RIGIDITY FOR BIEXTENSIONS OF FORMAL GROUPS

CHING-LI CHAI[1] & FRANS OORT

version 4c, 01/04/2017

This is a draft version for part of a chapter on local rigidity in the *Hecke Orbits* book project of the authors.

§1. Introduction

Let p be a prime number, fixed throughout this article..

Given three commutative group schemes X, Y, Z over a base field k, a *biextension* of $X \times Y$ by Z is a morphism $E \to X \times Y$ plus two relative group laws. The first group law, for $E \to Y$, makes $E \to Y$ an extension of $X_Y := X \times Y$ by $Z_Y := Z \times Y$, while the second group law, for $E \to X$, makes $E \to X$ and extension of Y_X by Z_X. The best-known example is the Poincare bundle for an abelian variety A; it is a biextension of $A \times A^t$ by $\mathbb{G}_m$, where A^t is the dual abelian variety of A. Mumford invented the concept of bi-extension in [6] to treat deformation and lifting problems for polarized abelian varieties. In standard applications of biextensions the "fiber group" Z is usually $\mathbb{G}_m$.

Biextensions also arise when one tries to deform a p-divisible group in such a way that all p-adic invariants of the deformed p-divisible group are fixed. Suppose that U_1, U_2, U_3 are three isoclinic p-divisible formal groups over a perfect field $k \supset \mathbb{F}_p$, such that

$$\mathrm{slope}(U_1) > \mathrm{slope}(U_2) > \mathrm{slope}(U_3).$$

The equi-characteristic-p deformation space $\mathcal{D} = \mathrm{Def}(U_1 \times U_2 \times U_3)$ of the product $U_1 \times U_2 \times U_3$ is a smooth formal scheme. There exists a closed formal subscheme $\mathcal{S} = \mathcal{S}(U_1 \times U_2 \times U_3)$ of $\mathcal{D}$ such that the restriction to $\mathcal{S}$ of the universal p-divisible group $\mathcal{U}$ is *sustained*, and every closed subscheme $\mathcal{S}'$ with this property is contained is $\mathcal{S}$. That $\mathcal{U}|_{\mathcal{S}}$ is sustained means that for every $n \in \mathbb{N}$, there exists a faithfully flat cover $\mathcal{T} \to \mathcal{S}$ such that $\mathcal{U}[p^n] \times_{\mathcal{S}} \mathcal{T}$ is isomorphic to $(U_1 \times U_2 \times U_3) \times_{\mathrm{Spec}(k)} \mathcal{T}$. Similarly one has the maximal sustained locus $\mathcal{S}(U_i \times U_j)$ in the deformation space $\mathcal{D}(U_i \times U_j)$ for any pair (i, j) with $1 \le i < j \le 3$. We will call $\mathcal{S}(U_1 \times U_2 \times U_3)$ the (central) *leaf* in the deformation sapce $\mathrm{Def}(U_1 \times U_2 \times U_3)$ which passes through the closed point. Similarly $\mathcal{S}(U_i \times U_j)$ is the leaf in $\mathrm{Def}(U_i \times U_j)$ through the closed point.

It turn out that in the two-slope case, the leaf $\mathcal{S}(U_i \times U_j)$ has a natural structure as an isoclinic p-divisible group whose slope is equal to $\mathrm{slope}(U_i) - \mathrm{slope}(U_j)$ for any pair (i, j) with $1 \le i \le j \le 3$. In the three-slope case, the leaf $\mathcal{S}(U_1 \times U_2 \times U_3)$ is not a p-divisible group, but it has a natural structure as a biextension of p-divisible formal groups: there exists a canonical morphism

$$\pi : \mathcal{S}(U_1 \times U_2 \times U_3) \to \mathcal{S}(U_1 \times U_2) \times \mathcal{S}(U_2 \times U_3)$$

plus two relative group laws

$$+_1 : \mathcal{S}(U_1 \times U_2 \times U_3) \times_{\times \mathcal{S}(U_2 \times U_3)} \mathcal{S}(U_1 \times U_2 \times U_3) \to \mathcal{S}(U_1 \times U_2 \times U_3)$$

and

$$+_2 : \mathcal{S}(U_1 \times U_2 \times U_3) \times_{\times \mathcal{S}(U_1 \times U_2)} \mathcal{S}(U_1 \times U_2 \times U_3) \to \mathcal{S}(U_1 \times U_2 \times U_3),$$

making $\mathcal{S}(U_1 \times U_2 \times U_3)$ a biextension of $\mathcal{S}(U_1 \times U_2) \times \mathcal{S}(U_2 \times U_3)$ by $\mathcal{S}(U_1 \times U_3)$.

Suppose that G is a closed subgroup of the group $\mathrm{Aut}(U_1 \times U_2 \times U_3)$ of automorphisms of the p-divisible group $U_1 \times U_2 \times U_3$. By functoriality the group G also acts on $\mathcal{S}(U_1 \times U_2 \times U_3)$ We assume that the action of G on $\mathcal{S}(U_1 \times U_2 \times U_3)$ is *strongly nontrivial*, in the sense that there is no open subgroup of G which fixes all points of a non-trivial p-divisible subgroup of $\mathcal{S}(U_i \times U_j)$ for some pair (i, j) with $1 \leq i < j \leq 3$. The goal of the local rigidity problem for this biextension is:

Question (**local rigidity for** the **biextension** $\mathcal{S}(U_1 \times U_2 \times U_3)$). *Find a sharp constraint on formal subvarieties of the biextension $\mathcal{S}(U_1 \times U_2 \times U_3)$ which are stable under a strongly non-trivial action by a p-adic Lie group G.*

More generally one can ask the local rigidity question for general biextensions of p-divisible formal groups. One can also ask the (easier) local rigidity question for the leaves $\mathcal{S}(U_i \times U_j)$, $1 \leq i \leq j \leq 3$. Recall that $\mathcal{S}(U_i \times U_j)$ is a p-divisible formal group, and local rigidity question for p-divisible groups has a clean answer; see [3, Thm. 4.3].

THEOREM (local rigidity for p-divisible formal groups). *Suppose that G is a p-adic Lie group acting strongly nontrivially on a p-divisible formal group V over a base field $k \supset \mathbb{F}_p$. Every formal subvariety of V which is stable under the action of G is a p-divisible subgroup of V.*

For a long time it was unclear whether there is a good answer to the local rigidity question for biextensions of p-divisible formal groups. It turns out that the outline of the argument in [3] can be followed, but new ideas are needed to analyse the asymptotic behavior of the action on the biextension by elements sufficiently close to 1 in a one-parameter subgroup .

Suppose that a p-adic Lie group G acts on a p-divisible group V, and w is an element of the Lie algebra of G which operates on V through an endomorphism $C \in \mathrm{End}(V)$. Let V_1 be the largest among isoclinic subgroups of whose slope μ_1 is bigger than other slopes of V. Assume that V is the product of V_1 and another p-divisible subgroup V_2 of V, and let $\mathrm{pr}_{V_1} : V \to V_1$ be the projection to V_1. Then for all $n \gg 0$, the action of the element $\exp(p^n w) \in G$ on V is very closely approximated by $\mathrm{Id}_V + p^n \cdot C|_{V_1} \circ \mathrm{pr}_{V_1}$. The precise meaning of "very closely approximated" is provided by the following estimates for the "main term" $p^n \cdot C|_{V_1} \circ \mathrm{pr}_{V_1}$ and the difference of $\exp(p^n w)$ and $\mathrm{Id}_V + p^n \cdot C|_{V_1} \circ \mathrm{pr}_{V_1}$. The size of the main term and the error term will be estimated by powers of the maximal ideal $\mathfrak{m} = \mathfrak{m}_V$

- There are constants $c_1, c_2 \in \mathbb{N}_{>0}$ such that the main term $p^n C \cdot |_{V_1} \circ \mathrm{pr}_{V_1}$ has coordinates in $\mathfrak{m}^{c_1 \cdot p^{\lfloor n/\mu_1 \rfloor}}$ and is non-zero modulo $\mathfrak{m}^{c_1 \cdot p^{\lfloor n/\mu_1 \rfloor} + c_2}$, for all $n \gg 0$.

- There is a constant μ_2 with $0 < \mu_2 < \mu_1$ such that the error term

$$\exp(p^n w) - \mathrm{Id}_V - p^n \cdot C|_{V_1} \circ \mathrm{pr}_{V_1}$$

  is congruent to 0 modulo $\mathfrak{m}^{p^{\lfloor n/\mu_2 \rfloor}}$ for all $n \gg 0$.

With the above analysis of the action by a one-parameter subgroup, one is in a position to apply the *identity principle* [3, 3.1], recalled in 6.1.1, to conclude that the given formal subvariety of V stable under G is stable under translation by elements of the p-divisible subgroup $C \cdot V_1$ of V.

For the case of a biextension $\pi : E \to X \times Y$ of two p-visible formal groups X, Y by a p-divisible formal group Z, one does not have an analog of "the projection from E to the isoclinic factor of Z of maximal slope", nor an analog of "the projection to Z" for that matter, no matter how one modifies E by isogenies. The first step to deal with this difficulty is the construction of a morphism $\eta_n : \pi^{-1}(X[p^n] \times Y[p^n]) \to Z$ in 2.7. After modifying Z by a suitable isogeny so that Z is a product of Z_1 with a p-divisible subgroup Z_2 of Z, we can compose η_n with the projection pr_1 from Z to Z_1, and obtain a morphism $\rho_n' : \pi^{-1}(X[p^n] \times Y[p^n]) \to Z_1$. This morphism ρ_n' is an analog of $p^n \cdot \mathrm{pr}_{V_1}$ (but not pr_{V_1}).

To make use of the maps ρ_n', one needs the existence of a single object $\tilde{\rho}$ such that each ρ_n' "is" $p^n \cdot \tilde{\rho}$ in a suitable sense. To figure out where this animal $\tilde{\rho}$ might be found, we first remind ourselves that if we choose a coordinate system for Z_1, a map from E to Z_1 is determined by a sequence of functions on E, one for each coordinate of Z_1. If we think of the coordinate ring of E, which is isomorphic to a power series ring $k[[t_1, \ldots, t_m]]$, as functions on E, what we need is to introduce a suitable ring of "generalized functions". Then we can define the sought-after object $\tilde{\rho}$ as a "generalized map" whose components with respect to the chosen coordinate system for Z_1 are generalized functions.

There are a few related procedures, each depending on some parameters, which take Noetherian complete equi-characteristic-p local domains as input, and produce "generalized functions" as outputs. We call the resulting rings *complete restricted perfections* of the input, because they are completions of suitable subrings of the perfection of the input complete local domains. Here we provide a sample, denoted by $k\langle\langle t_1^{p^{-\infty}}, \ldots, t_m^{p^{-\infty}}\rangle\rangle_{C;d}^{E,\flat}$, The where $E > 0, C \geq 1, d \geq 0$ are real parameters. The *support set* $\mathrm{supp}(m : E; C, d)$ for this ring is a subset of $\mathbb{Z}[1/p]_{\geq 0}$, defined by

$$\mathrm{supp}(m : E; C, d) = \left\{ I \in \mathbb{Z}[1/p]_{\geq 0}^m \colon |I|_p \leq C \cdot (|I|_\sigma + d)^E \right\}.$$

Here for any $I = (i_1, \ldots, i_m) \in \mathbb{Z}[1/p]_{\geq 0}$, $|I|_\sigma := i_1 + \cdots + i_m$ is the usual archimedean norm of I, $|I|_p = \max(|i_1|_p, \ldots, |i_m|_p)$ is the normalized p-adic norm of I, and $|\cdot|_p$ is the normalized p-adic absolute value on $\mathbb{Q}$ with $|p|_p = 1/p$. By definition

$$k\langle\langle t_1^{p^{-\infty}}, \ldots, t_m^{p^{-\infty}}\rangle\rangle_{C;d}^{E,\flat} := \Big\{ \sum_{I \in \mathrm{supp}(m:E;C,d)} a_I \cdot \underline{t}^I \mid a_I \in k \ \ \forall I \in \mathrm{supp}(m : E; C, d) \Big\},$$

where $\underline{t}^I$ stands for the monomial $\underline{t}^I = t_1^{i_1} \cdots t_m^{i_m}$ for every $I = (i_1, \ldots, t_m) \in \mathbb{Z}[1/p]_{\geq 0}^m$. The standard formula for multiplication of formal series make sense in the ring $k\langle\langle t_1^{p^{-\infty}}, \ldots, t_m^{p^{-\infty}}\rangle\rangle_{C;d}^{E,\flat}$. One can also compose generalized function, and substitute the variables $t_1, \ldots, t_m$ of an element

$$f \in k\langle\langle t_1^{p^{-\infty}}, \ldots, t_m^{p^{-\infty}}\rangle\rangle_{C;d}^{E,\flat}$$

by elements $g_1, \ldots, g_m \in k\langle\langle u_1^{p^{-\infty}}, \ldots, u_n^{p^{-\infty}}\rangle\rangle_{C_1;d_1}^{E_1,\flat}$. The result is a function

$$f(g_1(\underline{u}), \ldots, g_m(\underline{u})) \in k\langle\langle u_1^{p^{-\infty}}, \ldots, u_n^{p^{-\infty}}\rangle\rangle_{C_2;d_2}^{E_2,\flat}$$

for suitable parameters E_2, C_2, d_2. Details about the construction of the coordinates of $\tilde{\rho}$ in suitable complete restricted perfections are explained in §3. Basic properties of complete restricted perfections are in §3 and §4. The identity principle in [3, 3.1] is extended to complete restricted perfection of complete equi-characteristic-p local rings in 6.4.

We don't know whether the rings $\kappa\langle\langle t_1^{p^{-\infty}},\ldots,t_m^{p^{-\infty}}\rangle\rangle_{C;d}^{E,\flat}$ have applications to other problems. These local rings are not Noetherian, but smaller and more manageable than the completion of the perfection $\kappa[t_1^{-\infty},\ldots,t_m^{-p^{\infty}}]$ $\kappa[t_1,\ldots,t_m]$ with respect to the filtration given by the total degree of monomials. We provide a form of the Weierstrass preparation theorem for these rings and compute the integral closure of $\kappa\langle\langle t_1^{p^{-\infty}},\ldots,t_m^{p^{-\infty}}\rangle\rangle_{C;d}^{E,\flat}$ in its field of fractions, in 4.4.2 and 4.5 respectively. These two results are not needed for rigidity of biextensions. Most of the basic algebraic properties of these rings are still unexplored.

Armed with the above tools, the same train of thoughts in the proof of local rigidity for p-divisible group leads to a satisfactory answer of the local rigidity question for biextensions of p-divisible formal groups, theorems 7.2 and 7.5. The latter is easy to state: *in a biextension E of p-divisible formal groups $X\times Y$ by Z such that X, Y, Z have mutually distinct slopes, every formal subvariety of E which is stable under a strongly non-trivial action of a p-adic Lie group is a sub-biextension.*

From the perspective of the Hecke orbit problem, a good answer to the local rigidity question for leaves in deformation spaces of p-divisible groups is quite useful. It provides a tight structural constraint on what the Zariski closure of a Hecke orbit can possibly be, when examined at any $\overline{\mathbb{F}}_p$-point of the intersection of the Zariski closure of the given Hecke orbit with the leaf containing the Hecke orbit. It is hoped that the tools introduced to solve the three-slope case will bring us closer to the answer of the general local rigidity problem for leaves in deformation spaces of p-divisible groups.

§2. Biextension basics

The notion of biextensions of commutative groups was first introduced by Mumford in [6] and further developed by Grothendieck in expositions VI, VII of [5].

(2.1) Definition. Let R be a noetherian complete local ring whose residue $R/\mathfrak{m}$ is a field of characteristic p, and $S:=\mathrm{Spf}(R)$. Let X,Y,Z be p-divisible groups over R (resp. commutative formal groups) over R. A *biextension* of $X\times_S Y$ by Z is a 5-tuple

$$(\pi: E\to X\times_S Y,\ +_1: E\times_Y E\to E,\ +_2: E\times_X E\to E,\ \varepsilon_1: Y\to E,\ \varepsilon_2: X\to E)$$

where E is the formal spectrum of a Noetherian complete local ring formally smooth over R, π is an S-morphism, $+_1$ and ε_1 are Y-morphisms, $+_2$ and ε_2 are X-morphisms. In addition the following properties are satisfied.

(0) The morphism π is formally smooth and faithfully flat.

(1a) The pair $(+_1,\varepsilon_1)$ makes E a p-divisible group (resp. commutative smooth formal group) over Y.

(1b) The projection map $\pi: E\to X\times_S Y$ is a group homomorphism for the group law $+_1$ and the base change to Y of the group law $+_X: X\times_S X\to X$ of the p-divisible group X.

(2a) The pair $(+_2, \varepsilon_2)$ makes E a p-divisible group (resp. commutative smooth formal group) over X.

(2b) The projection map $\pi : E \to X \times_S Y$ is a group homomorphism for the group law $+_2$ and the base change to X of the group law $+_Y : Y \times_S Y \to Y$ of the p-divisible group Y.

(3a) The S-morphism

$$Z \times_S Y \to E, \quad (z, y) \mapsto z +_2 \varepsilon_1(y)$$

defines an S-isomorphism from $Z \times_S Y$ to $E \times_{(X \times_S Y)} (0_X \times_S Y)$.

(3b) The S-morphism

$$Z \times_S X \to E, \quad (z, x) \mapsto z +_1 \varepsilon_2(x)$$

defines an S-isomorphism from $Z \times_S X$ to $E \times_{(X \times_S Y)} (X \times_S 0_Y)$.

