ASIAN J. MATH.
Vol. 12, No. 2, pp. 193–202, June 2008

003

A RIGIDITY RESULT FOR p-DIVISIBLE FORMAL GROUPS*

CHING-LI CHAI†

Key words. p-divisible formal groups

AMS subject classifications. 14K10, 14G35, 13H99

1. Introduction.

In this article we prove a rigidity result for p-divisible formal groups; see Thm. 4.3 for the statement. An important special case is the following. Consider a formal torus T over an algebraically closed field k of characteristic $p > 0$. Suppose $Z \subseteq T$ is an irreducible closed formal subscheme of T which is stable under the endomorphism $[1 + p^n]_T$ for some $n \geq 2$, where $[1 + p^n]_T : T \to T$ denotes "multiplication by $1 + p^n$" on the formal torus T. Then 4.3 asserts that Z is a formal subtorus of T.

If one assumes that k is equal to the algebraic closure $\overline{\mathbb{F}_p}$ of the prime field $\mathbb{F}_p$ and the closed formal subscheme Z in Thm. 4.3 is formally smooth over k, then the proof of 4.3 can be simplified. Section 2 contains lemmas in commutative algebra used to remove the extra assumptions above. For instance a weak desingularization result Prop. 2.1 for complete local integral domains over k with residue field k is used to remove the smoothness assumption on Z. The main tool for the proof of 4.3 is Prop. 3.1, a result on power series. The proof of Prop. 3.1 is elementary, so this article has the flavor of an excursion in "high school algebra" in the sense of Abhyankar.

The motivation of this article comes from the Hecke orbit problem for the reduction of a Shimura variety in characteristic p. See Conj. 6.2 in [10] for a statement of the conjecture for Siegel modular varieties, and [3] for a survey of the Hecke orbit problem and a sketch of a proof of the Hecke orbit conjecture for the Siegel modular varieties; see also [4]. The rigidity result 4.3 in this article, when combined with the theory of canonical coordinates on leaves in [6], allows one to linearize the Hecke orbit problem and reduce it to a question on global p-adic monodromy; see [3], [4]. See also [7, §6, §9] for an exposition of this linearization procedure in the case of ordinary abelian varieties. Thm. 4.3 has also been used in Hida's recent works [9] on the Iwasawa μ-invariant for p-adic L-functions; see §3 of [9].

In the present set-up, the statement of Thm. 4.3 appears to be in its optimal form. On the other hand one expects that 4.3 can be generlized and adapted to the situation of canonical coordinates for leaves, where the ambient formal scheme has, instead of a group structure, a *cascade* structure in the sense of B. Moonen. We hope to address this point in the near future.

2. Lemmas in commutative algebra.

PROPOSITION 2.1. *Let k be an algebraically closed field. Let R be a topologically finitely generated complete local domain over k. In other words, R is isomorphic to a quotient $k[[x_1, \ldots, x_n]]/P$, where P is a prime ideal of the power series*

*Received February 13, 2006; accepted for publication November 7, 2007.
†Department of Mathematics, University of Pennsylvania, Philadelphia, PA 19104-6395, USA (chai@math.upenn.edu). Partially supported by grant DMS01-00441 from the National Science Foundation.

ring $k[[x_1,\dots,x_n]]$. *Then there exists an injective local homomorphism* $\iota : R \hookrightarrow k[[y_1,\dots,y_d]]$ *of complete local* k*-algebras, where* $d = \dim(R)$.

Proof. Denote by $f : X \to \operatorname{Spec} R$ the normalization of the blowing-up of the closed point s_0 of $S := \operatorname{Spec} R$. Let $D = (f^{-1}(s_0))_{\mathrm{red}}$ be the exceptional divisor with reduced structure; it is a scheme of finite type over k. The maximal points of D are contained in the regular locus X_{reg} of X, hence there exists a dense open subscheme $U \subset D$ such that $U \subset X_{\mathrm{reg}}$. Pick a closed point x_0 in U. Then the completion $\mathcal{O}^{\wedge}_{X,x_0}$ of the local ring $\mathcal{O}_{X,x_0}$ is isomorphic to $k[[y_1,\dots,y_d]]$, and the natural map $R \to \mathcal{O}^{\wedge}_{X,x_0}$ is an injection. ☐

REMARK 2.1.1. (i) Prop. 2.1 can be regarded as a very weak version of desingularization. In fact if Spf R is the completion of an algebraic variety X over k at a closed point x of X, and $f : Y \to X$ is a generically finite morphism of algebraic varieties such that there exists a closed point $y \in Y$ above x and Y is smooth at y. Then the natural map $R := \mathcal{O}^{\wedge}_{X,x} \to \mathcal{O}^{\wedge}_{Y,y}$ gives the desired inclusion.

(ii) It is also possible to prove Prop. 2.1 using Néron's desingularization: One first produces an injective homomorphism $k[[t]] \to R$ which is "generically smooth" in a suitable sense, and a finite extension $k[[t]] \to k[[x]]$ such that there exists a $k[[t]]$-algebra homomorphism $e : R \to k[[x]]$. Then one uses Néron's desingularization procedure to smoothen $R \otimes_{k[[t]]} k[[x]]$ along the section e. This proof is more complicated than the one given above though. The author would like to acknowledge discussions with F. Pop along this direction.

PROPOSITION 2.2. *Let* k *be a field of characteristic* $p > 0$. *Let* r *be a positive integer and let* $q = p^r$. *Let* $F(x_1,\dots,x_m) \in k[x_1,\dots,x_m]$ *be a polynomial with coefficients in* k. *Suppose that we are given elements* $c_1,\dots,c_m$ *in* k *and a natural number* $n_0 \in \mathbb{N}$ *such that* $F(c_1^{q^n},\dots,c_m^{q^n}) = 0$ *in* k *for all* $n \geq n_0$, $n \in \mathbb{N}$. *Then* $F(c_1^{q^n},\dots,c_m^{q^n}) = 0$ *for all* $n \in \mathbb{N}$*; in particular* $F(c_1,\dots,c_m) = 0$.

