, though for a finite extension $K/\mathbf{Q}_p$ inside of $\overline{\mathbf{Q}}_p$ we will sometimes write $\mathbf{C}_K$ for $\mathbf{C}_p$ when we wish to just consider the G_K-module structure rather than the D_p-module structure. All G_K-modules are topological, with the topology always clear from the context.

There are several Galois characters that we will need to use. The local p-adic cyclotomic character is denoted $\epsilon : D_p \to \mathbf{Z}_p^\times$, and $\omega = \epsilon \bmod p$. For a topological ring R, $x \in R^\times$, and $K \subseteq \overline{\mathbf{Q}}_p$ a finite extension of $\mathbf{Q}_p$, we let

$$\eta_{K,x} : G_K \to R^\times$$

denote the unique unramified character sending arithmetic Frobenius to x (for $K = \mathbf{Q}_p$, this is abbreviated to η_x). If $L \subseteq \overline{\mathbf{Q}}_p$ is totally ramified of finite degree over K, note that $\eta_{K,x}|_{G_L} = \eta_{L,x}$. We let $\psi : I_p \twoheadrightarrow \mathbf{F}_{p^2}^\times$ denote the fundamental character of level 2, which is the canonical tame character given by

$$I_p \twoheadrightarrow I_p^{\mathrm{tame}} \simeq \varprojlim \mathbf{F}_{p^n}^\times \to \mathbf{F}_{p^2}^\times.$$

This lifts to a character $\psi_0 : D_{p^2} \to \mathbf{F}_{p^2}^\times$ which sends Frob_{p^2} to -1. For any *totally ramified* finite extension $K/\mathbf{Q}_p$ inside of $\overline{\mathbf{Q}}_p$, $\psi_K : I_K \to \mathbf{F}_{p^2}^\times$ denotes the fundamental character of level 2 for K, so $\psi|_{I_K} = \psi_K^{e(K/\mathbf{Q}_p)}$. The fundamental character of level 1 for K is denoted $\psi_{1,K} : I_K \to \mathbf{F}_p^\times$.

For any local ring R, we let $\mathfrak{m}_R$ denote the maximal ideal. If we have a fixed separable closure of the residue field, then we write R^{sh} for the strict henselization. If K is a field complete with respect to a non-trivial discrete valuation, we write K^{un} for the fraction field of a strict henselization of the valuation ring. For any field k, we let $k[\epsilon] = k[T]/(T^2)$ denote the ring of 'dual numbers'; there is no risk of confusion with the cyclotomic character ϵ. We sometimes write $\epsilon_1, \epsilon_2, \ldots$ for basis vectors in the context of Honda systems, but this too should cause no confusion.

If $X \to S$ is a morphism of schemes, this is sometimes denoted $X_{/S}$. If $S' \to S$ is another S-scheme, we sometimes let $X_{/S'}$ denote the S'-scheme $X \times_S S'$. If $S = \mathrm{Spec}(A)$, we write $X_{/A}$ or X_A instead. For a finite fppf commutative group scheme $G_{/S}$, we write $\widehat{G}_{/S}$ for the Cartier dual group scheme. We say that a finite fppf commutative group scheme $G_{/R}$ over a henselian local base ring R is *unipotent* if the Cartier dual is connected, and likewise for p-divisible groups Γ over such a base. The connected-étale sequences of $G_{/R}$ and $\Gamma_{/R}$ show that Γ is connected (resp. unipotent) if and only if $\Gamma[p]$ is, and this can be checked on the closed fiber.

For a field K with a fixed choice of separable closure K_s, we identify finite étale commutative K-group schemes with finite discrete $\mathrm{Gal}(K_s/K)$-modules. If K has characteristic 0 and is the fraction field of a discrete valuation ring $\mathcal{O}_K$, we say that a finite $\mathrm{Gal}(K_s/K)$-module ρ is $\mathcal{O}_K$*-flat* if ρ is the generic fiber of a finite flat $\mathcal{O}_K$-group scheme. If K is a perfect field of characteristic $p > 0$, then for $G_{/K}$ a finite p-power order commutative K-group scheme, we let $\mathcal{M}(G)$ denote the Dieudonne module of G, as constructed in [7, Ch III]. This is a finite-length $W(K)$-module with the structure of a module over the *Dieudonne ring* $D_K = W(K)[F, V]$ (non-commutative for $K \neq \mathbf{F}_p$), generated by the relations $FV = VF = p$ and $Fa = \mathrm{Frob}(a)F$, $Va = \mathrm{Frob}^{-1}(a)V$ for all $a \in W(K)$, where $\mathrm{Frob} : W(K) \simeq W(K)$ is the usual Frobenius map (lifting absolute Frobenius on K).

For $n \in \mathbf{Z}$ and two perfect fields k_1, k_2 with characteristic p, and $\mathcal{O}$ a mixed characteristic complete discrete valuation ring with residue field k_2, we let $t \mapsto t^{(p^n)}$ denote the nth iterate of the map

$$\mathrm{Frob} \otimes 1 : W(k_1) \otimes_{\mathbf{Z}_p} \mathcal{O} \simeq W(k_1) \otimes_{\mathbf{Z}_p} \mathcal{O};$$

the same notation is used for the induced map modulo $\mathfrak{m}_{\mathcal{O}}^m$ for any positive integer m. Because our matrix representations have entries in $W(k)$-algebras and not just $\mathbf{Z}_p$-algebras, we will sometimes need to use modified Dieudonne rings of the form $(W(k_1) \otimes_{\mathbf{Z}_p} \mathcal{O})[F, V] = D_{k_1} \otimes_{\mathbf{Z}_p} \mathcal{O}$ in which F and V *commute* with the action of $\mathcal{O}$. The context should make it clear when this occurs; e.g., whether we are working with D_k or $W(k)[F, V] = W(k)[X, Y]/(XY - p)$.

In addition to the theory developed in [2], which we will use constantly (and whose notation we also use), we assume familiarity with the basic formalism of the deformation theory of Galois representations and we sometimes use a common abuse of notation by treating deformations as liftings rather than as equivalence classes of liftings. This should cause no confusion and simplifies the exposition.

Review of Honda Systems

We give here a rapid review of some basic facts from the theory of finite Honda systems. For complete details, see [2]. Fix a mixed characteristic complete discrete valuation ring $(A', \mathfrak{m})$ with a residue field k that is perfect of characteristic p. Define $A = W(k)$. Assume $e(A') \leq p - 1$. We consider the category $\mathcal{FF}_{A'}$ of finite flat commutative A'-group schemes with p-power order, and let $\mathcal{FF}^c_{A'}$, $\mathcal{FF}^u_{A'}$ denote the full subcategories which consist of connected and unipotent objects, respectively. The (contravariant) Dieudonne module functor $\mathcal{M}$ gives an equivalence of abelian categories between finite commutative k-group schemes G with p-power order and D_k-modules with finite A-length (in fact, $p^{\ell_A(\mathcal{M}(G))}$ is equal to the order of G). The theory of finite Honda systems gives an analogous functor on $\mathcal{FF}_{A'}$, as we now explain.

A general construction due to Fontaine associates to any D_k-module M a certain A'-module $M_{A'}$. The idea is to manufacture an A'-module with a structure resembling F and V operators (which, strictly speaking, won't make sense if $e(A') > 1$ since there is in general no canonical meaning of 'Frobenius-semilinearity' on an A'-module). The definition is as follows. Define $M^{(1)} = A \otimes_A M$ as an A-module, where $A \to A$ is absolute Frobenius. We have A*-linear* maps $F_0 : M^{(1)} \to M$, $V_0 : M \to M^{(1)}$, with $F_0 V_0 = p_M$, $V_0 F_0 = p_{M^{(1)}}$. Define $M_{A'}$ to be the direct limit of the diagram

$$\begin{array}{ccc} \mathfrak{m} \otimes_A M & \stackrel{V^{M,A'}}{\longrightarrow} & p^{-1}\mathfrak{m} \otimes_A M^{(1)} \\ \varphi_0^{M,A'} \downarrow & & \uparrow \varphi_1^{M,A'} \\ A' \otimes_A M & \stackrel{F^{M,A'}}{\longleftarrow} & A' \otimes_A M^{(1)} \end{array}$$

in the category of A'-modules, where $\varphi_0^{M,A'}$, $\varphi_1^{M,A'}$ are the obvious 'inclusion' maps (which might not be injective!), $V^{M,A'}(\lambda \otimes x) = p^{-1}\lambda \otimes V_0(x)$, $F^{M,A'}(\lambda \otimes x) = \lambda \otimes F_0(x)$. More explicitly, $M_{A'}$ is the quotient of $(A' \otimes_A M) \oplus (p^{-1}\mathfrak{m} \otimes_A M^{(1)})$ by the submodule

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

There are canonical A'-linear maps $\mathcal{F}_{M,A'} : p^{-1}\mathfrak{m} \otimes_A M^{(1)} \to M_{A'}$ and $\mathcal{V}_{M,A'} : M_{A'} \to A' \otimes_A M^{(1)}$ (the latter induced by $1 \otimes V_0$ on $A' \otimes_A M$ and $p \otimes \mathrm{id}$ on $p^{-1}\mathfrak{m} \otimes_A M^{(1)}$), and when $A' = A$ this can all be identified with the A-module M with its structure as a D_k-module. In general, the A'-modules given by the kernels and cokernels of $\mathcal{F}_{M,A'}$, $\mathcal{V}_{M,A'}$ are annihilated by $\mathfrak{m}$ and so can be viewed as k-vector spaces.

When M has finite A-length, then $M_{A'}$ has finite A'-length and the functor $M \rightsquigarrow M_{A'}$ is exact on the category of D_k-modules with finite A-length. If G is an object in $\mathcal{FF}_{A'}$, one can define a certain natural A'-submodule $L_{A'}(G)$ of 'logarithms' inside of $\mathcal{M}(G_{/k})_{A'}$. We define $LM_{A'}(G) = (L_{A'}(G), \mathcal{M}(G_{/k}))$. We define the category $PSH^f_{A'}$ *finite pre-Honda systems over* A' to consist of triples (L, M, j) with M a D_k-module with finite A-length, L an A'-module, and $j : L \to M_{A'}$ an A'-linear map. We define the full subcategories $PSH^{f,c}_{A'}$ and $PSH^{f,u}_{A'}$ of connected and unipotent objects to consist of the objects which satisfy the extra condition that the action of F (respectively V) on M is nilpotent. These are convenient abelian categories, but do not lie at the heart of the matter.

We define the full subcategory $SH^f_{A'}$ of *finite Honda systems over* A' to consist of those objects in $PSH^f_{A'}$ for which the canonical k-linear map

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

is an isomorphism and $\mathcal{V}_{M,A'} \circ j$ is injective (and in this case, the map j is automatically injective, so it is usually dropped from the notation and we identify L with an A'-submodule of $M_{A'}$). It is important to note that in the presence of the first condition, the second condition is equivalent to the natural k-linear map

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

being an isomorphism [2, Lemma 2.7]. One defines the categories of connected and unipotent finite Honda systems (denoted $SH^{f,c}_{A'}$, $SH^{f,u}_{A'}$) in a similar manner. The full subcategories of objects killed by p are denoted $\widetilde{SH}^f_{A'}$, etc. The categories such as 'finite pre-Honda systems with descent data' (denoted $DPSH^f_{A'}$, etc.) are defined in [2, §5]

For any G in $\mathcal{FF}_{A'}$ with $e(A') < p-1$ (resp. in $\mathcal{FF}^c_{A'}$, $\mathcal{FF}^u_{A'}$ with $e(A') \leq p-1$), the finite pre-Honda system $LM_{A'}(G)$ is in fact a finite Honda system (and is connected/unipotent if and only if G is). The contravariant functor $LM_{A'} : \mathcal{FF}_{A'} \to SH^f_{A'}$ is fully faithful and essentially surjective when $e(A') < p-1$. If we restrict to the categories of connected objects, or unipotent objects, then the resulting functors (denoted $LM^c_{A'}$, $LM^u_{A'}$) are fully faithful and essentially surjective when $e(A') \leq p-1$. What is important to also note is that in these cases, all of the relevant categories are abelian, with kernels and cokernels on the group scheme side given by the usual scheme-theoretic constructions (which yield *flat* results!), and on the module side the functors such as $SH^f_{A'} \to PSH^f_{A'}$, etc. are exact. This enables one to carry out explicit computations with short exact sequences in terms of Honda systems.

For more detailed discussions of base change in terms of Honda systems, as well as convenient criteria to determine when an abstractly constructed finite pre-Honda system is actually a finite Honda system, etc., see [2].

1. The Deformation Problem

1.1. **Formulation of Problem.**

Fix a prime p and a finite field k with characteristic p, as well as a representation $\overline{\rho} : D_p \to \mathrm{GL}_2(k)$. Choose a subfield $\mathcal{K}' \subseteq \overline{\mathbf{Q}}_p$ with finite degree over $\mathbf{Q}_p$ and with absolute ramification index $e = e(\mathcal{K}') \leq p-1$. We write $\mathcal{A}'$ the for valuation ring of $\mathcal{K}'$ and κ for the residue field of $\mathcal{A}'$.

Assume that $\overline{\rho}|_{G_{\mathcal{K}'}}$ is $\mathcal{A}'$-flat, and in fact that it is the generic fiber of a finite flat group scheme $\mathcal{G}(\overline{\rho}|_{G_{\mathcal{K}'}})_{/\mathcal{A}'}$ which is connected and unipotent. We claim that under these conditions, $\mathcal{G}(\overline{\rho}|_{G_{\mathcal{K}'}})$ is unique up to canonical isomorphism (and is the unique finite flat $\mathcal{A}'$-group scheme with generic fiber $\overline{\rho}|_{G_{\mathcal{K}'}}$).

The only point to check for this uniqueness is that any finite flat $\mathcal{A}'$-group scheme $\mathcal{G}$ with generic finite $\overline{\rho}|_{G_{\mathcal{K}'}}$ must be connected (this is actually only an issue if $e(\mathcal{K}') = p-1$), in which case we can use Raynaud's full faithfulness theorem, which asserts that passage to the generic fiber is fully faithful on the category of finite flat commutative connected $\mathcal{A}'$-group schemes [2, Lemma 4.1]. Assume otherwise, so $\mathcal{G}$ admits a non-trivial étale quotient $\mathcal{G}^{\text{ét}}$ (with p-power order, and therefore unipotent). Passing to generic fibers, this gives rise to a non-zero unramified quotient of $\overline{\rho}|_{G_{\mathcal{K}'}}$, viewed as an $\mathbf{F}_p$-representation space. By the full faithfulness in Raynaud's theorem for *unipotent* group schemes, this generic fiber quotient map must be induced by a non-zero map from the unipotent (and *connected*) $\mathcal{G}(\overline{\rho}|_{G_{\mathcal{K}'}})$ to the étale $\mathcal{G}^{\text{ét}}$. This is impossible.

Note that if $\mathcal{K}'$ is an unramified extension of a subextension $K'/\mathbf{Q}_p$ with valuation ring A', then $\overline{\rho}|_{G_{K'}}$ is A'-flat by Galois descent from $\operatorname{Spec}(\mathcal{A}')$ to $\operatorname{Spec}(A')$. For details about Galois descent formalism over rings in the limited context we need, see [1, Example B, §6.2]. The reason Galois descent is applicable here is because of Raynaud's full faithfulness theorem for passage to the generic fiber for finite flat commutative group schemes [2, Lemma 4.1]. In down-to-earth terms, any Galois descent data on the generic fiber ring *as a* $\mathcal{K}'$*-group scheme* must respect the subring of the $\mathcal{A}'$-group scheme which we start with. Moreover, the finite flat A'-group scheme $\mathcal{G}(\overline{\rho}|_{G_{K'}})$ with generic fiber $\overline{\rho}|_{G_{K'}}$ is unique up to canonical isomorphism, is connected and unipotent, and we have canonically

$$\mathcal{G}(\overline{\rho}|_{G_{K'}}) \times_{A'} \mathcal{A}' \simeq \mathcal{G}(\overline{\rho}|_{G_{\mathcal{K}'}})$$

as $\mathcal{A}'$-group schemes. We will often abuse notation and write things like $\mathcal{M}(\overline{\rho}|_{G_{\mathcal{K}'}})$ rather than $\mathcal{M}(\mathcal{G}(\overline{\rho}|_{G_{\mathcal{K}'}})_{/\kappa})$; because of the uniqueness of $\mathcal{G}(\overline{\rho}|_{G_{\mathcal{K}'}})$, no confusion is possible.

The final hypothesis we impose is that for $M = \mathcal{M}(\overline{\rho}|_{G_{\mathcal{K}'}})$, the canonical sequence of groups

$$0 \to M/VM \xrightarrow{F} M = M/p \to M/FM \to 0 \tag{1}$$

is *exact*. Because of how formation of Dieudonne modules behaves with respect to base change of the perfect base field (see [7, Ch III, §2.2, Prop 2.2(i)] for the case of a finite algebraic extension; the case of a general extension follows from this — see the proof of [2, Thm 4.6]), the exactness property (1) depends only on $\overline{\rho}|_{I_{\mathcal{K}'}}$ (this amounts to checking (1) after applying $\otimes_\kappa \overline{\kappa}$). In particular, for $\mathcal{K}'$ and K' as above, $\overline{\rho}|_{G_{\mathcal{K}'}}$ satisfies the exactness condition (1) if and only if $\overline{\rho}|_{G_{K'}}$ does. We will later describe which $\overline{\rho}$ arise.

An important point to note here is that if k'/k is a finite extension, then $\overline{\rho}$ satisfies the above hypotheses if and only if $\overline{\rho}' = \overline{\rho} \otimes_k k'$ does. The 'only if' direction is seen by choosing a k-basis for k'. For the 'if' direction, we use the method of scheme-theoretic closure to see that $\overline{\rho}|_{G_{\mathcal{K}'}}$ arises from a closed finite flat subgroupscheme of $\overline{\rho}'|_{G_{\mathcal{K}'}}$. Since a closed flat subgroupscheme of a finite flat connected and unipotent commutative $\mathcal{A}'$-group scheme is again connected and unipotent, it remains to check that the exactness condition on Dieudonne modules descends. By choosing a k-basis of k', this is readily seen.

Fix a mixed characteristic discrete valuation ring $\mathcal{O}$ with residue field k and let $\mathcal{C}(\mathcal{O})$ denote the category of complete local noetherian $\mathcal{O}$-algebras with residue field k (and morphisms are local maps of $\mathcal{O}$-algebras). We make the following general definition:

Definition 1.1.1. The functor

$$F_{\mathcal{K}',\mathcal{O}} = F_{\mathcal{K}',\mathcal{O}}(\overline{\rho}) : \mathcal{C}(\mathcal{O}) \to \mathbf{Set}$$

is defined by letting $F_{\mathcal{K}',\mathcal{O}}(R)$ be the set of all deformations ρ of $\overline{\rho}$ to $\mathrm{GL}_2(R)$ such that for all $n \geq 1$, $\rho|_{G_{\mathcal{K}'}} \bmod \mathfrak{m}_R^n$ is the generic fiber of a finite flat group scheme $\mathcal{G}_n(\rho|_{G_{\mathcal{K}'}})$ over $\mathcal{A}'$. An element in $F_{\mathcal{K}',\mathcal{O}}(R)$ is called an $\mathcal{O}_{\mathcal{K}'}$*-flat* deformation of $\overline{\rho}$.

The result [15, Prop 1.1] shows that $F_{\mathcal{K}',\mathcal{O}}$ is a functor in the obvious manner. The ramification hypothesis on $\mathcal{K}'$ ensures that $\mathcal{G}_n(\rho|_{G_{\mathcal{K}'}})$ is unique up to canonical isomorphism if it exists, so our deformation problem is a reasonable one. Indeed, by [2, Lemma 4.1], we need only to check that $\mathcal{G}_n(\rho|_{G_{\mathcal{K}'}})$ is necessarily connected. This is checked by a slight generalization of the above proof that $\mathcal{G}(\overline{\rho}|_{G_{\mathcal{K}'}})$ is connected, as we now explain. Use the method of scheme-theoretic closure [16, §2.1, §2.2] and the filtration of $\rho \bmod \mathfrak{m}_R^n$ by powers of $\mathfrak{m}_R$ to get a filtration of $\mathcal{G}_n(\rho|_{G_{\mathcal{K}'}})$ by finite flat group schemes whose successive quotients have generic fibers which are quotients of $\overline{\rho}|_{G_{\mathcal{K}'}}$. In a short exact sequence of finite flat $\mathcal{A}'$-group schemes, if any two objects are connected, so is the third. Thus, it suffices to show that a quotient of the $\mathbf{F}_p[G_{\mathcal{K}'}]$-module $\overline{\rho}|_{G_{\mathcal{K}'}}$ cannot arise as the generic fiber of a finite flat $\mathcal{A}'$-group scheme with a non-trivial étale quotient. This follows from Raynaud's full faithfulness theorem for unipotent $\mathcal{A}'$-group schemes.

We note that by the method of scheme-theoretic closure, subrepresentations and quotients of the generic fiber representation of a finite flat commutative $\mathcal{O}_{\mathcal{K}'}$-group scheme are again $\mathcal{O}_{\mathcal{K}'}$-flat. This is often used without comment.

1.2. **Changing the Data.**

Assume that $\overline{\rho}$ has trivial centralizer (we will prove this in Theorem 2.2.1). By [15, Thm 1.1], $F_{\mathcal{K}',\mathcal{O}}(\overline{\rho})$ satisfies Schlessinger's criteria. Thus, a universal $\mathcal{O}_{\mathcal{K}'}$-flat deformation

$$\overline{\rho}^{\text{univ}} : D_p \to \mathrm{GL}_2(R^{\text{univ}}_{\mathcal{K}',\mathcal{O}}(\overline{\rho}))$$

exists. Our main task is to determine the structure of the universal deformation ring $R^{\text{univ}}_{\mathcal{K}',\mathcal{O}}(\overline{\rho})$. When $\det \overline{\rho}|_{I_p} = \omega|_{I_p}$, $\overline{\rho}$ is irreducible, $\mathcal{K}' = \mathbf{Q}_p$, $\mathcal{O} = W(k)$, and $p \neq 2$, it is proven by Ramakrishna in [15, Thm 3.1] that the universal deformation ring is (abstractly) isomorphic to $\mathcal{O}[\![T_1, T_2]\!]$.

An argument due to Faltings explains how the deformation ring changes if we enlarge the residue field k or the 'coefficient ring' $\mathcal{O}$. Consider an extension $\mathcal{O} \to \mathcal{O}'$ inducing a finite extension $k \to k'$ on residue fields, so the representation $\overline{\rho}' = \overline{\rho} \otimes_k k' : D_p \to \mathrm{GL}_2(k')$ has a trivial centralizer and satisfies the same hypotheses as $\overline{\rho}$ (with k' replacing k). Let $R = R^{\text{univ}}_{\mathcal{K}',\mathcal{O}}(\overline{\rho})$ and $R' = R^{\text{univ}}_{\mathcal{K}',\mathcal{O}'}(\overline{\rho}')$ be the corresponding deformation rings. Since $\mathcal{O} \to \mathcal{O}'$ is a finite flat local map, the ring $\mathcal{O}' \otimes_{\mathcal{O}} R$ is a complete local noetherian $\mathcal{O}'$-algebra with residue field k'. Using the $\mathcal{A}'$-flat $\overline{\rho}'$-deformation $\mathcal{O}' \otimes_{\mathcal{O}} \overline{\rho}^{\text{univ}}$ and the universality of $\overline{\rho}'^{\text{univ}}$, we get a natural local $\mathcal{O}'$-algebra map

$$r_{\mathcal{O},\mathcal{O}'} : R' \to \mathcal{O}' \otimes_{\mathcal{O}} R.$$

A related map is defined as follows. The extension of scalars $k[\epsilon] \to k'[\epsilon]$ gives rise to a natural map of sets $F_{\mathcal{K}',\mathcal{O}}(\overline{\rho})(k[\epsilon]) \to F_{\mathcal{K}',\mathcal{O}'}(\overline{\rho}')(k'[\epsilon])$ which is compatible with the intrinsic k- and k'-vector space structures, so in terms of deformation rings, this induces a k'-linear map of dual spaces

$$\overline{r}_{\mathcal{O},\mathcal{O}'} : (\mathfrak{m}_R/(\mathfrak{m}_R^2, \mathfrak{m}_{\mathcal{O}} R))^* \otimes_k k' \to (\mathfrak{m}_{R'}/(\mathfrak{m}_{R'}^2, \mathfrak{m}_{\mathcal{O}'} R'))^*.$$

It is straightfoward to check that $\overline{r}_{\mathcal{O},\mathcal{O}'}$ is exactly the map obtained by applying $\mathrm{Hom}_{\mathcal{C}(\mathcal{O}')}(-, k'[\epsilon])$ to $r_{\mathcal{O},\mathcal{O}'}$ and composing with the inverse of the canonical k'-linear isomorphism $k' \otimes_k V^* \simeq (k' \otimes_k V)^*$ for the finite-dimensional k-vector space $V = \mathfrak{m}_R/(\mathfrak{m}_R^2, \mathfrak{m}_{\mathcal{O}} R)$.

Lemma 1.2.1. *The maps $r_{\mathcal{O},\mathcal{O}'}$ and $\overline{r}_{\mathcal{O},\mathcal{O}'}$ are isomorphisms. Also, $R^{\text{univ}}_{\mathcal{K}',\mathcal{O}'}(\overline{\rho}') \simeq \mathcal{O}'[\![T_1, \ldots, T_n]\!]$ as an $\mathcal{O}'$-algebra if and only if $R^{\text{univ}}_{\mathcal{K}',\mathcal{O}}(\overline{\rho}) \simeq \mathcal{O}[\![T_1, \ldots, T_n]\!]$ as an $\mathcal{O}$-algebra.*

Proof. See [22, Ch 1, pp.457-8] for an outline of Faltings' proof that $r_{\mathcal{O},\mathcal{O}'}$ is an isomorphism (for complete details, see [3, Thm 1.1]). From this it follows that $\overline{r}_{\mathcal{O},\mathcal{O}'}$ is an isomorphism, by applying $\mathrm{Hom}_{\mathcal{C}(\mathcal{O}')}(-, k'[\epsilon])$ to $r_{\mathcal{O},\mathcal{O}'}$. For the second assertion, the 'only if' direction is clear. To prove the 'if' direction, note that by [13, Thm 23.7(i)], R is a priori regular of dimension $n+1$ because the local map $R \to R \otimes_{\mathcal{O}} \mathcal{O}'$ is finite flat and $\mathcal{O}'[\![T_1, \ldots, T_n]\!]$ is regular with dimension $n+1$. Also, since $\overline{r}_{\mathcal{O},\mathcal{O}'}$ is an isomorphism, the k-dimension of $\mathfrak{m}_R/(\mathfrak{m}_R^2, \mathfrak{m}_{\mathcal{O}} R)$ is n. Lifting a basis to $\mathfrak{m}_R$, we get a surjective $\mathcal{O}$-algebra map $\mathcal{O}[\![T_1, \ldots, T_n]\!] \to R$. By dimension considerations, the kernel is 0. ■

An important consequence of this lemma is that when studying the tangent spaces of deformation functors and proving structure theorems for deformation rings, we often do not really lose any generality by working with $\mathcal{O} = W(k)$ or replacing k by a subfield to which the representation $\overline{\rho}$ descends (note that descending the field of definition of $\overline{\rho}$ does not harm any of the original hypotheses).