(4) (compatibility of the two relative group laws) For any formal scheme T over S and any four T-valued points $w_{11}, w_{12}, w_{21}, w_{22}$ of E such that

$$\pi_1(w_{11}) = \pi_1(w_{12}),\ \pi_1(w_{21}) = \pi_1(w_{22}),\ \pi_2(w_{11}) = \pi_2(w_{21}),\ \pi_2(w_{12}) = \pi_1(w_{22})$$

where $\pi_1 := \mathrm{pr}_1 \circ \pi$ and $\pi_2 := \mathrm{pr}_2 \circ \pi$ are the two projections from E to X and Y respectively, the equality

$$(w_{11} +_2 w_{12}) +_1 (w_{21} +_2 w_{22}) = (w_{11} +_1 w_{21}) +_2 (w_{12} +_1 w_{22})$$

holds.

(2.1.1) REMARK. Conditions (1a) and (1b) assert that the relative group law $+_1$ on E over Y is an extension of (the base change to Y of) X by (the base change to Y of) Z. Similarly (2a) and (2b) say that the relative group law $+_2$ on E over X is an extension of (the base change to X of) Y by (the base change to X of) Z.

(2.1.2) REMARK. Of course the definition 2.1 of biextension works in other contexts, for instance sheaves of commutative groups for the fppf site for a general scheme S. For our purpose the case when X, Y and Z are all p-divisible groups will be sufficient. For the main result on local rigidity for p-divisible groups, S will be the spectrum of a field k of characteristic $p > 0$ and X, Y, Z are p-divisible formal groups over k.

(2.1.3) REMARK. The following properties are easily verified.

(i) For any formal scheme T over S, any T-valued points y_1, y_2 of Y and any T-valued points x_1, x_2 of X, we have

$$\varepsilon_1(y_1) +_2 \varepsilon_1(y_2) = \varepsilon_2(y_1 + y_2), \ \ \varepsilon_2(x_1) +_1 \varepsilon_2(x_2) = \varepsilon_2(x_1 + x_2).$$

(ii) For any formal scheme T over S, any T-valued points z of Z and any T-valued point w of E, we have

$$(z +_1 \varepsilon_2(\pi_1(w))) +_2 w = (z +_2 \varepsilon_1(\pi_2(w))) +_1 w.$$

This equality means that the Z-actions on E induced by the relative group laws $+_1$ and $+_2$ are equal, given $\pi : E \to X \times_S Y$ a natural structure as a Z-torsor. Let

$$* : Z \times_S E = (Z \times_S (X \times_S Y)) \times_{(X \times Y)} E \to E$$

be the morphism defining this Z-torsor structure on E.

(iii) The restriction of $+_1$ to $Z \times_S Z \subset E \times_Y E$ is equal to the group law of Z. Similarly for the restriction of $+_2$ to $Z \times_S Z \subset E \times_X E$.

(iv) The S-isomorphism $(z,y) \mapsto z +_2 \varepsilon_1(y)$ in (3a) is a group isomorphism from the product group $Z \times_S Y$ to the group law on $E \times_{(X \times Y)} (0_X \times Y)$ induced by $+_2$. In other words the restriction to $0_X \subset X$ of the extension of Y by Z over X, given by the partial group law $+_2$, splits canonically. Similarly for the S-isomorphism $(z,x) \mapsto z +_1 \varepsilon_2(x)$ in (3b) is a group isomorphism from the product group $Z \times_S X$ to the group law on $E \times_{(X \times Y)} (X \times 0_Y)$ induced by $+_1$.

(v) The restriction of ε_1 to 0_Y is equal to the restriction of ε_2 to 0_X. Over the scheme-theoretic union Δ of the images of $X \times_S 0_Y$ and $0_X \times_S Y$, i.e. the smallest closed subscheme of $X \times_S Y$ containing both, we have an S-morphism $\varepsilon : \Delta \to E$ such that $\pi \circ \Delta = \mathrm{id}_\Delta$ which is equal to ε_2 on $X \times_S 0_Y$ and equal to ε_1 on $0_X \times_S Y$. Because $\pi : E \to X \times_S Y$ is formally smooth, there exists a section $s : X \times_S Y \to E$ of π which extends ε.

(2.2) The biextension structure can be made explicit in terms of cocycles as follows.

(2.2.1) DEFINITION. Let $\pi : E \to X \times_S Y$ be a biextension of $X \times_S Y$ by Z as in 2.1, and let $s : X \times_S Y \to E$ be a section of π which extends both ε_1 and ε_2 as in 2.1.3 (v). Define S-morphisms

$$\tau : (X \times_S X) \times_S Y \to Z \quad \text{and} \quad \sigma : X \times_S (Y \times_S Y) \to Z$$

by the following formulas expressed in terms of T-valued points x, x_1, x_2, y, y_1, y_2 in X and Y for formal schemes T over S:

(a) $$s(x_1, y) +_1 s(x_2, y) = \tau(x_1, x_2; y) * s(x_1 + x_2, y)$$

(b) $$s(x, y_1) +_2 s(x, y_2) = \sigma(x; y_1, y_2) * s(x, y_1 + y_2)$$

(2.2.2) Cocycle identities. The S-morphisms τ and σ satisfy properties (1)–(5) below, for all formal schemes T over S, all T-valued points x, x_1, x_2, x_3 of X and all points y, y_1, y_2, y_3 of Y. Identities (1) and (2) are consequences of the fact that the section s of π extends ε_1 and ε_2. Identities (3) and (4) hold because the two relative group laws $+_1$ and $+_2$ are commutative and associative. The identity (5) follows from the compatibility of the two relative group laws.

(1) $\sigma(x; 0, y_2) = 0 = \sigma(x; y_1, 0)$, $\tau(0, x_2; y) = 0 = \tau(x_1, 0; y)$.

(2) $\sigma(0; y_1, y_2) = 0$, $\tau(x_1, x_2; 0) = 0$.

(3) (symmetry)

$$\sigma(x; y_1, y_2) = \sigma(x; y_2, y_1), \quad \tau(x_1, x_2; y) = \tau(x_2, x_1; y)$$

(4) (associativity)

$$\begin{aligned}\sigma(x;y_1,y_2)+\sigma(x;y_1+y_2,y_3) &= \sigma(x;y_1,y_2+y_3)+\sigma(x;y_2,y_3)\\ \tau(x_1,x_2;y)+\tau(x_1+x_2,x_3;y) &= \tau(x_1,x_2+x_3;y)+\tau(x_2,x_3;y)\end{aligned}$$

(5) (compatibility)

$$\begin{aligned}&\sigma(x_1+x_2;y_1,y_2)-\sigma(x_1;y_1,y_2)-\sigma(x_2;y_1,y_2)\\ &=\tau(x_1,x_2;y_1+y_2)-\tau(x_1,x_2;y_1)-\tau(x_1,x_2;y_2)\end{aligned}$$

(2.2.3) Coboundary. If we replace $s(x,y)$ by a another section

(2.2.3.1) $$s'(x,y)=f(x,y)*s(x,y),$$

where $f(x,y):X\times_S Y\to Z$ is an S-morphism such that $f(x,0)=0=f(0,y)$ (so that s' extends ε_1 and ε_2), then the resulting maps $\tau':(X\times_S X)\times_Y\to Z$ and $\sigma':X\times_S(Y\times_S Y)\to Z$ are related to the maps σ and τ by

(2.2.3.2) $$\tau'(x_1,x_2;y)-\tau(x_1,x_2;y)=f(x_1,y)+f(x_2,y)-f(x_1+x_2,y),$$

(2.2.3.3) $$\sigma'(x;y_1,y_2)-\sigma(x;y_1,y_2)=f(x,y_1)+f(x,y_2)-f(x,y_1+y_2).$$

(2.2.4) Conversely given a pair (α,β) of S-morphisms satisfying equations (1)–(5) in 2.2.2, there exists a biextension of $X\times_S Y$ by Z naturally attached to the cocycle (α,β). Moreover the biextensions attached to two cocycles (α,β), (α',β') are isomorphic as biextensions of $X\times_S Y$ by Z in the sense of 2.3.1 (c) below if and only if the two cocycles differ by a coboundary in the sense that there exists an S-morphism $f:X\times_S Y\to Z$ such that 2.2.3.2 and 2.2.3.3 hold.

(2.3) Homomorphisms between biextensions

(2.3.1) Definition. Let X,Y,Z,X',Y',Z' be p-divisible groups (resp. commutative smooth formal groups) over $S=\mathrm{Spf}(R)$ as in 2.1. Let $\pi:E\to X\times_S Y$ be a biextension of $X\times_S Y$ by Z, and $\pi':E'\to X'\times_S Y'$ be a biextension of $X'\times_S Y'$ by Z'.

(a) An *S-homomorphism of biextensions* from the biextension E to the biextension E' is a quadruple of S-morphisms

$$(\psi:E\to E',\alpha:X\to X',\beta:Y\to Y',\gamma:Z\to Z')$$

where α,β,γ are S-homomorphisms of commutative formal groups, and ψ is compatible with the biextension structure of E and E', in the sense that the following properties are satisfied.

(i) $\pi'\circ\psi=(\alpha\times\beta)\circ\pi$,

(ii) $\psi\circ +_1=+_1'\circ(\psi\times_Y\psi)$, $\psi\circ +_2=+_2'\circ(\psi\times_X\psi)$,

(iii) $\psi\circ\varepsilon_1=\varepsilon_1'\circ\beta$, $\psi\circ\varepsilon_1=\varepsilon_2'\circ\alpha$.

(b) A homomorphism of biextensions $(\psi, \alpha, \beta, \gamma)$ is an *isomorphism of biextensions* if ψ, α, β and γ are all isomorphism of formal schemes, in which case $(\psi^{-1}, \alpha^{-1}, \beta^{-1}, \gamma^{-1})$ is a homomorphism of biextensions from E' to E.

(c) Suppose that $X' = X$, $Y' = Y$ and $Z' = Z$. We say that the E and E' are isomorphic as biextensions of $X \times Y$ by Z if there exists a isomorphism $(\psi, \mathrm{id}_X, \mathrm{id}_Y, \mathrm{id}_Z)$ from E to E'.

(d) An S-homomorphism $(\psi, \alpha, \beta, \gamma)$ between biextensions of p-divisible groups (respectively commutative smooth formal groups) is an *isogeny* if the homomorphism α, β and γ between p-divisible groups are all isogenies.

Note that an isomorphism $(\psi, \alpha, \beta, \gamma)$ from E to E' as in 2.3.1 (b) above induces an isomorphism $(\psi', \mathrm{id}_X, \mathrm{id}_Y, \mathrm{id}_Z)$ from $\gamma_* E$ to $(\alpha \times \beta)^* E'$, so that the two biextensions $\gamma_* E$ and $(\alpha \times \beta)^* E'$ of $X \times Y$ by Z' are isomorphic in the sense of 2.3.1 (c).

(2.3.2) It is clear that for a homomorphism $(\psi, \alpha, \beta, \gamma)$ from a biextension E to a biextension E' as in 2.3.1, the homomorphisms of formal groups α, β and γ are uniquely determined by the morphism ψ.

Conversely, it is easily seen that if $(\psi_1, \alpha, \beta, \gamma)$ and $(\psi_2, \alpha, \beta, \gamma)$ are two homomorphisms of biextensions from E to E' with the same individual components α, β, γ, then there exists an S-morphism $g : X \times_S Y \to Z'$ such that $\psi_2 = (g \circ \pi') * \psi'$. Moreover $g : X \times_S Y \to Z'$ is a *bihomomorphism* in the sense that

$$g(x_1 + x_2, y) = g(x_1, y) + g(x_2, y), \; g(x, y_1 + y_2) = g(x, y_1) + g(x, y_2)$$

for all formal scheme T over S, all T-valued points x, x_1, x_2 of X and all T-valued points y, y_1, y_2 of Y. In 2.3.3 below we will see that such a bihomomorphism $g : X \times_S Y \to Z'$ is necessarily equal to the zero map if X and Y are both p-divisible groups over S. Therefore the natural map

$$\begin{array}{rcl} \mathrm{Hom}_{\mathrm{biext}}(E, E') & \longrightarrow & \mathrm{Hom}(X, X') \times \mathrm{Hom}(Y, Y') \times \mathrm{Hom}(Z, Z') \\ (\psi, \alpha, \beta, \gamma) & \mapsto & (\alpha, \beta, \gamma) \end{array}$$

is injective when X and Y are both p-divisible groups over S.

(2.3.3) It is an easy formal fact that if X and Y are both p-divisible groups over S, then every bihomomorphism $g : X \times_S Y \to Z$ from $X \times_S Y$ to a sheaf of groups Z over S is identically zero:

(a) The bi-additivity of g implies that

$$g([p^n]_X(x_1), [p^n]_Y(y_1)) = [p^{2n}]_Z(g(x_1, y_1)) = 0$$

for all S-scheme T_1, all $x_1 \in X[p^{2n}](T_1)$ and all $y_1 \in Y[p^{2n}(T_1)$.

(b) Recall that the morphisms $[p^n]_{X[p^{2n}] \to X[p^n]} : X[p^{2n}] \to X[p^n]$ and $[p^n]_{Y[p^{2n}] \to X[p^n]} : Y[p^{2n}] \to Y[p^n]$ induced by "multiplication by p^n" are both faithfully flat. So for every S-scheme T, every $x \in X[p^n](T)$, and every $y \in Y[p^n](T)$, there exists a faithfully flat morphism $f : T_1 \to T$, an element $x_1 \in X[p^{2n}](T_1)$ and an element $y_1 \in Y[p^{2n}](T_1)$ such that

$$x \circ f = [p^n]_{X[p^{2n}] \to X[p^n]} \circ x_1 \quad \text{and} \quad y \circ f = [p^n]_{Y[p^{2n}] \to Y[p^n]} \circ y_1.$$

The desired conclusion that $g : X \times_S Y \to Z$ is equal to the zero map follows immediately from (a) and (b).

(2.3.4) Let E, E' be biextensions as in 2.3.1. Let $s(x,y)$ be a section of $\pi : E \to X \times_S Y$ extending ε_1 and ε_2, and let τ, σ be defined as in 2.2. Similarly let $s'(x',y')$ be a section of $\pi : E' \to X' \times_S Y')$ extending ε_1' and ε_2', and define $\tau' : (X' \times_S X') \times_S Y' \to Z')$ and $\sigma' : X' \times_S (Y' \times_S Y') \to Z'$ in the same way. Define an S-morphism

$$\mu = \mu_\psi : X \times_S Y \to Z'$$

by

$$\psi(s(x,y)) = \mu(x,y) * s'(\alpha(x), \beta(y)) \tag{2.3.4.1}$$

for all points x of X and all points y of Y with values in the same formal scheme over S. It is easy to verify that

$$\gamma(\tau(x_1,x_2;y)) - \tau'(\alpha(x_1),\alpha(x_2);\beta(y)) = \mu(x_1,y) + \mu(x_2,y) - \mu(x_1+x_2,y) \tag{2.3.4.2}$$

$$\gamma(\sigma(x;y_1,y_2)) - \sigma'(\alpha(x);\beta(y_1),\beta(y_2)) = \mu(x,y_1) + \mu(x,y_2) - \mu(x,y_1+y_2) \tag{2.3.4.3}$$

for all formal schemes T over S, all T-points x, x_1, x_2 of X and all T-points y, y_1, y_2 of Y.

Conversely it is easy to see that every S-morphism $\mu : X \times_S Y \to Z'$ satisfying the two displayed equations above defines a homomorphism of biextensions from E to E'.

(2.3.5) REMARK. Let E, E' be biextensions as in 2.3.1. The set $\mathrm{Hom}_{\mathrm{biext}}(E,E')$ of all biextension homomorphisms from E to E' does not have a natural group structure. Instead there are two relative group laws

$$\mathrm{Hom}_{\mathrm{biext}}(E,E') \times_{\mathrm{Hom}(Y,Y')} \mathrm{Hom}_{\mathrm{biext}}(E,E') \longrightarrow \mathrm{Hom}_{\mathrm{biext}}(E,E')$$
$$\mathrm{Hom}_{\mathrm{biext}}(E,E') \times_{\mathrm{Hom}(X,X')} \mathrm{Hom}_{\mathrm{biext}}(E,E') \longrightarrow \mathrm{Hom}_{\mathrm{biext}}(E,E')$$

However even in the case when X, Y, Z, X', Y', Z' are all p-divisible, the natural map

$$\mathrm{Hom}_{\mathrm{biext}}(E,E') \to \mathrm{Hom}(X,X') \times \mathrm{Hom}(Y,Y')$$

may not be surjective. So in general the set $\mathrm{Hom}_{\mathrm{biextn}}(E,E')$ does not have a natural structure as a biextension of $\mathrm{Hom}(X,X') \times \mathrm{Hom}(Y,Y')$ by $\mathrm{Hom}(Z,Z')$.

(2.4) Let R be a noetherian complete local ring whose residue field $R/\mathfrak{m}$ has characteristic p. Let X, Y, Z be p-divisible groups over $S = \mathrm{Spf}(R)$ as in 2.1.

(2.4.1) The *trivial biextension* of $X \times_S Y$ by Z is the natural biextension structure on $X \times_S Y \times Z$, where the two relative group laws are given by

$$(x_1,y,z_1) +_1 (x_2,y,z_2) = (x_1+x_2, y, z_1+z_2), \quad (x,y_1,z_1) +_2 (x,y_2,z_2) = (x, y_1+y_2, z_1+z_2).$$

A biextension $E \to X \times_S Y$ by Z is *trivial* if there is an biextension isomorphism ψ from the trivial biextension to E which induces $\mathrm{id}_X, \mathrm{id}_Y, \mathrm{id}_Z$ on X, Y, Z respectively. We know from 2.3.3 that such an isomorphism is unique if one exists. The restriction of ψ to $X \times_S Y \times_S 0_Z$ is called the *canonical splitting* of a trivial biextension of $X \times_S Y$ by Z.