Proof. We may and do assume that k is perfect. Let $\sigma : k \to k$ be the automorphism of k such that $\sigma(y) = y^{q^{-1}}$ for all $y \in k$. For each $n \in \mathbb{N}$ and each polynomial $f(\mathbf{x}) = \sum_{I\in\mathbb{N}^m} a_I\,\mathbf{x}^I \in k[\mathbf{x}]$, denote by $\sigma^n(f(\mathbf{x}))$ the result of applying σ^n to the coefficients of $f(\mathbf{x})$; i.e. $\sigma^n(f(\mathbf{x})) := \sum_{I\in\mathbb{N}^m} \sigma^n(a_I)\,\mathbf{x}^I \in k[\mathbf{x}]$. Here $\mathbf{x}$ stands for $(x_1,\dots,x_m)$. The map $f \mapsto \sigma(f)$ is a σ-linear automorphism of the ring $k[\mathbf{x}]$, and it preserves the increasing filtration of $k[\mathbf{x}]$ by degree: For each $a \in \mathbb{N}$, let V_a be the k-subspace of $k[\mathbf{x}]$ consisting of all polynomials in $k[\mathbf{x}]$ of degree at most a. Then $\sigma : f \to \sigma(f)$ is a σ-linear isomorphism from V_a to itself, for each $a \in \mathbb{N}$.

Let I be the ideal in $k[\mathbf{x}]$ generated by all polynomials $\sigma^n(F(\mathbf{x}))$ with $n \geq n_0$. We claim that $\sigma(I) = I$. It is clear that $\sigma(I) \subseteq I$, for $\sigma(I)$ is generated by the polynomials $\sigma^n(F(\mathbf{x}))$, $n \geq n_0 + 1$. On the other hand, for each $a \in \mathbb{N}$, σ induces a σ-linear isomorphism from $I \cap V_a$ to $\sigma(I) \cap V_a$. Therefore $\dim_k(I \cap V_a) = \dim_k(\sigma(I) \cap V_a)$. Since $I \cap V_a \supseteq \sigma(I) \cap V_a$, we deduce that $I \cap V_a = \sigma(I) \cap V_a$, for every $a \in \mathbb{N}$. A standard descent argument tells us that the k-vector space $I \cap V_a$ is spanned by $\mathbb{F}_q[\mathbf{x}] \cap I \cap V_a$, for each $a \in \mathbb{N}$. It follows that the ideal $I \subset k[\mathbf{x}]$ is generated by $I \cap \mathbb{F}_q[\mathbf{x}]$. Since $(c_1,\dots,c_m) \in \operatorname{Spec}(k[x_1,\dots,x_m]/I)(k)$ and I is defined over $\mathbb{F}_q$, $(\sigma^b(c_1),\dots,\sigma^b(c_m))$ lies in the zero locus of I for every $b \in \mathbb{N}$. The proposition follows. ☐

The following proposition strengthens 2.2; it will not be used in the rest of this article.

PROPOSITION 2.3. *Notation as in 2.2. Let d be the degree of $F(x_1,\dots,x_m)$. Let V be the set of all homogeneous polynomials in $k[x_1,\dots,x_m]$ of degree d if $F(x_1,\dots,x_m)$ is homogeneous; otherwise let V be the set of all polynomials in $k[x_1,\dots,x_m]$ of degree at most d if $F(x_1,\dots,x_m)$ is not homogeneous. Let n_0, n_1 be natural numbers such that $n_1 - n_0 \geq \dim_k(V)$. Assume that $F(c_1^{q^n},\dots,c_m^{q^n}) = 0$ in k for all n satisfying $n_0 \leq n \leq n_1$. Then $F(c_1^{q^n},\dots,c_m^{q^n}) = 0$ for all $n \in \mathbb{N}$.*

Proof. For each $a \in \mathbb{N}$, let $W_a = \sum_{n_0 \leq n \leq n_0 + a} k \cdot \sigma^n(F(\mathbf{x}))$. Clearly $W_a \subseteq W_{a+1} \subseteq V$ for all $a \in \mathbb{N}$. Suppose that $W_a = W_{a+1}$ for some a, then

$$W_{a+2} = k\langle \sigma^{n_0}(F(\mathbf{x})), \sigma(W_{a+1})\rangle = k\langle \sigma^{n_0}(F(\mathbf{x})), \sigma(W_a)\rangle = W_{a+1}\,,$$

where $k\langle S\rangle$ denotes the k-linear span of S for any subset $S \subseteq V$. Therefore $W_a = W_{a+1}$ implies that $W_a = W_b$ for all $b \geq a$. Since $n_1 - n_0 \geq \dim(V)$, the ideal I in the proof of 2.2 is generated by $W_{n_1 - n_0}$. So the apparently weaker assumption here is actually the same as that in 2.2. □

3. A result on power series.

PROPOSITION 3.1. *Let k be a field of characteristic $p > 0$. Let $f(\mathbf{u},\mathbf{v}) \in k[[\mathbf{u},\mathbf{v}]]$, $\mathbf{u} = (u_1,\dots,u_a)$, $\mathbf{v} = (v_1,\dots,v_b)$, be a formal power series in the variables $u_1,\dots,u_a, v_1,\dots,v_b$ with coefficients in k. Let $\mathbf{x} = (x_1,\dots,x_m)$, $\mathbf{y} = (y_1,\dots,y_m)$ be two new sets of variables. Let $\mathbf{g}(\mathbf{x}) = (g_1(\mathbf{x}),\dots,g_a(\mathbf{x}))$ be an a-tuple of power series without the constant terms, i.e. $g_i(\mathbf{x}) \in (\mathbf{x})k[[\mathbf{x}]]$ for $i = 1,\dots,a$. Let $\mathbf{h}(\mathbf{y}) = (h_1(\mathbf{y}),\dots,h_b(\mathbf{y}))$, with $h_j(\mathbf{y}) \in (\mathbf{y})k[[\mathbf{y}]]$ for $j = 1,\dots,b$. Let $q = p^r$ be a positive power of p. Let $n_0 \in \mathbb{N}$ be a natural number, and let b' be a natural number with $1 \leq b' \leq b$. Let $(d_n)_{n\in\mathbb{N}}$ be a sequence of natural numbers such that $\lim_{n\to\infty} \frac{q^n}{d_n} = 0$. Suppose we are given power series $R_{j,n}(\mathbf{v}) \in k[[\mathbf{v}]]$, $j = 1,\dots,b$, $n \geq n_0$, such that $R_{j,n}(\mathbf{v}) \equiv 0 \pmod{(\mathbf{v})^{d_n}}$ for all $j = 1,\dots,b$ and all $n \geq n_0$. For each $n \geq n_0$, let $\phi_{j,n}(\mathbf{v}) = v_j^{q^n} + R_{j,n}(\mathbf{v})$ if $1 \leq j \leq b'$, and let $\phi_{j,n}(\mathbf{v}) = R_{j,n}(\mathbf{v})$ if $b'+1 \leq j \leq b$. Let $\Phi_n(\mathbf{v}) = (\phi_{1,n}(\mathbf{v}),\dots,\phi_{b,n}(\mathbf{v}))$ for each $n \geq n_0$. Assume that*