2. Some Applications of Finite Honda Systems

2.1. **Preliminaries.**

Recall that *any* two finite extensions $\mathcal{K}_1, \mathcal{K}_2$ of $\mathbf{Q}_p$ inside of $\overline{\mathbf{Q}}_p$ with the same *tame* absolute ramification index have the same composite with $\mathbf{Q}_p^{\text{un}}$. By Galois descent of valuation rings and Raynaud's full faithfulness results [2, Lemma 4.1], it follows that the corresponding flat deformation functors $F_{\mathcal{K}_1,\mathcal{O}}(\overline{\rho})$ and $F_{\mathcal{K}_2,\mathcal{O}}(\overline{\rho})$ are *the same.* Also, since $I_{\mathcal{K}_1} = I_{\mathcal{K}_2}$, the two Theorems in the Introduction are insenstive to replacing $\mathcal{K}_1$ by $\mathcal{K}_2$. Thus, our problem depends on $\mathcal{K}'$ only through $e = e(\mathcal{K}'/\mathbf{Q}_p)$ (recall that the Dieudonne module hypothesis (1) depends only on $\overline{\rho}|_{I_{\mathcal{K}'}}$), so we can choose a convenient $\mathcal{K}'$ if we so desire. For example, we can take $\mathcal{K}'$ to be the Galois closure of a *totally ramified* finite extension $K'/\mathbf{Q}_p$ with $e = e(K') \leq p-1$, so $\mathcal{K}' = K'(\zeta_e)$ and $e(\mathcal{K}') = e(K')$ also. We often immediately reduce to the case of such special $\mathcal{K}'$ in our proofs, and we generally indicate this by saying that we choose $\mathcal{K}'$ to be *of special type* (and this implicitly includes a choice of K' too).

We introduce some notation in the case of a $\mathcal{K}'$ of special type. Pick such $\mathcal{K}'$ and K'. Since $K'/\mathbf{Q}_p$ is totally tamely ramified, in general we can fix a choice of uniformizer π such that $\pi^e = pu_0$ with $u_0 \in \mathbf{Z}_p^\times$. It will often be enough to work with K' in place of $\mathcal{K}'$. The fact that $\mathcal{O}_{K'}$ has residue field $\mathbf{F}_p$ makes K' somewhat useful in calculations; on the other hand, $\mathcal{K}'/\mathbf{Q}_p$ is Galois, a fact that is useful also. Trivially K' and $\mathbf{Q}_p(\zeta_e)$ are linearly disjoint over $\mathbf{Q}_p$, so $\mathrm{Gal}(\mathcal{K}'/K') \simeq \mathrm{Gal}(\mathbf{Q}_p(\zeta_e)/\mathbf{Q}_p)$. Hence,

$$\mathrm{Gal}(\mathcal{K}'/\mathbf{Q}_p) \simeq \mathrm{Gal}(\mathcal{K}'/\mathbf{Q}_p(\zeta_e)) \rtimes \mathrm{Gal}(\mathcal{K}'/K') \simeq \mu_e \rtimes \mathrm{Gal}(\mathbf{Q}_p(\zeta_e)/\mathbf{Q}_p),$$

with $\mu_e = \mu_e(\overline{\mathbf{Q}}_p)$, and we have the usual semidirect product structure

$$\sigma \cdot \zeta \cdot \sigma^{-1} = \zeta^\sigma$$

for $\zeta \in \mu_e$ and $\sigma \in \mathrm{Gal}(\mathbf{Q}_p(\zeta_e)/\mathbf{Q}_p)$ (and ζ^σ denotes the canonical action of σ on $\zeta \in \mu_e(\overline{\mathbf{Q}}_p)$). This will be used frequently.

Let $\mathfrak{m}$ and $\mathfrak{n}$ denote the maximal ideals of A' and $\mathcal{A}'$ respectively, and let $\kappa = \mathcal{A}'/\mathfrak{n} \simeq \mathbf{F}_p(\zeta_e)$ denote the residue field of $\mathcal{A}'$ (so we identify μ_e with $\mu_e(\kappa)$). At this point we will begin to use the results and notation introduced in [2], with A' there equal to our A' above, so A now denotes $\mathbf{Z}_p$. The categories of finite (pre-)Honda systems and finite (pre-)Honda systems with descent data are defined as in [2, §5].

Let $LM_{\mathcal{A}'}(\overline{\rho}) \overset{\mathrm{def}}{=} (\mathcal{L}, \mathcal{M})$ be the p-torsion object in $SH^{f,c}_{\mathcal{A}'}$ corresponding to the generic fiber $\overline{\rho}|_{G_{\mathcal{K}'}}$; as we noted in §1.1, this is unique up to canonical isomorphism [2, Lemma 4.1]. Where convenient, we'll later use the analogous notation $LM_{A'}(\overline{\rho})$ for the Honda system of the descended finite A'-group scheme (the unique one with generic fiber $\overline{\rho}|_{G_{K'}}$). Let $\mathcal{D}(\overline{\rho})$ be the descent data on $LM_{\mathcal{A}'}(\overline{\rho})$ obtained from $\overline{\rho}|_{G_{\mathcal{K}'}}$ via $\overline{\rho}$, as in the discussion in [2, §5], so $(LM_{\mathcal{A}'}(\overline{\rho}), \mathcal{D}(\overline{\rho}))$ is an object in $\widetilde{DPSH}^f_{\mathcal{A}'}$.

Before stating the next lemma, we need to restrict the Honda systems we consider. Since our representation spaces admit an action of $\mathcal{O}$, we only wish to consider finite Honda systems which admit an action of $\mathcal{O}$. We let $SH^f_{\mathcal{A}',\mathcal{O}}$, $DPSH^f_{\mathcal{A}',\mathcal{O}}$, etc. denote the categories whose underlying objects are finite Honda systems over $\mathcal{A}'$, finite pre-Honda systems over $\mathcal{A}'$ with 'descent data', etc. equipped with the structure of a map from $\mathcal{O}$ to the endomorphism ring of the object (compatible with the Honda system structures, the descent data, etc.). Morphisms are required to respect the action of $\mathcal{O}$. These new categories are abelian and the 'forget the $\mathcal{O}$-action' functors are visibly exact. As an example, when $\mathcal{O} = W(k)$, $(LM_{\mathcal{A}'}(\overline{\rho}), \mathcal{D}(\overline{\rho}))$ is an object in $\widetilde{DPSH}^f_{\mathcal{A}',W(k)}$. In order to allow for the case $\mathcal{O} \neq W(k)$, the definitions of $\widetilde{PSH}^f_{\mathcal{A}',\mathcal{O}}$ and $\widetilde{DPSH}^f_{\mathcal{A}',\mathcal{O}}$ should include an $\mathfrak{m}_{\mathcal{O}}$*-torsion hypothesis*, not just a p-torsion hypothesis.

We will sometimes need to consider a finite extension of scalars $k \to k'$. It is very important to interpret this in terms of Honda systems with descent data. This requires some care to treat rigorously. Since k'/k is separable, there is a natural k-linear section $\mathrm{Tr}_{k'/k} : k' \to k$, so there is a natural k-linear surjective map $\overline{\rho}' = \overline{\rho} \otimes_k k' \to \overline{\rho}$. By contravariance, we get a k-linear injective map

$$LM_{\mathcal{A}'}(\overline{\rho}) \to LM_{\mathcal{A}'}(\overline{\rho} \otimes_k k'),$$

visibly *compatible with the descent data* on both sides. Thus, we get a k'-linear map

$$LM_{\mathcal{A}'}(\overline{\rho}) \otimes_k k' \to LM_{\mathcal{A}'}(\overline{\rho} \otimes_k k'),$$

where the left side is defined in the obvious manner (preserving the Honda system conditions, which were k-linear at the start). Moreover, there is an obvious descent data $\mathcal{D}(\overline{\rho}) \otimes 1$ defined on the left side and this makes the map a morphism in the category in $DSH^f_{\mathcal{A}',\mathcal{O}}$. We claim this is an isomorphism.

It is not important that the k-linear section $k' \to k$ was taken to be the trace map; the claim certainly holds for all such sections if it holds for a single one (since $\mathrm{Hom}_k(k', k)$ is 1-dimensional over k'). However, using the trace is technically convenient due to the transitivity and Galois invariance properties of traces. By transitivity, we see that in order to check that the above map is an isomorphism, we can check over a larger finite extension k''/k over k'/k. Thus, we are reduced to the case in which k'/k is a finite Galois extension (the point here is that the argument we are giving can be applied to settings in which the residue fields are merely perfect of characteristic p and not necessarily finite). The isomorphism condition can be checked on the Dieudonne module parts. Let G and G' be the $\mathbf{F}_p$-group scheme closed fibers of $\mathcal{G}(\overline{\rho}|_{G_{K'}})$ and $\mathcal{G}(\overline{\rho}'|_{G_{K'}})$ respectively, so there are natural actions of k and k' on G and G' respectively. Also, there is a natural 'semilinear' right action of $\mathrm{Gal}(k'/k)$ on G'.

The epimorphism $G' \to G$ is $\mathrm{Gal}(k'/k)$-equivariant, because the trace map $k' \to k$ is $\mathrm{Gal}(k'/k)$-invariant. Thus, we get a k-linear injection $\mathcal{M}(G) \hookrightarrow \mathcal{M}(G')$ which is invariant under the semilinear left $\mathrm{Gal}(k'/k)$-action on the finite-dimensional k'-vector space $\mathcal{M}(G')$ induced by $\mathcal{M}$-functoriality. Our task is to show that the natural k'-linear map $k' \otimes_k \mathcal{M}(G) \to \mathcal{M}(G')$ is an isomorphism. Since $k' \otimes_k \mathcal{M}(G')^{\mathrm{Gal}(k'/k)} = \mathcal{M}(G')$, it is enough to show that the k-linear *injection* $\mathcal{M}(G) \hookrightarrow \mathcal{M}(G')^{\mathrm{Gal}(k'/k)}$ is an isomorphism. In other words, we need to check that $\dim_k(\mathcal{M}(G)) = \dim_{k'}(\mathcal{M}(G'))$. Since our group schemes are over $\mathbf{F}_p$, [2, Thm 4.4] implies

$$\dim_k \mathcal{M}(G) = \dim_k \overline{\rho} = \dim_{k'} \overline{\rho}' = \dim_{k'} \mathcal{M}(G'),$$

as desired. We will frequently use this compatibility with finite extension of scalars on k.

The tangent space

$$t_{F_{\mathcal{K}',\mathcal{O}}(\overline{\rho})} = (F_{\mathcal{K}',\mathcal{O}}(\overline{\rho}))(k[\epsilon])$$

is naturally a k-vector space [17, Lemma 2.10]. The following lemma will be essential, and is an application of [2, Theorems 3.6, 4.1, 4.9].

Lemma 2.1.1. *For $\mathcal{K}'$ of special type, there is a canonical isomorphism of k-modules*

$$t_{F_{\mathcal{K}',\mathcal{O}}(\overline{\rho})} \simeq \mathrm{Ext}^1_{\widetilde{DPSH}^f_{\mathcal{A}',\mathcal{O}}}((LM_{\mathcal{A}'}(\overline{\rho}), \mathcal{D}(\overline{\rho})), (LM_{\mathcal{A}'}(\overline{\rho}), \mathcal{D}(\overline{\rho}))).$$

2.2. **Initial Description of $\overline{\rho}$.**

Fix an algebraic closure $\overline{k}$ of k.

Twisting $\overline{\rho}$ by an unramified continuous character $\chi : D_p \to k^\times$ has no effect on our original hypotheses on $\overline{\rho}$, nor does it affect the flat deformation ring, because the property of being $\mathcal{A}'$-flat can be checked on I_p or even $I_{\mathcal{K}'}$ (and deformations of $\overline{\rho}$ and $\overline{\rho}\otimes\chi$ are related via twisting by the unramified Teichmüller lifting of χ). Thus, if some unramified twist of $\overline{\rho}\otimes_k\overline{k}$ can be defined over $\mathbf{F}_p$, then it is enough to consider the deformation ring attached to the associated 2-dimensional $\mathbf{F}_p$-representation. Before we explain how to reduce to this case in some situations, we introduce some representations which make explicit which $\mathbf{F}_p$-representations will arise from our 'descent'.

Choose an integer m. The representation

$$\overline{\rho}_m : D_p \to \mathrm{GL}_2(\mathbf{F}_p)$$

is defined to be the unique $\mathbf{F}_p$-descent of the two-dimensional *semisimple* $\mathbf{F}_{p^2}$-representation $\mathrm{Ind}_{D_{p^2}}^{D_p}(\psi_0^m)$. The uniqueness of $\overline{\rho}_m$ follows from the Brauer-Nesbitt Theorem. The existence follows from the fact that $\mathrm{Ind}_{D_{p^2}}^{D_p}(\psi_0^m)$ has all characteristic polynomials with $\mathbf{F}_p$ coefficients (because the 'twist' of ψ_0 by $\mathrm{Frob}_p \in D_p$ is ψ_0^p), and this allows one to carry out a descent argument in which the obstruction vanishes because the Brauer group of a finite field is trivial. A more conceptual argument (which ultimately reduces to the same vanishing result for Brauer groups) is given in [5, Lemme 6.13].

We have the following two useful facts, which we will prove shortly:

Theorem 2.2.1. *Either $\overline{\rho}$ is absolutely irreducible or is reducible with a trivial centralizer.*

Theorem 2.2.2. *Assume $\overline{\rho}$ is absolutely irreducible. For some unramified character $\chi : D_p \to \overline{k}^\times$ and some integer m, there is an isomorphism of $\overline{k}[D_p]$-modules*

$$(\overline{\rho} \otimes_k \overline{k}) \otimes \chi \simeq \overline{\rho}_m \otimes_{\mathbf{F}_p} \overline{k}.$$

The usefulness of Theorem 2.2.2 lies in the fact that when $\overline{\rho}$ is irreducible, the study of its 'flat' deformation theory can be reduced to the case $k = \mathbf{F}_p$, which drastically simplifies the descent calculations we will carry out later. Thus, the complications really arise in order to treat reducible representations. We note in passing that Raynaud's classification of finite flat group schemes with simple generic fibers allows us to determine exactly which m arise in Theorem 2.2.2. The precise result is:

Corollary 2.2.3. *Choose an irreducible continuous representation $\overline{\rho} : D_p \to \mathrm{GL}_2(k)$. There exists a connected and unipotent finite flat commutative group scheme $\mathcal{G}_{/\mathcal{A}'}$ for which the sequence*

$$0 \to \mathcal{M}(\mathcal{G}_{/k})/V \xrightarrow{F} \mathcal{M}(\mathcal{G}_{/k})/p \to \mathcal{M}(\mathcal{G}_{/k})/F \to 0$$

is exact and $\mathcal{G}(\overline{\mathbf{Q}}_p) \simeq \overline{\rho}|_{G_{\mathcal{K}'}}$ as $G_{\mathcal{K}'}$-modules if and only if $\overline{\rho}|_{I_p} \otimes_k \overline{k} \simeq \psi^m \oplus \psi^{mp}$, where $em \equiv e \bmod p^2 - 1$.

In particular, $\det \overline{\rho}|_{I_{\mathcal{K}'}} = \omega|_{I_{\mathcal{K}'}}$, $\overline{\rho}$ is absolutely irreducible, and $\overline{\rho}|_{I_{\mathcal{K}'}} \otimes_k \overline{k} \simeq \overline{\rho}_1|_{I_{\mathcal{K}'}} \otimes_{\mathbf{F}_p} \overline{k}$ (and this latter condition is equivalent to the conditions in the first part).

Proof. Without loss of generality, $\mathcal{K}'$ is of special type. We first prove the 'only if' direction. We at least know that $\overline{\rho}$ is absolutely irreducible; passing to a finite extension of scalars and and replacing $\overline{\rho}$ by an unramified twist without loss of generality, we may assume $\overline{\rho} = \overline{\rho}_m \otimes_{\mathbf{F}_p} k$ for some m. It is easy to compute that $\det \overline{\rho}_m = \omega^m \sigma_m$, with $\sigma_m : D_p \to \mathbf{F}_p^\times$ the unique unramified character for which $\sigma_m(\mathrm{Frob}_p) = (-1)^{m+1}$. The condition that $\overline{\rho}_m$ be absolutely irreducible is equivalent to requiring that the character ψ_0^m be distinct from its Frobenius twist $g \mapsto \psi_0^m(\mathrm{Frob}_p\, g\, \mathrm{Frob}_p^{-1}) = \psi_0^{mp}(g)$, so this says that $m \not\equiv 0 \bmod p+1$. Finally, the $\mathcal{A}'$-flatness condition, or equivalently the A'-flatness condition, can be checked on $I_{K'}$, over which $\overline{\rho}_m$ splits (after extension of scalars to $\mathbf{F}_{p^2}$). Since $\psi_0|_{I_{K'}} = \psi_{K'}^e$, by Raynaud's classification [16, Thm 3.4.3] we get the constraint $em = a + pb$ with $0 \le a, b \le e$.

Next, we determine when an A'^{sh}-group schemes $\mathcal{G}$ with generic fiber $\psi_{K'}^{em} : I_{K'} \to \mathbf{F}_{p^2}^\times$ is connected with a connected dual (in which case $\mathcal{G}$ is unique up to canonical isomorphism). By considering separately the cases when $\psi_{K'}^{em}$ takes values in $\mathbf{F}_p^\times$ and when it does not, we need to rule out the possibility of this character or its Cartier dual being the generic fiber of an étale group scheme. By Raynaud's classification of finite group schemes with simple generic fibers (including the case $e = p-1$), this becomes the condition that $\psi_{K'}^{em}$ and its Cartier dual are trivial. That is, we want

$$em \not\equiv 0 \bmod p^2 - 1.$$

Now we impose the extra exactness hypothesis on the Dieudonne module of the closed fiber. In view of the connectedness and unipotence, together with $\dim_{\overline{\mathbf{F}}_p} \mathcal{M}(\mathcal{G}_{/\overline{\mathbf{F}}_p}) = 2$ and the fact that the sequence (1) is always at least right exact, exactness is equivalent to saying that F and V both have non-zero action on M. Equivalently, using the formulation of Cartier duality in terms of Dieudonne modules [7, Ch III, §5.3, Cor 2], the action of F is non-zero on both M and the dual Dieudonne module M^* attached to the Cartier dual group scheme. Thus, if we can write down the affine rings of the A'^{sh}-group schemes with generic fibers $\psi_{K'}^{em}$ and $\omega\psi_{K'}^{-em} = \psi_{K'}^{(p+1-m)e}$, we need only ensure that the closed fiber rings do not have the augmentation ideal killed by the pth power map.

By [16, Thm 3.4.1], the affine ring corresponding to $\psi_{K'}^{em} = \psi_{K'}^{a+pb}$ is

$$A'^{\mathrm{sh}}[X_1, X_2]/(X_1^p - \delta_1 X_2, X_2^p - \delta_2 X_1),$$

where $\mathrm{ord}(\delta_1) = a$, $\mathrm{ord}(\delta_2) = b$, and $0 \le a, b \le e < p$ (here, ord denotes the normalized order function on the discrete valuation ring A'^{sh}). Thus, we must have (by the $F \ne 0$ condition on closed fiber) either a or b vanishing, yet by connectedness at least one of these must not vanish. This yields $a = 0$, $0 < b \le e$ or $b = 0$, $0 < a \le e$. Applying the same considerations to the dual, where a and b are replaced by $e - a$ and $e - b$ respectively, we see that the possibilities for (a, b) are $(0, e), (e, 0)$. This corresponds to $em \equiv e, pe \bmod p^2 - 1$. Replacing m by mp if necessary, we may suppose $em \equiv e \bmod p^2 - 1$ (which implies $m \not\equiv 0 \bmod p+1$).

It is straightfoward to run the argument in reverse to see that all $\overline{\rho}$ having the desired form as $\overline{k}[I_p]$-modules do indeed satisfy the required irreducibility and $\mathcal{A}'$-flatness conditions. For any such $\overline{\rho}$, we have

$$\det \overline{\rho}|_{I_{\mathcal{K}'}} = \psi_{\mathcal{K}'}^{(em)(p+1)} = (\psi_{\mathcal{K}'}^e)^{p+1} = (\psi|_{I_{\mathcal{K}'}})^{p+1} = \omega|_{I_{\mathcal{K}'}}$$

(recall $\psi_{\mathcal{K}'} = \psi_{K'}$ on $I_{\mathcal{K}'} = I_{K'}$). It is straightfoward to check that the conditions in the Corollary are equivalent to saying that $\overline{\rho}|_{I_{\mathcal{K}'}} \otimes_k \overline{k} \simeq \overline{\rho}_1|_{I_{\mathcal{K}'}} \otimes_{\mathbf{F}_p} \overline{k}$.

■

With the corollary settled, we return to the theorems:

Proof. (of Theorem 2.2.1) First we claim that if $\overline{\rho}$ is irreducible, then it is automatically absolutely irreducible. If not, then after a finite extension of scalars we are in the case of a reducible $\overline{\rho} \simeq \chi_1 \oplus \chi_2$, which has non-trivial centralizer. More generally, if $\overline{\rho}$ is reducible, so

$$\overline{\rho} \simeq \begin{pmatrix} \chi_2 & * \\ 0 & \chi_1 \end{pmatrix},$$

it remains to show that $\overline{\rho}$ has trivial centralizer. As we shall see via an intricate Honda system computation in §2.3, $\chi_1 \neq \chi_2$. Thus, the condition of $\overline{\rho}$ having a trivial centralizer is equivalent to $\overline{\rho}$ not being a split extension of χ_2 by χ_1. So assume $\overline{\rho} \simeq \chi_1 \oplus \chi_2$. We seek a contradiction.

We claim that the χ_i are ramified. If some χ_i is unramified, then it can be expressed as the generic fiber of a finite étale p-power order group scheme G over $\mathbf{Z}_p$, so over $\mathcal{K}'$ we have a non-zero group scheme map between the *generic fibers* of the étale $G \times_{\mathbf{Z}_p} \mathcal{A}'$ and the connected $\mathcal{G}(\overline{\rho}|_{G_{\mathcal{K}'}})$. Since both of these group schemes are unipotent, this generic fiber map comes from a non-zero map between the group schemes over $\mathcal{A}'$ [2, Lemma 4.1]. But there are no non-zero group scheme maps between a connected group scheme and an étale one. By a similar argument, the χ_i have ramified Cartier duals.

Thus, $\chi_i = \omega^{n_i}\eta_i$ with $\eta_i : D_p \to k^\times$ unramified and $n_i \in \mathbf{Z}/(p-1)$ satisfying $n_i \neq 0, 1$ (in particular, $p \neq 2$). Using scheme-theoretic closure, each χ_i is the generic fiber of a finite flat $\mathcal{A}'$-group scheme $\mathcal{G}_i$, fitting into a short exact sequence of finite flat commutative $\mathcal{A}'$-group schemes

$$0 \to \mathcal{G}_2 \to \mathcal{G}(\overline{\rho}|_{G_{\mathcal{K}'}}) \to \mathcal{G}_1 \to 0. \tag{2}$$

Since the middle term is connected with a connected dual, the same holds for each $\mathcal{G}_i$. We claim that the closed fiber of each $\mathcal{G}_i$ is a product of copies of $\alpha_{p_{/\kappa}}$. In terms of Dieudonne modules, this says simply that the actions of F and V on the Dieudonne module of the closed fiber $\mathcal{G}_{i_{/\kappa}}$ are zero. This can be checked over an algebraic closure of κ, so by the compatibility of Dieudonne modules and base change of the (perfect) base field, it is enough to check that the geometric closed fibers of the $\mathcal{G}_i$'s are products of α_p's.

Passing to a geometric closed fiber corresponds to passage to the closed fiber of the base change to the strict henselization of $\mathcal{A}'$. On the generic fiber, base changing to $\mathcal{A}'^{\mathrm{sh}}$ corresponds to restriction to the inertia group. That is, we need to look at $\omega^{n_i} \otimes_{\mathbf{F}_p} k$ restricted to $I_{\mathcal{K}'}$. Picking an $\mathbf{F}_p$-basis for k, we are reduced to checking that if $\omega^{n_i}|_{G_{\mathcal{K}'}}$ is the generic fiber of a finite flat $\mathcal{A}'$-group scheme $\mathcal{G}$, then $\mathcal{G}$ has geometric closed fiber α_p. If not, then the geometric closed fiber is μ_p or $\underline{\mathbf{Z}/p}$. Passing to duals if necessary, it follows that the geometric closed fiber of $\mathcal{G}(\overline{\rho}|_{G_{\mathcal{K}'}})$ or its dual has a non-trivial étale factor, contrary to connectedness.

We want to translate (2) into the language of Dieudonne modules, assuming $\mathcal{K}'$ to be of special type without loss of generality. Recall that K' has residue field $\mathbf{F}_p$ and every finite flat $\mathcal{A}'$-group scheme equipped with a generic fiber descent to $\mathbf{Q}_p$ (or even K') admits a canonical descent to an A'-group scheme. This enables us to apply [2, Thm 4.4] to conclude that the Dieudonne module M of the closed fiber of $\mathcal{G}(\overline{\rho}|_{G_{K'}})$ has the structure of a 2-dimensional k-vector space on which F and V act *linearly* and the Dieudonne module M_i of the closed fiber of the A'-descent of $\mathcal{G}_i$ has the structure of a 1-dimensional k-vector space on which F and V act as *zero* (here is where the above α_p result is used). In other words, applying the Dieudonne module functor to the closed fiber of the A'-descent of (2) yields a short exact sequence of $k[F, V] = k[X, Y]/(XY - p)$ modules

$$0 \to M_1 \to M \to M_2 \to 0. \tag{3}$$

This sequence is certainly split, since $\overline{\rho}|_{G_{K'}}$ is split. But in fact this sequence *cannot* be split. Indeed, it splits if and only if F and V act as zero on M; but this possibility is ruled out by the hypothesis that the sequence (1) is exact!

■

Now we prove Theorem 2.2.2.