The uniqueness in the previous paragraph implies that for any faithfully flat morphism $T \to S$ and any biextension $E \to X \times_S Y$ by Z, the base change of the biextension E to T is trivial if and only if E is trivial.

(2.4.2) For every biextension E of $X \times_S Y$ by Z, there is an associated family $\theta_E = (\theta_{n,E})_{n\in\mathbb{N}}$ of bilinear pairings

$$\theta_n = \theta_{n,E} : X[p^n] \times_S Y[p^n] \to Z[p^n], \;\; n \in \mathbb{N}$$

called the *Weil pairing*, attached to this biextension $E \to X \times_S Y$. A definition of the Weil pairing and its basic properties will be reviewed in 2.7. The bilinear pairings θ_n are compatible in the sense that

$$\theta_n([p]_X(x_{n+1}), [p]_Y(y_{n+1})) = [p]_Z(\theta_{n+1}(x_{n+1}, y_{n+1})) \tag{2.4.2.1}$$

for all $x_{n+1} \in X[p^{n+1}]$, all $y_{n+1} \in Y[p^{n+1}]$ and all $n \in \mathbb{N}$; or equivalently,

$$\theta_{n+1}(x_n, y_{n+1}) = \theta_n(x_n, [p]_Y(y_{n+1})) \tag{2.4.2.2}$$

$$\theta_{n+1}(x_{n+1}, y_n) = \theta_n([p]_X(x_{n+1}), y_n) \tag{2.4.2.3}$$

for all $x_n \in X[p^n]$, $x_{n+1} \in X[p^{n+1}]$, $y_n \in Y[p^n]$, $y_{n+1} \in Y[p^{n+1}]$ and all $n \in \mathbb{N}$. See Exp. VIII of [5] for details.

Denote by $\mathrm{Biext}^1(X,Y;Z)$ the set of all biextensions of $X \times_S Y$ by Z up to isomorphisms which induce $\mathrm{id}_X, \mathrm{id}_Y, \mathrm{id}_Z$ on X, Y and Z; c.f. 2.3.1 (c). It is shown in [6, Prop. 4, p. 319] and also in Exp. VIII of [5] that the map $E \mapsto \theta_E$ establishes a bijection from $\mathrm{Biext}^1(X,Y;Z)$ to the set of all compatible families of bilinear pairings $(\theta_n : X[p^n] \times Y[p^n] \to Z[p^n])_{n\in\mathbb{N}}$; see also 2.6.3.

Remark. One knows from [5, VII 3.6.5] that for sheaves of abelian groups P, Q, G over a topos, the set $\mathrm{Biext}^1(P,Q;G)$ of isomorphism classes of biextensions of $P \times Q$ by G is naturally isomorphic to $\mathrm{Ext}^1(P \otimes^{\mathbb{L}} Q, G)$. On the other hand, for p-divisible groups X, Y we have $\mathrm{Tor}^1(X[p^n], Y[p^n]) \cong X[p^n] \otimes Y[p^n]$. The construction of the Weil pairing attached to a biextension reflects these two facts.

(2.4.3) The functoriality of the Weil pairing is as follows. Let X, Y, Z, X', Y', Z' be p-divisible groups over S, let E be a biextension of $X \times_S Y$ by Z, and let E' be a biextension of $X' \times_S Y'$ by Z'. Let $(\theta_{n,E})_{n\in\mathbb{N}}$ and $(\theta_{n,E'})_{n\in\mathbb{N}}$ be the Weil pairings attached to E and E' respectively. Suppose that $(\psi, \alpha, \beta, \gamma)$ is a homomorphism of biextensions from E to E'. Then

$$\gamma(\theta_{n,E}(x_n, y_n)) = \theta_{n,E'}(\alpha(x_n), \beta(y_n))$$

for all $x_n \in X[p^n]$ and all $y_n \in Y[p^n]$.

(2.4.4) Let $E \to X \times_S Y$ be a biextension of $X \times_S Y$ by Z. For any p-divisible formal group Z' over S and any homomorphism $\xi : Z \to Z'$, the standard push-forward construction yields a biextension $\xi_*(E \to X \times_S Y)$ of $X \times_S Y$ by Z', plus a homomorphism ψ_1 from $E \to X \times_S Y$ to $\xi_*(E \to X \times_S Y)$, which induces $\mathrm{id}_X, \mathrm{id}_Y, \xi$ on X, Y, Z respectively. In addition $\xi_*(E \to X \times_S Y)$ satisfies the universal property that every biextension homomorphisms $(\psi, \alpha, \beta, \xi)$ from E to a biextension E' of $X' \times Y'$ by Z' factors through ψ_1. Similarly for any p-divisible groups X_1, Y_1 over S and any homomorphisms $\zeta : X_1 \to X$, $\eta : Y_1 \to Y$, the standard pull-back construction yields a biextension $(\zeta, \eta)^*(E \to X \times_S Y)$ of $X_1 \times_S Y_1$ by Z, which satisfies an obvious universal property among biextension homomorphisms $(\psi_1, \alpha_1, \beta_1, \gamma_1)$ from biextensions $E_1 \to X_1 \times_S Y_1$ to E with $\alpha_1 = \alpha$ and $\beta_1 = \beta$.

It is clear from the consideration of associated Weil pairings that for any isogeny $\xi : Z \to Z'$, the push-forward biextension $\xi_*(E \to X \times_S Y)$ is trivial if and only if $E \to X \times_S Y$ is. Similarly for any pair of isogenies $\zeta : X_1 \to X$, $\eta : Y_1 \to Y$, the pull-back biextension $(\zeta, \eta)^*(E \to X \times_S Y)$ is trivial if and only if $E \to X \times_S Y$ is.

(2.4.5) LEMMA. *Suppose that X, Y, Z are p-divisible groups over a field $k \supset \mathbb{F}_p$. Let $E \to X \times_{\mathrm{Spec}(k)} Y$ be a biextension of $X \times_{\mathrm{Spec}(k)} Y$ by Z. If we have $\lambda + \mu \neq \nu$ for every slope λ of X, every slope μ of Y and every slope ν of Z, then the biextension E is trivial.*

PROOF. By the last paragraph of 2.4, we may assume that k is a perfect field. By 2.4.4, we may assume that X, Y Z are all product of isoclinic p-divisible groups after suitable push-forward and pull-back by isogenies. So we are reduced to the case when X, Y, Z are all isoclinic with slopes λ, μ and ν respectively. The assumption that $\nu \neq \lambda + \mu$ implies immediately that the Weil pairing attached to E vanishes identically. □

(2.5) The Weil pairing as descent data over torsion subgroup schemes

We review in 2.5.1

(a) the definition of the Weil pairing attached to a biextension $E \to X \times Y$ of p-divisible groups $X \times Y$ by a p-divisible group Z, and

(b) how to construct a biextension E_n of $X[p^n] \times Y[p^n]$ by Z by descending the split biextension

$$Z \times X[p^n] \times Y[p^{2n}] \to X[p^n] \times Y[p^{2n}]$$

along the faithfully flat morphism

$$1 \times p^n : X[p^n] \times Y[p^{2n}] \to X[p^n] \times Y[p^n]$$

using the descent datum given by a bihomomorphism $\theta_n : X[p^n] \times Y[p^n] \to Z[p^n]$.

The descent construction reviewed in 2.5.1 (iii), (iv) has many applications. For instance it implies that if the Weil pairings $\theta_{n_1,E}$, $\theta_{n_1,E'}$ attached biextensions E, E' of p-divisible groups $X \times Y$ by Z at a fixed level $[p^{n_1}]$ coincide, then there exists a canonical isomorphism between the restrictions of the biextensions E and E' to $X[p^{n_1}] \times Y[p^{n_1}]$; see 2.5.4 and its Dieudonné theory version 2.6.3, 2.6.4.

(2.5.1) We first recall the explicit construction of the Weil pairing $\theta_n : X[p^n] \times Y[p^n] \to Z[p^n]$ in [6, pp. 320–321].

(i) Construct a natural map

$$\xi_n : X[p^n] \times Y[p^{2n}] \to E_n$$

such that the diagram

$$\begin{tikzcd} X[p^n] \times Y[p^{2n}] \arrow[r, "\xi_n"] \arrow[d, "="'] & E_n \arrow[d, "\pi_n"] \\ X[p^n] \times Y[p^{2n}] \arrow[r, "1\times p^n"] & X[p^n] \times Y[p^n] \end{tikzcd}$$

commutes.

Given any S-scheme T, any $x \in X[p^n](T)$, any $y \in Y[p^{2n}](T)$, there exist a scheme T_1 faithfully flat and locally of finite presentation over T and an element $z_1 \in E(T_1)$ which lies above (x,y) such that when one multiplies z_1 by p^n with respect to the first partial group law $+_1$, we have

$$[p^n]_{+_1}(z_1) = \varepsilon_1(y).$$

Such an element z_1 is not unique, but any two choices differ by an element of $Z[p^n]$. Define $\xi_n(x,y)$ as p^n times z_1 with respect to the second group law $+_2$:

$$\xi_n(x,y) := [p^n]_{+_2}(z_1).$$

Clearly the right hand size of the above equality is independent of the choice of the element z_1, where we have used the first group law $+_1$ to produce a $Z[p^n]$-torsor lying above the S-point (x,y) of $X[p^n] \times Y[p^{2n}]$. By descent we conclude that $\xi_n(x,y) \in E_n(S)$. We have produced the desired morphism $\xi_n : X[p^n] \times Y[p^{2n}] \to E_n$.

(ii) Define a morphism $\alpha_n : Z \times X[p^n] \times Y[p^{2n}] \longrightarrow E_n = \pi^{-1}(X[p^n] \times Y[p^n])$ by

$$\alpha_n(z,x,y) := z * \xi_n(x,y)$$

for all S-scheme T, all $z \in Z(T)$, all $x \in X[p^n](T)$ and all $y \in Y[p^{2n}](T)$. It is easy to see that the following commutative diagram

$$\begin{tikzcd} Z \times X[p^n] \times Y[p^{2n}] \arrow[r, "\alpha_n"] \arrow[d, "\mathrm{pr}_{23}"'] & E_n \arrow[d, "\pi|_{E_n}"] \\ X[p^n] \times Y[p^{2n}] \arrow[r, "1\times p^n"] & X[p^n] \times Y[p^n] \end{tikzcd}$$

is cartesian. So the biextension $\pi_n : E_n \to X[p^n] \times Y[p^n]$ is descended along the faithfully flat morphism

$$1 \times p^n : X[p^n] \times Y[p^{2n}] \longrightarrow X[p^n] \times Y[p^{2n}]$$

from the trivial biextension $\mathrm{pr}_{23} : Z \times X[p^n] \times Y[p^{2n}] \longrightarrow X[p^n] \times Y[p^{2n}]$.

(iii) Construct a bihomomorphism

$$\theta_n : X[p^n] \times Y[p^n] \longrightarrow Z[p^n]$$

using the descent datum for α_n.

The effect of translation by elements of $Y[p^n]$ to the isomorphism α_n is recorded by a map $\theta_n' : X[p^n] \times Y[p^{2n}] \times Y[p^n] \to Z$, defined by

$$\alpha_n(\lambda,x,y) = \alpha_n(\lambda + \theta_n'(x,y,b), x, y+b)$$

for all S-scheme T, all $\lambda \in Z(T)$, all $x \in X[p^n](T)$, all $y \in Y[p^{2n}](T)$ and all $b \in Y[p^n](T)$. An easy calculation shows that $\theta_n'(x,y,b)$ is independent of y. In other words there exists an S-morphism $\theta_n : X[p^n] \times Y[p^n] \to Z$ such that the last displayed equation simplifies to

$$\alpha_n(\lambda,x,y,b) = \alpha_n(\lambda + \theta_n(x,b), x, y+b).$$

An easy calculation shows that θ_n is a bihomomorphism, hence it factors through the closed subgroup scheme $Z[p^n] \hookrightarrow Z$.

(iv) Reversing the construction, it is easy to see that θ_n encodes the descent datum from the trivial biextension $Z\times X[p^n]\times Y[p^{2n}]$ down to E_n: the bihomomorphism θ_n gives an $X[p^n]$-action of the base change to $X[p^n]$ of the group scheme $Y[p^n]$, on the $X[p^n]$-scheme $Z\times X[p^n]\times Y[p^{2n}]$.

(2.5.2) REMARK. The two partial group laws play different roles in the construction the morphisms ξ_n and θ_n. If one interchanges the roles played by the two partial group laws, we get another bihomomorphism $\eta_n : X[p^n]\times Y[p^n]\to Z[p^n]$.

Claim. The bihomomorphism $\eta_n : X[p^n]\times Y[p^n]\to Z[p^n]$ is equal to $-\theta_n$.

Before proving the claim, it is convenient to rephrase the definition of θ_n as follows.

(a) The fiber product

$$\mathfrak{T}_n := \pi^{-1}(X[p^n]\times Y[p^n])\times_{([p^n]_{+_1},E,\varepsilon_1)} Y$$

has a natural structure as a biextension of $X[p^n]\times Y[p^n]$ by $Z[p^n]$, contained in the biextension $\pi^{-1}(X[p^n]\times Y[p^n])$, of $(X[p^n]\times Y[p^n])$ by Z.

(b) The bihomomorphism $\theta : X[p^n]\times Y[p^n]\to Z[p^n]$ is characterised by the property that

$$[p^n]_{+_2}|_{\mathfrak{T}_n} = (\theta_n\circ\pi|_{\mathfrak{T}_n}) * (\varepsilon_2\circ \mathrm{pr}_1)|_{\mathfrak{T}_n}$$

We verify the above claim by descent. Suppose that R is a commutative algebra over the base field k, and we are given elements $x\in X[p^n](R)$, $b\in Y[p^n](R)$, and an element $e\in E(R)$ with $\pi(e) = (x,y)$ which satisfies the normalization condition $[p^n]_{+_1}(e) = \varepsilon_1(b)$ with respect to the group law $+_1$. By definition $\theta_n(x,b)$ is the unique element in $Z[p^n](R)$ such that $[p^n]_{+_2}(e) = \theta_n(x,b)*\varepsilon_2(x)$.

Pick a finite faithfully flat R-algebra S such that there exists an element $\xi\in Z[p^{2n}](S)$ with $[p^n]_Z(\xi) = -\theta_n(x,b)$. Then we have $[p^n]_{+_2}(\xi * e) = \varepsilon_2(x)$, so the element $\xi * e\in E(S)$ over (x,b) satisfies the normalization condition with respect to the group law $+_2$. Moreover we have

$$[p^n]_{+_1}(\xi * e) = [p^n]_Z(\xi)*\varepsilon_1(x).$$

So $\eta_n(x,b) = [p^n]_Z(\xi)$ according to the definition of η_n, i.e. $\eta_n(x,b) = -\theta_n(x,b)$. $\square$

(2.5.3) LEMMA. *Let $\pi : E\to X\times Y$ be a biextension of p-divisible groups $X\times_S Y$ by a p-divisible group Z over a base scheme Y. For each positive integer n, let $\theta_n : X[p^n]\times_S Y[p^n]\to Z[p^n]$ be the canonical bihomomorphism as described in* 2.5.1.

(1) *Suppose that n_1 is a positive integer and θ_{n_1} is equal to the trivial bihomomorphism from $X[p^{n_1}]\times_S Y[p^{n_1}]$ to $Z[p^{n_1}]$. Then the biextension $\pi^{-1}(X[p^{n_1}]\times_S Y[p^{n_1}])$ of $X[p^{n_1}]\times_S Y[p^{n_1}]$ by Z splits canonically. In other words there exists a canonical isomorphism*

$$\zeta_{n_1}^{\mathrm{can}} : \pi^{-1}(X[p^{n_1}]\times_S Y[p^{n_1}]) \xrightarrow{\sim} Z\times_S X[p^{n_1}]\times_S Y[p^{n_1}].$$

(2) *Suppose that n_2 is a positive integer, $n_2 > n_1$ and θ_{n_2} is equal to the trivial bihomomorphism. Then θ_{n_1} is also equal to the trivial bihomomorphism. Moreover the canonical trivializations $\zeta_{n_1}^{\mathrm{can}}$ and $\zeta_{n_2}^{\mathrm{can}}$ are compatible, i.e. $\zeta_{n_1}^{\mathrm{can}}$ is equal to the restriction to $\pi^{-1}(X[p^{n_1}]\times_S Y[p^{n_1}])$ of $\zeta_{n_2}^{\mathrm{can}}$.*

PROOF. We saw in 2.5.1 that the pull-back of $\pi^{-1}(X[p^{n_1}]\times_S Y[p^{n_1}])$ to $X[p^{n_1}]\times_S Y[p^{2n_1}]$ by the faithfully flat morphism $1\times p^{n_1}: X[p^{n_1}]\times_S Y[p^{2n_1}]\to X[p^{n_1}]\times_S Y[p^{n_1}]$ is canonically trivial, and the bihomomorphism θ_{n_1} corresponds to the descent data from the trivial biextension $Z\times X[p^{n_1}]\times_S Y[p^{2n_1}]$ down to π_{n_1} along the morphism $1\times p^{n_1}: X[p^{n_1}]\times_S Y[p^{2n_1}]\to X[p^{n_1}]\times_S Y[p^{n_1}]$. So if θ_{n_1} is the trivial homomorphism, then this descent datum defines a canonical isomorphism between the $\pi^{-1}(X[p^{n_1}]\times_S Y[p^{n_1}])$ and the trivial biextension $Z\times X[p^{n_1}]\times Y[p^{n_1}])$. We have proved statement (1).

The first part of (2) follows from the compatibility of Weil pairings 2.4.2.2 and 2.4.2.3. The compatibility statement (2) follows from the same descent argument used in the proof of (1). □

Proposition 2.5.4 and Corollary 2.5.5 below are applications of 2.5.1 (iv). It enables us to determine the restriction of a homomorphism between two biextensions to torsion subgroups schemes $X[p^n]\times Y[p^n]$.