$$f(\mathbf{g}(\mathbf{x}), \Phi_n(\mathbf{h}(\mathbf{x}))) = f\left(g_1(\mathbf{x}),\dots,g_a(\mathbf{x}), \phi_{1,n}(h(\mathbf{x})),\dots,\phi_{b,n}(h(\mathbf{x}))\right) = 0$$

in $k[[\mathbf{x}]]$, for all $n \geq n_0$. Then $f(g_1(\mathbf{x}),\dots,g_a(\mathbf{x}), h_1(\mathbf{y}),\dots,h_{b'}(\mathbf{y}),0,\dots,0) = 0$ in $k[[\mathbf{x},\mathbf{y}]]$.

Proof. Let $\mathbf{t} = (t_{i,J})$ be an infinite set of variables parametrized by indices $(i,J) \in \{1,\dots,b\} \times (\mathbb{N}^m - \{0\})$. Let

$$H_i(\mathbf{t}; y) = \sum_{i,J} t_{i,J}\,\mathbf{y}^J\,,$$

so that if we write $h_i(\mathbf{y}) = \sum_{i,J} c_{i,J}\,\mathbf{y}^J$ with $c_{i,J} \in k$, and let $\mathbf{c} = (c_{i,J})_{i,J}$, then $h_i(\mathbf{y}) = H_i(\mathbf{c};\mathbf{y})$ for each $i = 1,\dots,b$. Write $\mathbf{t} = (\mathbf{t}_1,\mathbf{t}_2)$, with $\mathbf{t}_1 = (t_{iJ})_{1\leq i\leq b'}$, $\mathbf{t}_2 = (t_{iJ})_{b'+1\leq i\leq b}$. Similarly we write $\mathbf{c} = (\mathbf{c}_1,\mathbf{c}_2)$

Consider the formal power series

$$f(g_1(\mathbf{x}),\dots,g_a(\mathbf{x}), H_1(\mathbf{t}_1;\mathbf{y}),\dots,H_{b'}(\mathbf{t}_1;\mathbf{y}), H_{b'+1}(\mathbf{t}_2;\mathbf{y}),\dots,H_b(\mathbf{t}_2;\mathbf{y})) \in k[\mathbf{t}][[\mathbf{x},\mathbf{y}]]$$

and write it as

$$f(\mathbf{g}(\mathbf{x}), \mathbf{H}(\mathbf{t};\mathbf{y})) = \sum_{I,J\in\mathbb{N}^m} A_{I,J}(\mathbf{t}_1)\,\mathbf{x}^I\mathbf{y}^J + \sum_{I,J\in\mathbb{N}^m} B_{I,J}(\mathbf{t}_1,\mathbf{t}_2)\,\mathbf{x}^I\mathbf{y}^J\,,$$

where $\mathbf{H}(\mathbf{t})$ is short for $(H_1(\mathbf{t}),\ldots,H_b(\mathbf{t}))$, and $B_{I,J}(\mathbf{t}_1,\mathbf{0})=0$ for all I,J. Notice that each $A_{I,J}(\mathbf{t}_1)$ is a polynomial in $\mathbf{t}_1$, so is each $B_{I,J}(\mathbf{t})$. We must show that $A_{I,J}(\mathbf{c}_1)=0$ for all I,J. The assumption on $\Phi_n(\mathbf{v})$ implies that

$$\begin{aligned} 0 &= f(\mathbf{g}(\mathbf{x}),\Phi_n(\mathbf{h}(\mathbf{x}))) \\ &\equiv f(\mathbf{g}(\mathbf{x}),h_1(\mathbf{x})^{q^n},\ldots,h_{b'}(\mathbf{x})^{q^n},0,\ldots,0) \pmod{(\mathbf{x})^{d_n}} \quad \forall\, n\geq n_0\,. \end{aligned}$$

In the above $\mathbf{c}_1^{q^n}$ is short for the vector $\left(c_{i,J}^{q^n}\right)_{1\leq i\leq b',\, J\in\mathbb{N}^m-\{0\}}$.

Suppose that $f(\mathbf{g}(\mathbf{x}),h_1(\mathbf{y}),\ldots,h_{b'}(\mathbf{y}),0,\ldots,0)=\sum_{I,J}A_{I,J}(\mathbf{c}_1)\,\mathbf{x}^I\mathbf{y}^J\neq 0$. Let

$$M_2 := \inf\{\,|J| : \exists\, I \text{ s.t. } A_{I,J}(\mathbf{c}_1^{q^n})\neq 0 \text{ for infinitely many } n\in\mathbb{N}\}\,,$$

and let

$$M_1 := \inf\{\,|I| : \exists\, J \text{ with } |J|=M_2 \text{ s.t. } A_{I,J}(\mathbf{c}_1^{q^n})\neq 0 \text{ for infinitely many } n\in\mathbb{N}\,\}\,.$$