Proof. This is a standard argument, which we reproduce for completeness. Since $\overline{\rho} \otimes_k \overline{k}$ is irreducible and therefore semisimple, the normality of I_p in D_p implies that $\overline{\rho}|_{I_p}$ is semisimple and therefore tame. Thus, the absolutely irreducible $\overline{\rho}$ is abelian on tame inertia, so the conjugation action of Frobenius on tame inertia yields

$$\overline{\rho}|_{I_p} \otimes_k \overline{k} \simeq \psi' \oplus \psi'^p$$

with $\psi'^{p^2} = \psi'$, so $\psi' = \psi_0^m|_{I_p}$ for some m. This gives

$$\overline{\rho}|_{D_{p^2}} \otimes_k \overline{k} \simeq \psi_0^m \chi_1 \oplus \psi_0^{mp} \chi_2$$

with $\chi_i : D_{p^2} \to \overline{k}^\times$ unramified characters. Since $\widehat{\mathbf{Z}}$ has no non-trivial 2-torsion, we can construct an unramified square root of χ_1^{-1}; twisting through by this, we may suppose

$$\overline{\rho}|_{D_{p^2}} \otimes_k \overline{k} \simeq \psi_0^m \oplus \psi_0^{mp} \chi$$

with an unramified $\chi : D_{p^2} \to \overline{k}^\times$.

Since $\overline{\rho}$ is absolutely irreducible, it is now clear that

$$\overline{\rho} \otimes_k \overline{k} \simeq \mathrm{Ind}_{D_{p^2}}^{D_p}(\psi_0^m) \otimes_{\mathbf{F}_{p^2}} \overline{k} \simeq \overline{\rho}_m \otimes_{\mathbf{F}_p} \overline{k},$$

as desired.

■

2.3. **Translation into Honda systems.**

As a warm-up for the descent computations we will later need to perform with Honda systems, we would like to illustrate the procedure by describing the possible $\overline{\rho}$ which can arise. This also involves standardizing some notation we always will use in our descent calculations. In the reducible case, we suppose we have an exact sequence

$$0 \to \chi_2 \to \overline{\rho} \to \chi_1 \to 0.$$

In the case of $\mathcal{K}'$ of special type, we want to determine all possibilities for $LM_{\mathcal{A}'}(\overline{\rho})$ and the descent data, as well as for $LM_{A'}(\overline{\rho})$. We will then translate this into a more representation-theoretic description and will easily remove the special type condition on $\mathcal{K}'$.

By using scheme-theoretic closure, we know that in the reducible cases, each $\chi_i|_{G_{\mathcal{K}'}}$ is the generic fiber of a connected, unipotent $\mathcal{A}'$-group scheme $\mathcal{G}_i$, fitting into the exact sequence (2). On the closed fibers this gives a non-split Dieudonne module sequence, as argued earlier. Since the only simple finite flat commutative group schemes over $\mathbf{Z}_2^{\mathrm{un}}$ with 2-power order are μ_2 and $\underline{\mathbf{Z}/2}$, neither of which is connected and unipotent, we see that $p \neq 2$ in the reducible cases.

Since (3) does not split, either F or V is non-zero on M. In fact, both are non-zero. Indeed, by the exactness (1) it is enough to show that neither FM nor VM can fill up all of M. Since the closed fiber of $\mathcal{G}(\overline{\rho}|_{G_{\mathcal{K}'}})$ and its Cartier dual are both connected, the description of Cartier duality in terms of Dieudonne modules [7, Ch III, §5.3, Cor 2] shows that both F and V act in a nilpotent manner on M. Hence, $FM, VM \neq M, 0$. Pick $e_2 \notin \ker F$ and define $e_1 = Fe_2 \neq 0$, so $\ker F = ke_1$ and $\{e_1, e_2\}$ is an ordered k-basis of M, with respect to which we have

$$F = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad V = \begin{pmatrix} 0 & s^{-1} \\ 0 & 0 \end{pmatrix},$$

with $s \in k^\times$.

The condition that the Dieudonne module sequence (3) is induced by a sequence of finite flat group schemes over $\mathcal{A}'$, and even over A', imposes serious constraints. We will now use the full force of the classification established in [2] in order to compute what the actual constraints are. The resulting computation will be lengthy. In the reducible cases, let $(L_i, M_i) = LM_{A'}(\chi_i)$ be the finite Honda system over A' attached to the unique finite flat A'-group scheme with generic fiber $\chi_i|_{G_{K'}}$. The exact sequence

$$0 \to (L_1, M_1) \to (L, M) \to (L_2, M_2) \to 0 \tag{4}$$

is what we want to study in the reducible cases. On the level of Dieudonne modules, it is just the sequence (3), made 'explicit' with the ordered k-basis $\{e_1, e_2\}$ of M, where e_2 necessarily maps to a k-basis $\overline{e}_2$ of M_2 and e_1 is necessarily a k-basis of M_1.

Before carrying out our study of (4), we need to give a somewhat explicit description of what $LM_{A'}(\overline{\rho})$ looks like. The reducibility is not relevant for this part. View the $(A'/p) \otimes_{\mathbf{F}_p} k$-module $M_{A'}$ as a quotient of $(A' \otimes_A M) \oplus (p^{-1}\mathfrak{m} \otimes_A M^{(1)})$ by the submodule

$$\{(u_1 \otimes a_1 e_1 + u_2 \otimes a_2 e_2 - w_2 \otimes b_2 e_1, w_1 \otimes b_1 e_1 + w_2 \otimes b_2 e_2 - p^{-1} u_2 \otimes s^{-1} a_2 e_1) | u_i \in \mathfrak{m},\ w_i \in A', a_i, b_i \in k\},$$

as in its definition [2, §2] (here, we've also invoked the explicit matrix formulas for F and V as k-linear maps). At this point, a word of warning should be given about the $M^{(1)}$ term above. Since $A = \mathbf{Z}_p$, so Frobenius on A is trivial, $M^{(1)}$ is the same as M as a k-module. However, we will shortly be making base changes that enlarge the residue field from $\mathbf{F}_p$ to κ, so in the calculations done after base change it will be very important to remember this twisting by Frobenius (since over $W(\kappa)$ it cannot generally be ignored). A possible source of confusion below is that we have two finite fields floating around, with very different roles: there is the field κ from the closed fiber of $\mathcal{A}'$ and there is the field k from the generic fiber representation space; F and V act κ-semilinearly and k-linearly.

Let ϵ_1 denote the image of $(1 \otimes e_2, 0)$ in the quotient $M_{A'}$ and let ϵ_2 denote the image of $(0, p^{-1}\pi \otimes e_2)$ in the quotient $M_{A'}$. It is easy to check that the $(A'/p) \otimes_{\mathbf{F}_p} k$-module map

$$((A'/p) \otimes_{\mathbf{F}_p} k)\epsilon_1 \oplus ((A'/p) \otimes_{\mathbf{F}_p} k)\epsilon_2 \to M_{A'}$$

is surjective and so by a length comparison, using [2, Lemma 2.1], this is an isomorphism. In particular, $M_{A'}$ is free of rank 2 as an $(A'/p) \otimes_{\mathbf{F}_p} k$-module. Note that the residue class of $(1 \otimes e_1, 0)$ in $M_{A'}$ is equal to $(p/\pi)\epsilon_2$ and the residue class of $(0, p^{-1}\pi \otimes e_1)$ in $M_{A'}$ is equal to $s\pi\epsilon_1$. Also, note that ϵ_2 is not entirely canonical, as it involves a choice of π. This will be important below for our descent calculations.

Since L surjects onto $\operatorname{coker} \mathcal{F}_M$, $L = ((A'/p) \otimes_{\mathbf{F}_p} k)(\epsilon_1 + \alpha\epsilon_2)$ for some $\alpha \in (A'/p) \otimes_{\mathbf{F}_p} k \simeq k[\pi]/\pi^e$. Making the change of basis $e_2 \rightsquigarrow e_2 + te_1$ for $t \in k$, we get the change

$$\alpha \rightsquigarrow (1 - \alpha ts\pi)^{-1}(\alpha - tp/\pi),$$

so we can (*and do*) always suppose either that $\alpha = 0$ (which 'rigidifies' the choice of basis up to scaling $\{e_1, e_2\}$ by the same element of $k^\times$) or that $\alpha = a_i\pi^i + \pi^{i+1}(\dots)$ for a unique $a_i \in k^\times$ and $0 \le i \le e-2$, with a_i and i independent of the choice of basis $\{e_1, e_2\}$ as above. In particular, $\alpha = 0$ whenever $e = 1$. We emphasize that from now on we only work with bases such that one of the above conditions holds (and exactly one of these conditions can hold). This is visibly compatible with base change of Honda systems.

Making the étale base change $A' \to \mathcal{A}'$, we obtain $LM_{\mathcal{A}'}(\overline{\rho}) = (\mathcal{L}, \mathcal{M})$ with

$$\mathcal{M} = W(\kappa) \otimes_A M = (\kappa \otimes_{\mathbf{F}_p} k)e_1 \oplus (\kappa \otimes_{\mathbf{F}_p} k)e_2$$

and the maps F, V are semilinear with respect to κ, linear with respect to k, and satisfy $F(e_1) = V(e_1) = 0$, $F(e_2) = e_1$, $V(e_2) = s^{-1}e_1$ [7, Ch III, §2, Prop 2.2(*i*)]. Also, $\mathcal{L} \subseteq \mathcal{A}' \otimes_{A'} M_{A'} \simeq \mathcal{M}_{\mathcal{A}'}$ is given by $\mathcal{A}' \otimes_{A'} L$. See [2, Lemma 4.7] for more details.

We encode $\overline{\rho}$ as descent data (relative to $A \to \mathcal{A}'$) on the finite Honda system $(\mathcal{L}, \mathcal{M})$ over $\mathcal{A}'$. This is nothing other than a $\mathrm{Gal}(\mathbf{Q}_p(\zeta_e)/\mathbf{Q}_p) \simeq \mathrm{Gal}(\kappa/\mathbf{F}_p)$-semilinear action of $\mathrm{Gal}(\mathcal{K}'/\mathbf{Q}_p)$ on $\mathcal{M}$ such that the induced action on $\mathcal{M}_{\mathcal{A}'}$ takes $\mathcal{L}$ back to itself. In order that the descent to A' is $LM_{A'}(\overline{\rho})$, we need to require that the action of $\mathrm{Gal}(\mathcal{K}'/K') \simeq \mathrm{Gal}(\kappa/\mathbf{F}_p)$ on $\mathcal{M} = W(\kappa) \otimes_A M$ is the usual semilinear one fixing M. The only issue is how $\mathrm{Gal}(\mathcal{K}'/\mathbf{Q}_p(\zeta_e)) \simeq \mu_e$ acts on the pair $(\mathcal{L}, \mathcal{M})$ (recall that the isomorphism with μ_e is given by the scaling action on π, denoted $\pi^\zeta = \zeta\pi$). We must keep in mind the constraint arising from $\mathcal{L}$, which says that the induced semilinear action on $\mathcal{M}_{\mathcal{A}'}$ must take $\mathcal{L}$ isomorphically back to itself.

We now examine the reducibile cases in more detail. Consider the short exact sequence of $(A'/p) \otimes_{\mathbf{F}_p} k$-modules

$$0 \to (M_1)_{A'} \to M_{A'} \to (M_2)_{A'} \to 0. \tag{5}$$

Let's makes this more explicit. Let $x_1 \in (M_1)_{A'}$ denote the class of $(1 \otimes e_1, 0)$, let $x_2 \in (M_1)_{A'}$ denote the class of $(0, p^{-1}\pi \otimes e_1)$, let $y_1 \in (M_2)_{A'}$ denote the class of $(1 \otimes e_2, 0)$, and let $y_2 \in (M_2)_{A'}$ denote the class of $(0, p^{-1}\pi \otimes e_2)$. It is fairly straightfoward to check that

$$((A'/\mathfrak{m}) \otimes_{\mathbf{F}_p} k)x_1 \oplus ((A'/\mathfrak{m}^{e-1}) \otimes_{\mathbf{F}_p} k)x_2 = (M_1)_{A'}, \ \ ((A'/\mathfrak{m}) \otimes_{\mathbf{F}_p} k)y_1 \oplus ((A'/\mathfrak{m}^{e-1}) \otimes_{\mathbf{F}_p} k)y_2 = (M_2)_{A'}.$$

The short exact sequence of $(A'/p)\otimes_{\mathbf{F}_p} k$-modules (5) is characterized by

$$x_1 \mapsto (p/\pi)\epsilon_2,\ \ x_2 \mapsto s\pi\epsilon_1,\ \ \epsilon_i \mapsto y_i.$$

Just as in our analysis of L in the general setting, we see that L_1 is generated over $(A'/p)\otimes_{\mathbf{F}_p} k$ by $x_1+\beta x_2$ for some $\beta\in(A'/p)\otimes_{\mathbf{F}_p} k$. The element $x_1+\beta x_2\in L_1$ maps to $(p/\pi)\epsilon_2+\beta s\pi\epsilon_1$ in $M_{A'}$. Since $L_1=(M_1)_{A'}\cap L$ by [2, Thm 4.3], we see that $\beta s\pi\alpha=p/\pi$ in $(A'/p)\otimes_{\mathbf{F}_p} k$. Hence, $\alpha\neq 0$ and $\beta\neq 0$ (in fact, β has non-zero image in $(A'/\mathfrak{m}^{e-1})\otimes_{\mathbf{F}_p} k$), so we may consider the unique representative of α of the form

$$a_i\pi^i+\cdots+a_{e-1}\pi^{e-1}$$

(with all $a_r\in k$, $a_i\in k^\times$), with $0\leq i\leq e-2$. This is very important. In particular, this shows that $\alpha\neq 0$ in the reducible cases.

We can write $\beta=b_j\pi^j(1+\pi(\dots))$ with $b_j\in k^\times$ and $0\leq j\leq e-2$. Since x_1 is $\mathfrak{m}$-torsion, we can scale $x_1+\beta x_2$ by $(1+\pi(\dots))^{-1}$ so that we may (and do) suppose $\beta=b_j\pi^j$ for a canonical $b_j\in k^\times$ and $0\leq j\leq e-2$ independent of the choice of basis e_2. The condition $\beta s\pi\alpha=p/\pi$ gives $i+j+2\equiv 0 \bmod e$ and $b_j s a_i=u_0^{-1}$ in k. Since $0<i+j+2<2e$, we conclude that $\alpha=a\pi^i+\pi^{i+1}(\dots)$ for a unique $a\in k^\times$, $0\leq i\leq e-2$ and $\beta=(asu_0)^{-1}\pi^{e-2-i}$.

Now return to the general (i.e., possibly irreducible) case. We have descent data on $LM_{A'}(\overline{\rho})$, compatible with the short exact sequence (4) when $\overline{\rho}$ is reducible. The condition that the $W(\kappa)$-linear action $[\zeta]$ on $\mathcal{M}=W(\kappa)\otimes_A M\simeq \kappa\otimes_{\mathbf{F}_p} M$ commutes with F and V (for $\zeta\in\mu_e$) is that

$$[\zeta]=\begin{pmatrix} d_\zeta^{(p)} & c_\zeta \\ 0 & d_\zeta\end{pmatrix},$$

where $c_\zeta, d_\zeta\in\kappa\otimes_{\mathbf{F}_p} k$, d_ζ is a unit, and $d_\zeta^{(p^2)}=d_\zeta$. For $\sigma\in\mathrm{Gal}(\mathcal{K}'/K')\simeq\mathrm{Gal}(\kappa/\mathbf{F}_p)$ we have

$$\sigma(d_\zeta)=d_{\zeta^\sigma},\ \ \sigma(c_\zeta)=c_{\zeta^\sigma} \tag{6}$$

from the condition $[\sigma]\circ[\zeta]=[\zeta^\sigma]\circ[\sigma]$. The multiplicative property $[\zeta_1]\circ[\zeta_2]=[\zeta_1\zeta_2]$ yields

$$c_{\zeta_1\zeta_2}=d_{\zeta_1}^{(p)}c_{\zeta_2}+d_{\zeta_2}c_{\zeta_1}, \tag{7}$$

and $\zeta\mapsto d_\zeta$ is a group map from $\mu_e(\kappa)$ to $\mu_e(\kappa\otimes_{\mathbf{F}_p} k)$.

It is easy to compute that the ζ-semilinear automorphism $[\zeta]_{\mathcal{A}'}:\mathcal{M}_{\mathcal{A}'}\simeq\mathcal{M}_{\mathcal{A}'}$ is given by

$$[\zeta]_{\mathcal{A}'}(\epsilon_1)=d_\zeta\epsilon_1+c_\zeta(p/\pi)\epsilon_2,\ \ [\zeta]_{\mathcal{A}'}(\epsilon_2)=\zeta(d_\zeta^{(p)}\epsilon_2+c_\zeta^{(p)}s\pi\epsilon_1),$$

so

$$[\zeta]_{\mathcal{A}'}(\epsilon_1+\alpha\epsilon_2)=(d_\zeta+\zeta\alpha^\zeta c_\zeta^{(p)}s\pi)\epsilon_1+(c_\zeta(p/\pi)+\zeta\alpha^\zeta d_\zeta^{(p)})\epsilon_2.$$

Hence, $[\zeta]_{\mathcal{A}'}$ takes $\mathcal{L}$ to itself (inside of $\mathcal{M}_{\mathcal{A}'}\simeq\mathcal{A}'\otimes_{A'}M_{A'}$) if and only if the following relation holds, which we'll call (for ease of reference) the *Fundamental Relation*:

$$\alpha(d_\zeta+\zeta\alpha^\zeta c_\zeta^{(p)}s\pi)=c_\zeta(p/\pi)+\zeta\alpha^\zeta d_\zeta^{(p)}. \tag{8}$$

In particular, we see that $c_\zeta=0$ for all $\zeta\in\mu_e$ in cases with $\alpha=0$ (which, as we will see below, is equivalent to $\overline{\rho}$ being irreducible).

Suppose now that $\overline{\rho}$ is reducible, so $\alpha=a\pi^i+\cdots\neq 0$. Since $i+1\leq e-1$, p/π vanishes modulo $\mathfrak{m}^{i+1}$, so if we reduce the Fundamental Relation modulo $\mathfrak{m}^{i+1}$ then the c_ζ terms go away and we get

$$a_i d_\zeta=\zeta^{i+1}a_i d_\zeta^{(p)}$$

in $\kappa\otimes_{\mathbf{F}_p} k$, with $a_i\in k^\times$, so therefore

$$d_\zeta=\zeta^{i+1}d_\zeta^{(p)}. \tag{9}$$

Iterating this twice and recalling that $d_\zeta^{(p^2)}=d_\zeta$, we obtain $\zeta^{(i+1)(p+1)}=1$ for all $\zeta\in\mu_e$, so

$$e|(i+1)(p+1). \tag{10}$$

The final condition on the Honda system is that $\mathcal{A}' \otimes_{A'} L_1$ must be stable under $[\zeta]_{\mathcal{A}'}$ (this is required by the definition of descent data in the context of Honda systems). This translates into the constraint that

$$(p/\pi)(d_\zeta^{(p)}\epsilon_2 + c_\zeta^{(p)} s\pi\epsilon_1) + \beta^\zeta s\zeta\pi(d_\zeta\epsilon_1 + c_\zeta(p/\pi)\epsilon_2) = (p/\pi)d_\zeta^{(p)}\epsilon_2 + \beta^\zeta s\zeta\pi d_\zeta\epsilon_1$$

must be a multiple of $(p/\pi)\epsilon_2 + \beta s\pi\epsilon_1$. This is equivalent to having a relation of the form

$$\beta(d_\zeta^{(p)} + \pi(\dots)) = \beta^\zeta\zeta d_\zeta$$

in $(\mathcal{A}'/\mathfrak{n}^{e-1}) \otimes_{\mathbf{F}_p} k$. Since $\beta = (asu_0)^{-1}\pi^{e-2-i}$, this is equivalent to having

$$d_\zeta^{(p)} = \zeta^{-i-1} d_\zeta \tag{11}$$

in $\kappa \otimes_{\mathbf{F}_p} k$. By (9), this automatically holds.

Next we check that in the reducible cases, χ_1 and χ_2 have non-isomorphic Honda systems with descent data over $\mathcal{K}'$, so $\chi_1 \neq \chi_2$. This is the important unproven fact mentioned in the proof of Theorem 2.2.1, and therefore completes the proofs of Theorem 2.5 and Corollary 2.6. In order to analyze these Honda systems with descent data, we compute

$$[\zeta]_{\mathcal{A}'}(x_1) = d_\zeta^{(p)} x_1, \quad [\zeta]_{\mathcal{A}'}(x_2) = \zeta d_\zeta x_2,$$

$$[\zeta]_{\mathcal{A}'}(y_1) = d_\zeta y_1, \quad [\zeta]_{\mathcal{A}'}(y_2) = \zeta d_\zeta^{(p)} y_2.$$

Thus, if we have an isomorphism between $LM_{\mathcal{A}'}(\chi_1)$ and $LM_{\mathcal{A}'}(\chi_2)$ compatible with the descent data (i.e., if $\chi_1 = \chi_2$), then $d_\zeta = d_\zeta^{(p)}$ for all $\zeta \in \mu_e$, and also $i = e-2-i$, so $i+1 = e/2$ (in particular, e must be even). Since $d_\zeta = \zeta^{i+1} d_\zeta^{(p)}$ for all $\zeta \in \mu_e$, it follows that $\zeta^{e/2} = \zeta^{i+1} = 1$ for all $\zeta \in \mu_e$. This is a contradiction and therefore proves that necessarily $\chi_1 \neq \chi_2$.

As a final basic observation, we check that in the irreducible cases, necessarily $\alpha = 0$ (so $\alpha = 0$ is equivalent to $\overline{\rho}$ being irreducible). We can make a finite extension of scalars on k, so by Corollary 2.2.3 we can assume $\overline{\rho}|_{G_E} \simeq \overline{\rho}_1|_{G_E} \otimes_{\mathbf{F}_p} k$ for E/K' some unramified finite extension inside of $\overline{\mathbf{Q}}_p$ (with valuation ring $\mathcal{O}_E$ and uniformizer π). Since $e(A) = 1$, certainly the Honda system $LM_A(\overline{\rho}_1) = (L_0, M_0)$ has its own α parameter equal to 0, so the same holds after applying $\otimes_{\mathbf{F}_p} k$. Let $e_1^1, e_2^1, \epsilon_1^1, \epsilon_2^1$ denote basis vectors associated to $LM_A(\overline{\rho}_1 \otimes_{\mathbf{F}_p} k)$. Let k_E denote the residue field of E, so the isomorphism $LM_{\mathcal{O}_E}(\overline{\rho}_1 \otimes_{\mathbf{F}_p} k|_{G_E}) \simeq LM_{\mathcal{O}_E}(\overline{\rho}|_{G_E})$ gives rise to a $(k_E \otimes_{\mathbf{F}_p} k)[F,V]$-module isomorphism of Dieudonne modules

$$(k_E \otimes_{\mathbf{F}_p} k)e_1^1 \oplus (k_E \otimes_{\mathbf{F}_p} k)e_2^1 \to (k_E \otimes_{\mathbf{F}_p} k)e_1 \oplus (k_E \otimes_{\mathbf{F}_p} k)e_2$$

given by $e_1^1 \mapsto ae_1$, $e_2^1 \mapsto be_1 + a^{(p)}e_2$, for some $a \in (k_E \otimes_{\mathbf{F}_p} k)^\times$ and $b \in k_E \otimes_{\mathbf{F}_p} k$. This yields

$$\epsilon_1^1 \mapsto a^{(p)}\epsilon_1 + bp/\pi\epsilon_2,$$

so we must have $\alpha = (a^{(p)})^{-1}bp/\pi$ in $(\mathcal{O}_E/p) \otimes_{\mathbf{F}_p} k$, so α is a multiple of π^{e-1} in $(A'/p) \otimes_{\mathbf{F}_p} k$. But we have already set up the choices of bases so that when $\alpha \neq 0$, there is a non-zero π^i term appearing in α with $i < e-1$. Thus, we must have $\alpha = 0$, as desired.

2.4. **Classification of Possible $\overline{\rho}$.** The computational method in the analysis of the reducible possibilities will now be carried out in more detail, in order to get a more precise description of $(L, M) = LM_{A'}(\overline{\rho})$. In particular, we will interpret the parameter a as an 'unramified' factor and the parameters i and d_ζ as 'ramified' factors which determine $\overline{\rho}$ up to unramified twisting. If we replace e_2 by $e_2 + te_1$ for $t \in k$, this gives rise to

$$c_\zeta \rightsquigarrow c_\zeta + t(d_\zeta^{(p)} - d_\zeta), \quad \alpha \rightsquigarrow (1 - \alpha ts\pi)^{-1}(\alpha - tp/\pi). \tag{12}$$

Observe as before that when $\alpha \neq 0$, the 'lowest order term' $a\pi^i$ in α is unaffected by changing e_2, and so is 'intrinsic' (note that essentially the only other way to change the basis is to scale e_1 and e_2 by the same element of $k^\times$). Keep in mind that the reducible cases are *precisely* the ones with $\alpha \neq 0$.

Our first task in this section is to explicitly describe the characters occuring in the reducible cases. More generally, consider the following finite Honda system over K'. Define $M = k$ with $F = V = 0$, so $M_{A'} = ((A'/\mathfrak{m}) \otimes_{\mathbf{F}_p} k)z_1 \oplus ((A'/\mathfrak{m}^{e-1}) \otimes_{\mathbf{F}_p} k)z_2$, with z_1 the class of $(1, 0)$ and z_2 the class of $(0, p^{-1}\pi)$.

Define L to be the submodule generated by $z_1 + a\pi^i z_2$ for some $0 \le i \le e-2$ and $a \in k^\times$. It is readily checked that this is a finite Honda system over A'. The associated representation $\chi : G_{K'} \to k^\times$ will be computed below.

The descent data for a D_p-representation requires us to base change to $\mathcal{A}'$ and let $\sigma \in \mathrm{Gal}(\mathcal{K}'/K')$ act on $W(\kappa) \otimes_{\mathbf{Z}_p} M \simeq \kappa \otimes_{\mathbf{F}_p} k$ as usual. The 'unknown' part is $[\zeta]$, which acts via a ζ-semilinear map which sends 1 to some $d_\zeta \in \kappa \otimes_{\mathbf{F}_p} k$. Note that changing the k-basis of M has no effect on d_ζ. The necessary and sufficient conditions on d_ζ are that $\zeta \mapsto d_\zeta$ is a $\mathrm{Gal}(\kappa/\mathbf{F}_p)$-semilinear map from $\mu_e(\kappa)$ to $\mu_e(\kappa \otimes_{\mathbf{F}_p} k)$ and $d_\zeta = \zeta^{i+1} d_\zeta^{(p)}$. Note that d_ζ is independent of the choice of k-basis of M. The next theorem interprets the Honda system parameters in terms of Galois representations.