(2.5.4) PROPOSITION. *Let $\pi: E\to X\times_S Y$ and $\pi': E'\to X\times_S Y$ be two biextensions of p-divisible groups $X\times_S Y$ by a p-divisible group Z over S. Let $(\theta_n,\theta'_n: X[p^n]\times Y[p^n]\to Z[p^n])_{n\in\mathbb{N}}$ be the bihomomorphisms attached to the biextensions E and E' respectively.*

(1) *If n_1 is a positive integer and $\theta_{n_1}=\theta'_{n_1}$, then there exists a canonical isomorphism*

$$\zeta_n:\pi^{-1}(X[p^{n_1}]\times Y[p^{n_1}])\xrightarrow{\sim}(\pi')^{-1}(X[p^{n_1}]\times Y[p^{n_1}])$$

determined by θ_n and θ'_n.

(2) *Suppose that $n_2>n_1$ and $\theta_{n_2}=\theta'_{n_2}$. Then $\theta_{n_1}=\theta'_{n_1}$ and the canonical isomorphism*

$$\zeta_{n_1}:\pi^{-1}(X[p^{n_1}]\times Y[p^{n_1}])\xrightarrow{\sim}(\pi')^{-1}(X[p^{n_1}]\times Y[p^{n_1}])$$

is compatible with the canonical isomorphism

$$\zeta_{n_2}:\pi^{-1}(X[p^{n_2}]\times Y[p^{n_2}])\xrightarrow{\sim}(\pi')^{-1}(X[p^{n_2}]\times Y[p^{n_2}]).$$

(3) *Suppose that $\theta_n=\theta'_n$ for all $n\in\mathbb{N}$. Then the collection of canonical isomorphisms*

$$\zeta_n:\pi^{-n}(X[p^n]\times Y[p^n])\xrightarrow{\sim}(\pi')^{-n}(X[p^n]\times Y[p^n]),\qquad n\in\mathbb{N}$$

defines an isomorphism from the biextension E to the biextension E' which induces $\mathrm{id}_X,\mathrm{id}_Y$ and id_Z on the p-divisible groups X, Y and Z.

(4) *Suppose that $\zeta: E\to E'$ is an isomorphism of biextensions which induces $\mathrm{id}_X,\mathrm{id}_Y$ and id_Z on the p-divisible groups X, Y and Z. Then $\theta_n=\theta'_n$ for all $n\in\mathbb{N}$, and the restriction of ζ to $\pi^{-1}(X[p^n]\times Y[p^n])$ is equal to the canonical isomorphism*

$$\zeta_n:\pi^{-1}(X[p^{n_1}]\times Y[p^{n_1}])\xrightarrow{\sim}(\pi')^{-1}(X[p^{n_1}]\times Y[p^{n_1}])$$

attached to θ_n and θ'_n, for all $n\in\mathbb{N}$.

PROOF. The biextension structures on E and E' endow the Z-torsor $E \wedge^Z ([-1]_Z)_* E'$ over $X \times Y$ a structure of a biextension of $X \times Y$ by Z. The statements (1), (2) follow from 2.5.3 applied to $E \wedge^Z ([-1]_Z)_* E'$. The statement (3) follows from (2).

To prove the statement (4), we observe first that the functoriality of the Weil pairings tell us that $\theta_n = \theta'_n$ for all n. By (3), the canonical isomorphisms ζ_n are compatible and defines an isomorphism of biextensions $\zeta' : E \to E'$ over $X \times Y$. There exists a unique morphism

$$b : X \times_S Y \to Z$$

such that

$$\zeta'(e) = b(\pi(e)) * \zeta(e)$$

for all S-scheme T and all $e \in E(T)$. Clearly $b : X \times_S Y \to Z$ is a bihomomorphism in the sense that

$$b(x_1 + x_2, y) = b(x_1, y) \quad \text{and} \quad b(x, y_1 + y_2) = b(x, y_1) + b(x, y_2)$$

for all S-schemes T, all $x, x_1, x_2 \in X(T)$ and all $y, y_1, y_2 \in Y(T)$. We know from 2.3.3 that such a bihomomorphism is necessarily zero. We have shown that $\zeta' = \zeta$. □

(2.5.5) COROLLARY. *Let X, Y, Z, X', Y', Z' be p-divisible groups over S. Let E be a biextension of $X \times_S Y$ by Z, and let E' be a biextension of $X' \times_S Y'$ by Z'. There is a natural bijection from the set* $\mathrm{Hom}_{\mathrm{biext}}(E, E')$ *of all S-bihomomorphisms from E to E', to the set of all triples* $(\alpha, \beta, \gamma) \in \mathrm{Hom}_S(X, X') \times \mathrm{Hom}_S(Y, Y') \times \mathrm{Hom}_S(Z, Z')$ *such that*

$$\gamma(\theta_{n,E}(x_n, y_n)) = \theta_{n,E'}(\alpha(x_n), \beta(y_n))$$

for all $n \in \mathbb{N}$, all schemes T over S, all $x_n \in X[p^n](T)$, and all $y_n \in Y[p^n](T)$.

(2.6) Dieudonné theory for biextensions

Suppose that k is a perfect field of characteristic $p > 0$. We review the covariant Dieudonné theory for biextensions of p-divisible groups over k the associated Weil pairings. Let $W = W(k)$ be the ring of all p-adic Witt vectors with entries in k. It is well-known that $W(k)$ is a complete discrete valuation ring of mixed characteristics $(0, p)$, $pW(k)$ is the maximal ideal of $W(k)$ and $W(k)/pW(k)$ is naturally isomorphic to k. Let $\sigma : W(k) \to W(k)$ be the map

$$x = (x_0, x_1, x_2, \ldots) \mapsto {}^{\sigma}x = (x_0^p, x_1^p, x^p, \ldots),$$

and let $V : W(k) \to W(k)$ be the map

$$x = (x_0, x_1, x_2, \ldots) \mapsto {}^{V}x = (0, x_0, x_1, x_2, \ldots)$$

on $W(k)$. It is well-known that σ is a ring automorphism of $W(k)$ (because the field k is assumed to be perfect), V is an additive endomorphism of $W(k)$, and

$${}^{V}({}^{\sigma}x) = px = {}^{\sigma}({}^{V}x) \qquad \forall x \in W(k).$$

(2.6.1) The classical covariant Dieudonné theory attaches to every p-divisible formal group X over k a free $W(k)$-module $\mathrm{M}_*(X)$ whose rank is equal to $\mathrm{height}(X)$, together with additive endomorphisms

$$F,\ V : \mathrm{M}_*(X) \longrightarrow \mathrm{M}_*(X)$$

of $\mathrm{M}_*(X)$ such that

$$F(ax) = {}^{\sigma}a F(x), \qquad V({}^{\sigma}ax) = aV(x) \quad \text{and} \quad F(V(x)) = px = V(F(x))$$

for all $a \in W(k)$ and all $x \in \mathrm{M}_*(X)$. A triple (M, F, V), where M is a free $W(k)$-module of finite rank, and F, V are additive endomorphisms of M satisfying the conditions in the above displayed formula, is called a *Dieudonné module* for k.

The main theorem of the classical covariant Dieudonné theory asserts that the assignment

$$X \mapsto \mathrm{M}_*(X)$$

establishes an equivalence of categories from the additive category of p-divisible groups over k to the additive category of Dieudonné modules for the perfect base field k.

(2.6.2) Let X, Y, Z, X', Y', Z' be p-divisible groups and let $\mathrm{M}_*(X), \mathrm{M}_*(Y), \ldots, \mathrm{M}_*(Z')$ be their covariant Dieudonné modules.

We have seen in 2.5.4 and 2.5.5 that the map which to every biextension E of $X \times Y$ associates the compatible family of Weil pairing $(\theta_{n,E})_{n\in\mathbb{N}}$ establishes an equivalence of categories, from the category of biextensions of $X \times Y$ by Z, to the category of compatible families of bilinear pairings

$$(b_n : X[p^n] \times Y[p^n] \to Z[p^n])_{n\in\mathbb{N}}\,.$$

Moreover the set of all bihomomorphisms $\psi : E \to E'$ from a biextension E of $X \times Y$ by Z to a biextension E' of $X' \times Y'$ by Z' is in natural bijection with the set of all triples

$$(\alpha, \beta, \gamma) \in \mathrm{Hom}_k(X, X') \times \mathrm{Hom}_k(Y, Y') \times \mathrm{Hom}_k(Z, Z')$$

such that

$$\gamma(\theta_{n,E}(x_n, y_n)) = \theta_{n,E'}(\alpha(x_n), \beta(y_n))$$

for all k-schemes T, all $x_n \in X[p^n](T)$ and all $y_n \in Y[p^n](T)$. We explain how to express these statements in terms of Dieudonné modules.

(2.6.3) Proposition. *Notation as above.*

(i) *To every biextension E of $X \times Y$ by F, there is an associated $W(k)$-bilinear map*

$$\Theta_E : \mathrm{M}_*(X) \times \mathrm{M}_*(Y) \longrightarrow \mathrm{M}_*(Z)$$

such that

$$\Theta_E(F_{\mathrm{M}_*(X)}(x), y) = F_{\mathrm{M}_*}(Z)\left(\Theta_E(x, V_{\mathrm{M}_*(Y)}(y))\right),\ \ \Theta_E(x, F_{\mathrm{M}_*(Y)}(y)) = F_{\mathrm{M}_*(Z)}\left(\Theta_E(V_{\mathrm{M}_*(X)}x, y)\right)$$

and

$$\Theta_E\left(V_{\mathrm{M}_*(X)}x, V_{\mathrm{M}_*(Y)}y\right) = V_{\mathrm{M}_*(Z)}\left(B_E(x, y)\right)$$

for all $x \in \mathrm{M}_*(X)$ and all $y \in \mathrm{M}_*(Y)$.

(ii) *For every $W(k)$-bilinear map*

$$\Theta : \mathrm{M}_*(X) \times \mathrm{M}_*(Y) \longrightarrow \mathrm{M}_*(Z)$$

satisfying the conditions that

$$\Theta(F_{\mathrm{M}_*(X)}(x), y) = F_{\mathrm{M}_*}(Z)\left(\Theta(x, V_{\mathrm{M}_*(Y)}(y))\right), \quad \Theta(x, F_{\mathrm{M}_*(Y)}(y)) = F_{\mathrm{M}_*(Z)}\left(\Theta(V_{\mathrm{M}_*(X)}x, y)\right)$$

and

$$\Theta\left(V_{\mathrm{M}_*(X)}x, V_{\mathrm{M}_*(Y)}y\right) = V_{\mathrm{M}_*(Z)}\left(B(x,y)\right)$$

for all $x \in \mathrm{M}_*(X)$ and all $y \in \mathrm{M}_*(Y)$, there exists a biextension E of $X \times Y$ by Z such that $B = B_E$. Moreover such a biextension E is unique up to unique isomorphism.

(iii) *Given a biextension E of $X \times Y$ by Z and a biextension E' of $X' \times Y'$ by Z', the natural map from the set of all homomorphisms of biextensions*

$$(\psi : E \to E', \alpha : X \to X', \beta : Y \to Y', \gamma : Z \to Z') \in \mathrm{Hom}_{\mathrm{biext}}(E, E')$$

to the set of all triples (f, g, h) satisfying the conditions

- $f \in \mathrm{Hom}_{W(k),F,V}(\mathrm{M}_*(X), \mathrm{M}_*(X'))$,
- $g \in \mathrm{Hom}_{W(k),F,V}(\mathrm{M}_*(Y), \mathrm{M}_*(Y'))$,
- $h \in \mathrm{Hom}_{W(k),F,V}(\mathrm{M}_*(Z), \mathrm{M}_*(Z'))$,
- $h(\Theta_E(x,y)) = \Theta'_E(f(x), g(y)) \qquad \forall x \in \mathrm{M}_*(X),\ \forall y \in \mathrm{M}_*(y)$

is a bijection.

(2.6.4) Corollary. *Notation as in* 2.6.3. *In particular $E \to X \times Y$ is a biextension of $X \times Y$ by Z and Θ_E is the $W(k)$-bilinear map from $\mathrm{M}_*(X) \times \mathrm{M}_*(Y)$ to $\mathrm{M}_*(Z)$ attached to the biextension Z.*

(1) *The group $\mathrm{Aut}_{\mathrm{biext}}(E)$ of all automorphisms of the biextension E has a natural structure as a compact p-adic Lie group. It is naturally isomorphic to the closed subgroup of*

$$\mathrm{Aut}_{W,F,V}(\mathrm{M}_*(X)) \times \mathrm{Aut}_{W,F,V}(\mathrm{M}_*(Y)) \times \mathrm{Aut}_W(\mathrm{M}_*(Z))$$

consisting of all triples

$$(\alpha, \beta, \gamma) \in \mathrm{Aut}_{W,F,V}(\mathrm{M}_*(X)) \times \mathrm{Aut}_{W,F,V}(\mathrm{M}_*(Y)) \times \mathrm{Aut}_{W,F,V}(\mathrm{M}_*(Z))$$

such that

$$\gamma(\Theta_E(x,y)) = \Theta_E(\alpha(x), \beta(y)) \qquad \forall x \in \mathrm{M}_*(X),\ \forall y \in \mathrm{M}_*(Y).$$

Here $\mathrm{Aut}_{W,F,V}(\mathrm{M}_*(X))$ denotes the compact p-adic Lie group consisting of all $W(k)$-linear automorphisms of $\mathrm{M}_*(X)$ which commute with $F_{\mathrm{M}_*(X))}$ and $V_{\mathrm{M}_*(X))}$; it is naturally isomorphic to the group $\mathrm{Aut}(X)$ of all automorphisms of the p-divisible group X. The same notation scheme is applied to $\mathrm{Aut}_{W,F,V}(\mathrm{M}_*(Y))$ and $\mathrm{Aut}_{W,F,V}(\mathrm{M}_*(Z))$.

(2) *The Lie algebra of the compact p-adic Lie group* $\mathrm{Aut}_{\mathrm{biext}}(E)$ *is naturally isomorphic to the Lie subalgebra of* $\mathrm{End}_{K,F,V}(\mathrm{M}_*(X)_{\mathbb{Q}}) \oplus \mathrm{End}_{K,F,V}(\mathrm{M}_*(Y)_{\mathbb{Q}}) \oplus \mathrm{End}_{K,F,V}(\mathrm{M}_*(Z)_{\mathbb{Q}})$ *consisting of all triples*

$$(A,B,C) \in \mathrm{End}_{W,F,V}(\mathrm{M}_*(X))_{\mathbb{Q}} \oplus \mathrm{End}_{K,F,V}(\mathrm{M}_*(Y))_{\mathbb{Q}} \oplus \mathrm{End}_{K,F,V}(\mathrm{M}_*(Z))_{\mathbb{Q}}$$

which satisfy the condition that

$$C(\Theta_E(x,y)) = \Theta_E(Ax,y) + \Theta_E(x,By) \qquad \forall x \in \mathrm{M}_*(X), \forall y \in \mathrm{M}_*(Y).$$

Here $K := W(k)[1/p] = W(k) \otimes_{\mathbb{Z}} \mathbb{Q}$, $\mathrm{M}_*(X)_{\mathbb{Q}} := \mathrm{M}_*(X)[1/p]$ *and* $\mathrm{End}_{K,F,V}(\mathrm{M}_*(X))$ *denotes the set of all K-linear endomorphisms of* $\mathrm{M}_*(X)_{\mathbb{Q}}$ *which commute with F and V; it is naturally isomorphic to the Lie algebra of the compact p-adic Lie group* $\mathrm{Aut}_{W,F,V}(\mathrm{M}_*(X)) \cong \mathrm{Aut}(X)$.

(2.6.5) DEFINITION. Let G be a compact p-adic Lie group, which is closed subgroup of the group of all $\mathbb{Q}_p$-points of a linear algebraic group over $\mathbb{Q}_p$. Let $k \supset \mathbb{F}_p$ be a perfect field of characteristic p. Let $W = W(k)$ be the ring of p-adic Witt vectors with entries in k, and let $K = W[1/p]$ be the fraction field of W.

(a) Let U be a p-divisible group over k, and let $\mathrm{M}(U)$ be the covariant Dieudonné module of $U \times_{\mathrm{Spec}(k)} \mathrm{Spec}(k)$. Let $\zeta : G \to \mathrm{Aut}(U)$ be a continuous homomorphism. We say that the action of G on U is *strongly non-trivial* if there does not exist a pair $N_1 \subsetneqq N_2$ of K-vector subspaces of $M \otimes_W K$ stable under the action of $\mathrm{Lie}(G)$ such that the induced action of $\mathrm{Lie}(G)$ on N_2/N_1 is trivial.

(b) Let X,Y,Z be p-divisible groups over k. Let $E \to X \times_{\mathrm{Spec}(k)} Y$ be a biextension of $X \times_{\mathrm{Spec}(k)} Y$ by Z. Let $\rho : G \to \mathrm{Aut}_{\mathrm{biext}}(E)$ be a continuous action of G on E which respects the biextension structure of E. Let $\alpha : G \to \mathrm{Aut}(X)$, $\beta : G \to \mathrm{Aut}(Y)$, and $\gamma : G \to \mathrm{Aut}(Z)$ be the continuous actions of G on X, Y and Z induced by ρ. We say that the action of G on E is *strongly non-trivial* if the actions α, β γ of G on X, Y, Z are all strongly non-trivial, or equivalently if the action of G on $X \times Y \times Z$ is strongly non-trivial.

REMARK. In the definition (a) above, if we require in addition that N_1, N_2 are both stable under F and V, the resulting new definition of the notion "strongly non-trivial", though apparently weaker, is actually equivalent to the definition in (a). The proof is left as an exercise.

(2.7) Canonical trivializations over torsion subgroup schemes.