According to Prop. 2.2, M_2,M_1 are well-defined natural numbers. Moreover $A_{I,J}(\mathbf{c}_1^{q^n})=0$ for all $n\in\mathbb{N}$ if $|J|<M_2$, or if $|J|=M_2$ and $|I|<M_1$. Since $\lim_{n\to\infty}\frac{q^n}{d_n}=0$, there exists a natural number n_2 such that $q^{n_2}>2M_1$ and $M_1+q^nM_2<d_n$ for all $n\geq n_2$. We have

$$\begin{aligned} f(\mathbf{g}(\mathbf{x}),h_1(\mathbf{x})^{q^n},\ldots,h_{b'}(\mathbf{x})^{q^n},0,\ldots,0) &= f(\mathbf{g}(\mathbf{x}),H_1(\mathbf{c}_1^{q^n};\mathbf{x}^{q^n}),H_{b'}(\mathbf{c}_1^{q^n};\mathbf{x}^{q^n}),0\ldots,0) \\ &= \sum_{I,J}A_{I,J}(\mathbf{c}_1^{q^n})\,\mathbf{x}^{I+q^nJ}\,, \end{aligned}$$

hence

$$\begin{aligned} 0=f(\mathbf{g}(\mathbf{x}),\Phi_n(\mathbf{h}(\mathbf{x}))) &\equiv f(\mathbf{g}(\mathbf{x}),h_1(\mathbf{x})^{q^n},\ldots,h_{b'}(\mathbf{x})^{q^n},0,\ldots,0) \pmod{(\mathbf{x})^{d_n}} \\ &\equiv \textstyle\sum_{|I|=M_1,|J|=M_2}A_{I,J}(\mathbf{c}_1^{q^n})\,\mathbf{x}^{I+q^nJ} \pmod{(\mathbf{x})^{M_1+q^nM_2+1}} \end{aligned}$$

for all $n\geq n_2$. The above congruence gives us equalities

$$\sum_{|I|=M_1,|J|=M_2}A_{I,J}(\mathbf{c}_1^{q^n})\,\mathbf{x}^{I+q^nJ}=0 \quad \forall\ n\geq n_2$$

in the polynomial ring $k[\mathbf{x}]$. If two pairs of indices (I_1,J_1), (I_2,J_2) both satisfy $|I_1|=|I_2|=M_1$, $|J_1|=|J_2|=M_2$, and $I_1+q^nJ_1=I_2+q^nJ_2$ for some $n\geq n_2$. Then $I_1=I_2$ and $J_1=J_2$ because $q^n>2M_1$. Therefore $A_{I,J}(\mathbf{c}_1^{q^n})=0$ if $|I|=M_1$, $|J|=M_2$, and $n\geq n_2$. By Prop. 2.2 applied to the polynomials $A_{I,J}(\mathbf{t}_1)\in k[\mathbf{t}]$ with $|I|=M_1$ and $|J|=M_2$, we deduce that $A_{I,J}(\mathbf{c}_1^{q^n})=0$ for all $n\in\mathbb{N}$ if $|I|=M_1$, $|J|=M_2$. This is a contradiction. □

Remark 3.1.1. (i) In the case when $a=b=b'$ and $g_i(\mathbf{x})=h_i(\mathbf{x})$ for $i=1,\ldots,a$, one can reformulate Prop. 3.1 as follows. Let $X=\mathrm{Spf}\ k[[u_1,\ldots,u_a]]$, and let $\Phi_n : X\to X$, $n\geq n_0$, be a family of morphisms which are very close to the Frobenius morphisms Fr_{q^n} as in the statement of Prop. 3.1, where $\mathrm{Fr}_{q^n}:X\to X$ corresponds to the k-endomorphism $u_i\mapsto u_i^{q^n}$ of the power series ring $k[[u_1,\ldots,u_a]]$. Then for any closed formal scheme Z of X, the schematic closure of the union of the graph of Φ_n, n running over all integers $n\geq n_0$, contains $Z\times Z$.

(ii) The assertion of Prop. 3.1 still holds if the assumption

$$f(\mathbf{g}(\mathbf{x}), \Phi_n(\mathbf{h}(\mathbf{x}))) = f\left(g_1(\mathbf{x}), \ldots, g_a(\mathbf{x}), \phi_{1,n}(h(\mathbf{x})), \ldots, \phi_{b,n}(h(\mathbf{x}))\right) = 0$$

for all $n \geq n_0$ is weakened to

$$f(\mathbf{g}(\mathbf{x}), \Phi_n(\mathbf{h}(\mathbf{x}))) = f\left(g_1(\mathbf{x}), \ldots, g_a(\mathbf{x}), \phi_{1,n}(h(\mathbf{x})), \ldots, \phi_{b,n}(h(\mathbf{x}))\right) \equiv 0 \pmod{(\mathbf{x})^{d_n}}$$

for all $n \geq n_0$. The same proof works.

4. The main rigidity result.

4.1. Let K be a field of characteristic 0. Let E be a finite dimensional algebra E over K, denote by $\underline{E}^\times$ the linear algebraic group over K such that $\underline{E}^\times(R) = (E \otimes_K R)^\times$ for any commutative K-algebra R. In particular $E^\times$ is the set of all K-rational points of $\underline{E}^\times$.

Let G be a connected linear algebraic group over K, and let $\rho : G \to \underline{E}^\times$ be a K-rational homomorphism between algebraic groups over K. Denote by $\mathfrak{g} = \mathrm{Lie}(G)$ the Lie algebra of G, and let $d\rho : \mathfrak{g} \to E$ be the differential of ρ. We regard ρ as a linear representation on E via the canonical embedding $\underline{E}^\times \subset \mathrm{GL}(E)$, where $\mathrm{GL}(E)$ is the general linear group over K attached to the K-vector space E.