Theorem 2.4.1. *The character χ above is equal to $\eta_{K',a^{-1}}\chi_{-p/\pi^{i+1}}$, where the character $\chi_x : G_{K'} \to \mathbf{F}_p^\times$ gives the action on the $(p-1)$th roots of x in $\overline{\mathbf{Q}}_p^\times$. In particular, $\chi|_{I_{K'}} = \psi_{1,K'}^{e-i-1}$.*

Suppose we are given a descent of χ to a continuous character $\chi_0 : D_p \to k^\times$, via some data $\zeta \mapsto d_\zeta$ on the Honda system for $\chi|_{G_{\mathcal{K}'}}$. Then any $\mathcal{A}'$-flat continuous character $\chi_0' : D_p \to k^\times$ is an unramified twist of χ_0 if and only if $\chi_0'|_{G_{K'}}$ has the same descent data d_ζ on its Honda system over $\mathcal{A}'$.

Proof. Using the fact that F and V act as 0 on $M = k$, the explicit knowledge of the F and V torsion in the formal group scheme $\widehat{CW}_{\mathbf{F}_p}$ unravels all of the complications implicit in [2, Thm 1.9, Remark 4.2], so the $k[G_{K'}]$-module χ has for its underlying group the group of all $\mathbf{F}_p$-linear maps

$$\phi : k \to \pi^{1/p}\mathcal{O}_{\mathbf{C}_{K'}}/\pi\mathcal{O}_{\mathbf{C}_{K'}} \tag{13}$$

such that for all $b \in k$,

$$\widehat{\phi(b)} + (\pi^{i+1}/p)\widehat{\phi(ab)}^{\,p} \in \mathbf{C}_{K'}$$

lies in $\pi\mathcal{O}_{\mathbf{C}_{K'}}$. Here, $\widehat{\phi(\cdot)}$ denotes a lifting to $\pi^{1/p}\mathcal{O}_{\mathbf{C}_{K'}}$, and the action of k and $G_{K'}$ are the obvious ones, using the respective actions on k and $\mathbf{C}_{K'}$ in (13).

Since [2, Thm 4.4] guarantees that this abstract $k[G_{K'}]$-module is a 1-dimensional k-vector space, in order to study the action of $g \in G_{K'}$ on $\phi \neq 0$, we need to determine for which $\chi(g) \in k^\times$ we have the congruence $g(\widehat{\phi(1)}) \equiv \widehat{\phi(\chi(g))} \bmod \pi\mathcal{O}_{\mathbf{C}_{K'}}$. By using extension of scalars (or rather, descent of scalars), we can assume $k = \mathbf{F}_p(a) = \mathbf{F}_p[a]$. Say $[k : \mathbf{F}_p] = m$, so $\{1, a, \dots, a^{m-1}\}$ is an $\mathbf{F}_p$-basis for k and knowledge of ϕ comes down to knowledge of $\phi_j = \widehat{\phi(a^j)} \in \pi^{1/p}\mathcal{O}_{\mathbf{C}_{K'}}$ for $j \in \mathbf{Z}$. Defining $\ell = e-i-1$ (so $1 \le \ell \le e-1 \le p-2$), we write $\mathrm{ord}_\pi(\phi_j) = r_j/p$ with $j \in \mathbf{Z}$, $r_j \in \mathbf{Q}$, $1 \le r_j \le p$, so we must have

$$\phi_j + u_0\pi^{-\ell}\phi_{j+1}^p \in \pi\mathcal{O}_{\mathbf{C}_{K'}}.$$

If $r_{j+1} = p$ then $r_j = p$ so by iteration $\phi = 0$. Since $\phi \neq 0$, we have $1 \le r_j < p$ for all j. This forces $r_{j+1} = \ell + r_j/p$ for all j. Sending $j \to \infty$, we get $r_j = \ell p/(p-1)$ for all j, so $\mathrm{ord}_\pi(\phi_j) = \ell/(p-1)$ for all j. A careful check of powers of π shows that it is safe to iterate the congruences in $\pi^{1/p}\mathcal{O}_{\mathbf{C}_{K'}}/\pi\mathcal{O}_{\mathbf{C}_{K'}}$. This gives

$$\phi_j \equiv \left(-\frac{u_0}{\pi^\ell}\right)^{1+p+\cdots+p^{m-j-1}} \phi_m^{p^{m-j}} \bmod \pi\mathcal{O}_{\mathbf{C}_{K'}}.$$

Let $X^m + t_{m-1}X^{m-1} + \cdots + t_0 \in \mathbf{F}_p[X]$ be the minimal polynomial of a, so we must have

$$\phi_m + \sum_{j=0}^{m-1} t_j \left(-\frac{u_0}{\pi^\ell}\right)^{\frac{p^{m-j}-1}{p-1}} \phi_m^{p^{m-j}} \equiv 0 \bmod \pi.$$

If we choose a $(p-1)$th root w of $-u_0/\pi^\ell$ in $\mathbf{C}_{K'}$ (coming from a choice of $(p-1)$th root of π, to be precise) and define $w_j = w\phi_j \in \mathcal{O}_{\mathbf{C}_{K'}}^\times$, then we arrive at the conditions

$$w_j \equiv w_m^{p^{m-j}} \bmod \pi^{p/(p-1)}$$

and

$$w_m + \sum_{j=0}^{m-1} t_j w_m^{p^{m-j}} \equiv 0 \bmod \pi^{p/(p-1)}.$$

That is, if we define the *separable* polynomial $P_a(X) = X + t_{m-1}X^p + \cdots + t_0X^{p^m} \in \mathbf{F}_p[X]$ (and note $t_0 \neq 0$), we see that w_m is the reduction of the Hensel's Lemma lift to $\mathcal{O}_{\mathbf{C}_{K'}}/p$ of a unique root of P_a and then $w_j \equiv w_m^{p^{m-j}}$ for $0 \leq j \leq m-1$ determines the other w_j's. In particular, this construction sets up a bijection between elements of our abstract 1-dimensional k-vector space and the p^m roots to P_a in $\overline{\mathbf{F}}_p$.

Let's first determine the answer on $I_{K'}$, where things are a little simpler. The assertion of the Theorem is that we get the character $\psi^\ell_{1,K'}$. For $g \in I_{K'}$, the action of g on $\overline{\mathbf{F}}_p$ is *trivial.* Choose the lifts $(g(\phi))_j$ to be $g(\phi_j)$. It follows from the formula for w_m in terms of ϕ_m, as well as the condition $g(w_m) \equiv w_m \bmod \mathfrak{m}_{\mathcal{O}_{\mathbf{C}_{K'}}}$, that $(g(\phi))_m = (\psi^\ell_{1,K'}(g)(\phi))_m$. The formula for w_j in terms of w_m now yields

$$(g(\phi))_j = (\psi^\ell_{1,K'}(g)(\phi))_j$$

for $0 \leq j \leq m-1$. In other words, $g(\phi)$ and $\psi^\ell_{1,K'}(g)\phi$ have the same values on the $\mathbf{F}_p$-basis $1, a, \ldots, a^{m-1}$, so $g(\phi) = \psi^\ell_{1,K'}(g)\phi$. Since ϕ was arbitrary in our representation space, this shows that the $I_{K'}$-action is via $\psi^\ell_{1,K'}$, as desired.

Now consider a general $g \in G_{K'}$. Since we have checked things over $I_{K'}$, it is enough to choose g which is a Frobenius element, so g induces the pth power map on $\overline{\mathbf{F}}_p$. To avoid ambiguity, we write $w_j(\phi)$ and $w_j(\phi_a)$, so

$$g(w_j(\phi)) \equiv w_j(\phi)^p \equiv w_m(\phi)^{p^{m-(j-1)}} \equiv w_{j-1}(\phi) \equiv w_j(\phi_a) \bmod \mathfrak{m}_{\mathcal{O}_{\mathbf{C}_{K'}}},$$

where $\phi_a(x) \stackrel{\text{def}}{=} \phi(a^{-1}x)$. In fact, it readily follows that the above congruence must hold modulo p (since P_a is separable, with roots lifting uniquely to roots in $\mathcal{O}_{\mathbf{C}_{K'}}/p$), so

$$g(\phi_j) \equiv \frac{w}{g(w)}(\phi_a)_j \bmod p\mathcal{O}_{\mathbf{C}_{K'}}.$$

Since $w/g(w) = g(w^{-1})/w^{-1} = \chi_x(g)$ for $g = -\pi^\ell/u_0 = -p/\pi^{i+1}$, we're done.

Finally, we need to show that if $\chi_0, {\chi'}_0 : D_p \to k^\times$ are two characters of the type we are considering, then χ_0 and χ'_0 are related by an unramified twist if and only if the parameters d_ζ, ${d'}_\zeta$ are the same. In other words, we need to work out the Honda system interpretation of the equality $\chi_0|_{I_p} = {\chi'}_0|_{I_p}$. This is equivalent to saying that for some large N (taken to be divisible by f without loss of generality) $\chi_0|_{G_{E_N}} = {\chi'}_0|_{G_{E_N}}$, where $E_N = \mathbf{Q}_p(\zeta_{p^N-1})$ is the degree N unramified extension of $\mathbf{Q}_p$ inside of $\overline{\mathbf{Q}}_p$ (note that $\mathbf{Q}_p(\zeta_e) \subseteq E_N$ when $f|N$). This equality amouts to having an isomorphism of the Honda systems attached to χ_0 and ${\chi'}_0$ on $G_{K'E_N}$, compatible with the Honda system descent data for the totally ramified extension $K'E_N/E_N$. Note that $\mathcal{A}'$ lies inside of the valuation ring $\mathcal{A}'_N$ of $K'E_N \simeq K' \otimes_{\mathbf{Q}_p} E_N$.

Since $K'E_N/K'$ is unramified, we readily compute that the Honda systems over $\mathcal{A}'_N$ have Dieudonne module parts $k_N \otimes_{\mathbf{F}_p} k$ (where $k_N = \mathbf{F}_{p^N}$ denotes the residue field of $K'E_N$) and lattices L and L' spanned over $(\mathcal{A}'_N/p) \otimes_{\mathbf{F}_p} k$ by $z_1 + a\pi^i z_2$ and $z_1 + a'\pi^i z_2$ respectively (for $a, a' \in k^\times$), where z_1 is the class of $(1, 0)$ and z_2 is the class of $(0, p^{-1}\pi)$ as above (the values of i must be the same for χ_0 and ${\chi'}_0$, since we have seen above that the inertial restriction determines i). The linear disjointness of $\mathcal{K}'$ and E_N over $\mathbf{Q}_p(\zeta_e)$ implies that the descent data relative to $K'E_N/E_N$ are 'the same' as that we originally have for $\mathcal{K}'/\mathbf{Q}_p(\zeta_e)$, which is to say that this data is given by $1 \mapsto d_\zeta, {d'}_\zeta \in (\mathcal{A}'_N/p) \otimes_{\mathbf{F}_p} k$.

The isomorphism of $k[G_{K'E_N}]$-modules $\chi_0|_{G_{K'E_N}} \simeq {\chi'}_0|_{G_{K'E_N}}$ translates into a map $1 \mapsto v \in (k_N \otimes_{\mathbf{F}_p} k)^\times$, which has the effect $z_1 + a\pi^i z_2 \mapsto vz_1 + av^{(p)}\pi^i z_2$. Thus, the necessary and sufficient condition for 'L-compatibility' is $v^{(p)} = (a'/a)v$, while descent data compatibility is the condition $d_\zeta = {d'}_\zeta$ for all ζ. As long as N is so large that $(a'/a)^N = 1$, then a solution $v \in (k_N \otimes_{\mathbf{F}_p} k)^\times$ exists (see the discussion at the beginning of §4 for more details). In terms of characters, this condition says exactly that the unramified factors of χ_0 and ${\chi'}_0$ should coincide on G_{E_N}, which is what we expect. This completes the proof.

■

Lemma 2.4.2. *When $\overline{\rho}$ is reducible, then e does not divide $p-1$. Consider $\mathcal{K}'$ of special type. There exists a choice of basis $\{e_1, e_2\}$ such that $\alpha = a\pi^i$ and $c_\zeta = 0$ for all $\zeta \in \mu_e$; this basis is unique up to scaling e_1 and e_2 by the same element of $k^\times$.*

Proof. We may assume that $\mathcal{K}'$ is of special type. Recall the Fundamental Relation from before,

$$\alpha(d_\zeta + \zeta\alpha^\zeta c_\zeta^{(p)} s\pi) = c_\zeta(p/\pi) + \zeta\alpha^\zeta d_\zeta^{(p)}. \tag{14}$$

Since $\overline{\rho}$ is reducible, $\alpha \neq 0$ and $e > 1$. If $e|(p-1)$, then $\kappa = \mathbf{F}_p(\zeta_e) = \mathbf{F}_p$, so $d_\zeta^{(p)} = d_\zeta$. Thus, $d_\zeta = \zeta^{i+1} d_\zeta$, so $\zeta^{i+1} = 1$ for all ζ. Since $0 \leq i \leq e-2$, this gives a contradiction if we take ζ to be a primitive eth root of unity. Thus, e can't divide $p-1$ in reducible cases.

If we can find a basis for which $c_\zeta = 0$ for all ζ, then it follows from (14) that for this basis, α has the desired form. We will show that

$$c_\zeta = t(d_\zeta - d_\zeta^{(p)})$$

for some $t \in k$. Replacing e_2 by $e_2 - te_1$ then gives the sought-after basis for which $c_\zeta = 0$ for all ζ. Using (7) and $c_{\zeta_1\zeta_2} = c_{\zeta_2\zeta_1}$, we see that for a primitive eth root of unity ζ_0 and any $\zeta \in \mu_e$,

$$c_\zeta = t(d_\zeta - d_\zeta^{(p)})$$

with $t = c_{\zeta_0}/(d_{\zeta_0} - d_{\zeta_0}^{(p)})$ (the denominator is a unit in $\kappa \otimes_{\mathbf{F}_p} k$ since $d_{\zeta_0} = \zeta_0^{i+1} d_{\zeta_0}^{(p)}$ and ζ_0 is a primitive eth root of unity).

Taking ζ to be another primitive eth root of unity, we see that the definition of t can be given using any choice of primitive eth root of unity. We now use this to see that $t \in \kappa \otimes_{\mathbf{F}_p} k$ actually lies in k. All we need to check is that $\sigma(t) = t$ for $\sigma \in \mathrm{Gal}(\kappa/\mathbf{F}_p)$. But by (6), $\sigma(c_\zeta) = c_{\zeta^\sigma}$ and similarly $\sigma(d_\zeta) = d_{\zeta^\sigma}$, $\sigma(d_\zeta^{(p)}) = d_{\zeta^\sigma}^{(p)}$, so $\sigma(t) = t$, using the primitive eth root of unity ζ^σ in place of ζ to define t.

The uniqueness of the basis $\{e_1, e_2\}$ follows from the transformation formula (12) for c_ζ (since $d_\zeta = \zeta^{i+1} d_\zeta^{(p)} \neq d_\zeta^{(p)}$ for ζ a primitive eth root of unity). ∎

We can now completely describe the reducible $\overline{\rho}$'s (the irreducible cases having been worked out earlier). Suppose $\mathcal{K}'$ is of special type. We have worked out conditions on Honda systems over A'; it remains to determine the possible descent data parameters d_ζ and to then compute the associated representations of D_p. Since we can write $\chi_1|_{I_p} = \omega^n|_{I_p}$ for a unique $n \in \mathbf{Z}/(p-1)$, we get upon restriction to $I_{K'}$ that $\psi_{1,K'}^{ne} = \psi_{1,K'}^{i+1}$, so the existence of $n \in \mathbf{Z}/(p-1)$ such that

$$ne \equiv i+1 \bmod p-1$$

is certainly a necessary condition on i. For such n, there exists a unique $r \in \mathbf{Z}/e$ such that

$$ne + r(p-1) \equiv i+1 \bmod e(p-1).$$

Define $\delta_\zeta = \zeta^r \otimes 1$ for $\zeta \in \mu_e$. It is easy to check that $\delta_\zeta = \zeta^{i+1}\delta_\zeta^{(p)}$ and $\zeta \to \delta_\zeta$ is a $\mathrm{Gal}(\kappa/\mathbf{F}_p)$-equivariant homomorphism from $\mu_e(\kappa)$ to $\mu_e(\kappa \otimes_{\mathbf{F}_p} k)$. Thus, the ratio $\Delta_\zeta = d_\zeta/\delta_\zeta$ is another such homomorphism, except it satisfies $\Delta_\zeta^{(p)} = \Delta_\zeta$, so in fact Δ_ζ takes values in $k \subseteq \kappa \otimes_{\mathbf{F}_p} k$. In other words, $d_\zeta = \zeta^{-r} \otimes x_\zeta$, with $\zeta \mapsto x_\zeta$ a homomorphism from $\mu_e(\kappa)$ to $k^\times$ satisfying $x_{\zeta^\sigma} = x_\zeta$ for all $\zeta \in \mu_e(\kappa)$ and $\sigma \in \mathrm{Gal}(\kappa/\mathbf{F}_p)$. That is, $x_{\zeta^p} = x_\zeta$ for all $\zeta \in \mu_e(\kappa)$. But $x_{\zeta^p} = x_\zeta^p$, so necessarily $x_\zeta \in \mathbf{F}_p^\times$, and bringing it across the tensor, we have

$$d_\zeta = \zeta^{r'} \otimes 1,$$

with $r' \in \mathbf{Z}/e$ satisfying $(p-1)r' \equiv i+1 \bmod e$.

We want to work out the relationship between r' and n. In fact, it will turn out that $r' = r$.

Lemma 2.4.3. *For $r \in \mathbf{Z}/e$ satisfying $r(p-1) \equiv i+1 \bmod e$, the descent data $d_\zeta = \zeta^r$ on the $\mathcal{A}'$ Honda system attached to $\chi_{-p/\pi^{i+1}}|_{G_{\mathcal{K}'}}$ gives rise to a descended character $\eta_v\omega^n : D_p \to \mathbf{F}_p^\times$, where $v \in \mathbf{F}_p^\times$ and $n \in \mathbf{Z}/(p-1)$ is the unique solution to*

$$ne + r(p-1) \equiv i+1 \bmod e(p-1).$$

Proof. Note that the existence and uniqueness of an $n \in \mathbf{Z}/(p-1)$ satisfying $ne + r(p-1) \equiv i+1 \bmod e(p-1)$ is clear, given that $r(p-1) \equiv i+1 \bmod e$. The d_ζ data does encode the descent of $\chi_{-p/\pi^{i+1}}$ to some character $\eta_v \omega^n : D_p \to k^\times$. In order to compute n, it is enough to restrict to I_p. If we identify I_p with the absolute Galois group of the completion E of $\mathbf{Q}_p^{\mathrm{un}}$, then the calculations in the proof of Theorem 2.4.1 go through with E in place of E_N there. This reduces us to a problem entirely over E.

More precisely, consider $n \in \mathbf{Z}/(p-1)$ the unique solution to $ne + r(p-1) \equiv i+1 \bmod e(p-1)$. The character $\omega^n : G_E \to \mathbf{F}_p^\times$ has the property that $\omega^n|_{G_{K'E}}$ is the generic fiber of a finite flat group scheme $\mathcal{G}_{/\mathcal{O}_{K'E}}$ with order p. This gives rise to a Honda system (L, M) over $\mathcal{O}_{K'E}$ with descent data down to $\mathcal{O}_E$. Since $\mu_e \simeq \mathrm{Gal}(K'E/E)$ and $M = \overline{\mathbf{F}}_p$ (with vanishing F and V operators), the descent data is determined by a group homomorphism $\mu_e \to \overline{\mathbf{F}}_p^\times$ given by $d_\zeta = \zeta^{r'}$ for some $r' \in \mathbf{Z}/e$. We need to show that $r' = r$.

Let $L = K'E$ and fix the lift of r to $\mathbf{Z}$ in the range $0 < r < e$ and then choose the lift $n \in \mathbf{Z}$ so that $ne + r(p-1) = i+1$ in $\mathbf{Z}$. By [16, Thm 3.4.1], the finite group scheme H over E with generic fiber representation $\omega^n|_{I_p}$ has affine E-algebra $E[X]/(X^p - p^n X)$ (with augmentation ideal generated by X). Thus, $\omega^n|_{G_L}$ is the generic fiber representation of a finite L-group scheme with affine L-algebra $L[X]/(X^p - p^n X) \simeq L[X]/(X^p - \pi^{ne} X) \simeq L[Y]/(Y^p - \pi^{i+1} Y)$, where $Y = \pi^{-r} X$. By [16, Prop 3.3.2], the unique finite flat $\mathcal{O}_L$-group scheme $\mathcal{G}$ with generic fiber $\omega^n|_{I_p}$ has affine $\mathcal{O}_L$-algebra $\mathcal{O}(\mathcal{G}) = \mathcal{O}_L[Y]/(Y^p - \pi^r Y)$.

For $\zeta \in \mu_e \simeq \mathrm{Gal}(L/E)$, consider the L-group scheme isomorphism

$$\mathcal{G}_{/L} \simeq \mathcal{G}_{/L} \times_L L$$

arising from using the base change $\zeta : L \to L$ and the fact that $\mathcal{G}_{/L} = H \times_E L$. By Raynaud's full faithfulness theorem, this isomorphism extends to a unique isomorphism of $\mathcal{O}_L$-group schemes $\mathcal{G} \simeq \mathcal{G} \times_{\mathcal{O}_L} \mathcal{O}_L$ (using $\zeta : \mathcal{O}_L \simeq \mathcal{O}_L$ as the base change). On the closed fiber, this becomes an $\overline{\mathbf{F}}_p$-group scheme isomorphism $\alpha_p \simeq \alpha_p$ which is induced on 'points' by multiplication by some $d_\zeta \in \overline{\mathbf{F}}_p^\times$ (look at the endomorphism ring of the Dieudonne module). It is this d_ζ which we must compute.

Since $Y = \pi^r X$, it follows from unwinding the above constructions that $Y \mapsto \zeta^r Y$ realizes the unique ζ-semilinear $\mathcal{O}_L$-algebra automorphism $\mathcal{O}(\mathcal{G}) \to \mathcal{O}(\mathcal{G})$ lifting $\mathcal{G}_{/L} \simeq \mathcal{G}_{/L} \times_L L$. On the level of the closed fiber group scheme $\mathrm{Spec}(\overline{\mathbf{F}}_p[Y]/Y^p)$, the induced map is given by $Y \mapsto \zeta^r Y$. In terms of the *definition* of the $\overline{\mathbf{F}}_p$-module structure on $\mathcal{M}(\mathcal{G}_{/\overline{\mathbf{F}}_p}) = \mathcal{M}(\alpha_{p/\overline{\mathbf{F}}_p})$, this translates into multiplication by $\zeta^r \in \overline{\mathbf{F}}_p$ on the Dieudonne module. Thus, $d_\zeta = \zeta^r$.

■

Now we can give the list of reducible $\overline{\rho}$ which arise. Before stating the precise result, it will be convenient to introduce some notation. Choose $v, w \in k^\times$, $n, m \in \mathbf{Z}/(p-1)$, and define $\chi_2 = \eta_v \omega^m$, $\chi_1 = \eta_w \omega^n$. Assume $\chi_2 \neq \chi_1, \omega\chi_1$ (i.e., $v \neq w$ or $m \neq n, n+1$), so $H^1(D_p, \chi_1^{-1}\chi_2)$ is a 1-dimensional k-vector space (by Tate duality). In this case, all non-zero elements in this space correspond to isomorphic $k[D_p]$-modules. Indeed, for any group H and any two *distinct* homomorphisms $\xi_1, \xi_2 : H \to L^\times$ to the multiplicative group of a field L, all isomorphic representations $\rho_1, \rho_2 : H \to \mathrm{GL}_2(L)$ which are non-trivial extensions of ξ_1 by ξ_2 fit into a commutative diagram

$$\begin{array}{ccccccc} 0 \to & \xi_2 & \to & \rho_1 & \to & \xi_1 & \to 0 \\ & a \downarrow & & \downarrow & & \downarrow b & \\ 0 \to & \xi_2 & \to & \rho_2 & \to & \xi_1 & \to 0 \end{array}$$

where the outer columns are multiplication by $a, b \in L^\times$. In other words, $\rho_2 \in \mathrm{Ext}^1_{L[H]}(\xi_1, \xi_2)$ is obtained from ρ_1 by mutliplication by ab^{-1}. Thus, the L-span of ρ_1 in this Ext^1-space consists of all the extensions which are isomorphic to ρ_1 as an $L[H]$-module. The same argument applies if we consider H a topological group and we work with $L[H]$-modules with the discrete topology with respect to which the action of H is continuous.

Thus, for $v \neq w$ or $m \neq n, n+1$ we can define $\overline{\rho}_{v,w,m,n}$ to be the unique (up to isomporphism) non-split $k[D_p]$-module which is an extension of χ_1 by χ_2. Recall that the reducible cases must have e not dividing $p-1$, and in particular $e > 2$.

Theorem 2.4.4. *For $p \equiv -1 \bmod 4$, the reducible possibilities for $\overline{\rho}$ are precisely the representations $\overline{\rho}_{v,w,m,n}$ with arbitrary $v, w \in k^\times$ and with $m, n \in \mathbf{Z}/(p-1)$ satisfying $en = i+1 \bmod p-1$ for some $0 \le i \le e-2$, $e|(i+1)(p+1)$, and $m = n+1-(i+1)(p+1)/e$ (these conditions always force $m \neq n$, and for $p \equiv -1 \bmod 4$ they force $m \neq n+1$ also).*

If $p \equiv 1 \bmod 4$, the reducible $\overline{\rho}$ which arise are the ones given by the above list of $\overline{\rho}_{v,w,m,n}$'s for $v \neq w$ or $m \neq n+1$, together with the unramified twists of a certain non-semisimple $\mathbf{F}_p$-representation of the form

$$\begin{pmatrix} \omega^{(p+1)/2} & * \\ 0 & \omega^{(p-1)/2} \end{pmatrix}$$

when $e = (p+1)/2$.