Let X,Y,Z be p-divisible groups over a base scheme S. Let $\pi : E \to X \times_S Y$ be a biextension of $X \times_S Y$ by Z. Let $E_n := \pi^{-1}(X[p^n] \times_S Y[p^n])$ be the restriction of the biextension E to $X[p^n] \times_S Y[p^n]$; it is a biextension of $X[p^n] \times_S Y[p^n]$ by Z The push-forward $([p^n]_Z)_* E_n$ of E_n by the homomorphism $[p^n]_Z : Z \to Z$ is again a biextension of $X[p^n] \times_S Y[p^n]$ by Z. In this subsection we will construct a natural splitting of the biextension $([p^n]_Z)_* E_n$.

(2.7.1) Definition of $\eta_n : E_n \to Z$ Let $([p^n]_Z)_*(E)$ be the push-forward of the biextension $\pi : E \to X \times_S Y$ by $[p^n]_Z$, and let $f_n : E \to ([p^n]_Z)_*(E)$ be the tautological map from E to its push-forword by $[p^n]_Z$. Clearly bihomomorphism $\theta_{n,([p^n]_Z)_*(E)} : X[p^n] \times_S Y[p^n] \to Z[p^n]$ attached to the biextension $([p^n]_Z)_*(E)$ is equal to 0, by the functoriality of the Weil pairings. Let

$$\zeta^{\mathrm{can}}_{n,([p^n]_Z)_*(E)} : ([p^n]_Z)_*(E) \xrightarrow{\sim} Z \times_S \times X[p^n] \times_S Y[p^n]$$

be the canonical splitting as in 2.5.3. Let $\mathrm{pr}_1 : Z \times_S X[p^n] \times_S Y[p^n] \to Z$ be the projection to Z. Define $\eta_n : E_n \to Z$ to be the composition

$$\eta_n := \mathrm{pr}_1 \circ \zeta^{\mathrm{can}}_{n,([p^n]_Z)_*(E)} \circ f_n.$$

(2.7.2) ALTERNATIVE DEFINITION of η_n. One can also define η_n directly using the construction of the biextension $E_n \to X[p^n] \times_S Y[p^n]$ by descent in 2.5, with the descent datum given by the Weil pairing θ_n of the biextension E. We will use the notation in 2.5.

Let

$$\eta_n' := [p^n]_Z \circ \mathrm{pr}_1 : Z \times_S X[p^n] \times_S Y[p^{2n}] \longrightarrow Z$$

be the composition of the projection $\mathrm{pr}_1 : Z \times_S X[p^n] \times_S Y[p^{2n}] \to Z$ with the endomorphism $[p^n]_Z : Z \to Z$ of Z. Obviously $\eta_n'((\lambda,x,y)) = \eta_n'(\lambda + \theta_n'(x,y,b),x,y+b)$ for all S-scheme T, all $x \in X[p^n](T)$, all $y \in Y[p^n](T)$ and all $b \in Y[p^n](T)$. Therefore η_n' factors through the faithfully flat morphism $\alpha_n : Z \times X[p^n] \times_S Y[p^{2n}] \longrightarrow E_n$. Here α_n is the faithfully flat morphism in 2.5 which expresses the biextension $E_n \to X[p^n] \times_S Y[p^n]$ as a descent of the trivial biextension $Z \times_S X[p^n] \times_S Y[p^{2n}]$, with the descent datum encoded by the Weil pairing θ_n. By descent there exists a unique morphism $\eta_n : E_n \to Z$ such that

$$\eta_n' = \eta_n \circ \alpha_n\,.$$

An easy exercise shows that the morphism η_n defined above coincides with the morphism η_n defined in 2.7.1.

(2.7.3) From the definitions of α_n and η_n it is not difficulty to verify that the compatibility relation

$$[p]_Z \circ \eta_n = \eta_{n+1} \circ (E_n \hookrightarrow E_{n+1})$$

holds for all $n \in \mathbb{N}$.

§3. Complete restricted perfections in characteristics p, I

In §2.7 we defined a compatible sequence of morphisms $\left\{\eta_n : \pi^{-1}E =: E_n \to Z\right\}_{n\in\mathbb{N}}$ for any biextension of E of p-divisible groups X,Y by another p-divisible group Z, over an arbitrary base scheme S. In this section we will consider the special case when S is the spectrum of a perfect field $k \supset \mathbb{F}_p$. An interesting phenomenon reveals itself in the special case described in 3.1, and the compatible sequence of morphisms (η_n) lead us to families commutative rings, whose elements consists of formal series of the form

$$\sum_{(i_1,\dots,i_m)\in\mathbb{Z}[1/p]^m_{\geq 0}} \in \mathbb{Z}[1/p]^m_{\geq 0}\, a_{i_1,\dots,i_m} t_1^{i_1} t_2^{i_2} \cdots t_m^{i_m}$$

with coefficients $a_{i_1,\dots,i_m} \in k$, subject to the condition roughly of the following form

$$|I|_p \leq C \cdot |I|^E_{\infty,\max}$$

for every I such that $a_I \neq 0$, where $C, E > 0$ are parameters which define the ring. Here for any multi-index $I = (i_1,\dots,i_m) \in \mathbb{Z}[1/p]^m_{\geq 0}$, $|I|_p$ is the p-adic norm of I and $|I|_{\infty,\max}$ is the archimedean norm of I, defined by

$$|I|_p := \max(p^{-\mathrm{ord}_p(i_1)},\dots,p^{-\mathrm{ord}_p(i_1)}), \quad \text{and} \quad |I|_{\infty,\max} := \max(i_1,i_2,\dots,i_m).$$

These rings do not seem to have appeared in the literature, but they hold the key to the local rigidity for biextensions of p-divisible groups. In this section we give the motivation and definition of these new rings.

(3.1) Assumptions. To focus on the key features in the proof of local rigidity of biextensions of p-divisible formal groups, we make three additional assumptions.

(0) The base field k is algebraically closed.

(1) The p-divisible group Z has a slope μ_1 which is strictly bigger than every slope of X and every slope of Y.

(2) The p-divisible group Z is isomorphic to a product $Z_1 \times Z_2$ of two p-divisible formal groups, such that Z_1 is isoclinic of slope μ_1.

(3) There exist positive integers $a, r > 0$ such that

$$\mu_1 = \frac{a}{r} \quad \text{and} \quad \mathrm{Ker}([p^a]_{Z_1}) = \mathrm{Fr}^r_{Z_1/k},$$

where $\mathrm{Fr}^r_{Z_1/k} : Z_1 \to Z_1^{(p^r)}$ is the r-th iterate of the relative Frobenius morphism for Z_1/k.

It follows from assumptions (0) and (3) that there exists elements $u_1, \ldots, u_b \in \Gamma(Z_1, \mathscr{O}_{Z_1})$ such that the affine coordinate ring of Z_1 is the formal power series ring $k[[u_1, \ldots, u_b]]$, and

$$[p^a]^*_{Z_1}(u_i) = u_i^{p^r} \quad \forall\, i = 1, \ldots, b.$$

REMARK. Suppose that E is a biextension of p-divisible formal groups $X \times Y$ over k by a p-divisible formal group Z' over k such that the Z' has a slope μ_1 which is strictly bigger than all slopes of X and Y. There exists an isogeny $\beta : Z' \to Z$ of p-divisible groups such that the assumptions (2) and (3) hold for Z and also for the push-forward $\beta_* E'$ of E by β.

(3.2) Choose and fix a positive rational number $\mu_0 < \frac{a}{r}$ such that μ_0 is strictly bigger than every slope of $Z_2 \times X \times Y$. Multiplying both a and r by a suitable positive integer, we may and do assume that μ_0 has the form

$$\mu_0 = \frac{a}{s}, \quad s > r, \;\; s \in \mathbb{N}_{>0}$$

From the general properties of slopes we know that there exists a constant m_0 such that

(3.2.1) $$X[p^m] \supset \mathrm{Ker}(\mathrm{Fr}^{\lfloor m/\mu_0 \rfloor}_{X/k}) \quad \text{and} \quad Y[p^m] \supset \mathrm{Ker}(\mathrm{Fr}^{\lfloor m/\mu_0 \rfloor}_{Y/k})$$

for all $m \geq m_0$. Therefore

(3.2.2) $$X[p^{na}] \supset \mathrm{Ker}(\mathrm{Fr}^{ns}_{X/k}) \quad \text{and} \quad Y[p^{na}] \supset \mathrm{Ker}(\mathrm{Fr}^{ns}_{Y/k})$$

for all $n \geq n_0 := \lceil \frac{m_0}{a} \rceil$. On the other hand, assumption (3) implies that

$$\mathrm{Ker}([p^{na}]_{Z_1}) = \mathrm{Ker}(\mathrm{Fr}^{nr}_{Z_1/k})$$

for all $n \in \mathbb{N}$.

REMARK. (a) In practice we will choose μ_0 to be "just a tiny bit bigger than the maximum of the slopes of X and Y".
(b) If we choose μ_0 to be the maximum of the slopes of X and Y, then the estimate in 3.2.2 needs to be changed to: there exists a constant e (depending on X and Y) such that

$$X[p^{na}] \supset \mathrm{Ker}(\mathrm{Fr}_{X/k}^{ns-e}), \quad \text{and} \quad Y[p^{na}] \supset \mathrm{Ker}(\mathrm{Fr}_{Y/k}^{ns-e}) \tag{3.2.3}$$

for all $n \geq n_0 := \lceil \frac{m_0}{a} \rceil$.

(3.3) Let $R = R_E$ be the coordinate ring of E, let $\mathfrak{m} = \mathfrak{m}_E$ be the maximal ideal of R. Let $\phi = \phi_R$ be the absolute Frobenius endomorphism of R which sends every element $x \in R$ to x^p. For every $n \in \mathbb{N}$, let

$$\mathfrak{m}^{(p^n)} := \phi^n(\mathfrak{m}) \cdot R$$

be the ideal of R generated by $\phi^n(\mathfrak{m})$. Clearly $\mathfrak{m}^{(p^n)} \subset \mathfrak{m}^{p^n}$ for all $n \in \mathbb{N}$, where $\mathfrak{m}^{p^n}$ is the p^n-th power of the maximal ideal m. In other words $\mathfrak{m}^{p^n}$ is the ideal of R generated by all products of the form $\prod_{1 \leq j \leq p^n} x_j$, with $x_j \in \mathfrak{m}$ for all j. If $t_1, \ldots, t_m$ is a regular system of parameters of the complete regular local ring R, then $\mathfrak{m}^{(p^n)}$ is the ideal $(t_1^{p^n}, \ldots, t_m^{p^n})$ in $R = k[[t_1, \ldots, t_m]]$, while $\mathfrak{m}^{p^n}$ is the ideal generated by all monomials of the form $\prod_{1 \leq j \leq m} t_j^{i_j}$ with $i_1, \ldots, i_m \in \mathbb{N}$ and $i_1 + \cdots + i_m \geq p^n$. It is clear from the above that

$$\mathfrak{m}^{p^n} \subseteq \mathfrak{m}^{(p^{n-a})} \quad \text{if} \quad p^a \geq m,$$

because if a multi-index $I = (i_1, \ldots, i_m) \in \mathbb{N}^m$ has the property that $||I|| := \sum_{j=1}^m i_j \geq p^n$, then at least one of the indices $i_1, \ldots, i_m$ is $\geq \frac{p^n}{m}$. Let

$$E[F^n] := \mathrm{Spec}\left(R/\mathfrak{m}^{(p^n)}\right) = \mathrm{Spec}\left(R/\phi^n(\mathfrak{m})R\right), \quad E \bmod \mathfrak{m}^{p^n} := \mathrm{Spec}\left(R/\mathfrak{m}^{p^n}\right).$$

Similarly we have Artinian subschemes $X[F^n]$, $X \bmod \mathfrak{m}_X^{p^n} \subset X$, $Z_1[F^n]$, $Z_1 \bmod \mathfrak{m}_{Z_1}^{p^n} \subset Z_1$, etc.

(3.3.1) In 2.7 we constructed a family of morphisms $\eta_n : E_n = \pi^{-1}(X[p^n] \times Y[p^n]) \to Z$ such that $[p]_Z \circ \eta_n = \eta_{n+1}|_{E_n}$ for all n. From 3.2.2 we know that $E[F^{ns}] \subset E_{na}$ for all $n \geq n_0$, where a and s are the positive integers chosen in 3.2 so that $\frac{a}{s}$ is strictly bigger than every slope of X or Y and both s and a are sufficiently divisible. The restriction of η_{na} to $E[F^{ns}]$ makes sense for all $n \geq n_0$ because $E[F^{ns}] \subset E_{na}$. This restriction is a morphism from $E[F^{ns}]$ to $Z[F^{ns}]$. The projection $\mathrm{pr}_{Z_1} : Z = Z_1 \times Z_2 \to Z_1$ induces a morphism $\mathrm{pr}_{Z_1} : Z[F^{ns}] \to Z_1[F^{ns}]$.

(3.3.2) DEFINITION. Define a morphism ρ_{na} by composing η_{na} with pr_{Z_1}:

$$\rho_{na} := \mathrm{pr}_{Z_1} \circ \eta_{na}|_{E[F^{ns}]} : E[F^{ns}] \longrightarrow Z_1[F^{ns}] \qquad \forall n \geq n_0$$

The morphisms $\left(\rho_{na}\right)_{n \geq n_0}$ satisfy the following compatibility relations

$$[p^a]_{Z_1} \circ \rho_{na} = \rho_{(n+1)a}|_{E[F^{ns}]} \qquad \forall n \geq n_0$$

Let $u_1, \ldots, u_b$ be a regular system of parameters of the coordinate ring of Z_1 as in 3.1, so that $Z_1 = \mathrm{Spf}(k[[u_1, \ldots, u_b]])$ and

$$[p^a]_{Z_1}^*(u_j) = u_j^{p^r} \qquad \forall j = 1, \ldots, b.$$

(3.3.3) Definition. Define elements $a_{j,n} \in R_E \Big/ \mathfrak{m}_E^{(p^{sn})}$ for all $j = 1, \ldots, b$ and all $n \geq n_0$, by

$$a_{j,n} = \rho_{na}^*(u_j) \ \in \ R_E \Big/ \mathfrak{m}_E^{(p^{ns})} \ .$$

The compatibility relations for the ρ_n's in 3.3.2 and the fact that $[p^a]_{Z_1}^*(u_j) = u_j^{p^r}$ imply that

$$(\dagger) \qquad a_{j,n}^{p^r} \equiv a_{j,n+1} \pmod{\mathfrak{m}_E^{(p^{ns+r})}}$$

for all $n \geq n_0$ and all $j = 1, \ldots, b$.

Remark. (a) The Frobenius map ϕ^r on R_E induces injective ring homomorphisms

$$\phi^r : R_E/\mathfrak{m}_E^{(p^{sn})} \to R_E/\mathfrak{m}_E^{(p^{sn+r})}$$

for all n. In particular the element $a_{j,n}^{p^r}$ on the left hand side of ($\dagger$) is an element of $R_E/\mathfrak{m}_E^{(p^{sn+r})}$ uniquely determined by the element $a_{j,n} \in R_E/\mathfrak{m}_E^{(p^{sn})}$.
(b) The compatibility relation ($\dagger$) makes the limit procedure in 3.4.2 a little neater than it would have been, had we used the slightly coarser congruence

$$a_{j,n}^{p^r} \equiv a_{j,n+1} \pmod{\mathfrak{m}_E^{(p^{ns})}}$$

instead of ($\dagger$).

(3.4) We saw in 3.3.3 that the compatible family of morphisms $\rho_n : E[F^{ns}] \to Z_1[F^{ns}]$ is given by b sequences

$$\left(a_{j,n} \in R_E/\mathfrak{m}_E^{(p^{ns})}\right)_{n \geq n_0}$$

of elements in Artinian local rings $R_E/\mathfrak{m}_E^{(p^{ns})}$ which satisfy the relation ($\dagger$) in 3.3.3. Each of the chosen coordinates $u_1, \ldots, u_b$ of the p-divisible formal group Z_1 gives rise to a compatible sequence of elements in $R_E/\mathfrak{m}_E^{(p^{ns})}$.

It is natural to try to formulate a convenient version of the "limit" of a given compatible sequence of elements in $R_E/\mathfrak{m}_E^{(p^{ns})}$ (other than just the sequence itself). We record the definition of ϕ^r-compatibility in 3.4.1 (a) below, together with a variant coarser version in 3.4.1 (b).

The following notations will be used in 3.4.1. Let $\kappa \supset \mathbb{F}_p$ be a perfect field. Let n_0 be a natural number. Let $r < s$ be positive integers. Let $t_1, \ldots, t_m$ be m variables. We adopt the notation $\underline{t} := (t_1, \ldots, t_m)$ and $\kappa[[\underline{t}]] := \kappa[[t_1, \ldots, t_m]]$. Let

$$(\underline{t}^{p^{ns}}) = (\underline{t})^{(p^{ns})} := (t_1^{p^{ns}}, \ldots, t_m^{p^{ns}}).$$

Let $(\underline{t})^{p^{ns}}$ be the ideal of $\kappa[[\underline{t}]]$ generated by all monomials $\underline{t}^I := t_1^{i_1} \cdots t_m^{i_m}$, where $I = (i_1, \ldots, i_m) \in \mathbb{N}^m$ ranges through all m-tuples in $\mathbb{N}^m$ with $|I|_\sigma := i_1 + \cdots + i_m = n$. Let ϕ be the Frobenius map on $\kappa[[\underline{t}]]$ which sends every element of $\kappa[[\underline{t}]]$ to its p-th power.

(3.4.1) Definition. We follow the notation in the previous paragraph.