Lemma 4.1.1. *Notation as above. Assume that E is a product of a finite number of finite dimensional central simple algebras over K. The following statements are equivalent:*

(i) *The trivial representation $\mathbf{1}_G$ is not a subquotient of (ρ, E).*

(ii) *There are elements $w_{i,j} \in \mathfrak{g}$, where $i = 1, \ldots, r$, $j = 1, \ldots, n_i$, such that*

$$\sum_{i=1}^{r} d\rho(w_{i,1}) \circ \cdots \circ d\rho(w_{i,n_i}) \in \mathrm{GL}(E)\,.$$

(iii) *There are elements $w_{i,j} \in \mathfrak{g}$, where $i = 1, \ldots, r$, $j = 1, \ldots, n_i$, such that*

$$\sum_{i=1}^{r} d\rho(w_{i,1}) \circ \cdots \circ d\rho(w_{i,n_i}) \in E^\times\,.$$

Proof. The implication (ii) $\Rightarrow$ (i) is obvious, so is (iii) $\Rightarrow$ (ii). It is clear that (ii) $\Rightarrow$ (iii) because $E \cap \mathrm{GL}(E) = E^\times$. It remains to show that (i) $\Rightarrow$ (ii).

Assume (i). Replacing the linear representation (ρ, E) by its semi-simplification, we may assume that (ρ, E) is isomorphic to a direct sum $\oplus_{m=1}^{b} (\rho_m, V_m)$ of irreducible representations of G. Each V_m is an irreducible $\mathfrak{g}$-module under $d\rho_m$. By Jacobson's density theorem, for each $m = 1, \ldots, b$, the statement (ii) holds with (ρ, E) replaced by (ρ_m, V_m). An application of Sublemma 4.1.2 with $r = b$ finishes the proof. ∎

4.1.2. Sublemma. *Let K be an infinite field. Let $V_1, \ldots, V_b$ be finite dimensional vector spaces over K, and let $A_1, \ldots, A_r$ be K-liner endomorphisms of $V = \oplus_{m=1}^{b} V_m$ such that $A_i(V_m) \subseteq V_m$ for each $i = 1, \ldots, r$ $m = 1, \ldots, b$. Assume that for each $m = 1, \ldots, b$, there exists an i, $1 \leq i \leq r$, such that $\det(A_i|V_m) \neq 0$. Then there exist elements $\lambda_1, \ldots, \lambda_r$ in K such that $\sum_{i=1}^{r} \lambda_i A_i \in \mathrm{GL}(V)$.*

Proof. Let $t_1, \ldots, t_r$ be variables, and consider the polynomial

$$f(t_1, \ldots, t_r) := \det\left(\sum_{i=1}^{r} t_i\, A_i\right) = \prod_{m=1}^{b} \det\left(\sum_{i=1}^{r} t_i\, A_i | V_m\right) \in K[t_1, \ldots, t_r]\,.$$

It suffices to show that $f(t_1, \ldots, t_r) \neq 0$: Every rational variety of positive dimension over an infinite field K has at least a K-rational point, and the variety $\mathrm{Spec}(K[t_1, \ldots, t_r, \frac{1}{f(t_1,\ldots,t_r)}])$ is clearly rational over K. For each $m = 1, \ldots, b$, the polynomial

$$f_m(t_1, \ldots, t_r) := \det(\sum_{i=1}^{r} t_i\, T_i | V_m) \in K[t_1, \ldots, t_r]$$

is not equal to zero by assumption, hence their product $f(t_1, \ldots, t_r)$ is not equal to zero. ∎

4.2. Let k be an algebraically closed field of characteristic $p > 0$. Let X be a finite dimensional p-divisible smooth formal group over k. Let $E_{\mathbb{Z}_p} = \mathrm{End}(X)$, and let $E = E_{\mathbb{Z}_p} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$; E is a product of central simple algebras over $\mathbb{Q}_p$, and $E_{\mathbb{Z}_p}$ is an order in E. Denote by $\underline{E}^{\times}$ the linear algebraic group over $\mathbb{Q}_p$ attached to E as in 4.1.

Let G be a connected linear algebraic group over $\mathbb{Q}_p$, and let $\rho : G \to \underline{E}^{\times}$ be a $\mathbb{Q}_p$-rational homomorphism between algebraic groups over $\mathbb{Q}_p$. Let $\mathfrak{g} = \mathrm{Lie}(G)$ and let $d\rho : \mathfrak{g} \to E$ be the differential of ρ as in 4.1. Let $G(\mathbb{Z}_p) = \rho^{-1}(E_{\mathbb{Z}_p}^{\times})$ be the inverse image of the units of $E_{\mathbb{Z}_p}^{\times}$ under ρ. Let $\mathfrak{g}_{\mathbb{Z}_p} = d\rho^{-1}(E_{\mathbb{Z}_p})$, a $\mathbb{Z}_p$-lattice in $\mathfrak{g}$. The compact p-adic group $G(\mathbb{Z}_p)$ operates on the p-divisible formal group X via ρ. For each element $w \in \mathfrak{g}_{\mathbb{Z}_p}$, denote by $\alpha(w)$ the endomorphism of the p-divisible formal group X given by $\mathrm{d}\rho(w)$.

Theorem 4.3. *Notation as above. Assume that the trivial representation $\mathbf{1}_G$ is not a subquotient of (ρ, E). Suppose that Z is a reduced and irreducible closed formal subscheme of the p-divisible formal group X which is closed under the action of an open subgroup U of $G(\mathbb{Z}_p)$. Then Z is stable under the group law of X and hence is a p-divisible smooth formal subgroup of X.*

Proof. We must show that Z is stable under the group law $\mu : X \times X \to X$ of X. Replacing X by a suitable p-divisible formal group isogenous to X, we may and do assume that X is isomorphic to the product of p-divisible formal groups $X_1, \ldots, X_e$ over k such that there exist natural numbers $0 < s \leq r_1 < \cdots < r_e$ such that

$$\mathrm{Ker}\,([p^s]_{X_i}) = \mathrm{Ker}\left(\mathrm{Fr}_{p^{r_i}, X_i/k}\right)$$

for $i = 1, \ldots, e$. In other words each X_i is isoclinic of Frobenius slope $\frac{s}{r_i}$, and the r_i-th iterate of the relative Frobenius of X_i is exactly divisible by p^s.