Proof. We may assume as usual that $\mathcal{K}'$ is of special type. Suppose we are given a reducible

$$\overline{\rho} \simeq \begin{pmatrix} \chi_2 & * \\ 0 & \chi_1 \end{pmatrix}$$

satisfying all of our group scheme conditions, and we introduce the parameters a, i, s, u_0, d_ζ as before. Writing $\chi_2|_{I_p} = \omega^m|_{I_p}$, $\chi_1|_{I_p} = \omega^n|_{I_p}$, Theorem 2.4.1 implies that $en = i+1 \bmod p-1$ (with $1 \le e-(i+1) \le e-1$). Our earlier descent computations demonstrated the necessity of the condition $e|(i+1)(p+1)$. Also, Lemma 2.4.3 implies that the descent data $d_\zeta = \zeta^r \otimes 1$ attached to χ_1 has $r \in \mathbf{Z}/e$ satisfying

$$ne + r(p-1) \equiv i+1 \bmod e(p-1).$$

Since χ_2 has descent data $d_\zeta^{(p)} = \zeta^{rp} \otimes 1$ and has 'α' parameter with the power π^{e-i-1}, we must have

$$me + pr(p-1) \equiv e-i-1 \bmod e(p-1).$$

Since $e|(i+1)(p+1)$, it readily follows that $m = n+1-(i+1)(p+1)/e$ in $\mathbf{Z}/(p-1)$.

Using $0 \le i \le e-2$ and $e \le p-1$, it is easy to check that $m, n \in \mathbf{Z}/(p-1)$ are distinct, and $m = n+1$ if and only $p \equiv 1 \bmod 4$, with $e = (p+1)/2$, $n = (p-1)/2$, $i = (p-3)/2$. The Honda system and descent data computations show that knowledge of either diagonal character determines the other character up to aribitrary unramified twisting and that knowledge of both characters determines the entire (nonsemisimple) representation of D_p. By varying $a, s \in k^\times$, we can freely change the 'unramified' factors of χ_1 and χ_2. In particular, when $m = n+1$ and $a = b$, our representation is an unramified k-twist of a certain non-semisimple extension of $\omega^{(p-1)/2}$ by $\omega^{(p+1)/2}$ over $\mathbf{F}_p$; since $\mathcal{O}_{\mathcal{K}'}$-flatness is insensitive to unramified twisting over $\mathbf{Q}_p$, this completes the proof that our list includes all possibilities.

To see that everything we list above really does arise, what we need to check is that if we are given v, w, m, n satisfying the list of conditions, then there is a $\overline{\rho}$ occuring which is an extension of $\eta_v\omega^m$ by $\eta_w\omega^n$. Define $a = v^{-1}$, $s = w(au_0)^{-1}$, $\alpha = a\pi^i$, $\beta = (asu_0)^{-1}\pi^{e-1-i}$. Also, define $d_\zeta = \zeta^r \otimes 1$, with $r \in \mathbf{Z}/e$ the unique solution to

$$ne + r(p-1) \equiv i+1 \bmod e(p-1)$$

(it is easy to check that such an r exists since $ne \equiv i+1 \bmod p-1$). This gives us a Honda system (L, M) over A' whose base change to $\mathcal{A}'$ is equipped with descent data down to $\mathbf{Z}_p$ which realizes a representation that is an extension of χ_1 by χ_2, where χ_1 and χ_2 are off from $\eta_v\omega^m$ and $\eta_w\omega^n$ by unramified characters. Changing a and s appropriately gives what we want. ■

3. Tangent Space Calculations

Until otherwise specified, throughout this section we assume that $\mathcal{K}'$ is of special type.

3.1. **Analysis of a Kernel.**

Let $M = \mathcal{M}(\overline{\rho}|_{G_{\mathcal{K}'}})$ and let $\mathcal{E}(M) \overset{\text{def}}{=} \text{Ext}^1_{k[F,V]}(M, M)$, where the ring $k[F, V]$ has F and V *commuting* with k. Using Galois descent on the closed fiber, we see that there is a natural map of sets

$$t_{F_{\mathcal{K}'}(\overline{\rho})} \to \mathcal{E}(M),$$

where the left side is the tangent space to the deformation functor $F_{\mathcal{K}'}(\overline{\rho}) = F_{\mathcal{K}',\mathcal{O}}(\overline{\rho})$. The *explicit* definition of the group structure and functoriality of Ext^1 for any (small) abelian category — that is, not the (compatible) definition using projective or injective resolutions, if that's also available — shows that this is actually a map of k-vector spaces. We introduce this map because $\mathcal{E}(M)$ looks easier to manage than the tangent space.

Definition 3.1.1. We say that $\overline{\rho}$ is *degenerate* if the group homomorphism

$$\zeta \mapsto d_\zeta^{-1} d_\zeta^{(p)} \in \mu_e(\kappa \otimes_{\mathbf{F}_p} k)$$

is either trivial or else does not have its image entirely inside of $\mu_e(\kappa)$. Otherwise, we say that $\overline{\rho}$ is *non-degenerate.*

The meaning of non-degeneracy is that for some $0 \le \ell \le e - 2$, $d_\zeta = \zeta^{\ell+1} d_\zeta^{(p)}$ for all ζ (in which case ℓ is unique). This always occurs in reducible cases. We will later see that in all degenerate cases, $d_\zeta = d_\zeta^{(p)}$ for all ζ.

Theorem 3.1.2. *The k-vector space $\mathcal{E}(M)$ is 2-dimensional. The natural map of k-vector spaces*

$$t_{F_{\mathcal{K}'}(\overline{\rho})} \to \mathcal{E}(M)$$

is injective *if we are in the degenerate case. There is a 1-dimensional kernel if we are in the non-degenerate case.*

Remark 3.1.3. The fact that Ext^1 admits a group structure in an explicit bifunctorial manner is absolutely critical to our argument and the importance of this fact cannot be overestimated. Also, by using $k[\epsilon]$-deformations of the form $\overline{\rho} \otimes_k (1 + \eta\epsilon)$ for $\eta : D_p \to k$ a continuous unramified *additive* character, we see that the tangent space is a priori at least 1-dimensional.

Proof. For any N' representing an element in $\mathcal{E}(M)$, we can write

$$N' = ke_1 \oplus ke_2 \oplus k\overline{e}_1 \oplus k\overline{e}_2$$

as a k-module, where the first two factors give the copy of M sitting inside N' and $\overline{e}_i$ projects onto e_i in the quotient M of N'. The remaining data (up to the non-canonical choice of k-linear section to $N' \twoheadrightarrow M$) is the action of F and V on N'. Since our extension sequence

$$0 \to M \to N' \to M \to 0$$

is compatible with these actions, we just need to specify $F(\overline{e}_i)$ and $V(\overline{e}_i)$ so that $FV = VF = 0$ on N' and $F(\overline{e}_i)$, $V(\overline{e}_i)$ lift $F(e_i)$, $V(e_i)$ respectively in the quotient $M \simeq N'/M$. We compute that $F(\overline{e}_1) = ae_1$, $F(\overline{e}_2) = be_1 - cse_2 + \overline{e}_1$, $V(\overline{e}_1) = ce_1$, and $V(\overline{e}_2) = de_1 - as^{-1}e_2 + s^{-1}\overline{e}_1$. If we make the change of basis

$$\overline{e}_1 \rightsquigarrow -ae_2 + \overline{e}_1, \quad \overline{e}_2 \rightsquigarrow -be_2 + \overline{e}_2,$$

we can suppose that $a = b = 0$ and with these constraints the values of c and d are unaffected by any further permissable change of the $\overline{e}_i$'s (i.e., $\overline{e}_1 \rightsquigarrow ue_1 + \overline{e}_1$, $\overline{e}_2 \rightsquigarrow ve_1 + ue_2 + \overline{e}_2$, $u, v \in k$). Thus, elements of $\mathcal{E}(M)$ are parameterized by $(c, d) \in k \times k$, so this Ext space has dimension 2 over k (and $(c, d) = (0, 0)$ corresponds to the trivial element).

We now must determine the kernel of $t_{F_{\mathcal{K}'}(\overline{\rho})} \to \mathcal{E}(M)$. We pick an element in the kernel and try to show it is the trivial element in $t_{F_{\mathcal{K}'}(\overline{\rho})}$. We will study this by carrying out a very explicit descent computation. We do not know of any more conceptual method that could be used instead.

Choose an object $(\lambda', \mathcal{N}')$ in the kernel, with descent data $\mathcal{D}$. By the usual Galois descent reasoning from $\mathcal{A}'$ down to A', we can suppose that this object is the base extension (from A' to $\mathcal{A}'$) of an object (Λ', N') in $\mathrm{Ext}^1_{\widetilde{PSH}^f_{A',W(k)}}((L,M),(L,M))$, so $N' = M \oplus M$ as a $k[F,V]$-module. In particular,

$$\mathcal{N}' = W(\kappa)\otimes_A N' = (\kappa\otimes_{\mathbf{F}_p} k)e_1 \oplus (\kappa\otimes_{\mathbf{F}_p} k)e_2 \oplus (\kappa\otimes_{\mathbf{F}_p} k)\overline{e}_1 \oplus (\kappa\otimes_{\mathbf{F}_p} k)\overline{e}_2$$

as $(\kappa\otimes_{\mathbf{F}_p} k)[F,V]$-modules and

$$N'_{A'} = M_{A'} \oplus M_{A'} = ((A'/p)\otimes_{\mathbf{F}_p} k)\epsilon_1 \oplus ((A'/p)\otimes_{\mathbf{F}_p} k)\epsilon_2 \oplus ((A'/p)\otimes_{\mathbf{F}_p} k)\overline{\epsilon}_1 \oplus ((A'/p)\otimes_{\mathbf{F}_p} k)\overline{\epsilon}_2$$

as $(A'/p)\otimes_{\mathbf{F}_p} k$-modules, with $\Lambda' \subseteq N'_{A'}$ of the form

$$\Lambda' = ((A'/p)\otimes_{\mathbf{F}_p} k)(\epsilon_1 + \alpha\epsilon_2) \oplus ((A'/p)\otimes_{\mathbf{F}_p} k)(\gamma\epsilon_2 + \overline{\epsilon}_1 + \alpha\overline{\epsilon}_2)$$

for some $\gamma \in (A'/p)\otimes_{\mathbf{F}_p} k$. We define ϵ_1, ϵ_2, $\overline{\epsilon}_1$, $\overline{\epsilon}_2$ to be the residue classes in $N'_{A'}$ of the respective elements $(1\otimes e_2, 0)$, $(0, p^{-1}\pi\otimes e_2)$, $(1\otimes\overline{e}_2, 0)$, $(0, p^{-1}\pi\otimes\overline{e}_2)$ (viewing $N'_{A'}$ as a quotient of $(A'\otimes_A N')\oplus(p^{-1}\mathfrak{m}\otimes_A N'^{(1)})$). Recall also that $\mathcal{A}'\otimes_{A'}(N'_{A'}) \simeq \mathcal{N}'_{\mathcal{A}'}$ compatibly with $\mathcal{A}'\otimes_{A'}\Lambda' \simeq \lambda'$ [2, Lemma 4.5].

For $\sigma \in \mathrm{Gal}(\mathcal{K}'/K') \simeq \mathrm{Gal}(\kappa/\mathbf{F}_p)$, the descent data $\mathcal{D}$ has σ acting on $\mathcal{N}'$ in the usual $\kappa\otimes_{\mathbf{F}_p} k$-semilinear manner ($k$-linear and fixing $e_1, e_2, \overline{e}_1, \overline{e}_2$). As for $\zeta \in \mathrm{Gal}(\mathcal{K}'/\mathbf{Q}_p(\zeta_e)) \simeq \mu_e$, $[\zeta] : \mathcal{N}' \to \mathcal{N}'$ is a map of $D_\kappa/p = \kappa[F,V]$-modules and k-modules, with κ-linearity holding because ζ has a trivial image in $\mathrm{Gal}(\kappa/\mathbf{F}_p)$. Also, $[\zeta_1]\circ[\zeta_2] = [\zeta_1\zeta_2]$, $[\sigma]\circ[\zeta] = [\zeta^\sigma]\circ[\sigma]$, and $[\zeta]_{\mathcal{A}'} : \mathcal{N}'_{\mathcal{A}'} \to \mathcal{N}'_{\mathcal{A}'}$ carries λ' back to itself. In addition, $[\zeta]$ must act in accordance with the descent data on $\mathcal{M} \subseteq \mathcal{N}'$ and on $\mathcal{M} \simeq \mathcal{N}'/\mathcal{M}$. With respect to the above ordered $\kappa\otimes_{\mathbf{F}_p} k$-basis $\{e_1, e_2, \overline{e}_1, \overline{e}_2\}$ of $\mathcal{N}'$, let's write the matrix for the $\kappa\otimes_{\mathbf{F}_p} k$-*linear* $[\zeta]$ as

$$[\zeta] = \begin{pmatrix} d_\zeta^{(p)} & 0 & x_\zeta & y_\zeta \\ 0 & d_\zeta & z_\zeta & w_\zeta \\ 0 & 0 & d_\zeta^{(p)} & 0 \\ 0 & 0 & 0 & d_\zeta \end{pmatrix}.$$

Since $\mathcal{N}' = \mathcal{M}\oplus\mathcal{M} \simeq W(\kappa)\otimes_A (M\oplus M)$ as $(\kappa\otimes_{\mathbf{F}_p} k)[F,V]$-modules, we can write down the explicit 'matrices' for the *semilinear* maps F and V on $\mathcal{N}'$. The condition that $[\zeta]$ commutes with F and V gives $x_\zeta = w_\zeta^{(p)} = w_\zeta^{(p^{-1})}$ and $z_\zeta = 0$. From $[\sigma]\circ[\zeta] = [\zeta^\sigma]\circ[\sigma]$ we get $\sigma(w_\zeta) = w_{\zeta^\sigma}$, $\sigma(y_\zeta) = y_{\zeta^\sigma}$, while $[\zeta_1]\circ[\zeta_2] = [\zeta_1\zeta_2]$ yields

$$w_{\zeta_1\zeta_2} = d_{\zeta_1}w_{\zeta_2} + d_{\zeta_2}w_{\zeta_1},\ \ y_{\zeta_1\zeta_2} = d_{\zeta_1}^{(p)}y_{\zeta_2} + d_{\zeta_2}y_{\zeta_1}. \tag{15}$$

In particular, $w_1 = 0$ and by induction it is easy to see that $w_{\zeta^n} = nd_\zeta^{n-1}w_\zeta$ for $n \geq 1$, so

$$0 = w_1 = w_{\zeta^e} = ed_\zeta^{e-1}w_\zeta.$$

This forces $w_\zeta = 0$, so $x_\zeta = 0$. It remains to consider $y_\zeta \in \kappa\otimes_{\mathbf{F}_p} k$ and $\gamma \in (A'/p)\otimes_{\mathbf{F}_p} k$.

A simple computation gives

$$[\zeta]_{\mathcal{A}'}(\epsilon_1) = d_\zeta\epsilon_1,\ \ [\zeta]_{\mathcal{A}'}(\epsilon_2) = \zeta d_\zeta^{(p)}\epsilon_2$$

(for the latter, recall the presence of $\mathcal{M}'^{(1)}$ in the definition of $\mathcal{M}'_{\mathcal{A}'}$) and

$$[\zeta]_{\mathcal{A}'}(\overline{\epsilon}_1) = y_\zeta(p/\pi)\epsilon_2 + d_\zeta\overline{\epsilon}_1,\ \ [\zeta]_{\mathcal{A}'}(\overline{\epsilon}_2) = s\zeta\pi y_\zeta^{(p)}\epsilon_1 + \zeta d_\zeta^{(p)}\overline{\epsilon}_2. \tag{16}$$

Thus, $[\zeta]_{\mathcal{A}'}(\gamma\epsilon_2 + \overline{\epsilon}_1 + \alpha\overline{\epsilon}_2) = \zeta s\pi\alpha^\zeta y_\zeta^{(p)}\epsilon_1 + (\zeta\gamma^\zeta d_\zeta^{(p)} + y_\zeta(p/\pi))\epsilon_2 + d_\zeta\overline{\epsilon}_1 + \zeta\alpha^\zeta d_\zeta^{(p)}\overline{\epsilon}_2$. In order for this to stay inside of

$$\lambda' = ((\mathcal{A}'/p)\otimes_{\mathbf{F}_p} k)(\epsilon_1 + \alpha\epsilon_2) \oplus ((\mathcal{A}'/p)\otimes_{\mathbf{F}_p} k)(\gamma\epsilon_2 + \overline{\epsilon}_1 + \alpha\overline{\epsilon}_2),$$

we see that the condition is

$$y_\zeta(p/\pi) = \gamma d_\zeta - \zeta\gamma^\zeta d_\zeta^{(p)} + \zeta\alpha\alpha^\zeta s\pi y_\zeta^{(p)} \tag{17}$$

in $(\mathcal{A}'/p)\otimes_{\mathbf{F}_p} k$ (recall that $\alpha^\zeta d_\zeta^{(p)} = \zeta^{i+1}d_\zeta^{(p)}a\pi^i = d_\zeta a\pi^i = d_\zeta\alpha$).

At this point, it is convenient to observe that what we have done do far does not depend on our choice of $k[F,V]$-module splitting. Below we will have to be a little more careful about which splitting we choose (in terms of trying to count possibilities up to equivalence), so we record here the possible splittings: they are

$$\overline{e}_1 \rightsquigarrow ue_1 + \overline{e}_1, \quad \overline{e}_2 \rightsquigarrow ve_1 + ue_2 + \overline{e}_2, \tag{18}$$

with $u, v \in k$. This has the effect

$$\overline{\epsilon}_1 \rightsquigarrow u\epsilon_1 + (p/\pi)v\epsilon_2 + \overline{\epsilon}_1, \quad \overline{\epsilon}_2 \rightsquigarrow s\pi v\epsilon_1 + u\epsilon_2 + \overline{\epsilon}_2$$

and hence

$$y_\zeta \rightsquigarrow y_\zeta + v(d_\zeta^{(p)} - d_\zeta), \quad \gamma \rightsquigarrow \gamma - (p/\pi)v + \alpha^2 s\pi v. \tag{19}$$

Under the $\kappa \otimes_{\mathbf{F}_p} k$-algebra isomorphism $(\mathcal{A}'/p) \otimes_{\mathbf{F}_p} k \simeq (\kappa \otimes_{\mathbf{F}_p} k)[\pi]/\pi^e$, we have

$$\gamma \mapsto g_0 + g_1\pi + \cdots + g_{e-1}\pi^{e-1}$$

for suitable $g_0, \ldots, g_{e-1} \in k$ ($g_i \in k$ because γ lies in $(A'/p) \otimes_{\mathbf{F}_p} k \subseteq (\mathcal{A}'/p) \otimes_{\mathbf{F}_p} k$).

First assume that if $\alpha \neq 0$, then $2(i+1) \neq e$ (we will come back to cases with $\alpha \neq 0$, $2(i+1) = e$ at the end; in terms of representation theory, these are the reducible cases in which the diagonal characters have the same restriction to $I_{\mathcal{K}'}$). The transformation law (19) for γ shows that if we make a change of splitting with $v = g_{e-1}u_0$ and take $u \in k$ to be whatever we wish, we can assume that $g_{e-1} = 0$. Note that if $\alpha \neq 0$ and $2(i+1) = e$, then this goes through as long as $a^2 su_0 \neq 1$. This will be used below.

With the vanishing of g_{e-1} fixed, any further change of splitting (governed just by $u \in k$) has no effect on our parameters y_ζ and γ. Since $g_{e-1} = 0$, and $2(i+1) \neq e$ if $\alpha \neq 0$ (so $\gamma = 0$ if $e = 1$), the condition (17) yields $y_\zeta = 0$ and thus for $0 \leq \ell \leq e-2$ (a vacuous condition when $e = 1$) that

$$g_\ell(d_\zeta - \zeta^{\ell+1}d_\zeta^{(p)}) = 0.$$

The non-degenerate case is precisely the condition that $\zeta \mapsto d_\zeta^{-1}d_\zeta^{(p)}$ is a non-trivial group map from μ_e to $\mu_e(\kappa)$, which is equivalent to the existence of some $0 \leq \ell \leq e-2$ such that $d_\zeta - \zeta^{\ell+1}d_\zeta^{(p)} = 0$ for all ζ (in which case ℓ is unique, and for $\alpha \neq 0$ we have $\ell = i$). Since $g_\ell \in k$ is a unit in $\kappa \otimes_{\mathbf{F}_p} k$ precisely when $g_\ell \neq 0$, we conclude that in the degenerate case $\gamma = 0$, so there is a splitting in $\widetilde{DPSH}^f_{\mathcal{A}',\mathcal{O}}$, giving the injectivity.

In the non-degenerate case, there is a unique ℓ_0 in the allowed range for which $g_{\ell_0} \in k$ could be non-zero (with $\ell_0 = i$ in cases where $\alpha \neq 0$). In other words, elements of the kernel of the map $t_{F_{\mathcal{K}'}(\overline{\rho})} \to \mathcal{E}(M)$ are parameterized by an element $g_{\ell_0} \in k$ which is independent of the choice of $k[F,V]$-module splitting chosen at the start. This implies that there is a 1-dimensional kernel.

Finally, there remain the (necessarily non-degenerate) cases in which $\alpha = a\pi^i \neq 0$ and $2(i+1) = e$. Since $2(i+1) = e$, $d_\zeta = \zeta^{i+1}d_\zeta^{(p)} = \zeta^{e/2}d_\zeta^{(p)}$. If ζ_0 is a primitive eth root of unity in κ, then d_{ζ_0} is a non-zero solution to $t^{(p)} = -t$ in $\kappa \otimes_{\mathbf{F}_p} k$. Let f denote the order of p in $(\mathbf{Z}/e)^\times$ (so $|\kappa| = p^f$).

We begin by checking that for $x \in k^\times$, the equation $t^{(p)} = xt$ has a non-zero solution in $\kappa \otimes_{\mathbf{F}_p} k$ if and only if $x^f = 1$, in which case the set of solutions is 1-dimensional over k and all non-zero solutions are units. It clearly suffices to check this statement with $\overline{k}$ in place of k. Pick an embedding of κ into $\overline{k}$, so we have a composite field κk. Under the canonical identification

$$\kappa \otimes_{\mathbf{F}_p} \overline{k} \simeq \prod_{j \in \mathbf{Z}/f} \kappa k,$$

if we write $t = (t_0, \ldots, t_{f-1})$ for an element, then $t^{(p)} = (t_1, \ldots, t_{f-1}, t_0)$. Thus, $t^{(p)} = xt$ if and only if $t_j = xt_{j-1}$ for all $j \in \mathbf{Z}/f$. From this, it is clear that a non-zero solution exists if and only if $x^f = 1$, in which case the set of solutions is the $\overline{k}$-span of $(1, x, \ldots, x^{f-1})$.

The existence of $d_{\zeta_0} \neq 0$ implies that $(-1)^f = 1$ in k, so f is even. Comparing coefficients of π^ℓ on both sides of (17) for $0 \leq \ell \leq e-2$ and using $2(i+1) = e$, we get

$$0 = g_\ell(d_\zeta - \zeta^{\ell+1}d_\zeta^{(p)}),$$

so $g_\ell = 0$ for $\ell \neq i, e-1$, with $i = e/2 - 1$. That is, we have

$$\gamma = g_i\pi^i + g_{e-1}\pi^{e-1}.$$

Plugging this into (17), we get

$$u_0^{-1}y_\zeta\pi^{e-1} = (\zeta^{e/2}y_\zeta^{(p)}a^2s + g_{e-1}(d_\zeta - d_\zeta^{(p)}))\pi^{e-1}.$$

Changing the lifts $\overline{e}_1, \overline{e}_2$ does *not* change g_i and gives rise to

$$g_{e-1} \rightsquigarrow g_{e-1} + v(-1 + a^2su_0), \quad y_\zeta \rightsquigarrow y_\zeta + v(d_\zeta^{(p)} - d_\zeta)$$

(where we may use the change of bases as in (18)).

Thus, when $a^2su_0 \neq 1$ we can change $\overline{e}_2$ so that $g_{e-1} = 0$, in which case $y_\zeta = (\zeta^{e/2}a^2su_0)y_\zeta^{(p)}$. Supppose instead that $a^2su_0 = 1$, so the value of g_{e-1} is 'intrinsic'. Let's show that necessarily $g_{e-1} = 0$ in these cases too. Choosing for ζ a primitive eth root of unity ζ_0 (so $\zeta_0^{e/2} = -1$) and dropping the ζ_0 subscripts, we get

$$y = -y^{(p)} + 2g_{e-1}u_0d,$$

so

$$y^{(p)} = -y + 2g_{e-1}u_0d.$$

If we iterate the equation for $y^{(p)}$, using $d^{(p)} = -d$, we get

$$y^{(p^m)} = (-1)^my + (-1)^{m+1}2mg_{e-1}u_0d$$

for all $m \geq 1$. Setting $m = f$ the equations $y^{(p^f)} = y$ and $(-1)^f = 1$ yield

$$0 = -2fg_{e-1}u_0d,$$

so $g_{e-1} = 0$ when $a^2su_0 = 1$. In terms of representation theory, the conditions $\alpha \neq 0$, $2(i+1) = e$ and $a^2su_0 = 1$ are equivalent to $\overline{\rho}$ being reducible with diagonal characters have the same restriction to $G_{K'}$.

Now that we have modified the basis so that $g_{e-1} = 0$, we have $\gamma = g_i\pi^i$ for $g_i \in k$ and

$$y_\zeta = \zeta^{e/2}a^2u_0sy_\zeta^{(p)},$$

$$\sigma(y_\zeta) = y_{\zeta^\sigma}, \quad y_{\zeta_1\zeta_2} = \zeta_1^{e/2}d_{\zeta_1}y_{\zeta_2} + d_{\zeta_2}y_{\zeta_1}. \tag{20}$$

We will now find a better basis in which $y_\zeta = 0$ for all ζ (in which case (14) ensures $g_{e-1} = 0$ with respect to this new basis too).

Consider the condition

$$y_{\zeta_0} = -a^2u_0sy_{\zeta_0}^{(p)},$$

with ζ_0 a fixed primitive eth root of unity. For any solution $y_{\zeta_0} \in \kappa \otimes_{\mathbf{F}_p} k$ to this equation, the remaining y_ζ are uniquely determined by (20) as

$$y_\zeta = (y_{\zeta_0}(2d_{\zeta_0})^{-1})(d_\zeta - d_\zeta^{(p)}).$$

The leading coefficient $t = y_{\zeta_0}(2d_{\zeta_0})^{-1}$ is the same for any choice of primitive eth root of unity ζ_0. Thus, for $\sigma \in \mathrm{Gal}(\kappa/\mathbf{F}_p)$ a Frobenius element, we compute

$$\sigma(t) = \frac{y_{\zeta_0^\sigma}}{2d_{\zeta_0^\sigma}} = \frac{y_{\zeta_0^p}}{2d_{\zeta_0^p}} = t,$$

so $t \in \kappa \otimes_{\mathbf{F}_p} k$ lies in k. Make the change $\overline{e}_2 \rightsquigarrow -te_1 + \overline{e}_2$ (and leave $\overline{e}_1$ alone). Using (19), this makes $y_\zeta = 0$ for all ζ and at worst affects γ by changing g_{e-1}. But as noted above, the vanishing of y_ζ for all ζ forces $g_{e-1} = 0$.