(a) A sequence of elements $(a_n)_{n\geq n_0}$ with $a_n \in \kappa[[\underline{t}]]/(\underline{t}^{p^{ns}})$ for all n is ϕ^r-*compatible* if

$$a_n^{p^r} \equiv a_{n+1} \pmod{(\underline{t}^{p^{ns+r}})} \quad \forall n \geq n_0$$

(b) A sequence of elements $(a_n)_{n\geq n_0}$ with $a_n \in \kappa[[\underline{t}]]/(\underline{t})^{p^{ns}}$ for all n is ϕ^r-*compatible* if

$$a_n^{p^r} \equiv a_{n+1} \pmod{(\underline{t})^{p^{ns+r}}} \quad \forall n \geq n_0$$

REMARK. The version (b) is different from (a) in that the element a_n is in the congruence class modulo the ideal $(\underline{t})^{p^{ns}}$, which is bigger than the ideal $(\underline{t}^{p^{ns}})$. We will mostly use (a) because this version provides more information. For the proof of local rigidity version (b) will also be adequate.

(3.4.2) Suppose we are given a ϕ^r-compatible sequence $(a_n)_{n\geq n_0}$ with $a_n \in \kappa[[\underline{t}]]/(\underline{t}^{p^{ns}})$ for all $n \geq n_0$. Formally the compatibility relation suggests that

$$\phi^{-nr}(a_n^{p^r}) \equiv \phi^{-(n+1)r}(a_{n+1}) \pmod{\phi^{-nr}\big((\underline{t}^{p^{ns}})\big)} \quad \forall n \geq n_0.$$

Here we have used $\phi^{-nr}\big((\underline{t}^{p^{ns}})\big)$ instead of $\phi^{-(n+1)r}\big((\underline{t}^{p^{ns+r}})\big)$ to make the congruence relation look better and more suggestive. Thus it seems reasonable to try to produce a "limit" of the sequence $\phi^{-nr}a_n$ as $n \to \infty$ in some suitable way.

There is an obvious problem: a_n has representatives in $\kappa[[\underline{t}]]$, but in general none of the representatives is in $\phi^{nr}(\kappa[[\underline{t}]])$. We need to use at least some elements in the perfection

$$\kappa[[\underline{t}]]^{\mathrm{perf}} = \bigcup_n \kappa[[\underline{t}^{p^{-n}}]] = \bigcup_n \kappa[[t_1^{p^{-n}}, \ldots, t_m^{p^{-n}}]].$$

of $\kappa[[\underline{t}]]$. Note that this perfection is not complete for the topology defined by the filtration by total degree. For our purpose we don't have to be concerned too much about $\kappa[[\underline{t}]]^{\mathrm{perf}}$ or its completion. We will focus rather on what comes out of the limit procedure for ϕ^r-compatible sequences in the Artinian local rings $\kappa[[\underline{t}]]/(\underline{t}^{p^{ns}})$.

(3.4.3) Notation involving multi-indices.

(i) For each index $I = (i_1, \ldots, i_m) \in \mathbb{N}^m$, let

$$\underline{t}^I := t_1^{i_1} \cdots t_m^{i_m}$$

be the corresponding monomial in the variables $t_1, \ldots, t_m$.

(ii) Among the archimedean norms on $\mathbb{Q}^m$, we will use the following two: for $J = (j_1, \ldots, j_m) \in \mathbb{Q}^m$,

$$|J|_\infty := \max(|j_1|, \ldots, |j_m|), \qquad |J|_\sigma := |j_1| + \cdots + |j_m|.$$

Obviously

$$|J|_\infty \leq |J|_\sigma \leq m \cdot |J|_\infty \qquad \forall J \in \mathbb{Q}^m$$

(iii) There is also the following p-adic norm on $\mathbb{Q}^m$:

$$|J|_p := \max\left(|j_1|_p, \ldots, |j_m|_p\right)$$

where $|\cdot|_p$ is multiplicative p-adic absolute value on $\mathbb{Q}$, defined by $|x|_p = p^{-\mathrm{ord}_p(x)}$ for all $x \in \mathbb{Q}$, so that $|p| = \frac{1}{p}$ and $|x|_p = 1$ if both the numerator and denominator of x are prime to p. Define

$$\mathrm{ord}_p(J) := \mathrm{Min}\left(\mathrm{ord}_p(j_1), \ldots \mathrm{ord}_p(j_m)\right),$$

hence

$$|J|_p = p^{-\mathrm{ord}_p(J)}.$$

We will use the restriction of these norms to $\mathbb{N}[1/p]^m := \mathbb{Z}[1/p]^m_{\geq 0}$, the additive semigroup of exponents with p-power denominators.

(3.5) We will approach the limit problem in 3.4.2 in a lowbrow fashion first.

(3.5.1) Suppose we are given a ϕ^r-compatible sequence $(a_n)_{n \geq n_0}$ with $a_n \in \kappa[[\underline{t}]]/(\underline{t}^{p^{ns}})$ for all $n \geq n_0$. For each $n \geq n_0$, write the element $a_n \in \kappa[[\underline{t}]]/(\underline{t}^{p^{ns}})$ as

$$a_n = \sum_{J \in \mathbb{N}^m,\, |J|_\infty < p^{ns}} a_{n,J}\, \underline{t}^J \quad \mathrm{mod}\ (\underline{t}^{p^{ns}}).$$

Clearly the coefficients $a_{n,J} \in \kappa$ with $|J|_\infty$ are uniquely determined by a_n. The compatibility relation $a_n^{p^r} \equiv a_{n+1} \pmod{(\underline{t}^{p^{ns+r}})}$ means that $a_{n+1,J} = a_{n,p^{-r}J}$ for all $J \in \mathbb{N}^m$ with $|J|_\infty < p^{ns+r}$ and all $n \geq n_0$. More precisely,

$$(\ddagger) \qquad a_{n+1,J} = \begin{cases} 0 & \text{if} \quad |J|_\infty < p^{ns+r}, \quad p^{-r}J \notin \mathbb{N}^m \\ a_{n,p^{-r}J}^{p^r} & \text{if} \quad |J|_\infty < p^{ns+r}, \quad p^{-r}J \in \mathbb{N}^m \end{cases}$$

for all $n \geq n_0$. Thus the among the coefficients $a_{n,J}$ for a fixed natural number $n \geq n_0 + 1$, those with $|J|_\infty < p^{(n-1)s+r}$ arises from coefficients $a_{n',J'}$ with $n' < n$. More precisely suppose that $n \geq n_0 + 1$, then the following statements hold.

- If $|J|_\infty < p^{(n-1)s+r}$ and J is not divisible by p^r, then $a_{n,J} = 0$.
- If $|J|_\infty < p^{(n-1)s+r}$ and $J = p^{(n-n')r}J'$, where $n' < n$ and J' is not divisible by p^r, then $a_{n,J} = a_{n',J'}^{p^{(n-n')r}}$.

There is no constraint for those $a_{n,J}$'s with $|J|_\infty \geq p^{(n-1)s+r}$; these coefficients will be propagated to coefficients of $a_{n'',J}$'s with $n'' > n$.

(3.5.2) Construction of the limit. For each multi-index $I \in \mathbb{N}[1/p]^m$, define $b_I \in \kappa$ by

$$b_I := (a_{n,p^{nr}J})^{p^{-rn}} = \phi^{-rn}(a_{n,p^{nr}J}),$$

where $n \in \mathbb{N}$ is sufficiently large such that $p^{nr}I \in \mathbb{N}^m$ and $|p^{nr}I|_\infty < p^{sn}$, so that $a_{n,p^{nr}I}$ makes sense. The compatibility relation for the $a_{n,J}$'s immediately implies that the above definition does not depend on the choice of n, as long as

$$n \geq \mathrm{Max}\left(\frac{-\mathrm{ord}_p(J)}{r},\ \frac{\log_p(|J|_\infty)}{s-r}\right).$$

The formal series

$$\sum_{I\in\mathbb{N}[1/p]^m} b_I\, \underline{t}^I = \sum_{(i_1,\ldots,i_m)\in\mathbb{N}[1/p]^m} b_{i_1,\ldots,i_m}\, t_1^{i_1}\cdots t_m^{i_m}$$

attached to a given ϕ^r-compatible sequence of elements $\left(a_n \in \kappa[[\underline{t}]]/(\underline{t}^{p^{sn}})\right)_{n\geq n_0}$ according to the above construction will be called the *limit* of the ϕ^r-compatible sequence $(a_n)_{n\geq n_0}$.

(3.5.3) PROPOSITION. *The construction described in* 3.5.2 *establishes a bijection, from the set of all ϕ^r-compatible sequences of elements $\left(a_n \in \kappa[[\underline{t}]]/(\underline{t}^{p^{sn}})\right)_{n\geq n_0}$, to the set of all formal series*

$$\sum_{I\in\mathbb{N}[1/p]^m} b_I\, \underline{t}^I$$

such that $b_I \in \kappa$ for all $I \in \mathbb{N}[1/p]^m$, and

$$(*) \qquad -\mathrm{ord}_p(I) \leq \mathrm{Max}\left\{n_0,\ r\cdot\left(\left\lfloor\frac{\log_p(|I|_\infty)}{s-r}\right\rfloor+1\right)\right\}$$

for every $I \in \mathbb{N}[1/p]^m$ with $b_I \neq 0$.

PROOF. Although the estimate in the statement of 3.5.3 looks complicated, the proof is completely straight-forward from the construction explained in 3.5.2.

Suppose that $\sum_{I\in\mathbb{N}[1/p]^m} b_I\, \underline{t}^I$ is attached to a ϕ^r-compatible sequence $(a_n)_{n\geq n_0}$, $a_n \in \kappa[[\underline{t}]]/(\underline{t}^{p^{ns}})$ for all $n \geq n_0$. Let $I \in \mathbb{N}[1/p]^m$ be an index in the support of the above formal series, i.e. $b_I \neq 0$. We need to show that the inequality $(*)$ holds. Let n_1 be the smallest natural number such that $p^{n_1 r}I \in \mathbb{N}^m$. There is nothing to prove if $n_1 \leq n_0$, so we may assume that $n_1 \geq n_0+1$. In particular $\mathrm{ord}_p(I) < 0$, and $n_1 = \lceil\frac{-\mathrm{ord}_p(I)}{r}\rceil$.

From the definition of n_1 we know that $p^{n_1}I$ is not divisible by p^r. If $|p^{n_1}I|_\infty < p^{(n_1-1)s+r}$, we get from 3.5.1 (‡) that $b_I = 0$, a contradiction. We have shown that

$$|p^{n_1}I|_\infty \geq p^{(n_1-1)s+r}.$$

The last inequality is be equivalent to

$$\left\lceil\frac{-\mathrm{ord}_p(I)}{r}\right\rceil = n_1 \leq \frac{\log_p|I|_\infty}{s-r}+1,$$

which is easily seen to be equivalent to the asserted inequality $(*)$.

It remains to show that every formal series $\sum_{I\in\mathbb{N}[1/p]^m} b_I\, \underline{t}^I$ whose support satisfies the inequality $(*)$ arises from a ϕ^r-compatible sequence $(a_n)_{n\geq n_0}$. This statement is not difficult to see: one verifies using the inequality $(*)$ that for every natural number $n\geq n_0$, the truncated series

$$c_n := \sum_{I\in\mathbb{N}[1/p]^m,\, |p^{nr}I|_\infty < p^{ns}} b_I^{p^{nr}}\, \underline{t}^{p^{nr}I} \in \kappa[[\underline{t}]]$$

Let $a_n := c_n \mod (\underline{t}^{p^{ns}})$. It is easily verified that $(a_n)_{n\geq n_0}$ is a ϕ^r-compatible sequence, whose limit is the given formal series $\sum_{I\in\mathbb{N}[1/p]^m} b_I\, \underline{t}^I$. □

Remark. For ϕ^r-compatible sequences of elements $(a_n \in \kappa[[\underline{t}]]/(\underline{t})^{p^{sn}})$, the procedure 3.5.2 for constructing limits also works if the norm $|\cdot|_\infty$ for muliti-indices is replaced by the norm $|\cdot|_\sigma$. The corresponding results are similar, so are the proofs: in the statements and proofs of 3.5.1, 3.5.2 and 3.5.3, we need to replace $\kappa[[\underline{t}]]/(\underline{t}^{p^{sn}})$ by $\kappa[[\underline{t}]]/(\underline{t})^{p^{sn}}$ and replace $|\cdot|_\infty$ by $|\cdot|_\sigma$.

(3.5.4) Definition. Let $\kappa\supset\mathbb{F}_p$ be a perfect field of characteristic $p>0$, and let $\underline{t}=(t_1,\dots,t_m)$ be m variables. Let $r,s\in\mathbb{Z}_{>0}$ be two positive integers with $r<s$, and let n_0 be a natural number.

(a) Denote by $\kappa\langle\langle t_1^{p^{-\infty}},\dots,t_m^{p^{-\infty}}\rangle\rangle^{\#}_{s:\phi^r,\geq n_0}$ the commutative κ-algebra consisting of all formal series

$$\sum_{I\in\mathbb{N}[1/p]^m} b_I\, \underline{t}^I$$

such that $b_I\in\kappa$ for all $I\in\mathbb{N}[1/p]^m$, and

$$(*)\qquad -\mathrm{ord}_p(I) \leq \mathrm{Max}\left\{n_0,\ r\cdot\left(\left\lfloor\frac{\log_p(|I|_\infty)}{s-r}\right\rfloor+1\right)\right\}$$

for every $I\in\mathbb{N}[1/p]^m$ such that $b_I\neq 0$.

(b) Denote by $\kappa\langle\langle t_1^{p^{-\infty}},\dots,t_m^{p^{-\infty}}\rangle\rangle^{\flat}_{s:\phi^r,\geq n_0}$ the commutative κ-algebra consisting of all formal series

$$\sum_{I\in\mathbb{N}[1/p]^m} b_I\, \underline{t}^I$$

such that $b_I\in\kappa$ for all $I\in\mathbb{N}[1/p]^m$, and

$$(**)\qquad -\mathrm{ord}_p(I) \leq \mathrm{Max}\left\{n_0,\ r\cdot\left(\left\lfloor\frac{\log_p(|I|_\sigma)}{s-r}\right\rfloor+1\right)\right\}$$

for every $I\in\mathbb{N}[1/p]^m$ such that $b_I\neq 0$.

(c) Let $\mathrm{supp}\big(\kappa\langle\langle t_1^{p^{-\infty}},\dots,t_m^{p^{-\infty}}\rangle\rangle^{\#}_{s:\phi^r,\geq n_0}\big)$ be the subset of $\mathbb{N}[1/p]^m$ consisting of all multi-indices $I\in\mathbb{N}[1/p]^m$ such that the inequality $(*)$ holds. Similarly let $\mathrm{supp}\big(\kappa\langle\langle t_1^{p^{-\infty}},\dots,t_m^{p^{-\infty}}\rangle\rangle^{\flat}_{s:\phi^r,\geq n_0}\big)$ be the subset of $\mathbb{N}[1/p]^m$ consisting of all multi-indices $I\in\mathbb{N}[1/p]^m$ such that the inequality $(**)$ holds.

REMARK. (i) The two support sets

$$\mathrm{supp}\big(\kappa\langle\langle t_1^{p^{-\infty}},\ldots,t_m^{p^{-\infty}}\rangle\rangle^{\#}_{s:\phi^r,\geq n_0}\big) \quad\text{and}\quad \mathrm{supp}\big(\kappa\langle\langle t_1^{p^{-\infty}},\ldots,t_m^{p^{-\infty}}\rangle\rangle^{\flat}_{s:\phi^r,\geq n_0}\big)$$

are sub-semigroups of $\mathbb{N}[1/p]^m$. Moreover for every $M > 0$, there are only a finite number elements I in either sub-semigroup such that $|I|_\infty \leq M$. The last property implies that for each I, there are only a finite number of pairs (I_1,I_2) of elements in either sub-semigroup such that $I_1+I_2 = I$. Therefore the standard formula for multiplication of formal power series defines multiplication on $\kappa\langle\langle t_1^{p^{-\infty}},\ldots,t_m^{p^{-\infty}}\rangle\rangle^{\#}_{s:\phi^r,\geq n_0}$ and $\kappa\langle\langle t_1^{p^{-\infty}},\ldots,t_m^{p^{-\infty}}\rangle\rangle^{\flat}_{s:\phi^r,\geq n_0}$, making them augmented local domains over κ.

(ii) Let $m \geq 1$ be a positive integer. It is easy to see that the rings $\langle\langle t_1,\ldots,t_m\rangle\rangle^{\#}_{s:\phi^r,\geq n_0}$ and $\kappa\langle\langle t_1^{p^{-\infty}},\ldots,t_m^{p^{-\infty}}\rangle\rangle^{\flat}_{s:\phi^r,\geq n_0}$ are non-Neotherian local domains. In can be shown that neither of the two local domains is normal. Moreover the integral closure of $\kappa\langle\langle t_1^{p^{-\infty}},\ldots,t_m^{p^{-\infty}}\rangle\rangle^{\#}_{s:\phi^r,\geq n_0}$ (respectively $\kappa\langle\langle t_1^{p^{-\infty}},\ldots,t_m^{p^{-\infty}}\rangle\rangle^{\flat}_{s:\phi^r,\geq n_0}$) in its own fraction field is *not* a finitely generated module over $\kappa\langle\langle t_1^{p^{-\infty}},\ldots,t_m^{p^{-\infty}}\rangle\rangle^{\#}_{s:\phi^r,\geq n_0}$ (respectively $\kappa\langle\langle t_1^{p^{-\infty}},\ldots,t_m^{p^{-\infty}}\rangle\rangle^{\flat}_{s:\phi^r,\geq n_0}$), because the fraction field of either ring contains t_i^j for any $j \in \mathbb{N}[1/p]$ and any $i = 1,\ldots,m$. However these integral closures can be described explicitly.

Below is a slightly different version of the rings defined in 3.5.4.