Since $X = X_1 \times \cdots \times X_e$ and the slopes $\frac{s}{r_i}$ are distinct, we have natural decompositions $E = E_1 \times \cdots E_e$ and $E_{\mathbb{Z}_p} = E_{1,\mathbb{Z}_p} \times \cdots E_{e,\mathbb{Z}_p}$, where $E_{i,\mathbb{Z}_p} = \mathrm{End}(X_i)$ and $E_i = E_{i,\mathbb{Z}_p} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ for $i = 1, \ldots, e$. Denote by $\mathrm{pr}_i : E \to E_i$ and $\mathrm{pr}_i : X \to X_i$ the projection to the i-th factor for E and X respectively, $i = 1, \ldots, e$. To simplify some later formulas, we assume that $E_{i,\mathbb{Z}_p}$ is a maximal order in E_i for each i; this can be achieved by modifying X_j with a suitable isogeny.

Recall that $\mathfrak{g}_{\mathbb{Z}_p} = d\rho^{-1}(E_{\mathbb{Z}_p})$, a $\mathbb{Z}_p$-lattice in the Lie algebra $\mathfrak{g}$ of G, and the p-adic group $G(\mathbb{Z}_p)$ is the inverse image of $(E_{\mathbb{Z}_p})^\times$ in $G(\mathbb{Q}_p)$. Choose an integer $n_0 \geq 2$ such that $\exp_G(p^{n_0}w) \in U \subseteq G(\mathbb{Z}_p)$ for every $w \in \mathfrak{g}_{\mathbb{Z}_p}$. The rest of the proof is organized into several steps. Among them the first step is the crucial one; it uses Prop. 2.1 and Prop. 3.1.

Step 1. Let $w \in \mathrm{pr}_1(d\rho(\mathfrak{g}_{\mathbb{Z}_p}))$, that is w is the first projection of some element of $d\rho(\mathfrak{p}_{\mathbb{Z}_p})$. Then

$$\mu \circ (\mathrm{Id} \times \alpha(w))(Z \times Z) \subseteq Z\,.$$

We recall that $\alpha(w)$ is the endomorphism of X induced by the w, an endomorphism of X_1.

Proof of Step 1. Choose coordinates $u_1, \ldots, u_d$ for X_1 and similarly choose coordinates for $X_2, \ldots, X_e$. Put these coordinate together, we obtain a system of coordinates $u_1, \ldots, u_d, u_{d+1}, \ldots, u_a$ of X, so that $X_1 = \mathrm{Spf}(k[[u_1, \ldots, u_d]])$ and $X = \mathrm{Spf}(k[[u_1, \ldots, u_a]])$. We may and do assume that the coordinate system $\mathbf{u}_j$ for X_j has the property that the endomorphism $[p^s]_{X_j}$ corresponds to the endomorphism $\mathbf{u}_j \mapsto \mathbf{u}_j^{p^{r_j}}$ for each $j = 1, \ldots, e$. Let

$$\mu^* : k[[u_1, \ldots, u_a]] \to k[[u_1, \ldots, u_a, v_1, \ldots, v_a]]$$

be the comutliplication for the p-divisible formal group X. The closed formal subscheme $Z \subseteq X$ corresponds to a prime ideal P of $k[[u_1, \ldots, u_a]]$. Prop. 2.1 gives an injective k-algebra homomorphism

$$\iota \,:\, k[[u_1 \ldots, u_a]]/P \hookrightarrow k[[x_1, \ldots, x_m]] \quad m = \dim(Z)\,.$$

Let $g_i(\mathbf{x}) = \iota(u_i)$, $i = 1, \ldots, a$, where $\mathbf{x} = (x_1, \ldots, x_m)$. For any given element $f_1(\mathbf{u}) \in P$, we want to show that the element $f_2(\mathbf{u}, \mathbf{v}) := (\mathrm{Id} \times \alpha(w))^* \circ \mu^*(f_1)$ of $k[[\mathbf{u}, \mathbf{v}]]$ lies in the ideal generated by P_1 and P_2, where $P_1 = i_1(P)k[[\mathbf{u}, \mathbf{v}]]$, $P_2 = i_2(P)k[[\mathbf{u}, \mathbf{v}]]$, and $i_1, i_2 : k[[\mathbf{u}]] \to k[[\mathbf{u}, \mathbf{v}]]$ are the two continuous homomorphisms with $u_j \mapsto u_j$ and $u_j \mapsto v_j$ respectively, for all $j = 1, \ldots, a$. Equivalently, we must show that $f_2(g_1(\mathbf{x}), \ldots, g_a(\mathbf{x}), g_1(\mathbf{y}), \ldots, g_a(\mathbf{y})) = 0$ in $k[[\mathbf{x}, \mathbf{y}]]$, where $\mathbf{y} = (y_1, \ldots, y_m)$ is another set of variables. Notice that for any element $w' \in E_{2,\mathbb{Z}_p} \times \cdots \times E_{e,\mathbb{Z}_p}$, we have

$$\begin{aligned}((\mathrm{Id} \times \alpha(w + w'))^*(f_1))(g_1(\mathbf{x}), \ldots, g_a(\mathbf{x}), g_1(\mathbf{y}), \ldots, g_d(\mathbf{y}), 0, \ldots, 0)\\ = f_2(g_1(\mathbf{x}), \ldots, g_a(\mathbf{x}), g_1(\mathbf{y}), \ldots, g_a(\mathbf{y}))\,.\end{aligned}$$

For each $\xi \in \mathfrak{g}_{\mathbb{Z}_p}$ and $n \geq n_0$, we know that $\exp_G(p^n\xi) \in U$ if $n \geq n_0$, therefore

$$\begin{aligned}\rho(\exp_G(p^n\xi)) &= \mathrm{Id} + d\rho(\xi) \cdot \textstyle\sum_{i \geq 1} \frac{p^{in}}{i!}\, d\rho(\xi)^{i-1}\\ &= \mathrm{Id} + d\rho(\xi) \left(p^n \cdot \mathrm{Id} + \frac{p^{2n}}{2!}\, d\rho(\xi) + \frac{p^{3n}}{3!}\, d\rho(\xi)^2 + \cdots\right)\,.\end{aligned}$$

Since $n \geq n_0 \geq 2$, we have $\lim_{i \to \infty} \frac{p^{in}}{i!} = 0$ in $\mathbb{Z}_p$ by the following estimate on the p-adic valuation ord_p of $\frac{p^{in}}{i!}$:

$$\mathrm{ord}_p\left(\frac{p^{in}}{i!}\right) = in - \sum_{m \geq 1} \left\lfloor \frac{i}{p^m} \right\rfloor \geq in - \frac{i}{p-1}\,.$$