Thus, the elements of the kernel of $t_{F_{\mathcal{K}',W(k)}(\overline{\rho})} \to \mathcal{E}(M)$ are parameterized by $g_i \in k$, as before.

■

The above theorem shows that the determination of $\dim_k t_{F_{\mathcal{K}'}(\overline{\rho})}$ is reduced to determining the dimension of the image of $t_{F_{\mathcal{K}'}(\overline{\rho})}$ in $\mathcal{E}(M)$. In other words, we must choose a representative sequence

$$0 \to M \to N \to M \to 0$$

in $\mathcal{E}(M)$ and determine when we can construct an A'-submodule $\Lambda' \subseteq N'_{A'}$ fitting into an exact sequence

$$0 \to L' \to \Lambda' \to L' \to 0$$

compatible with $0 \to M_{A'} \to N'_{A'} \to M_{A'} \to 0$ in an obvious sense and such that for $\lambda' = \mathcal{A}' \otimes_{A'} \Lambda'$ and $\mathcal{N}' = W(\kappa) \otimes_A N'$, the pair $(\lambda', \mathcal{N}')$ in $\mathrm{Ext}^1_{\widetilde{PSH}^f_{A',\mathcal{O}}}((\mathcal{L},\mathcal{M}),(\mathcal{L},\mathcal{M}))$ admits descent data $\mathcal{D}$ compatible with $\mathcal{D}(\overline{\rho})$ on the two $(\mathcal{L},\mathcal{M})$'s. Our next task is to settle this issue. It will turn out that the image of $t_{F_{\mathcal{K}'}(\overline{\rho})}$ in the degenerate case, which is essentially the situation considered in [15] (for $e = 1$), is generally different from the image in the non-degenerate case. This will 'compensate' for the distinction between these cases in Theorem 3.1.2.

3.2. **Analysis of an Image.**

Theorem 3.2.1. *The natural map $t_{F_{\mathcal{K}'}(\overline{\rho})} \to \mathcal{E}(M)$ is surjective when $d_\zeta = d_\zeta^{(p)}$ for all ζ. Otherwise, t_F has a 1-dimensional image in $\mathcal{E}(M)$. In degenerate cases, $d_\zeta = d_\zeta^{(p)}$ must hold, so $\dim_k t_{F_{\mathcal{K}'}(\overline{\rho})} = 2$ in all cases.*

Proof. We will show that under the identification of sets $\mathcal{E}(M) \simeq k \times k$ described earlier, the image of t_F is precisely the set of pairs (c,d) with $c(d_\zeta - d_\zeta^{(p)}) = 0$ for all $\zeta \in \mu_e$. This immediately implies the theorem (with the image consisting of all pairs $(0,d)$ in the non-degenerate case). The only other issue is to explain why the degenerate cases must have $d_\zeta = d_\zeta^{(p)}$ for all ζ. Consider a degenerate $\overline{\rho}$, so $\overline{\rho}$ is irreducible. The determination of the image and kernel of $t_{F_{\mathcal{K}'}(\overline{\rho})} \to \mathcal{E}(M)$ shows that the cases we are trying to rule out are precisely the ones for which $\dim_k t_{F_{\mathcal{K}'}(\overline{\rho})} = 1$ would hold (such cases are *necessarily* degenerate, if they occur at all). This condition can be checked after making a base change on k. Since passing to an unramified twist of $\overline{\rho}$ over a finite extension of k is all we need to do in order to descend the field of definition of $\overline{\rho}$ to $\mathbf{F}_p$ (by Theorem 2.2.2), and this does not affect the dimension of the reduced cotangent space of the associated $\mathcal{O}_{\mathcal{K}'}$-flat deformation ring (by Lemma 1.2.1), we may assume $k = \mathbf{F}_p$. A degenerate case with $k = \mathbf{F}_p$ has to have $d_\zeta^{-1} d_\zeta^{(p)} = 1$ for all ζ!

Choose a representative N' of an element in $\mathcal{E}(M)$, so as we saw at the beginning of the proof of Theorem 3.1.2, we may write (using the same notation that was used there)

$$N' = ke_1 \oplus ke_2 \oplus k\overline{e}_1 \oplus k\overline{e}_2,$$

with $F(\overline{e}_1) = 0$, $F(\overline{e}_2) = -cse_2 + \overline{e}_1$, $V(\overline{e}_1) = ce_1$, $V(\overline{e}_2) = de_1 + s^{-1}\overline{e}_1$.

In order to derive the constraint to be in the image of $t_{F_{\mathcal{K}'}(\overline{\rho})}$, we essentially just have to repeat the calculation in the proof of Theorem 3.1.2, exercising a little more care because we don't necessarily have a split sequence of $k[F,V]$-modules anymore. We still can write

$$\mathcal{N}' = (\kappa \otimes_{\mathbf{F}_p} k)e_1 \oplus (\kappa \otimes_{\mathbf{F}_p} k)e_2 \oplus (\kappa \otimes_{\mathbf{F}_p} k)\overline{e}_1 \oplus (\kappa \otimes_{\mathbf{F}_p} k)\overline{e}_2$$

as a $\kappa \otimes_{\mathbf{F}_p} k$-module, with base-extended actions of F and V. Also, from the exactness of the A'-module sequence

$$0 \to M_{A'} \to N'_{A'} \to M_{A'} \to 0$$

we can still write (as an $(A'/p) \otimes_{\mathbf{F}_p} k$-module)

$$N'_{A'} = ((A'/p) \otimes_{\mathbf{F}_p} k)\epsilon_1 \oplus ((A'/p) \otimes_{\mathbf{F}_p} k)\epsilon_2 \oplus ((A'/p) \otimes_{\mathbf{F}_p} k)\overline{\epsilon}_1 \oplus ((A'/p) \otimes_{\mathbf{F}_p} k)\overline{\epsilon}_2.$$

We need to find a suitable $A' \otimes_A W(k)$-submodule $\Lambda' \subseteq N'_{A'}$ of the form

$$\Lambda' = ((A'/p) \otimes_{\mathbf{F}_p} k)(\epsilon_1 + \alpha\epsilon_2) \oplus ((A'/p) \otimes_{\mathbf{F}_p} k)(\gamma\epsilon_2 + \overline{\epsilon}_1 + \alpha\overline{\epsilon}_2)$$

for some $\gamma \in (A'/p) \otimes_{\mathbf{F}_p} k$ such that we can construct descent data $\mathcal{D}$ on $(\mathcal{A}' \otimes_{A'} \Lambda', \mathcal{N}')$ compatible with the descent data $\mathcal{D}(\overline{\rho})$ on $LM_{A'}(\overline{\rho})$, and with $[\sigma]$ acting as usual for $\sigma \in \mathrm{Gal}(\mathcal{K}'/K') \simeq \mathrm{Gal}(\kappa/\mathbf{F}_p)$.

Our problem is to determine what conditions (if any) are imposed on (c,d) in order for appropriate $\gamma \in (A'/p)\otimes_{\mathbf{F}_p} k$ and $\mathcal{D}$ to exist, where for $\mathcal{D}$ the issue is to define D_κ-linear isomorphisms $[\zeta] : \mathcal{N}' \to \mathcal{N}'$ compatible with $\mathcal{D}(\overline{\rho})$ and satisfying $[\zeta_1]\circ[\zeta_2] = [\zeta_1\zeta_2]$, $[\sigma]\circ[\zeta] = [\zeta^\sigma]\circ[\sigma]$, and with $[\zeta]_{\mathcal{A}'} : {\mathcal{N}'}_{\mathcal{A}'} \to {\mathcal{N}'}_{\mathcal{A}'}$ taking $\lambda' \stackrel{\rm def}{=} \mathcal{A}'\otimes_{A'}\Lambda'$ back to itself. We write a matrix for the hypothetical $[\zeta]$ as in the proof of Theorem 3.1.2. A simple *semilinear* matrix calculation shows that $[\zeta]$ commutes with the semilinear F and V if and only if $z_\zeta = 0$, $x_\zeta = w_\zeta^{(p)} = w_\zeta^{(p^{-1})}$, and $c(d_\zeta^{(p)} - d_\zeta) = 0$ (be careful to not confuse $d\in k$ and d_ζ when checking this calculation). It is critical to observe in this computation that $c, d\in k$ are unaffected by $\mathrm{Frob}\otimes 1$ on $\kappa\otimes_{\mathbf{F}_p} k$. As before, the conditions $[\sigma]\circ[\zeta] = [\zeta^\sigma]\circ[\sigma]$ and $[\zeta_1]\circ[\zeta_2] = [\zeta_1\zeta_2]$ amount to the usual conditions $\sigma(w_\zeta) = w_{\zeta^\sigma}$, $\sigma(y_\zeta) = y_{\zeta^\sigma}$, and the same formulas (15) for $w_{\zeta_1\zeta_2}$, $y_{\zeta_1\zeta_2}$ as before. Once again, we can conclude that necessarily $w_\zeta = 0$.

The formulas (16) for the $[\zeta]_{A'}(\overline{e}_j)$'s remain the same, as do the allowed changes in $\overline{e}_1$ and $\overline{e}_2$, so it is easy to check that the condition (17) carries over. Thus, taking all $y_\zeta = 0$ and $\gamma = 0$ demonstrates the sufficiency of the condition that $c(d_\zeta - d_\zeta^{(p)}) = 0$ for all ζ.

■

4. Deformation Rings

4.1. **Structure Theorems.**

We are now in a position to determine the structure of the $\mathcal{O}_{\mathcal{K}'}$-flat deformation ring of $\overline{\rho}$.

Theorem 4.1.1. *Let $\mathcal{K}'$ be a finite extension of $\mathbf{Q}_p$ inside of $\overline{\mathbf{Q}}_p$ with $e(\mathcal{K}'/\mathbf{Q}_p)\le p-1$ and let $\overline{\rho}: D_p \to \mathrm{GL}_2(k)$ be a continuous representation. Assume that $\overline{\rho}|_{G_{\mathcal{K}'}}$ is the generic fiber of a finite flat $\mathcal{A}'$-group scheme which is unipotent and connected. For $M = \mathcal{M}(\overline{\rho}|_{G_{\mathcal{K}'}})$, assume that the sequence of groups*

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

is exact. Then $R^{\rm univ}_{F_{\mathcal{K}'},\mathcal{O}}(\overline{\rho}) \simeq \mathcal{O}[\![T_1,T_2]\!]$.

Proof. Following Ramakrishna [15], we count the size of $(F_{\mathcal{K}'}(\overline{\rho}))(\mathcal{O}/\mathfrak{m}_\mathcal{O}^n)$ for $n\ge 1$. Since $\dim_k t_{F_{\mathcal{K}',\mathcal{O}}(\overline{\rho})} = 2$, the universal deformation ring is an $\mathcal{O}$-algebra quotient of $\mathcal{O}[\![T_1,T_2]\!]$ (say by a projection map Π). If we always get the maximal possible answer $|k|^{2(n-1)}$ of $\mathcal{O}/\mathfrak{m}_\mathcal{O}^n$-valued points, then any $f\in\mathcal{O}[\![T_1,T_2]\!]$ for which $\Pi(f)=0$ must satisfy $f(t_1,t_2)\in\mathfrak{m}_\mathcal{O}^n$ for all $t_1,t_2\in\mathfrak{m}_\mathcal{O}$, so $f=0$, as desired. We could use Lemma 1.2.1 to reduce the calculation to the case $\mathcal{O}=W(k)$. However, we want to show that the computation really can be done directly over any $\mathcal{O}$ without resorting to a technical trick.

By [2, Thm 4.3], we need to count the number of equivalence classes of certain triples $((\Lambda', {M'}_n), i, \mathcal{D})$ with ${M'}_n$ an $\mathcal{O}[F,V]$-module having underlying $\mathcal{O}$-module $\mathcal{O}/\mathfrak{m}_\mathcal{O}^n\times\mathcal{O}/\mathfrak{m}_\mathcal{O}^n$, $\Lambda'\subseteq({M'}_n)_{A'}$ an A'-submodule making $(\Lambda', {M'}_n)$ an object in $SH^f_{A',\mathcal{O}}$, $i : (\Lambda'[\mathfrak{m}_\mathcal{O}], {M'}_n[\mathfrak{m}_\mathcal{O}]) \simeq (L', M)$ an isomorphism in $\widetilde{PSH}^f_{A',\mathcal{O}}$, and $\mathcal{D}$ a descent data relative to $A\to\mathcal{A}'$ on $(\lambda', {\mathcal{M}'}_n)$ (with $\lambda' \stackrel{\rm def}{=} \mathcal{A}'\otimes_{A'}\Lambda'$, ${\mathcal{M}'}_n \stackrel{\rm def}{=} W(\kappa)\otimes_{\mathbf{Z}_p}{M'}_n$) such that $\mathcal{D}$ encodes for its $\mathrm{Gal}(\mathcal{K}'/K')$-action the descent from $(\lambda', {\mathcal{M}'}_n)$ down to $(\Lambda', {M'}_n)$. The extra condition we demand on the triples we consider is that the base-extended isomorphism $i' : (\lambda'[\mathfrak{m}_\mathcal{O}], {\mathcal{M}'}_n[\mathfrak{m}_\mathcal{O}]) \simeq (\mathcal{L},\mathcal{M})$ in $\widetilde{PSH}^f_{\mathcal{A}',\mathcal{O}}$ takes the induced data from $\mathcal{D}$ on the left side over to $\mathcal{D}(\overline{\rho})$ on the right side (i.e., i' is an isomorphism in $\widetilde{DPSH}^f_{\mathcal{A}',\mathcal{O}}$).

Note that the compatibility of i' with the action of $\mathrm{Gal}(\mathcal{K}'/K')$ is automatic, so we won't have to bother checking it when we trying to write down possibilities. The notion of equivalence among these triples is defined in the obvious manner. The tricky part is to check that what we write down is really a Honda system and not just a pre-Honda system. In order to handle cases with $\mathcal{O}\neq W(k)$, in which case p-torsion is not the same as $\mathfrak{m}_\mathcal{O}$-torsion, we will need to prove an analogue of the second half of [2, Thm 4.9], adapted to our particular setting.

We begin by working out the possibilities for the Dieudonne modules. Choose a uniformizer $\pi_{\mathcal{O}}$ of $\mathcal{O}$, so the multiplication-by-$\pi_{\mathcal{O}}$ on M'_n induces an isomorphism of $k[F,V]$-modules $M'_n/\mathfrak{m}_{\mathcal{O}} \simeq M'_n[\mathfrak{m}_{\mathcal{O}}] \simeq M$. Thus, we can pick an $\mathcal{O}/\mathfrak{m}_{\mathcal{O}}^n$-module basis $e_2, e_1 = Fe_2$ of M'_n so that $Fe_1 = be_1 + ce_2$ for some $b, c \in \mathfrak{m}_{\mathcal{O}}$ and $Ve_2 = ue_1 + de_2$ for some $d \in \mathfrak{m}_{\mathcal{O}}$ and $u \bmod \mathfrak{m}_{\mathcal{O}} = s^{-1}$ (of course, $Ve_1 = VFe_2 = pe_2$). The conditions $VF = FV = p$ force $c = pu^{-1}$ and $d = -bu$, so the possibilities for the Dieudonne module are given as follows: choose $b \in \mathfrak{m}_{\mathcal{O}}/\mathfrak{m}_{\mathcal{O}}^n$, $u \in \mathcal{O}/\mathfrak{m}_{\mathcal{O}}^n$ lifting $s^{-1} \in k^\times$ and define $M'_n = \mathcal{O}/\mathfrak{m}_{\mathcal{O}}^n \times \mathcal{O}/\mathfrak{m}_{\mathcal{O}}^n$ with $\mathcal{O}$-*linear*

$$F = \begin{pmatrix} b & 1 \\ pu^{-1} & 0 \end{pmatrix}, \quad V = \begin{pmatrix} 0 & u \\ p & -bu \end{pmatrix}$$

(matrices with respect to the standard ordered basis $\mathbf{e}_1 = (1,0)$, $\mathbf{e}_2 = (0,1)$ of M'_n over $\mathcal{O}/\mathfrak{m}_{\mathcal{O}}^n$). It is easy to check that M'_n is an $\mathcal{O}[F,V]$-module with $M'_n[\mathfrak{m}_{\mathcal{O}}] \simeq M$ as such. We next need to define the $(W(\kappa)\otimes_{\mathbf{Z}_p}\mathcal{O})/\mathfrak{m}_{\mathcal{O}}^n$-linear automorphisms

$$[\zeta] : \mathcal{M}'_n \simeq \mathcal{M}'_n$$

such that $[\zeta_1]\circ[\zeta_2] = [\zeta_1\zeta_2]$, $[\sigma]\circ[\zeta] = [\zeta^\sigma]\circ[\sigma]$. Also, $[\zeta]$ must commute with F and V.

In the quotient $A'\otimes_{\mathbf{Z}_p}\mathcal{O}$-module $(M'_n)_{A'}$, define ε_1 to be the element represented by

$$(1\otimes \mathbf{e}_2, 0) \in (A'\otimes_A M'_n) \oplus (p^{-1}\mathfrak{m}\otimes_A {M'}^{(1)}_n),$$

and define ε_2 to be the element represented by $(0, p^{-1}\pi\otimes\mathbf{e}_2)$. Just as in the tangent space analysis, it is easy to see that the natural map of $A'\otimes_{\mathbf{Z}_p}(\mathcal{O}/\mathfrak{m}_{\mathcal{O}}^n)$-modules

$$(A'\otimes_{\mathbf{Z}_p}(\mathcal{O}/\mathfrak{m}_{\mathcal{O}}^n))\varepsilon_1 \oplus (A'\otimes_{\mathbf{Z}_p}(\mathcal{O}/\mathfrak{m}_{\mathcal{O}}^n))\varepsilon_2 \to (M'_n)_{A'}$$

is surjective and hence (via length considerations) is an isomorphism.

Constructing $[\zeta]$ to be commute with F and V is a more serious constraint (and we postpone for now the definition of Λ'). We write

$$[\zeta] = \begin{pmatrix} x_\zeta & y_\zeta \\ z_\zeta & w_\zeta \end{pmatrix} \equiv \begin{pmatrix} d_\zeta^{(p)} & 0 \\ 0 & d_\zeta \end{pmatrix} \bmod \mathfrak{m}_{\mathcal{O}}(W(\kappa)\otimes_{\mathbf{Z}_p}\mathcal{O})$$

with entries in $W(\kappa)\otimes_{\mathbf{Z}_p}(\mathcal{O}/\mathfrak{m}_{\mathcal{O}}^n)$. The compatibility conditions with F and V give rise to the constraints $x_\zeta = by_\zeta^{(p)} + w_\zeta^{(p)}$, $z_\zeta = pu^{-1}y_\zeta^{(p)}$, and (dropping the ζ subscripts for simplicity)

$$b(y^{(p)} - y) = w^{(p^{-1})} - w^{(p)}, \tag{21}$$

$$b^2(y^{(p^2)} - y^{(p)}) = b(w^{(p)} - w^{(p^2)}) + pu^{-1}(y - y^{(p^2)}), \tag{22}$$

$$pu^{-1}(y^{(p)} - y^{(p^{-1})}) = b(w^{(p^{-1})} - w). \tag{23}$$

Using these last three equations, we compute

$$b(w^{(p^{-1})} - w^{(p)}) = b^2(y^{(p)} - y) = b(w - w^{(p)}) - b(w^{(p^{-1})} - w),$$

so $2bw^{(p^{-1})} = 2bw$. Since $p \neq 2$, we obtain $bw = bw^{(p)}$. If $b \in \mathcal{O}/\mathfrak{m}_{\mathcal{O}}^n$ is non-zero, then we get $w \equiv w^{(p)} \bmod \mathfrak{m}_{\mathcal{O}}$ by looking at the 'leading term' of b. But $w \bmod \mathfrak{m}_{\mathcal{O}} = d_\zeta$, so if there is some ζ such that $d_\zeta \neq d_\zeta^{(p)}$, then we must set $b = 0$, so

$$[\zeta] = \begin{pmatrix} w_\zeta^{(p)} & y_\zeta \\ pu^{-1}y_\zeta & w_\zeta \end{pmatrix},$$

with $y_\zeta \in \mathfrak{m}_{\mathcal{O}}(W(\kappa)\otimes_{\mathbf{Z}_p}\mathcal{O})$, $w_\zeta \equiv d_\zeta \bmod \mathfrak{m}_{\mathcal{O}}(W(\kappa)\otimes_{\mathbf{Z}_p}\mathcal{O})$, and $w_\zeta^{(p^2)} = w_\zeta$, $p(y_\zeta^{(p)} - y_\zeta) = 0$.

Assume for now that $d_\zeta \neq d_\zeta^{(p)}$ for some ζ, so $d_\zeta = \zeta^{i+1}d_\zeta^{(p)}$ for some $0 \le i \le e-2$ (we'll return to the other case later). In particular, $e > 1$ and $p \neq 2$. We claim that the $\mathcal{O}/\mathfrak{m}_{\mathcal{O}}^n$-basis of our original Dieudonne module can always be chosen so that all $y_\zeta = 0$ (and this is to be done without affecting things on $\mathfrak{m}_{\mathcal{O}}$-torsion). The equality $[\zeta_1][\zeta] = [\zeta][\zeta_1]$ yields

$$(w_{\zeta_1}^{(p)} - w_{\zeta_1})y_\zeta = y_{\zeta_1}(w_\zeta^{(p)} - w_\zeta).$$

Taking ζ_1 to be a primitive eth root of unity, we have

$$w_{\zeta_1}^{(p)} - w_{\zeta_1} \bmod \mathfrak{m}_{\mathcal{O}} = d_{\zeta_1}^{(p)} - d_{\zeta_1} = (\zeta^{-i-1} - 1)d_\zeta \in (\kappa \otimes_{\mathbf{F}_p} k)^\times,$$

so we may reciprocate to get

$$y_\zeta = q(w_\zeta^{(p)} - w_\zeta) \tag{24}$$

for a constant $q \in W(\kappa) \otimes_{\mathbf{Z}_p} (\mathcal{O}/\mathfrak{m}_{\mathcal{O}}^n)$; note that the definition for q can be given using *any* primitive eth root of unity. This will be important shortly.

Since $y_{\zeta_1} \equiv 0 \bmod \mathfrak{m}_{\mathcal{O}}$, we know q is divisible by $\pi_{\mathcal{O}}$. In fact, we claim that $q^{(p)} = q$, so $q \in 1 \otimes (\mathfrak{m}_{\mathcal{O}}/\mathfrak{m}_{\mathcal{O}}^n)$. In order to compute $q^{(p)}$, we take $\sigma \in \mathrm{Gal}(\kappa/\mathbf{F}_p)$ to be the Frobenius element and we use the relation $[\sigma][\zeta] = [\zeta^p][\sigma]$ in order to conclude that $y_\zeta^{(p)} = y_{\zeta^p}$ and $w_\zeta^{(p)} = w_{\zeta^p}$. Writing q_{ζ_1} to keep in mind the choice of primitive eth root of unity used to define q, we conclude that $q_{\zeta_1}^{(p)} = q_{\zeta_1^p}$. Using (24) with $\zeta = \zeta_1^p$, we see that $q^{(p)} = q$, as required.

Making the change of basis $e_1 \rightsquigarrow e_1$ and $e_2 \rightsquigarrow -qe_1 + e_2$ does not affect the form of the matrices for F and V (since $b = 0$) and has no affect mod $\mathfrak{m}_{\mathcal{O}}$ since $q \in \mathfrak{m}_{\mathcal{O}}/\mathfrak{m}_{\mathcal{O}}^n$. It is easy to compute that after this change of basis, $y_\zeta = 0$ for all ζ. Since $[\zeta]^e = 1$, we are forced to use the definition

$$[\zeta] = \begin{pmatrix} \delta_\zeta^{(p)} & 0 \\ 0 & \delta_\zeta \end{pmatrix}, \tag{25}$$

where $\delta_\zeta \in W(\kappa) \otimes_{\mathbf{Z}_p} (\mathcal{O}/\mathfrak{m}_{\mathcal{O}}^n)$ is the Teichmüller lift of $d_\zeta \in (\kappa \otimes_{\mathbf{F}_p} k)^\times$.

Since $\dim_k t_{F_{\mathcal{K}',\mathcal{O}}(\overline{\rho})} = 2$, we want to find an extra parameter in addition to u. If $\alpha \neq 0$, then i also satisfies $\alpha = a\pi^i$ in $(A'/p) \otimes_{\mathbf{F}_p} k$, with $a \in k^\times$. Define $a = 0$ if $\alpha = 0$; for any value of α, define $\widehat{a} \in \mathcal{O}$ to be the Teichmüller lift of $a \in k$. By suitable unit scaling and the fact that our Honda system must have its $\mathfrak{m}_{\mathcal{O}}$-torsion isomorphic to its quotient by $\mathfrak{m}_{\mathcal{O}}$ via mutliplication by $\pi_{\mathcal{O}}^{n-1}$, we have to have

$$\Lambda' = (A' \otimes_A (\mathcal{O}/\mathfrak{m}_{\mathcal{O}}^n))(\varepsilon_1 + \alpha_n \varepsilon_2),$$

where $\alpha_n \bmod \mathfrak{m}_{\mathcal{O}} = \alpha$. There is an obvious isomorphism $(\Lambda'[\mathfrak{m}_{\mathcal{O}}], M'_n[\mathfrak{m}_{\mathcal{O}}]) \simeq (L, M)$ in $\widetilde{PSH}^f_{A',\mathcal{O}}$. It will be checked at the end that (Λ', M'_n) lies in $SH^f_{A'}$. The condition on α_n which ensures stability of λ' under $[\zeta]_{\mathcal{A}'}$ is

$$\alpha_n^\zeta = \zeta^i \alpha_n.$$

In other words, we need to have

$$\alpha_n = \widehat{a}\pi^i + a_1\pi_{\mathcal{O}}\pi^i + \cdots + a_{n-1}\pi_{\mathcal{O}}^{n-1}\pi^i,$$

with $a_i \in \mathcal{O}$ Teichmüller lifts of arbitrary elements of k. This gives us $|k|^{n-1}$ different definitions of α_n, so together with the choices of u, we have $|k|^{2(n-1)}$ objects, and these are the *only* possibilities.