(3.5.5) DEFINITION. Let $\kappa \subset \mathbb{F}_p$ be a perfect field. Let $r < s$ be two positive integers, and let $i_0 \in \mathbb{N}$ be a natural number. The perfection of the formal power series $\kappa[[t_1,\ldots,t_m]]$ is naturally isomorphic to

$$\bigcup_{n\in\mathbb{N}} \kappa[[t_1^{p^{-n}},\ldots,t_m^{p^{-n}}]].$$

Denote by ϕ the Frobenius automorphism of this perfect ring.

(a) Consider the following subring

$$\big(\kappa\langle\langle t_1^{p^{-\infty}},\ldots,t_m^{p^{-\infty}}\rangle\rangle^{\#}_{s:\phi^r;[i_0]}\big)_{\mathrm{fin}} := \sum_{n\in\mathbb{N}} \phi^{-nr}\big((\underline{t})^{(p^{ns-i_0})}\big)$$

of the perfection of the formal power series ring $\kappa[[t_1,\ldots,t_m]]$, where our convention is that $(\underline{t})^{(p^{ns-i_0})} = R$ if $ns-i_0 \leq 0$. Define a decreasing filtration $\Big(\mathrm{Fil}^{\#,p^\bullet}_{s:\phi^r,[i_0]}\Big)_{\bullet\in\mathbb{Z}}$ on the ring $\big(\kappa\langle\langle t_1^{p^{-\infty}},\ldots,t_m^{p^{-\infty}}\rangle\rangle^{\#}_{s:\phi^r;[i_0]}\big)_{\#,\,\mathrm{fin}}$ by

$$\mathrm{Fil}^{\#,p^j}_{s:\phi^r,[i_0]} := \Big\{x \in \big(\kappa\langle\langle t_1^{p^{-\infty}},\ldots,t_m^{p^{-\infty}}\rangle\rangle^{\#}_{s:\phi^r;[i_0]}\ \Big|\ \exists n \in \mathbb{N}_{>0}\ \text{ s.t. }\ n+j \geq 0 \text{ and } x^{p^n} \in (\underline{t})^{(p^{n+j})}\Big\},$$

where $(\underline{t} = (t_1,\ldots,t_m)$ is the maximal ideal of $\kappa[[t_1,\ldots,t_m]]$. Define

$$\kappa\langle\langle t_1^{p^{-\infty}},\ldots,t_m^{p^{-\infty}}\rangle\rangle^{\#}_{s:\phi^r;[i_0]}$$

to be the completion of $\big(\kappa\langle\langle t_1^{p^{-\infty}},\ldots,t_m^{p^{-\infty}}\rangle\rangle^{\#}_{s:\phi^r;[i_0]}\big)_{\mathrm{fin}}$ with respect to the above decreasing filtration.

(b) Consider the following subring

$$\left(\kappa\langle\langle t_1^{p^{-\infty}},\ldots,t_m^{p^{-\infty}}\rangle\rangle^{\flat}_{s:\phi^r;[i_0]}\right)_{\mathrm{fin}} := \sum_{n\in\mathbb{N}} \phi^{-nr}\left((\underline{t})^{p^{ns-i_0}}\right)$$

of the perfection of the formal power series ring $\kappa[[t_1,\ldots,t_m]]$. In the above our convention is that $(\underline{t})^{p^{ns-i_0}} = R$ if $ns-i_0 \leq 0$. Define a decreasing filtration $\left(\mathrm{Fil}^{\flat,\bullet}_{s:\phi^r,[i_0]}\right)_{\bullet\in\mathbb{Z}[1/p]_{\geq 0}}$ on the ring $\left(\kappa\langle\langle t_1^{p^{-\infty}},\ldots,t_m^{p^{-\infty}}\rangle\rangle^{\flat}_{s:\phi^r;[i_0]}\right)_{\mathrm{fin}}$ by

$$\mathrm{Fil}^{\flat,u}_{s:\phi^r,[i_0]} := \left\{ x\in\left(\kappa\langle\langle t_1^{p^{-\infty}},\ldots,t_m^{p^{-\infty}}\rangle\rangle^{\flat}_{s:\phi^r;[i_0]}\right. \,\middle|\, \exists n\in\mathbb{N}_{>0} \text{ such that } p^n u\in\mathbb{N} \text{ and } x^{p^n}\in(\underline{t})^{u\cdot p^n}\right\}.$$

Define $\kappa\langle\langle t_1^{p^{-\infty}},\ldots,t_m^{p^{-\infty}}\rangle\rangle^{\flat}_{s:\phi^r;[i_0]}$ to be the completion of $\left(\kappa\langle\langle t_1^{p^{-\infty}},\ldots,t_m^{p^{-\infty}}\rangle\rangle^{\flat}_{s:\phi^r;[i_0]}\right)_{\mathrm{fin}}$ with respect to the above filtration.

(3.6) Definitions of complete restricted perfections

We will introduce in 3.6.1 two other families, $\kappa\langle\langle t_1^{p^{-\infty}},\ldots,t_m^{p^{-\infty}}\rangle\rangle^{E,\#}_{C;d}$ and $\kappa\langle\langle t_1^{p^{-\infty}},\ldots,t_m^{p^{-\infty}}\rangle\rangle^{E,\flat}_{C;d}$ of complete restricted perfections of a given power series ring $\kappa[[t_1,\ldots,t_m]]$, related to the rings defined in 3.5.4 and 3.5.5. We will also see in 3.6.3 and 3.6.4 that the notion of complete restricted perfection in 3.5.4 and 3.5.5 can be extended to general complete Noetherian local domains of equi-characteristic $p>0$ with perfect residue fields.

(3.6.1) DEFINITION. Let $\kappa\supset\mathbb{F}_p$ be a perfect field and let $t_1,\ldots,t_m$ be variables. Let $C>0, d\geq 0, E>0$ be real numbers.

(a) Define a commutative κ-algebra

$$\kappa\langle\langle t_1^{p^{-\infty}},\ldots,t_m^{p^{-\infty}}\rangle\rangle^{E,\#}_{C;d}$$

whose underlying abelian group is the set of all formal series $\sum_I b_I \underline{t}^I$ with $b_I\in\kappa$ for all I, where I runs through all elements in $\mathbb{N}[1/p]^m$ such that

$$|I|_p \leq \mathrm{Max}\left(C\cdot(|I|_\infty + d)^E, 1\right).$$

The ring structure is given by the standard formula for product of power series.

(b) Define a commutative κ-algebra

$$\kappa\langle\langle t_1^{p^{-\infty}},\ldots,t_m^{p^{-\infty}}\rangle\rangle^{E,\flat}_{C;d}$$

whose underlying abelian group is the set of all formal series $\sum_I b_I \underline{t}^I$ with $b_I\in\kappa$ for all I, where I runs through all elements in $\mathbb{N}[1/p]^m$ such that

$$(\flat)\qquad |I|_p \leq \mathrm{Max}\left(C\cdot(|I|_\sigma + d)^E, 1\right).$$

The above condition on the support (of elements of this subset) shows that the standard formula for multiplication makes sense and gives $\kappa\langle\langle t_1^{p^{-\infty}},\ldots,t_m^{p^{-\infty}}\rangle\rangle^{E,\flat}_{C;d}$ a natural structure as an augmented commutative algebra over κ.

Denote by $\operatorname{supp}(m:E;C,d) = \operatorname{supp}(m:\flat:E;C,d)$ the subset of $\mathbb{N}[1/p]^m$ consisting of all elements $I \in \mathbb{N}[1/p]^m$ satisfying the inequality ($\flat$) above.

(3.6.2) LEMMA. *Denote by* $\mathrm{Fil}^{\bullet}_{\mathrm{t.deg}}$ *the decreasing filtration on* $\kappa\langle\langle t_1^{p^{-\infty}},\ldots,t_m^{p^{-\infty}}\rangle\rangle^{E,\flat}_{C;d}$ *such that*

$$\mathrm{Fil}^{u}_{\mathrm{t.deg}}\big(\kappa\langle\langle t_1^{p^{-\infty}},\ldots,t_m^{p^{-\infty}}\rangle\rangle^{E,\flat}_{C;d}\big) := \Big\{ \sum_{I\in\operatorname{supp}(m:E;C,d),\,|I|_\sigma\geq u} b_I \underline{t}^I \,:\, b_I \in \kappa\ \ \forall I \Big\}$$

for every $u \in \mathbb{R}$. *Let*

$$\mathrm{Fil}^{u+}_{\mathrm{t.deg}}\big(\kappa\langle\langle t_1^{p^{-\infty}},\ldots,t_m^{p^{-\infty}}\rangle\rangle^{E,\flat}_{C;d}\big) := \bigcup_{\varepsilon>0} \mathrm{Fil}^{u+\varepsilon}_{\mathrm{t.deg}}\big(\kappa\langle\langle t_1^{p^{-\infty}},\ldots,t_m^{p^{-\infty}}\rangle\rangle^{E,\flat}_{C;d}\big)$$

(i) *Both* $\mathrm{Fil}^{u}_{\mathrm{t.deg}}\big(\kappa\langle\langle t_1^{p^{-\infty}},\ldots,t_m^{p^{-\infty}}\rangle\rangle^{E,\flat}_{C;d}\big)$ *and* $\mathrm{Fil}^{u+}_{\mathrm{t.deg}}\big(\kappa\langle\langle t_1^{p^{-\infty}},\ldots,t_m^{p^{-\infty}}\rangle\rangle^{E,\flat}_{C;d}\big)$ *are ideals of the ring* $\kappa\langle\langle t_1^{p^{-\infty}},\ldots,t_m^{p^{-\infty}}\rangle\rangle^{E,\flat}_{C;d}$, *for every* $u \in \mathbb{R}$.

(ii) *Let* $\mathrm{gr}^{\bullet}\big(\kappa\langle\langle t_1^{p^{-\infty}},\ldots,t_m^{p^{-\infty}}\rangle\rangle^{E,\flat}_{C;d}\big)$ *be the graded ring attached to the filtration* $\mathrm{Fil}^{\bullet}_{\mathrm{t.deg}}$ *of the ring* $\kappa\langle\langle t_1^{p^{-\infty}},\ldots,t_m^{p^{-\infty}}\rangle\rangle^{E,\flat}_{C;d}$. *This graded ring is naturally isomorphic to the graded subring*

$$\bigoplus_{I\in\operatorname{supp}(m:E;C,d)} \kappa\cdot\underline{t}^I$$

of the perfection

$$\kappa[t_1^{p^{-\infty}},\ldots,t_m^{p^{-\infty}}] = \bigoplus_{I\in\mathbb{N}[1/p]^m} \kappa\cdot\underline{t}^I$$

of the polynomial ring $\kappa[t_1,\ldots,t_m]$, *where the latter is graded by the total degree* $|I|_\sigma$ *of monomials* $\underline{t}^I$.

The proof is easy/obvious, therefore omitted. □

(3.6.3) DEFINITION. Let $(R,\mathfrak{m})$ be a complete Noetherian local domain of equi-characteristic $p>0$, with perfect residue field κ. Let R^{perf} be the perfection of R, and let ϕ be the Frobenius automorphism on R. Let r,s,n_0 be natural numbers, $0<r<s$, $n_0\geq 0$.

(a) Consider the following subset

$$\big((R,\mathfrak{m})^{\mathrm{perf},\#}_{s:\phi^r;[i_0]}\big)_{\mathrm{fin}} := \sum_{n\geq 0} \phi^{-nr}\big(\mathfrak{m}^{(p^{ns-i_0})}\big)$$

of the perfect domain R^{perf}. In the above by convention $\mathfrak{m}^{(p^{ns-i_0})} = R$ if $ns-i_0\leq 0$. It is easy to see that this subset is a subring of R^{perf}. Define a decreasing filtration $\big(\mathrm{Fil}^{\#,p^\bullet}_{s:\phi^r;[i_0]}\big)_{j\in\mathbb{Z}}$ on $\big((R,\mathfrak{m})^{\mathrm{perf},\#}_{s:\phi^r;[i_0]}\big)_{\mathrm{fin}}$ by

$$\mathrm{Fil}^{\#,p^j}_{s:\phi^r;[i_0]} := \Big\{ x\in\big((R,\mathfrak{m})^{\mathrm{perf},\#}_{s:\phi^r;[i_0]}\big)_{\mathrm{fin}} \,\Big|\, \exists n\in\mathbb{N} \text{ s.t. } x^{p^n}\in\mathfrak{m}^{p^{n+j}} \Big\}.$$

It is easy to see that each Fil^{p^j} is an ideal of $\big((R,\mathfrak{m})^{\mathrm{perf},\#}_{s:\phi^r;[i_0]}\big)_{\mathrm{fin}}$. Define

$$(R,\mathfrak{m})^{\mathrm{perf},\#}_{s:\phi^r;[i_0]}$$

to be the completion of $\big((R,\mathfrak{m})^{\mathrm{perf},\#}_{s:\phi^r;[i_0]}\big)_{\mathrm{fin}}$ with respect to the above filtration $\big(\mathrm{Fil}^{\#,p^\bullet}_{s:\phi^r;[i_0]}\big)_{j\in\mathbb{Z}}$

(b) Consider the following subset

$$\big((R,\mathfrak{m})^{\mathrm{perf},\flat}_{s:\phi^r;[i_0]}\big)_{\mathrm{fin}} := \sum_{n\geq 0} \phi^{-nr}\big(\mathfrak{m}^{p^{ns-n_0}}\big)$$

of the perfect domain R^{perf}. Here $\mathfrak{m}^{p^{ns-i_0}} = R$ if $ns-n_0\leq 0$. It is easy to see that this subset is a subring of R^{perf}. Define a decreasing filtration $\big(\mathrm{Fil}^{\flat,p^\bullet}_{s:\phi^r;[i_0]}\big)_{j\in\mathbb{Z}}$ on $\big((R,\mathfrak{m})^{\mathrm{perf},\flat}_{s:\phi^r;[i_0]}\big)_{\mathrm{fin}}$ by

$$\mathrm{Fil}^{\flat,p^j}_{s:\phi^r;[i_0]} := \Big\{x\in \big((R,\mathfrak{m})^{\mathrm{perf},\flat}_{s:\phi^r;[i_0]}\big)_{\mathrm{fin}} \,\Big|\, \exists n\in\mathbb{N} \text{ s.t. } x^{p^n}\in \mathfrak{m}^{p^{n+j}}\Big\}.$$

Define

$$(R,\mathfrak{m})^{\mathrm{perf},\flat}_{s:\phi^r;[i_0]}$$

to be the completion of $\big((R,\mathfrak{m})^{\mathrm{perf},\flat}_{s:\phi^r;[i_0]}\big)_{\mathrm{fin}}$ with respect to the above filtration $\big(\mathrm{Fil}^{\flat,p^\bullet}_{s:\phi^r;[i_0]}\big)_{j\in\mathbb{Z}}$.

(3.6.4) Definition. Let $(R,\mathfrak{m})$ be a complete Noetherian local domain of equi-characteristic $p>0$ with perfect residue field κ. Let R^{perf} be the perfection of R, and let ϕ be the Frobenius automorphism on R. Let A,b,d be real numbers, with $A,b>0$ and $d\geq 0$.

(i) Define a decreasing filtrations $\big(\mathrm{Fil}^\bullet_{R^{\mathrm{perf}},\deg}\big)_{u\in\mathbb{R}_0}$ on R^{perf} indexed by real numbers u by

$$\mathrm{Fil}^u_{R^{\mathrm{perf}},\deg} := \Big\{x\in R^{\mathrm{perf}} \,\Big|\, \exists j\in\mathbb{N} \text{ s.t. } x^{p^j}\in\mathfrak{m}^{\lceil u\cdot p^j\rceil}\Big\} \qquad \text{if } u\geq 0$$

and

$$\mathrm{Fil}^u_{R^{\mathrm{perf}},\deg} := R^{\mathrm{perf}} \qquad \text{if } u\leq 0$$

It is easy to see that $\mathrm{Fil}^u_{R^{\mathrm{perf}},\deg}$ is an ideal of R^{perf} for every $u\in\mathbb{R}$.

(ii) Define a subset $\big((R,\mathfrak{m})^{\mathrm{perf},\flat}_{A,b;d}\big)_{\mathrm{fin}}$ of R^{perf} by

$$\big((R,\mathfrak{m})^{\mathrm{perf},\flat}_{A,b;d}\big)_{\mathrm{fin}} := \sum_{n\in\mathbb{N}} \big(\phi^{-n}R\cap \mathrm{Fil}^{b\cdot p^{An}-d}_{R^{\mathrm{perf}},\deg}\big)$$

It is not difficult to see that $\big((R,\mathfrak{m})^{\mathrm{perf},\flat}_{A,b;d}\big)_{\mathrm{fin}}$ is a subring of R^{perf}.