We also have $\frac{p^{in}}{i!} \in \mathbb{Z}_p$ for each $i \geq 1$. So

$$\mathbb{E}(p^n\xi) := \sum_{i\geq 1} \frac{p^{in}}{n!}\, d\rho(\xi)^{i-1} \ \in \ E_{\mathbb{Z}_p}\,.$$

Write $\mathbb{E}(p^n\xi) = \sum_{j=1}^{e} \eta_j(p^n\xi)$ with $\eta_j(p^n\xi) \in E_{j,\mathbb{Z}_p}$ for $j = 1,\dots,e$. The argument above shows that

$$\eta_j(p^n\xi) \equiv [p^n]_{X_j} \pmod{p^{2n-\lfloor\frac{2}{p-1}\rfloor} E_{j,\mathbb{Z}_p}} \qquad j = 1,\dots,e\,.$$

So the endomorphism $\eta_j(p^{sn}\xi)^*$ of the coordinate ring $k[[\mathbf{u}_j]]$ of X_j corresponding to $\eta_j(p^{sn}\xi)$ has the form

$$\mathbf{u}_j \ \mapsto \ \mathbf{u}_j^{r_j n} + \mathbf{Q}_j(\mathbf{u}_j)$$

with all components of the "error term" $\mathbf{Q}_j(p^{sn}\xi)(\mathbf{u}_j)$ in $(\mathbf{u}_j)^{p^{2r_j - \lceil \frac{r_j}{s} \lfloor \frac{2}{(p-1)} \rfloor \rceil}}$. Therefore there exist natural numbers $n_1 \geq n_0$ and δ such that all components of $\eta_j(p^{sn}\xi)^*$ are in $(\mathbf{u}_j)^{p^{r_j n}}$ if $n \geq n_1$ and $j = 2,\dots,e$, and all components of the error term $\eta_1(p^{sn}\xi)^*(\mathbf{u}_1)$ are in $(\mathbf{u}_1)^{p^{2r_1 n-\delta}}$ if $n \geq n_1$.

Suppose that the given element $w \in \mathrm{pr}_1(d\rho(\mathfrak{g}_{\mathbb{Z}_p}))$ is equal to $\mathrm{pr}_1(d\rho(\xi))$, $\xi \in \mathfrak{g}_{\mathbb{Z}_p}$. Write $d\rho(\xi) = w + w_2 + \cdots + w_e$ with $w_j = \mathrm{pr}_j(d\rho(\xi))$ for $j = 2,\dots,e$. Then

$$\rho(\exp_G(p^{sn}\xi)) = \mathrm{Id} + (w + w_2 + \cdots + w_e)\cdot \mathbb{E}(p^{sn}\xi)\,.$$

For every $n \geq n_1$, and each $i = 1,\dots,a$, let

$$\phi_{i,n}(\mathbf{u}) = \mathbb{E}(p^{sn}\xi)^*(u_i)\,.$$

Let $r = r_1$. Let

$$R_{i,n}(\mathbf{u}) = \begin{cases} \phi_{i,n}(\mathbf{u}) - u_i^{p^{rn}} & \text{if} \quad 1 \leq i \leq d = \dim(X_1) \\ \phi_{i,n}(\mathbf{u}) & \text{if} \quad d+1 \leq i \leq a = \dim(X)\,. \end{cases}$$

Define a sequence $(d_n)_{n\geq n_1}$ of natural numbers by $d_n = p^{\min(2rn-\delta,\, r_2)}$. Clearly $\lim_{n\to\infty} \frac{p^{rn}}{d_n} = 0$. Our previous estimates about $\mathbf{Q}_j(p^{sn}\xi)(\mathbf{u}_j)$ and $\eta_1(p^{sn}\xi)^*(\mathbf{u}_1)$ tell us that $R_{i,n}(\mathbf{u}) \equiv 0 \pmod{(\mathbf{u})^{d_n}}$ for all $n \geq n_1$ and for all $i = 1,\dots,a$.

Let $f(\mathbf{u},\mathbf{v}) = (\mathrm{Id}\times d\rho(\xi))^*(f_1) \in k[[\mathbf{u},\mathbf{v}]]$, where f_1 is any given element of the prime ideal P defining the irreducible closed formal subscheme $Z \subseteq X$. Recall that our goal is to show that

$$f(g_1(\mathbf{x}),\dots,g_a(\mathbf{x}),g_1(\mathbf{y}),\dots,g_d(\mathbf{y}),0,\dots,0) = 0$$

in $k[[\mathbf{x},\mathbf{y}]]$. We have

$$f(g_1(\mathbf{x}),\dots,g_a(\mathbf{x}),\phi_{1,n}(\mathbf{x}),\dots,\phi_{a,n}(\mathbf{x})) = f_1(\rho(\exp_G(p^{sn}\xi))\cdot \mathbf{x}) = 0$$

for all $n \geq n_1$. Now we can apply Prop. 3.1 and conclude that

$$f(g_1(\mathbf{x}),\dots,g_a(\mathbf{x}),g_1(\mathbf{y}),\dots,g_d(\mathbf{y}),0,\dots,0) = 0$$

in $k[[\mathbf{x}]]$. We have finished the proof of Step 1.

Step 2. Let $(w_{i,j})$, $i = 1, \dots, r$, $j = 1, \dots, n_i$ be a finite family of elements in $\mathrm{pr}_1(d\rho(\mathfrak{g}_{\mathbb{Z}_p}))$. Consider the following homomorphism

$$\begin{array}{cccc} s & : & \overbrace{X \times \cdots \times X}^{\text{(r+1)}-\text{times}} & \longrightarrow & X \\ & & (x_0, x_1, \dots, x_r) & \mapsto & x_0 + \sum_{i=1}^{r} \alpha(w_{i,1}) \circ \cdots \alpha(w_{i,n_i})(x_i) \end{array}$$

of p-divisible formal groups over k Then $s(Z \times Z \times \cdots \times Z) \subseteq Z$. In particular we have $\sigma(Z \times Z) \subseteq Z$, where

$$\sigma : X \times X \to X$$

is the homomorphism of formal groups defined by

$$\sigma \, : \, (x, y) \, \mapsto \, x + \sum_{i=1}^{a} \alpha(w_{i,1}) \circ \cdots \alpha(w_{i,n_i})(y) \, .$$

Proof of Step 2. One sees from Step 1 that the assertion in Step 2 holds when $r = 1 = n$. An easy induction on r and n finishes the proof.