Let's check these are mutually non-isomorphic. We will show that there are no isomorphisms, even ignoring the descent data compatibility (actually, one case will require special care, as we will see). We proceed by induction on n, the case $n = 1$ being trivial. Choose two pairs $(u^{(1)}, \alpha_n^{(1)})$ and $(u^{(2)}, \alpha_n^{(2)})$ and an isomorphism φ between the corresponding objects. By induction, we have $u^{(1)} \equiv u^{(2)} \bmod \mathfrak{m}_{\mathcal{O}}^{n-1}$ and $\alpha_n^{(1)} \equiv \alpha_n^{(2)} \bmod \mathfrak{m}_{\mathcal{O}}^{n-1}$. Thus, $\varphi \bmod \mathfrak{m}_{\mathcal{O}}^{n-1}$ can be viewed as an endomorphism of a representation $D_p \to \mathrm{GL}_2(\mathcal{O}/\mathfrak{m}_{\mathcal{O}}^n)$ whose residual form $\overline{\rho}$ has trivial centralizer. It is not hard to show that for any local artin ring B and any group H, any group homomorphism $\rho : H \to \mathrm{GL}_N(B)$ which has trivial residual centralizer must itself have trivial centralizer (induct on the length of the ring B, with the group H fixed). Thus, we can scale φ by a unit in $(\mathcal{O}/\mathfrak{m}_{\mathcal{O}}^n)^\times$ so that its matrix is the identity mod $\mathfrak{m}_{\mathcal{O}}^{n-1}$. More precisely, we have

$$\varphi(\mathbf{e}_1^{(1)}) = r\mathbf{e}_1^{(2)} + t\mathbf{e}_2^{(2)}, \quad \varphi(\mathbf{e}_2^{(1)}) = v\mathbf{e}_1^{(2)} + w\mathbf{e}_2^{(2)},$$

where $r \equiv w \equiv 1 \bmod \mathfrak{m}_{\mathcal{O}}^{n-1}$, $t \equiv v \equiv 0 \bmod \mathfrak{m}_{\mathcal{O}}^{n-1}$. The condition that φ takes $\Lambda'^{(1)}$ isomorphically over to $\Lambda'^{(2)}$ is that

$$\alpha_n^{(2)}(w + \alpha_n^{(1)}\pi v(u^{(1)})^{-1}) = vp/\pi + \alpha_n^{(1)}w.$$

If $v = 0$, then $\alpha_n^{(2)}w = \alpha_n^{(1)}w$, so $\alpha_n^{(1)} = \alpha_n^{(2)}$. Moreover, compatibility of φ with F and V yields $r = w$ and $ru^{(1)} = wu^{(2)}$, so $u^{(1)} = u^{(2)}$. Now suppose $v \neq 0$, so $v = v_0\pi_{\mathcal{O}}^{n-1}$ for $v_0 \in (\mathcal{O}/\mathfrak{m}_{\mathcal{O}}^n)^\times$. Writing $w = 1+w_0\pi_{\mathcal{O}}^{n-1}$, we obtain

$$\alpha_n^{(1)} - \alpha_n^{(2)} = v_0((p/\pi) \otimes \pi_{\mathcal{O}}^{n-1} - \widehat{a}^2(u^{(1)})^{-1}\pi^{2i+1} \otimes \pi_{\mathcal{O}}^{n-1}).$$

Since every term on the left side lies in $\pi^i \otimes \mathcal{O}$, with some $0 \leq i \leq e-2$, we must have (since v_0 is a unit) $\widehat{a} \neq 0$, $2i+1 = e-1$, $\alpha_n^{(1)} = \alpha_n^{(2)}$, and $0 = u_0^{-1} - a^2 s$ in k, which is to say $a^2 s u_0 = 1$. These conditions say exactly that $\overline{\rho}$ is reducible with diagonal characters coinciding on $G_{K'}$. Thus, as long as K' can be chosen in the reducible cases so that the diagonal characters χ_1 and χ_2 of $\overline{\rho}$ are distinct on $G_{K'}$, it follows that we have exactly $|k|^{2(n-1)}$ distinct $\mathcal{O}/\mathfrak{m}_{\mathcal{O}}^n$-valued points in the non-degenerate cases (granting that the pre-Honda systems we defined above really are Honda systems). In order to show that such K' can be chosen in the reducible cases, recall that $\chi_1 \neq \chi_2$. We need to check that if $\chi = \chi_1\chi_2^{-1} : D_p \to k^\times$ is non-trivial, then there exists a totally ramified degree e extension $K'/\mathbf{Q}_p$ inside of $\overline{\mathbf{Q}}_p$ so that $\chi|_{G_{K'}} \neq 1$. It is enough to check that the intersection of all such fields K' is $\mathbf{Q}_p$. This is an easy exercise.

Postponing the Honda system check, let's consider the degenerate cases with $d_\zeta = d_\zeta^{(p)}$ for all ζ. We must have $\alpha = 0$ in these cases. Since it suffices to find $|k|^{2(n-1)}$ distinct $\mathcal{O}/\mathfrak{m}_{\mathcal{O}}^n$-valued points of the deformation functor, simply *define* $[\zeta]$ as before, and fortunately we will get enough points with this condition. Note that even though we now allow for the possibility that $b \neq 0$ as a Dieudonne module parameter, $[\zeta]$ commutes with F and V because $d_\zeta = d_\zeta^{(p)}$ for all ζ!

Define $\Lambda' = (A' \otimes_{\mathbf{Z}_p} (\mathcal{O}/\mathfrak{m}_{\mathcal{O}}^n))(\varepsilon_1)$. We have in an obvious manner $i : (\Lambda'[\mathfrak{m}_{\mathcal{O}}], M'_n[\mathfrak{m}_{\mathcal{O}}]) \simeq (L, M)$ in $\widetilde{PSH}^f_{A',\mathcal{O}}$. We will check at the very end of the proof that (Λ', M'_n) lies in $SH^f_{A'}$. It is easy to check that $[\zeta]_{\mathcal{A}'}$ carries $\lambda' = \mathcal{A}' \otimes_{A'} \Lambda'$ back to itself and so we clearly have a triple $((\Lambda', M'_n), i, \mathcal{D})$ of the desired sort (note that we have omitted b and u from the notation, but this should not cause confusion). There are $|k|^{2(n-1)}$ of these triples, for the different values of b and u.

We claim that the objects $((\lambda', \mathcal{M}'_n), \mathcal{D})$ are pairwise non-isomorphic in $DPSH^f_{A'}$ (this is slightly stronger than we need, since we aren't even requring the isomorphisms to satisfy a compatibility on the p-torsion parts). Suppose for two pairs (b, u) and (b', u'), we have an isomorphism φ between the corresponding objects. We write the action on the Dieudonne modules as

$$\varphi(\mathbf{e}_1) = r\mathbf{e}'_1 + t\mathbf{e}'_2, \;\; \varphi(\mathbf{e}_2) = v\mathbf{e}'_1 + w\mathbf{e}'_2,$$

with $r, t, v, w \in \mathcal{O}/\mathfrak{m}_{\mathcal{O}}^n$. One computes

$$\varphi(\varepsilon_1) = w\varepsilon'_1 + v(p/\pi)\varepsilon'_2, \;\; \varphi(\varepsilon_2) = \pi v u^{-1}\varepsilon'_1 + (w + vb)\varepsilon'_2.$$

The condition that $\varphi(\varepsilon_1) = (\text{unit})\varepsilon'_1$ implies that w must be a unit and $vp/\pi = 0$ in $A' \otimes_{\mathbf{Z}_p} (\mathcal{O}/\mathfrak{m}_{\mathcal{O}}^n)$, so $v = 0$ (treat $e = 1$ and $e > 1$ separately). Thus, $vp = vb = vb' = 0$, and w is a unit. The commutativity of φ with F, V allows us to solve $r = b'v + w = w$, $t = vpu^{-1} = 0$, and then $br = rb'$, $ur = wu'$. Since $r = w$ is a unit, we get $b = b'$, $u = u'$, as desired.

As a 'double check' on our work, let's show directly that if we tried to use the parameter α_n in the cases with $d_\zeta \equiv d_\zeta^{(p)}$, we would not get $|k|^{3(n-1)}$ distinct $\mathcal{O}/\mathfrak{m}_{\mathcal{O}}^n$-valued points (coming from b, u, α_n). In fact, in this case the condition on α_n is $\alpha_n^\zeta = \zeta^{-1}\alpha_n$, which is to say $\alpha_n = -v_n p/\pi$ for some $v_n \in \mathcal{O}/\mathfrak{m}_{\mathcal{O}}^n$. The matrix

$$\begin{pmatrix} v_n b + 1 & v_n \\ v_n p u^{-1} & 1 \end{pmatrix}$$

gives an isomorphism between the objects attached to the data (b, u, α_n) and $(b, u, 0)$.

Finally, we have to verify that the pre-Honda systems we wrote down above are in fact Honda systems. We prove the general claim that if (L, M) is an object in $PSH^f_{A',\mathcal{O}}$ (with $L \to M_{A'}$ injective) for which $M \simeq (\mathcal{O}/\mathfrak{m}_{\mathcal{O}}^n)^{\oplus r}$ as an $\mathcal{O}$-module, $L \subseteq M_{A'}$ is an $\mathcal{O}$-module direct summand, and the $\mathfrak{m}_{\mathcal{O}}$-torsion pair

$(L[\mathfrak{m}_{\mathcal{O}}], M[\mathfrak{m}_{\mathcal{O}}])$ lies in $SH^f_{A',\mathcal{O}}$, then (L, M) is necessarily a Honda system over A'. Note that the exactness of the functor $N \rightsquigarrow N_{A'}$ on D_k-modules with finite $W(k)$-length [2, Lemma 2.2] gives rise to a natural injection of $A' \otimes_{\mathbf{Z}_p} \mathcal{O}$-modules

$$L[\mathfrak{m}_{\mathcal{O}}] \hookrightarrow (M_{A'})[\mathfrak{m}_{\mathcal{O}}] \simeq (M[\mathfrak{m}_{\mathcal{O}}])_{A'}$$

which is implicit in our consideration of the pair $(L[\mathfrak{m}_{\mathcal{O}}], M[\mathfrak{m}_{\mathcal{O}}])$ as an object in $PSH^f_{A',\mathcal{O}}$.

We prove our claim by induction on n, the case $n = 1$ being trivial. By induction, we know that the pair $(L[\mathfrak{m}^{n-1}_{\mathcal{O}}], M[\mathfrak{m}^{n-1}_{\mathcal{O}}])$ in $PSH^f_{A',\mathcal{O}}$ lies in $SH^f_{A',\mathcal{O}}$. Due to the $\mathcal{O}$-module structure of M and the direct summand hypothesis on L, we can use multiplication by $\pi_{\mathcal{O}}$ to get the following commutative diagram with *exact* rows and injective columns

$$\begin{array}{ccccccc} 0 \to & L[\mathfrak{m}_{\mathcal{O}}] & \to & L & \to & L[\mathfrak{m}^{n-1}_{\mathcal{O}}] & \to 0 \\ & \downarrow & & \downarrow & & \downarrow & \\ 0 \to & (M[\mathfrak{m}_{\mathcal{O}}])_{A'} & \to & M_{A'} & \to & (M[\mathfrak{m}^{n-1}_{\mathcal{O}}])_{A'} & \to 0 \end{array}$$

Consider the natural $\kappa \otimes_{\mathbf{F}_p} k$-linear map $\xi : L/\mathfrak{m} \to \operatorname{coker} \mathcal{F}_M$. The maps ξ', ξ'' for $(L[\mathfrak{m}_{\mathcal{O}}], M[\mathfrak{m}_{\mathcal{O}}])$ and $(L[\mathfrak{m}^{n-1}_{\mathcal{O}}], M[\mathfrak{m}^{n-1}_{\mathcal{O}}])$ are isomorphisms, due to the Honda system property. The above commutative diagram therefore gives a commutative diagram with right exact rows and columns ξ', ξ, ξ''. Therefore, ξ is at least a surjection. Proceeding similarly with a left exact argument and recalling the definition of $\mathcal{V}_M$, the natural $\kappa \otimes_{\mathbf{F}_p} k$-linear map $j : L[\mathfrak{m}] \oplus \ker \mathcal{V}_M \to M_{A'}[\mathfrak{m}]$ is an injection.

We need to show that the injection j is surjective and that the surjection ξ is injective. This will be accomplished by an A'-length computation. Since ξ is surjective, [2, Lemma 2.4] implies that $\ell_{A'}(L/\mathfrak{m}) \geq \ell_{\mathbf{F}_p}(\ker F)$, with equality if and only if ξ is an isomorphism. Note that this can be reformulated as

$$\ell_{A'}(L[\mathfrak{m}]) \geq \ell_{\mathbf{F}_p}(\ker F).$$

Since j is injective, using [2, Lemma 2.4, Lemma 2.7] it follows that

$$\ell_{A'}(L[\mathfrak{m}]) + \ell_{\mathbf{F}_p}(\ker V) \leq \ell_{\mathbf{F}_p}(\ker V) + \ell_{\mathbf{F}_p}(\ker F)$$

with equality if and only if j is an isomorphism. To be precise, when $e = 1$ (so $\mathfrak{m}$-torsion is p-torsion) we should replace the reference to [2, Lemma 2.7] with a reference to the proof of [2, Thm 1.1], where the exactness hypothesis on our Diedonne module M is shown to automatically always hold, and in particular that

$$\ell_{\mathbf{F}_p}(M[p]) = \ell_{\mathbf{F}_p}(M/pM) = \ell_{\mathbf{F}_p}(M/FM) + \ell_{\mathbf{F}_p}(M/VM) = \ell_{\mathbf{F}_p}(\ker F) + \ell_{\mathbf{F}_p}(\ker V).$$

Combining our inequalities, we see equalities are forced and so ξ and j are isomorphisms. This shows that (L, M) is a Honda system over A'.

■

We can now prove a result about determinants of deformations. The most important ingredient in our proof is Fontaine's theorem on the 'B-admissability' of p-adic representations coming from p-divisible groups [9, Thm 6.2]. The background (and notation) upon which Fontaine's theorem rests is quite substantial, and for reasons of space we cannot review it here. Thus, in the proof we will have to assume a familiarity with [9], as well as [7] (we have tried to give precise references for exactly what we need, and hopefully this will be somewhat helpful to the interested reader).

Theorem 4.1.2. (*i*) *If* $\overline{\rho}^{\text{univ}}$ *denotes the universal deformation, then*

$$\det \overline{\rho}^{\text{univ}}|_{I_{\mathcal{K}'}} = \epsilon|_{I_{\mathcal{K}'}}.$$

(*ii*) *If* $\chi : D_p \to \mathcal{O}^\times$ *is a continuous character with* $\chi|_{I_{\mathcal{K}'}} = \epsilon|_{I_{\mathcal{K}'}}$ *and* $\chi \bmod \mathfrak{m}_{\mathcal{O}} = \det \overline{\rho}$, *let* F_χ *denote the subfunctor of* $F_{\mathcal{K}',\mathcal{O}}(\overline{\rho})$ *given by the extra constraint that the determinant of a deformation coincides with* χ (*in the evident sense*). *Then* F_χ *is representable, with universal deformation ring isomorphic to* $\mathcal{O}[\![T]\!]$.

Proof. First we assume (*i*) and use it to deduce (*ii*). At least 1 dimension of $t_{F_{\mathcal{K}',\mathcal{O}}(\overline{\rho})}$ is filled up by $k[\epsilon]$-deformations of the form $\overline{\rho} \otimes_k (1 + \eta\epsilon)$, with additive continuous unramified characters $\eta : D_p \to k$ (see Remark 3.1.3). Clearly F_χ is representable, and it follows that F_χ has a tangent space with dimension at most $\dim_k t_{F_{\mathcal{K}',\mathcal{O}}(\overline{\rho})} - 1$ over k. Thus, R_{F_χ} is a quotient of a formal power series ring over $\mathcal{O}$ in $\dim_k t_{F_{\mathcal{K}',\mathcal{O}}(\overline{\rho})} - 1$

variables. If we can show that $\dim R_{F_\chi} \geq \dim_k t_{F_{\mathcal{K}',\mathcal{O}}(\overline{\rho})}$, then it follows from dimension theory that R_{F_χ} is a formal power series ring over $\mathcal{O}$ in $\dim_k t_{F_{\mathcal{K}',\mathcal{O}}(\overline{\rho})} - 1$ variables, as desired. Since χ and $\det \overline{\rho}^{\mathrm{univ}}$ coincide on I_p by (i), upon choosing $\mathrm{Frob}_p \in D_p$ which represents Frobenius in D_p/I_p we have

$$R_{F_\chi} \simeq R_{F_{\mathcal{K}',\mathcal{O}}}/(r),$$

with $r = \det \overline{\rho}^{\mathrm{univ}}(\mathrm{Frob}_p) - \chi(\mathrm{Frob}_p)$. But a quotient of the formal power series ring $R_{F_{\mathcal{K}',\mathcal{O}}}$ by a proper principal ideal has dimension at least $\dim R_{F_{\mathcal{K}',\mathcal{O}}} - 1 = \dim_k t_{F_{\mathcal{K}',\mathcal{O}}(\overline{\rho})}$. This finishes the proof of (ii).

Now we prove (i). Since $[I_p : I_{\mathcal{K}'}] = e$ is relatively prime to p, $\epsilon^{-1}\chi$ is the product of an unramified character and the Teichmüller lift of $\omega^{-1} \det \overline{\rho}$. Replacing χ by an unramified twist without loss of generality, we can assume that χ takes values in $W(k)^\times$. By [3, Thm 1.2] we may (and do) assume that $\mathcal{O} = W(k)$, a finite étale extension of $\mathbf{Z}_p$. This will be important later.

Since the universal flat deformation ring is a formal power series ring over $\mathcal{O}$ in $d = 2$ variables, it suffices to show that for all $\mathcal{O}$-valued points, the corresponding 'specialization'

$$\rho : D_p \to \mathrm{GL}_2(\mathcal{O})$$

satisfies $\det \rho|_{I_{\mathcal{K}'}} = \epsilon|_{I_{\mathcal{K}'}}$. The desired result then follows from basic non-archimedean analysis (i.e., if $f, g \in \mathcal{O}[\![T_1, \dots, T_d]\!]$ satisfy $f(t_1, \dots, t_d) = g(t_1, \dots, t_d)$ for all $t_j \in \mathfrak{m}_{\mathcal{O}}$, then $f = g$). Observe how essential the structure of the deformation ring is for this argument.

Without loss of generality, we can assume $\mathcal{K}'$ is of special type. We know that $\rho|_{G_{K'}}$ is the generic fiber of a p-divisible group Γ_ρ over A'. Since $\overline{\rho}|_{G_{K'}}$ and its Cartier dual are the generic fibers of connected unipotent finite flat A'-group schemes, both Γ_ρ and the dual p-divisible group $\widehat{\Gamma}_\rho$ are not étale (look at p-torsion). It is enough to prove that if $\Gamma_{/A'}$ is a p-divisible group for which Γ and $\widehat{\Gamma}$ are not étale and for which the generic fiber representation ρ of Γ has the structure of a rank two $\mathcal{O}$-module, then $\det \rho|_{I_{K'}} = \epsilon|_{I_{K'}}$. Here, we are computing the determinant relative to the $\mathcal{O}$-module structure.

Since it seems likely that there are reducible $\overline{\rho}$ which do not admit an unramified $\overline{k}$-twist having field of definition $\mathbf{F}_p$, it does not seem that we can reduce to the case $\mathcal{O} = \mathbf{Z}_p$. Thus, our analysis of the generic fiber determinant is not a formal consequence of Raynaud's work [16, Prop 4.3.1]. In order to handle the additional module structure on the generic fiber, we instead need to use Fontaine's work on p-divisible groups [9] (and the arguments we give allow one to recover [16, Prop 4.3.1] for discrete valuation rings having characteristic 0 and an algebraically closed residue field with characteristic p).

In order to clarify ideas, we consider a much more general situation. It will be clear that the above situation is included as a special case. To avoid conflicting with the notation in [7], we now abandon our previous conventions about k, K', etc. (this will cause no confusion because we will not be referring back to the above setting again). The new notation is as follows. Let K' be *any* characteristic 0 field complete with respect to a non-trivial discrete valuation, and with a valuation ring A' whose residue field k is perfect with characteristic p. We let $A = W(k)$ and K denote the fraction field of A. Denote by $\mathbf{C}_{K'}$ the completion of an algebraic closure of K'. Let Γ be a p-divisible group over A' such that neither Γ nor the Cartier dual $\widehat{\Gamma}$ is étale. Let $\mathcal{K}$ denote a finite extension of $\mathbf{Q}_p$ with valuation ring $\mathcal{O}$, and suppose that $\mathcal{O}$ acts on the $\mathbf{Z}_p[G_{K'}]$-module $\underline{T}_p(\Gamma) = \varprojlim \Gamma[p^n](\mathbf{C}_{K'})$ in such a way that the associated $\mathcal{K}[G_{K'}]$-module $\underline{V}_p(\Gamma) = \mathbf{Q}_p \otimes_{\mathbf{Z}_p} \underline{T}_p(\Gamma)$ has $\mathcal{K}$-dimension equal to 2. By Tate's full faithfulness theorem [20, Thm 4], there is also a canonical $\mathcal{O}$-action on Γ.

We are interested in studying the action of $G_{K'}$ on $\bigwedge^2_{\mathcal{K}}(\underline{V}_p(\Gamma))$, where the exeterior power is taken with respect to the $\mathcal{K}$-vector space structure. We want to prove the action of $I_{K'}$ is cyclotomic in certain cases. By [9, Thm 6.2], we have a natural isomorphism in the category $\underline{MF}_{K',B}$

$$\underline{D}^*_B(\underline{V}_p(\Gamma)) \simeq \underline{D}_{K'}(\Gamma).$$

The filtered K'-module $\underline{D}_{K'}(\Gamma)$ is defined to be the K-vector space $D = K \otimes_{W(k)} \mathcal{M}(\Gamma_{/k})$, together with the filtration of $D_{K'} = K' \otimes_K D \simeq K' \otimes_{A'} \mathcal{M}(\Gamma_{/k})_{A'}$ [7, Ch IV, §2.3, Prop 2.1] defined by $D^i_{K'} = D_{K'}$ for $i \leq 0$, $D^1_{K'} = \underline{L}_{K'}(\Gamma)$ [7, Ch IV, §5.2], and $D^i_{K'} = 0$ for $i \geq 2$. We claim that $\underline{L}_{K'}(\Gamma)$ is non-zero and does not fill up all of $D_{K'}$. To see this, note that by [7, Ch IV, Prop 2.1, Prop 4.2(ii)] and the proof of [7, Ch IV, Prop 5.1], the K'-vector space $\underline{L}_{K'}(\Gamma)$ has dimension equal to $\dim(\Gamma)$. If $\underline{L}_{K'}(\Gamma) = 0$ then Γ is étale, which we assumed is not the case. If $\underline{L}_{K'}(\Gamma) = D_{K'}$ then $\dim(\Gamma)$ is equal to the $W(k)$-rank of $\mathcal{M}(\Gamma_{/k})$, which is the height of Γ, which is always equal to $\dim(\Gamma) + \dim(\widehat{\Gamma})$. Hence, in this case $\dim(\widehat{\Gamma}) = 0$, so $\widehat{\Gamma}$ is étale, contrary to hypothesis.

The $\mathcal{O}$-action on Γ gives rise to a $\mathcal{K}$-action on the filtered module $\underline{D}_{K'}(\Gamma)$ by functoriality, so $D_{K'}$ acquires the structure of a $K' \otimes_{\mathbf{Q}_p} \mathcal{K}$-module in which $\underline{L}_{K'}(\Gamma)$ is a non-zero proper submodule. Now make the hypothesis that $E = K' \otimes_{\mathbf{Q}_p} \mathcal{K}$ is a *field*. For example, this is true when $\mathcal{K} = \mathbf{Q}_p$, or when K' is a totally ramified finite extension of $\mathbf{Q}_p$ and $\mathcal{K}$ is an unramified extension of $\mathbf{Q}_p$ (this latter case is what arises in the setting of interest — here is where we use our original reduction to the case where $\mathcal{O}$ is a ring of Witt vectors). Also, $\dim_{K'} D_{K'} = \dim_K D$ is the height of Γ, which is equal to $2[\mathcal{K} : \mathbf{Q}_p] = 2[K' \otimes_{\mathbf{Q}_p} \mathcal{K} : K']$. Thus, $\dim_E D_{K'} = 2$, so the non-zero proper E-subspace $\underline{L}_{K'}(\Gamma)$ must therefore have E-dimension equal to 1 (and in a similar manner, we see that $\dim_{\mathcal{K}'} D = 2$).

Choose (non-canonically) a primitive generator a for the field extension $\mathcal{K}/\mathbf{Q}_p$, so $\{1, a, \dots, a^{[\mathcal{K}:\mathbf{Q}_p]-1}\}$ is a $\mathbf{Q}_p$-basis of $\mathcal{K}$, and is also a K'-basis of E. There is a map of filtered modules

$$\underline{D}_{K'}(\Gamma) \otimes \underline{D}_{K'}(\Gamma) \to \bigoplus (\underline{D}_{K'}(\Gamma) \otimes \underline{D}_{K'}(\Gamma))$$

given by component maps $x \otimes y \mapsto x \otimes y + y \otimes x$ and $x \otimes y \mapsto a^j x \otimes y + x \otimes a^j y$ for $1 \le j \le [\mathcal{K} : \mathbf{Q}_p] - 1$. The kernel of this map is a filtered module Δ with $\mathcal{K}$-action such that $\underline{V}_B^*(\Delta) \simeq \bigwedge_{\mathcal{K}}^2(\underline{V}_p(\Gamma))$. It is straightfoward to compute that the filtered module Δ has filtration structure $\Delta_{K'}^i = \Delta_{K'}$ for $i \le 1$ and $\Delta_{K'}^i = 0$ for $i \ge 2$. Also, by [9, Thm 5.2(*ii*), Thm 6.2] the filtered K'-module Δ is B-admissable.