Step 3. Let Z_1 be the schematic closure in X_1 of the projection to the first factor X_1 of X. $\mathrm{pr}_1|_Z : Z \to X_1$.

(i) The irreducible formal subscheme $Z_1 \subset X_1$ is stable under the group law of X_1, hence Z_1 is a smooth formal subgroup of X_1.
(ii) Under the group law μ of X, we have $\mu(Z \times Z_1) \subseteq Z$. In other words Z is stable under addition with the smooth formal subgroup Z_1 of $X_1 \subseteq X$.

Proof of Step 3. According to Lemma 4.1.1, one can find $w_{i,j} \in \mathrm{pr}_1(d\rho(\mathfrak{g}_{\mathbb{Z}_p}))$, $i = 1, \dots, r$, $j = 1, \dots, n_i$, such that the element

$$A := \sum_{i=1}^{r} \alpha(w_{i,1}) \circ \cdots \circ \alpha(w_{i,n_i})$$

is an isogeny of X_1. Let $\alpha : X_1 \to X_1$ be the endomorphism of X_1 induced by A. Then $\mathrm{Id} \times \alpha : Z_1 \times Z_1 \to Z_1 \times Z_1$ is a dominant morphism. By Step 2, $\mu \circ (\mathrm{Id} \times \alpha)(Z \times Z_1) \subseteq Z$. Therefore $\mu(Z \times Z_1) \subseteq Z$ and $\mu(Z_1 \times Z_1) \subseteq Z_1$.

Since Z_1 is stable under addition, so is $Z_1 \cap X_1[p^n]$ for every $n \in \mathbb{N}$. Since $[-1] = [p^n - 1]$ on $Z_1 \cap X_1[p^n]$ for every $n \in \mathbb{N}$, $Z_1 \cap X_1[p^n]$ is a subgroup of $X_1[p^n]$ for every $n \in \mathbb{N}$. Hence Z is a subgroup of X_1. We have proved Step 3.

Step 4. The irreducible closed formal subscheme $Z \subseteq X$ is equal to the product $Z_1 \times Z'$ for a closed irreducible subscheme $Z' \subseteq X' = X_1 \times \cdots \times X_e$. Moreover Z' is stable under the action of the open subgroup $G(\mathbb{Z}_p) \subseteq G(\mathbb{Q}_p)$ induced by the composition $G \xrightarrow{\rho} \underline{E}^{\times} \xrightarrow{\mathrm{pr}'} \underline{E'}^{\times}$, where $E' = E_2 \times \cdots \times E_e$, and $\mathrm{pr}' : E = E_1 \times E' \to E'$ is the projection from E to E'.

This statement follows formally from Step 3. The formal subscheme $Z' \subseteq X'$ is equal to the image of Z under the projection map $\mathrm{pr}' : X \to X' = X_2 \times \cdots \times X_e$.

End of Proof of Theorem 4.3. Apply the argument of the above steps to the irreducible closed formal subscheme Z' of X', we see that Z' is a product of a smooth formal subgroup $Z_2 \subseteq X_2$ with an irreducible closed formal subgroup

$Z'' \subset X_3 \times \cdots \times X_e$. An induction on the number of isoclinic factors of X finishes the proof. □

REMARK 4.3.1. For application to the Hecke orbit problem, one only needs Thm. 4.3 when Z is formally smooth over k. Prop. 2.1 is not needed if Z is known to be smooth. In some sense the effect of Prop. 2.1 is to reduce the proof of Thm. 4.3 to the case when Z is formally smooth over k.

REMARK 4.3.2. A precursor of Thm. 4.3 appeared as Prop. 4 on page 471 of [1], however the point there is that the automorphism group is *big* — about the same size as the formal torus in question.

REFERENCES

[1] C.-L. CHAI, *Every ordinary symplectic isogeny class in positive characteristic is dense in the moduli*, Invent. Math., 121 (1995), pp. 439–479.

[2] C.-L. CHAI, *Monodromy of Hecke-invariant subvarieties*, Quaterly J. Pure Applied Math., 1 (2005), Borel Special Issue, part I, pp. 291–303.

[3] C.-L. CHAI, *Hecke orbits on Siegel modular varieties*, Geometric Methods in Algebra and Number Theory, Progress in Math., 235, pp. 71–107, Springer-Verlag, 2004.

[4] C.-L. CHAI, *Hecke orbits as Shimura varieties in positive characteristic,* Proc. ICM Madrid 2006, vol. II, pp. 295–312, European Math. Soc. 2006.

[5] C.-L. CHAI, *Families of ordinary abelian varieties: canonical coordinates, p-adic monodromy, Tate-linear subvarieties and Hecke orbits*, Preprint, 2003, 53 pages. Available from `http://www.math.upenn.edu/~chai`

[6] C.-L. CHAI, *Canonical coordinates on leaves: The two-slope case*, preprint, 77 pp., January 10, 2005. Available from `http://www.math.upenn.edu/~chai`

[7] C.-L. CHAI AND F. OORT, *Moduli of abelian varieties and p-divisible groups: Density of Hecke orbits, and a conjecture of Grothendieck*, to appear in the "Proceedings of Clay Mathematics Institute 2006 Summer School on Arithmetic Geometry".

[8] C.-L. CHAI AND F. OORT, *Hecke Orbits*, monograph in preparation.

[9] H. HIDA, *The Iwasawa μ-invariant of p-adic Hecke L-functions*, to appear in Ann. of Math.

[10] F. OORT, *Foliation in moduli spaces of abelian varieties*, J. Amer. Math. Soc., 17, pp. 267–296.