We want to show that the action of $I_{K'}$ on $\underline{V}_B^*(\Delta)$ is $\epsilon|_{I_{K'}}$. Twisting by $\epsilon|_{G_{K'}}^{-1}$, the filtration degrees shift down by 1, and so we want to show that a B-admissable filtered K'-module Δ with $\Delta_{K'}^i = \Delta_{K'}$ for $i \le 0$ and $\Delta_{K'}^i = 0$ for $i \ge 1$ has trivial $I_{K'}$-action on $\underline{V}_B^*(\Delta)$. Define $K'' = W(\overline{k}) \otimes_{W(k)} K'$, the completion of the maximal unramified extension of K', so $G_{K''} = I_{K'}$. Define $\Delta'' = W(\overline{k}) \otimes_{W(k)} \Delta$ in the evident manner, a filtered K''-module. If U is a *finite-dimensional* vector space over $K'' = W(\overline{k}) \otimes_{W(k)} K'$ with a *continuous* semi-linear action of $\mathrm{Gal}(\overline{k}/k)$, then the natural map of K''-vector spaces

$$W(\overline{k}) \otimes_{W(k)} U^{\mathrm{Gal}(\overline{k}/k)} \to U$$

is an isomorphism (one first checks injectivity by considering an element in the kernel which is a sum of a minimal number of elementary tensors, and for surjectivity one uses continuity to find a stable lattice; surjectivity is proven even for lattices by using Nakayama's Lemma to reduce to a $\overline{k}$-vector space setting, which is then classical). We apply this to $U = \mathrm{Hom}_{\mathbf{Q}_p[I_{K'}]}(\underline{\mathrm{Res}}_{G_{K'}/I_{K'}}(V), B)$, with $V = \underline{V}_B^*(\Delta)$. The continuity of the $G_{K'}$-action on U follows from the continuity of the $G_{K'}$-actions on V and on $G_{K'}$-stable finite-dimensional K'-subspaces of B. Thus, we see that $\Delta'' \simeq \underline{D}_B^*(\underline{\mathrm{Res}}_{G_{K'}/I_{K'}}(V_B^*(\Delta)))$. Using [9, §5.6], it follows that the filtered K''-module Δ'' is B-admissable, so we're reduced to checking that a B-admissable filtered K''-module D with $D_{K''}^i = D_{K''}$ for $i \le 0$ and $D_{K''}^i = 0$ for $i \ge 1$ has associated representation $V_B^*(\Delta'')$ of $I_{K'} = G_{K''}$ which is trivial.

Since K'' has valuation ring A'' with *algebraically closed* residue field, we can apply [12, p. 105, Thm 1.7] to see that there exists an étale p-divisible group Γ'' over A'' with $\Delta'' \simeq D_{K''}(\Gamma'')$. But then by [9, Thm 6.2], $\underline{V}_B^*(\Delta'') \simeq \underline{V}_B^*(\underline{D}_{K'}(\Gamma'')) \simeq \underline{V}_B^*\underline{D}_B^*(\underline{V}_p(\Gamma'')) \simeq \underline{V}_p(\Gamma'')$. Since $\Gamma''_{/A''}$ is étale and A'' is strictly henselian, the representation space $\underline{V}_p(\Gamma'')$ is trivial.

■

4.2. **Another Deformation Problem.**

In the study of elliptic curves over $\mathbf{Q}$ in [3], there is a slight variant on our deformation problem which turns out to be useful. After giving the relevant definitions, we explain how to modify the preceding arguments in order to carry them over to the new deformation problem. *Assume now that p is odd.* Using the same notation as in §1, we fix a quadratic (ramified) character χ on $G_{\mathcal{K}'}$. Instead of considering $\overline{\rho}$ whose restriction to $G_{\mathcal{K}'}$ is $\mathcal{O}_{\mathcal{K}'}$-flat (with connectedness and Dieudonne module hypotheses), together with $\mathcal{O}_{\mathcal{K}'}$-flat deformations of $\overline{\rho}$, we suppose that the $\mathcal{O}_{\mathcal{K}'}$-flatness conditions holding after twisting by χ. More precisely, we assume that $\chi \otimes \overline{\rho}|_{G_{\mathcal{K}'}}$ is the generic fiber of a finite flat $\mathcal{O}_{\mathcal{K}'}$-group scheme which is unipotent and connected, and we consider only deformations ρ of $\overline{\rho}$ for which $\chi \otimes \rho|_{G_{\mathcal{K}'}}$ is $\mathcal{O}_{\mathcal{K}'}$-flat. We still include the exact sequence hypothesis on the Dieudonne module coming from the $\mathcal{O}_{\mathcal{K}'}$-group scheme attached to $\chi \otimes \overline{\rho}|_{G_{\mathcal{K}'}}$. The entirety of §1.1 carries over to this new setting. We call this new deformation problem the χ-twisted $\mathcal{O}_{\mathcal{K}'}$-flat deformation problem. It is easy to see that this deformation condition is independent of which of the two ramified quadratic characters on $G_{\mathcal{K}'}$ we choose, and in fact the condition depends on $\mathcal{K}'$ only through the value of $e(\mathcal{K}') = e$. Thus, we can again use $\mathcal{K}'$ of special type in calculations.

A fortunate technical accident makes it possible to carry over the descent data formalism, though in a slightly different form. Consider a finite Galois extension $L/\mathbf{Q}_p$ and a finite *commutative* L-group scheme $\Gamma_{/L}$, with $\rho = \Gamma(\overline{\mathbf{Q}}_p)$ the associated G_L-module. Let χ be a (continuous) character on G_L with $\chi^2 = 1$ (we say χ is *quadratic*, though we allow for the possibility that $\chi = 1$). We want to describe, in terms of $\Gamma_{/L}$ and 'descent data', what it means to extend $\chi \otimes \rho$ to a D_p-module. Note that if G is the generic fiber of a finite flat $\mathcal{O}_L$-group scheme and χ is ramified, then $\chi \otimes \rho$ is almost never $\mathcal{O}_L$-flat. We do not want to work over the quadratic extension of L cut out by a non-trivial ramified χ, since this has ramification index $2e(L)$ and the case of interest for elliptic curves has $e(L) = p - 1$ already (and breaking the $p - 1$ bound ruins any hope of applying the theory of finite Honda systems).

Descent theory says that giving a D_p-module structure to the twisted representation $\chi \otimes \rho$ is the same as giving compatible L-group scheme isomorphisms

$$[\sigma] : \Gamma_\chi \simeq (\Gamma_\chi)_\sigma,$$

where the σ subscript denotes base change by the automorphism $\sigma : L \simeq L$ and Γ_χ is the finite commutative L-group scheme attached to $\chi \otimes \rho$. The 'cocycle' compatibility condition is

$$[\sigma_1 \circ \sigma_2] = \sigma_1^*([\sigma_2]) \circ [\sigma_1].$$

To be completely explicit about the twisting by χ, if χ is non-trivial then Γ_χ is the descent of $\Gamma \times_L L(\chi)$ relative to the Galois extension $L(\chi)/L$, using the descent data $-1_\Gamma \times \tau$, where τ is the non-trivial element in $\mathrm{Gal}(L(\chi)/L)$; here we use the fact that Γ is commutative in an essential way (otherwise the action of inversion on Γ would not respect the group scheme structure over $L(\chi)$).

Define the quadratic character χ^σ on G_L by

$$\chi^\sigma(g) = \chi(\overline{\sigma}^{-1} g \overline{\sigma}),$$

where $g \in G_L$ and $\overline{\sigma} \in D_p$ is a lift of $\sigma \in \mathrm{Gal}(L/\mathbf{Q}_p)$. By considering $\overline{\mathbf{Q}}_p$-valued points, it is a straightfoward but slightly tedious exercise in unwinding the dictionary between finite étale L-algebras and finite sets with continuous $\mathrm{Gal}(L/\mathbf{Q}_p)$-actions to construct a natural isomorphism

$$i_{\sigma,\chi,\Gamma} : (\Gamma_\chi)_\sigma \simeq (\Gamma_\sigma)_{\chi^\sigma}$$

(the definition involves making a choice of lifting of σ to D_p, but then one checks that this choice does not matter). We now mention two important properties of this isomorphism. For $\sigma_1, \sigma_2 \in G_L$, the composite map

$$(\Gamma_\chi)_{\sigma_1\sigma_2} \simeq ((\Gamma_\chi)_{\sigma_2})_{\sigma_1} \stackrel{(i_{\sigma_2,\chi,\Gamma})_{\sigma_1}}{\longrightarrow} ((\Gamma_{\sigma_2})_{\chi^{\sigma_2}})_{\sigma_1} \stackrel{i_{\sigma_1,\chi^{\sigma_2},\Gamma_{\sigma_2}}}{\longrightarrow} ((\Gamma_{\sigma_2})_{\sigma_1})_{(\chi^{\sigma_2})^{\sigma_1}} \simeq (\Gamma_{\sigma_1\sigma_2})_{\chi^{\sigma_1\sigma_2}}$$

is equal to $i_{\sigma_1\sigma_2,\chi,\Gamma}$. Also, for $\sigma \in G_L$ and two quadratic characters χ_1 and χ_2 on G_L, the composite map

$$(\Gamma_{\chi_1\chi_2})_\sigma \simeq ((\Gamma_{\chi_1})_{\chi_2})_\sigma \stackrel{i_{\sigma,\chi_2,\Gamma_{\chi_1}}}{\longrightarrow} ((\Gamma_{\chi_1})_\sigma)_{\chi_2^\sigma} \stackrel{(i_{\sigma,\chi_1,\Gamma})_{\chi_2^\sigma}}{\longrightarrow} (\Gamma_\sigma)_{\chi_1^\sigma\chi_2^\sigma} = (\Gamma_\sigma)_{(\chi_1\chi_2)^\sigma}$$

is equal to $i_{\sigma,\chi_1\chi_2,\Gamma}$. These are proven by a very careful examination on the level of $\overline{\mathbf{Q}}_p$-valued points. The arguments are not difficult, but there are a lot of diagrams one needs to check, so we leave this to the reader as an exercise. If our G_L-modules have the structure of $k[G_L]$-modules for a finite ring k, then the above carries over for characters χ taking values in $k^\times$.

Instead of working with the isomorphisms $[\sigma]$ above, we can twist through by $\chi^{-1} = \chi$ in terms of Galois representations, leaving us with L-group scheme isomorphisms

$$[\sigma]' : \Gamma \stackrel{[\sigma]_{\chi^{-1}}}{\longrightarrow} ((\Gamma_\chi)_\sigma)_{\chi^{-1}} \stackrel{(i_{\sigma,\chi,\Gamma})_{\chi^{-1}}}{\longrightarrow} (\Gamma_\sigma)_{\xi_\sigma},$$

where $\xi_\sigma = \chi^\sigma \chi^{-1}$. The fortunate technical accident is that G_L has exactly two ramified quadratic characters and one unramified non-trivial quadratic character, so the quadratic character ξ_σ is always *unramified* (perhaps trivial) and $\xi_{\sigma_1}^{\sigma_2} = \xi_{\sigma_1}$, so $\xi_{\sigma_1\sigma_2} = \xi_{\sigma_1}\xi_{\sigma_2}$. Thus, we have isomorphisms

$$j_{\sigma_1,\xi_{\sigma_2},\Gamma} : (\Gamma_{\sigma_1})_{\xi_{\sigma_2}} \simeq (\Gamma_{\xi_{\sigma_2}})_{\sigma_1}$$

inverse to $i_{\sigma_1,\xi_{\sigma_2},\Gamma}$. Twisting through $[\sigma]'$ by $\xi_\sigma = \xi_\sigma^{-1}$, we get L-group scheme isomorphisms

$$[\sigma]'' : \Gamma_{\xi_\sigma} \simeq \Gamma_\sigma.$$

It is another tedious (but not difficult) argument with many diagrams to check that the 'cocycle' compatibility condition on the isomorphisms $[\sigma]$ above is exactly the condition that the composite map

$$\Gamma_{\xi_{\sigma_1\sigma_2}} \simeq (\Gamma_{\sigma_1})_{\sigma_2} \stackrel{[\sigma_1]''{}_{\xi_{\sigma_2}}}{\longrightarrow} (\Gamma_{\sigma_1})_{\xi_{\sigma_2}} \stackrel{j_{\sigma_1,\xi_{\sigma_2},\Gamma}}{\longrightarrow} (\Gamma_{\xi_{\sigma_2}})_{\sigma_1} \stackrel{\sigma_1^*([\sigma_2]'')}{\longrightarrow} (\Gamma_{\sigma_2})_{\sigma_1} \simeq \Gamma_{\sigma_1\sigma_2}$$

is equal to $[\sigma_1\sigma_2]''$. This final formulation is suitable for translation into the language of finite Honda systems, since it only involves (isomorphism) base changes and *unramified* twists, both of which preserve the $\mathcal{O}_L$-flatness condition and extend nicely from $\mathrm{Spec}(L)$ over to $\mathrm{Spec}(\mathcal{O}_L)$.

Consider $\mathcal{K}'/\mathbf{Q}_p$ of special type. It is a straightfoward exercise to check that if $\mathbf{F}_p(\zeta_e) = \mathbf{F}_p(\zeta_{2e})$ (i.e., e is odd, $\mathrm{ord}_2(e) = 1$ and $p \equiv 1 \bmod 4$, or $\mathrm{ord}_2(e) = r \geq 2$ and $p \equiv 1, -1, -1+2^r \bmod 2^{r+1}$), then the quadratic ramified extensions of $\mathcal{K}'$ are Galois over $\mathbf{Q}_p$ and therefore $\xi_\sigma = 1$ for all $\sigma \in \mathrm{Gal}(\mathcal{K}'/\mathbf{Q}_p)$. In these cases, the descent formalism on Honda systems is identical to that which we have already dealt with, so the 'twisted' flat deformation rings (with and without determinant restrictions) have the same formal power series ring form as before. This is uninteresting from the point of view of elliptic curves over $\mathbf{Q}$ — the case of essential interest is $p = 3$, $e = 2$. When $\mathbf{F}_p(\zeta_e) \neq \mathbf{F}_p(\zeta_{2e})$ (so e is in particular even), then $\xi_\sigma = 1$ if and only if σ is trivial on the unique quadratic subextension of $K'/\mathbf{Q}_p$. *We now assume that* $e|(p-1)$. This has the effect of making $K' = \mathcal{K}'$ in the context of $\mathcal{K}'$ of special type, so $\kappa = \mathbf{F}_p$ and $G_{\mathcal{K}'} = \mu_e$. From a technial point of view, the elimination of $\mathrm{Gal}(\mathcal{K}'/K')$ will make it much easier to modify our previous work. Otherwise new complications arise and we lack the motivation to deal with the additional mess. The main result is as expected:

Theorem 4.2.1. *Fix $p \neq 2$, $e|(p-1)$, $\mathcal{K}'/\mathbf{Q}_p$ a finite extension with $e(\mathcal{K}') = e$, and χ a quadratic ramified character on $G_{\mathcal{K}'}$. Let $\overline{\rho} : D_p \to \mathrm{GL}_2(k)$ be a continuous representation for which $\chi \otimes \overline{\rho}$ is the generic fiber of a connected and unipotent $\mathcal{O}_{\mathcal{K}'}$-flat group scheme. Moreover, assume that this (unique) $\mathcal{O}_{\mathcal{K}'}$-flat group scheme has a closed fiber Dieudonne module M for which the sequence of groups*

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

is exact.

Such a $\overline{\rho}$ is either absolutely irreducible or reducible with trivial centralizer. Thus, a universal deformation χ-twisted $\mathcal{O}_{\mathcal{K}'}$-flat deformation ring for $\overline{\rho}$ exists. This ring is isomorphic to $\mathcal{O}[\![T_1,T_2]\!]$. The determinant of the associated universal deformation restricts to $\epsilon|_{I_{\mathcal{K}'}}$ on $I_{\mathcal{K}'}$. If we fix a character $\delta : D_p \to \mathcal{O}^\times$ which restricts to $\epsilon|_{I_{\mathcal{K}'}}$ on $I_{\mathcal{K}'}$, then the 'determinant δ' subfunctor of the χ-twisted $\mathcal{O}_{\mathcal{K}'}$-flat deformation functor of $\overline{\rho}$ is represented by a quotient $\mathcal{O}[\![T]\!]$ of the universal deformation ring.

Proof. As usual, we may assume that $\mathcal{K}'$ is of special type, so by our hypothesis on e, $\mathcal{K}' = K' = \mathbf{Q}_p(\pi)$ with $\pi^e = pu_0$ for $u_0 \in \mathbf{Z}_p^\times$. Also, as explained above, we may assume $\mathbf{F}_p(\zeta_e) \neq \mathbf{F}_p(\zeta_{2e})$. We will now explain how to modify our calculations so that they carry over to this new setting. It is for this reason that we assume $e|(p-1)$; any non-trivial contribution of $\mathrm{Gal}(\mathcal{K}'/K') \simeq \mathrm{Gal}(\kappa/\mathbf{F}_p) = \mathrm{Gal}(\mathbf{F}_p(\zeta_e)/\mathbf{F}_p)$ (in our old notation) would create significant complications, so we omit consideration of these other cases. Thus, all we have to work with in the descent computations are the $\zeta \in \mu_e \simeq \mathrm{Gal}(\mathcal{K}'/\mathbf{Q}_p(\zeta_e)) = \mathrm{Gal}(\mathcal{K}'/\mathbf{Q}_p)$. Recall that these ζ act $W(\kappa)$-linearly on the Dieudonne modules.

Aside from the descent data d_ζ's, the residual analysis as in §2.3 carries over without change, so we have (L, M) and $(\mathcal{L}, \mathcal{M})$, though these are now equal since $A' = \mathcal{K}'$. Let κ_2/κ denote the unique quadratic extension of $\kappa = \mathbf{F}_p$, and let $\kappa^\perp$ denote the -1-eigenspace in κ_2 for the action of the non-trivial element of $\mathrm{Gal}(\kappa_2/\kappa)$. This is a 1-dimensional κ-vector space, so $\kappa^\perp \otimes_{\mathbf{F}_p} k$ has the structure of a free rank one module over $\kappa \otimes_{\mathbf{F}_p} k$. From our above explicit description of χ-twisting on generic fiber group schemes, it follows that making unramified twists to $\mathcal{A}'$-flat representations translates into finite Honda systems as

$$(\mathcal{L}, \mathcal{M})_\chi = (\kappa^\perp[\pi](\epsilon_1 + \alpha\epsilon_2), (\kappa^\perp \otimes_{\mathbf{F}_p} k)e_1 \oplus (\kappa^\perp \otimes_{\mathbf{F}_p} k)e_2)$$

(this is to be viewed inside of $\mathcal{A}'(\chi) \otimes_{\mathcal{A}'} (\mathcal{L}, \mathcal{M})$, with $\mathcal{A}'(\chi)$ the unramified degree 2 extension of $\mathcal{A}'$ corresponding to κ_2/κ).

We compute the same form for the matrix of $[\zeta]$, except that when $\zeta^{e/2} \neq 1$ (so $\zeta \in \mathrm{Gal}(\mathcal{K}'/\mathbf{Q}_p)$ acts non-trivially on the quadratic subfield of $\mathcal{K}'/\mathbf{Q}_p$, which is to say $\xi_\zeta = \chi$, rather than $\xi_\zeta = 1$), we have the matrix entries in $\kappa^\perp \otimes_{\mathbf{F}_p} k$. The same relation $d_\zeta^{(p^2)} = d_\zeta$ still holds (though this is a tautology since $\kappa_2 = \mathbf{F}_{p^2}$ in the present cases), and

$$d_{\zeta_1\zeta_2} = d_{\zeta_1} d_{\zeta_2}, \quad c_{\zeta_1\zeta_2} = d_{\zeta_1}^{(p)} c_{\zeta_2} + d_{\zeta_2} c_{\zeta_1},$$

where the products are taken inside of $\kappa_2 \otimes_{\mathbf{F}_p} k$. The condition that $[\zeta]$ be an automorphism is that d_ζ is a $\kappa \otimes_{\mathbf{F}_p} k$-module generator of $\kappa^\perp \otimes_{\mathbf{F}_p} k$ (resp. $\kappa \otimes_{\mathbf{F}_p} k$) when $\zeta^{e/2} = -1$ (resp. $\zeta^{e/2} = 1$). The formulas for $[\zeta]_{\mathcal{A}'}$ carry over, as does the Fundamental Relation. The rest of §2.3 still works (with $\kappa^\perp$ replacing κ in a few places), so we again recover the fact that $\alpha = 0$ if and only if $\overline{\rho}$ is irreducible, $e|(i+1)(p+1)$ in the reducible cases, and $\overline{\rho}$ is absolutely irreducible or is reducible with a trivial centralizer. In particular, a universal χ-twisted $\mathcal{O}_{\mathcal{K}'}$-flat deformation ring does indeed exist.

Since the first part of Theorem 2.4.1 makes no use of the descent data, it carries over to our new setting. The proof of Lemma 2.4.2 still shows that we can find a basis $\{e_1, e_2\}$ (unique up to $k^\times$-scaling) so that $\alpha = a\pi^i$ for some $0 \le i \le e-2$ and $c_\zeta = 0$ for all $\zeta \in \mu_e$. The point is that if ζ_0 is a primitive eth root of unity, so $\zeta_0^{e/2} = -1$, then $d_{\zeta_0} - d_{\zeta_0}^{(p)} = (1 - \zeta_0^{-i-1})d_{\zeta_0}$ is a $\kappa \otimes_{\mathbf{F}_p} k$-module generator of $\kappa^\perp \otimes_{\mathbf{F}_p} k$ (since d_{ζ_0} is such a generator, and $1 - \zeta_0^{-i-1} \in \kappa^\times$). Thus, we can find $t \in \kappa \otimes_{\mathbf{F}_p} k = k$ such that $c_{\zeta_0} = t(d_{\zeta_0} - d_{\zeta_0}^{(p)})$, and by the same arguments (based on $c_{\zeta_1\zeta_2} = c_{\zeta_2\zeta_1}$ and the fact that $d_\zeta \in \mu_e(\kappa_2 \otimes_{\mathbf{F}_p} k) \subseteq (\kappa_2 \otimes_{\mathbf{F}_p} k)^\times$) the same $t \in k$ works for all $\zeta \in \mu_e$. Replacing e_2 by $e_2 - te_1$ gives the desired change of basis.

Now consider the tangent space calculations. If $\zeta^{e/2} = -1$, then $d_\zeta, d_\zeta^{(p)} \in \mu_e(\kappa_2 \otimes_{\mathbf{F}_p} k)$ are $\kappa \otimes_{\mathbf{F}_p} k$-generators of the rank one $\kappa \otimes_{\mathbf{F}_p} k$-module $\kappa^\perp \otimes_{\mathbf{F}_p} k$, so $d_\zeta^{-1} d_\zeta^{(p)} \in \mu_e(\kappa \otimes_{\mathbf{F}_p} k)$ makes sense. We define the notion of degeneracy for $\overline{\rho}$ as before. The proof of Theorem 3.1.2 still works (in fact, it is easier, since we don't have any non-trivial $\sigma \in \mathrm{Gal}(\mathcal{K}'/K')$ to worry about), except that in a couple of places where we consider solutions to $t^{(p)} = xt$ in $\kappa \otimes_{\mathbf{F}_p} k$, we need to work in $\kappa_2 \otimes_{\mathbf{F}_p} k$. Also, all references to interpretation of Honda system conditions in terms of $\overline{\rho}$ are irrelevant and are to be ignored. In a similar manner, the proof of Theorem 3.2.1 carries over. Actually, degenerate cases never occur. The reason is that the proof of Theorem 3.2.1 shows that the degenerate cases must have $d_\zeta = d_\zeta^{(p)}$ for all ζ, so $d_\zeta \in k = \kappa \otimes_{\mathbf{F}_p} k \subseteq \kappa_2 \otimes_{\mathbf{F}_p} k$. But if $\zeta^{e/2} = -1$ then $d_\zeta \in \kappa^\perp \otimes_{\mathbf{F}_p} k$. Since $d_\zeta \neq 0$ for all ζ, the degenerate cases lead to a contradiction. Therefore, we have $d_\zeta = \zeta^{i+1} d_\zeta^{(p)}$ for all ζ and some $0 \le i \le e-2$.

The proof of Theorem 4.1.1 is easily modified (we sometimes need to work over $W(\kappa_2)$ or the -1-eigenspace of $W(\tau)$ in here), and is made simpler since we do not need to consider degenerate cases. The proof of Theorem 4.1.2 remains valid once we twist through the specializations $\rho|_{G_{K'}}$ by χ. This has no effect on the $\mathcal{O}$-module determinant, but in the second part of the theorem, we should denote the character $D_p \to \mathcal{O}^\times$ by a letter other than χ in order to avoid confusion.

■

References

[1] S. Bosch, W. Lutkebohmert, M. Raynaud, *Néron Models*, Springer-Verlag, 1980.
[2] B. Conrad, *Finite Group Schemes over Bases with Low Ramification*, in preparation.
[3] B. Conrad, F. Diamond, R. Taylor, *On the Modularity of Certain Potentially Crystalline Representations*, in preparation.
[4] J.E. Cremona, *Algorithms for Modular Elliptic Curves*, Cambridge University Press, 1992.
[5] P. Deligne, J-P. Serre, *Formes Modulaires de Pois 1*, Ann. Sci. Éc. Norm. Sup., t.7 (1974), pp. 507-530.
[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 commutatiffs sur les vecteurs de Witt*, C.R. Acad. Sci. **280** (1975), pp. 1423-1425.
[9] J.-M. Fontaine, *Sur certain types de représentations p-adiques du groupe de Galois d'un corps local; construction d'un anneau de Barsotti-Tate*, Annals of Mathematics, **115** (1982), pp. 529-577.
[10] J.-M. Fontaine, G. Laffaille, *Construction de représentations p-adiques*, Ann. Sci. E.N.S. (1982), pp. 547-608.
[11] N. Katz, B. Mazur, *Arithmetic Moduli of Elliptic Curves*, Princeton University Press, 1985.
[12] G. Laffaille, *Construction de groupes p-divisibles: le cas de dimension 1*, Asterisque no. 65, Société Math. de France (1979), pp. 103-123.
[13] H. Matsumura, *Commutative Ring Theory*, Cambridge Univ. Press, 1986.
[14] F. Oort, J. Tate, *Group Schemes of Prime Order*, Ann. Sci. E.N.S. (1970), pp. 1-21.
[15] R. Ramakrishna, *On a Variation of Mazur's Deformation Functor*, Compositio Math. (3) **87** (1993), pp. 269-286.
[16] M. Raynaud, *Schémas en groupes de type $(p, p, \ldots, p)$*, Bull. Soc. Math. France **102** (1974), pp. 241-280.
[17] M. Schlessinger, *Functors on Artin Rings*, Transactions of the A.M.S. **130** (1968), pp. 208-222.
[18] G. Shimura, *On Elliptic Curves with Complex Multiplication as Factors of Jacobians of Modular Function Fields*, Nagoya Math. Journal, Vol 43 (1971), pp. 199-208.
[19] J. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, 1986.
[20] J. Tate, *p-divisible groups* in Proceedings of a Conference on Local Fields (Driebergen), pp. 158-183, 1966.
[21] R. Taylor, A. Wiles, *Ring-theoretic Properties of Certain Hecke Algebras*, Annals of Mathematics (3) **141** (1995), pp. 553-572.
[22] A. Wiles, *Modular Elliptic Curves and Fermat's Last Theorem*, Annals of Mathematics (3) **141** (1995), pp. 443-551.