(iii) Define

$$(R,\mathfrak{m})^{\mathrm{perf},\flat}_{A,b;d}$$

to be the completion of $\big((R,\mathfrak{m})^{\mathrm{perf},\flat}_{A,b;d}\big)_{\mathrm{fin}}$ with respect to the filtration induced by the filtration $\big(\mathrm{Fil}^\bullet_{R^{\mathrm{perf}},\deg}\big)$ of R^{perf}:

$$(R,\mathfrak{m})^{\mathrm{perf},\flat}_{A,b;d} = \lim_{u\to\infty} \big((R,\mathfrak{m})^{\mathrm{perf},\flat}_{A,b;d}\big)_{\mathrm{fin}} \Big/ \Big(\mathrm{Fil}^u_{R^{\mathrm{perf}},\deg}\cap \big((R,\mathfrak{m})^{\mathrm{perf},\flat}_{A,b;d}\big)_{\mathrm{fin}}\Big).$$

§4. Complete restricted perfections, II

(4.1) How various complete restricted perfections compare
In 3.6 we defined three families of rings. Each ring in these families consist of formal series of the form $\sum_{I\in\mathbb{N}[1/p]} b_I \underline{t}^I$, where $b_I \in \kappa\ \forall I$, subject uniform constraint (depending on parameters) on the support of such series. The three families are:

(1) $\kappa\langle\langle t_1^{p^{-\infty}},\ldots,t_m^{p^{-\infty}}\rangle\rangle^{\#}_{s:\phi^r,\geq n_0}$ and $\kappa\langle\langle t_1^{p^{-\infty}},\ldots,t_m^{p^{-\infty}}\rangle\rangle^{\flat}_{s:\phi^r,\geq n_0}$

(2) $\kappa\langle\langle t_1^{p^{-\infty}},\ldots,t_m^{p^{-\infty}}\rangle\rangle^{\#}_{s:\phi^r;[i_0]}$ and $\kappa\langle\langle t_1^{p^{-\infty}},\ldots,t_m^{p^{-\infty}}\rangle\rangle^{\flat}_{s:\phi^r;[i_0]}$

(3) $\kappa\langle\langle t_1^{p^{-\infty}},\ldots,t_m^{p^{-\infty}}\rangle\rangle^{E,\#}_{C;d}$ and $\kappa\langle\langle t_1^{p^{-\infty}},\ldots,t_m^{p^{-\infty}}\rangle\rangle^{E,\flat}_{C;d}$

We have defined two additional family of rings, attached to any given equi-characteristic-p complete Noetherian local domain $(R,\mathfrak{m})$:

(4) $(R,\mathfrak{m})^{\mathrm{perf},\#}_{s:\phi^r;[i_0]}$ and $(R,\mathfrak{m})^{\mathrm{perf},\flat}_{s:\phi^r;[i_0]}$

(5) $(R,\mathfrak{m})^{\mathrm{perf},\flat}_{A,b;d}$

(4.1.1) Remark. (i) The family (1) above was motivated by the compatible sequence of morphisms $(\rho_n)_{n\geq n_0}$ defined in 3.3.2, based on the sequence of morphisms $(\eta_n)_{n\in\mathbb{N}}$ constructed in 2.7. There are two versions for family of rings. The #-version is directly tied with compatible families $(\eta_n)_{n\geq n_0}$'s. The primary parameters are the positive integers $r<s$. With r,s fixed, the ring increases as the second parameter n_0 increases. The $\flat$-version results from the # version when one replaces congruences modulo $(t_1^{p^n},\ldots,t_m^{p^n})$ by the coarser congruences modulo $(t_1,\ldots,t_m)^{p^n}$.

(ii) The family (2) is a slight variant of the family (1). With the primary parameters $r<s$ fixed, the rings in the family (2) are closely related to the rings in the family (1); the rings in family (2) increases as the parameter i_0 increases. In some sense as i_0 increases, the rings in family (2) increases somewhat faster than the rings in family (1), to the extent that the rings in families (1) and (2) with the same primary parameters r,s are not co-final with each other as their respective secondary parameters n_0 and i_0 vary.

The family (2) is somewhat more convenient than the family (1). Generalization to complete Noetherian local domains 3.6.4 is straight forward. When the primary parameter r,s are fixed while the secondary parameter i_0 varies, the #-version interlaces with the $\flat$-version; see 4.1.2 (1) below.

(iii) In the family (3) the parameters $E,C>0$ and $d\geq 0$ are real numbers. The most significant parameter is the "exponent" E; it is written as a superscript in the notation, to indicate that it serves as an exponent in the estimate of p-adic absolute value in terms of archimedean absolute value for elements in the support of formal series in family (3).

The "multiplicative constant" C is secondary, while the parameter d is of least importance among the three. When E is fixed while C and d vary, the #-version and the $\flat$-version are interlaced; see 4.1.3 (1). Rings in family (2) with primary parameters $s>r>0$ are closely related to rings in family (3) with $E=\frac{r}{s-r}$; see 4.1.2 (3) and 4.1.3 (2).

(iv) Clearly the family (2) is a special case of the family (4). This is reflected in the notation for (2) and (4).

(v) The family (5) with real parameters $A>0, b>0, d\geq 0$ generalizes the family (3). When $(R,\mathfrak{m})=\big(\kappa[[t_1,\ldots,t_m]],(t_1,\ldots,t_m)\big)$, the parameters (A_1,b_1,d_1) corresponding to given parameters (E,C,d) are:

$$A_1=\tfrac{1}{E},\quad b_1=C^{1/E},\quad d_1=d.$$

When the parameters are related as above, the rings $\kappa\langle\langle t_1^{p^{-\infty}},\ldots,t_m^{p^{-\infty}}\rangle\rangle_{C;d}^{E,\flat}$ and $(R,\mathfrak{m})_{A_1,b_1;d_1}^{\mathrm{perf},\flat}$ are quite close.

(4.1.2) LEMMA. *Let $s>r>0$ be positive integers. and let $i_0\geq 0$ be a natural number. Let $\kappa\supset\mathbb{F}_p$ be a perfect field, and let $t_1,\ldots,t_m$ be variables.*

(1) *Let $i_0\geq 0$ be a natural number. We have inclusions*

$$\kappa\langle\langle t_1^{p^{-\infty}},\ldots,t_m^{p^{-\infty}}\rangle\rangle_{s:\phi^r;[i_0]}^{\#}\subset\kappa\langle\langle t_1^{p^{-\infty}},\ldots,t_m^{p^{-\infty}}\rangle\rangle_{s:\phi^r;[i_0]}^{\flat}$$

and

$$\kappa\langle\langle t_1^{p^{-\infty}},\ldots,t_m^{p^{-\infty}}\rangle\rangle_{s:\phi^r;[i_0]}^{\flat}\subset\kappa\langle\langle t_1^{p^{-\infty}},\ldots,t_m^{p^{-\infty}}\rangle\rangle_{s:\phi^r;[i_0+\lceil\log_p m\rceil]}^{\#}$$

as sets of formal series.

(2) *Let n_0 be a natural number. If i_1 is a natural number such that $i_1\geq\max\big(s-r,s\cdot\lceil\frac{n_0}{r}\rceil\big)$, then*

$$\kappa\langle\langle t_1^{p^{-\infty}},\ldots,t_m^{p^{-\infty}}\rangle\rangle_{s:\phi^r,\geq n_0}^{\#}\subset\kappa\langle\langle t_1^{p^{-\infty}},\ldots,t_m^{p^{-\infty}}\rangle\rangle_{s:\phi^r;[i_1]}^{\#}$$

and

$$\kappa\langle\langle t_1^{p^{-\infty}},\ldots,t_m^{p^{-\infty}}\rangle\rangle_{s:\phi^r,\geq n_0}^{\flat}\subset\kappa\langle\langle t_1^{p^{-\infty}},\ldots,t_m^{p^{-\infty}}\rangle\rangle_{s:\phi^r;[i_1]}^{\flat}.$$

(3) *Let i_0 be a natural number. We have*

$$\kappa\langle\langle t_1^{p^{-\infty}},\ldots,t_m^{p^{-\infty}}\rangle\rangle_{s:\phi^r;[i_0]}^{\#}\subset\kappa\langle\langle t_1^{p^{-\infty}},\ldots,t_m^{p^{-\infty}}\rangle\rangle_{p^{i_0r/(s-r)};0}^{r/(s-r),\#}$$

and

$$\kappa\langle\langle t_1^{p^{-\infty}},\ldots,t_m^{p^{-\infty}}\rangle\rangle_{s:\phi^r;[i_0]}^{\flat}\subset\kappa\langle\langle t_1^{p^{-\infty}},\ldots,t_m^{p^{-\infty}}\rangle\rangle_{p^{i_0r/(s-r)};0}^{r/(s-r),\flat}$$

PROOF. The first inclusion in (1) is obvious. The second inclusion in (1) holds because

$$(t_1,\ldots,t_m)^{p^{j+\lceil\log_p m\rceil}}\subset(t_1^{p^j},\ldots,t_m^{p^j})$$

for all $j\in\mathbb{N}$. The statements (2), (3) are easy exercises. □

(4.1.3) LEMMA. *Let $\kappa\supset\mathbb{F}_p$ be a perfect field. Let $E>0, C>0$ be positive real numbers. Let $d\geq 0$ be a non-negative real number as in* 3.6.1.

(1) *We have natural inclusions*

$$\kappa\langle\langle t_1^{p^{-\infty}},\ldots,t_m^{p^{-\infty}}\rangle\rangle_{C;d}^{E,\#}\subset\kappa\langle\langle t_1^{p^{-\infty}},\ldots,t_m^{p^{-\infty}}\rangle\rangle_{C;d}^{E,\flat}$$

and

$$\kappa\langle\langle t_1^{p^{-\infty}},\ldots,t_m^{p^{-\infty}}\rangle\rangle_{C;d}^{E,\flat}\subset\kappa\langle\langle t_1^{p^{-\infty}},\ldots,t_m^{p^{-\infty}}\rangle\rangle_{C\cdot m^E;d/m}^{E,\#}.$$

(2) *Let $r < s$ be positive integers such that*

$$E < \frac{r}{s-r}.$$

Suppose that i_2 a sufficiently natural number such that

$$p^{\lceil m/r \rceil \cdot (s-r) - i_2} \leq C^{-1/E} \cdot p^{m/E} - d$$

for every integer $m \geq \frac{r \cdot i_2}{s-r}$. Note that such an integer i_2 exists because $\frac{s-r}{r} < \frac{1}{E}$. Then

$$\kappa\langle\langle t_1^{p^{-\infty}}, \ldots, t_m^{p^{-\infty}} \rangle\rangle_{C;d}^{E,\#} \subset \kappa\langle\langle t_1^{p^{-\infty}}, \ldots, t_m^{p^{-\infty}} \rangle\rangle_{s:\phi^r;[i_2]}^{\#}$$

and

$$\kappa\langle\langle t_1^{p^{-\infty}}, \ldots, t_m^{p^{-\infty}} \rangle\rangle_{C;d}^{E,\flat} \subset \kappa\langle\langle t_1^{p^{-\infty}}, \ldots, t_m^{p^{-\infty}} \rangle\rangle_{s:\phi^r;[i_2]}^{\flat}.$$

(4.1.4) **Lemma.** *Let $(R, \mathfrak{m})$ be an equi-characteristic $p > 0$ complete Noetherian local ring. Let $s > r > 0$ be positive integers. Let i_0 be a natural number. We have*

$$(R, \mathfrak{m})_{s:\phi^r;[i_0]}^{\mathrm{perf},\#} \subset (R, \mathfrak{m})_{s:\phi^r;[i_0]}^{\mathrm{perf},\flat}.$$

Moreover if the maximal ideal $\mathfrak{m}$ can be generated by n elements, then

$$(R, \mathfrak{m})_{s:\phi^r;[i_0]}^{\mathrm{perf},\flat} \subset (R, \mathfrak{m})_{s:\phi^r;[i_0 + \lceil \log_p n \rceil]}^{\mathrm{perf},\#}.$$

(4.2) A local homomorphism h between two equi-characteristic-p complete Noetherian local domains induces ring homomorphisms between their complete restricted perfections. We show that injective local homomorphisms induce injections on complete restricted perfections.

(4.2.1) **Lemma.** *Let $(R_1, \mathfrak{m}_1)$, $(R_2, \mathfrak{m}_2)$ equi-characteristic-p complete Noetherian local domains with perfect residue fields κ_1 and κ_2. Let $h : R_1 \to R_2$ be a ring homomorphism such that $h(\mathfrak{m}_1) \subseteq \mathfrak{m}_2$.*

(a) *Let A, b, d be real numbers, $A, b > 0$, $d \geq 0$. Let $\iota_1 : R_1 \to (R_1, \mathfrak{m}_1)_{A,b;d}^{\mathrm{perf},\flat}$ be the natural ring homomorphism from R_1 to its complete restricted completion $(R_1, \mathfrak{m}_1)_{A,b;d}^{\mathrm{perf},\flat}$. Similarly we have a natural ring homomorphism $\iota_2 : R_2 \to (R_2, \mathfrak{m}_1)_{A,b;d}^{\mathrm{perf},\flat}$. The ring homomorphism h induces a homomorphism from*

$$\tilde{h} : (R_1, \mathfrak{m}_1)_{A,b;d}^{\mathrm{perf},\flat} \to (R_2, \mathfrak{m}_2)_{A,b;d}^{\mathrm{perf},\#}$$

such that $\tilde{h} \circ \iota_1 = \iota_2 \circ h$.

(b) *Let $r, s, i_0 \in \mathbb{N}$, $r, s > 0$, $i_0 \geq 0$ Let $\iota_1 : R_1 \to (R_1, \mathfrak{m}_1)_{b:\phi^A;[d]}^{\mathrm{perf},\#}$ be the natural ring homomorphism from R_1 to its complete restricted completion $(R_1, \mathfrak{m}_1)_{s:\phi^r;[i_0]}^{\mathrm{perf},\#}$. Similarly we have a ring homomorphism $\iota_2 : R_2 \to (R_2, \mathfrak{m}_1)_{s:\phi^r;[i_0]}^{\mathrm{perf},\#}$. The ring homomorphism h induces a homomorphism from*

$$h^\# : (R_1, \mathfrak{m}_1)_{s:\phi^r;[i_0]}^{\mathrm{perf},\#} \to (R_2, \mathfrak{m}_2)_{s:\phi^r;[i_0]}^{\mathrm{perf},\#}$$

such that $h^\# : \circ \iota_1 = \iota_2 \circ h$. Similarly h extends naturally to a ring homomorphism

$$h^\flat : \ (R_1, \mathfrak{m}_1)_{s:\phi^r;[i_0]}^{\mathrm{perf},\flat} \to (R_1, \mathfrak{m}_1)_{s:\phi^r;[i_0]}^{\mathrm{perf},\flat}.$$

The proof is easy, therefore omitted. $\square$

(4.2.2) PROPOSITION. *Let $(R,\mathfrak{m})$ be a Noetherian local domain. Assume that the integral closure S of R in the field of fraction of R is a finite R-module. There exists a natural number n_0 such that such that*

$$\{x \in R \mid x^a \in \mathfrak{m}^n\} \subset \mathfrak{m}^{\lfloor \frac{n}{a} - n_0 \rfloor} \quad \forall a \in \mathbb{N}_{>0},\ \forall n \geq a \cdot n_0.$$

PROOF. Let $\mathrm{Bl}_{\mathfrak{m}}(R) = \mathrm{Spec}\big(\oplus_{j\in\mathbb{N}} \mathfrak{m}^j\big)$ be the blow-up of $\mathrm{Spec}(R/\mathfrak{m}) \subset \mathrm{Spec}(R)$, and let Y be the normalization of $\mathrm{Bl}_{\mathfrak{m}}(R)$. The Noetherian normal domain S is semi-local; let $\tilde{\mathfrak{m}}_1,\ldots,\tilde{\mathfrak{m}}_s$ be the maximal ideals of S. The natural morphism $\pi : Y \to \mathrm{Spec}(R)$ factors through a unique morphism $f : Y \to \mathrm{Spec}(S)$: $\pi = g \circ f$, where $g : \mathrm{Spec}(S) \to \mathrm{Spec}(R)$ corresponds to the inclusion $R \hookrightarrow S$. We know that $\Gamma(Y,\mathscr{O}_Y) = S$ because S is normal.

Let $\mathscr{L} = \pi^*\mathfrak{m} = \mathfrak{m}\cdot\mathscr{O}_{Y_i}$ be the pull-back to Y of the maximal ideal $\mathfrak{m} \subset R$; it is an invertible sheaf of $\mathscr{O}_Y$-ideals on Y and is an ample invertible $\mathscr{O}_Y$-module. The closed subset $\mathcal{S}pec_Y(\mathscr{O}_Y/\mathfrak{m}\mathscr{O}_Y)$ of Y is the union of irreducible Weil divisors $E_1,\ldots,E_r$, where r is a positive integer. There exist positive integers $e_1,\ldots,e_r \in \mathbb{N}_{>0}$ such that

$$\mathscr{L} = \mathscr{O}_Y\big(-(e_1E_1 + \cdots + e_rE_r)\big).$$

Define for each $n \in \mathbb{N}$ an ideal $J_n \subset S$ by

$$J_n := \Gamma(Y,\mathscr{L}^n) \subseteq \Gamma(Y,\mathscr{O}_Y) = S.$$

It is clear that $J_1 \subset \tilde{\mathfrak{m}}_1 \cap \cdots \cap \tilde{\mathfrak{m}}_s$, and $\mathfrak{m}^n S \subseteq J_n$ for all $n \in \mathbb{N}$.

Claims.

1. There exist a positive natural number $n_1 \in \mathbb{N}$ such that $J_{n+1} = \mathfrak{m}J_n$ for all integers $n \geq n_1$. In particular $J_n \subseteq \mathfrak{m}^{n-n_1}S$ for all $n \geq n_1$
2. There exists a natural number $n_2 \in \mathbb{N}$ such that $R \cap (\mathfrak{m}^{n+n_2}S) \subset \mathfrak{m}^n$ for all $n \in \mathbb{N}$.
3. We have $J_{n+n_1+n_2} \cap R \subseteq \mathfrak{m}^n$ for all $n \in \mathbb{N}$, with the constants n_1, n_2 in claims 1 and 2 respectively.
4. If $y \in S$, $a \in \mathbb{N}_{>0}$, $n \in \mathbb{N}$ and $y^a \in J_n$, then $y \in J_{\lfloor n/a \rfloor}$.
5. If $x \in R$, $a \in \mathbb{N}_{>0}$, $n \in \mathbb{N}$, and $x^a \in \mathfrak{m}^n$, then $x \in \mathfrak{m}^{\lfloor n/a \rfloor - n_1 - n_2}$ for all $n \geq a(n_1+n_2)$.

Obviously proposition 4.2.2 follows from claim 5, with $n_0 = n_1 + n_2$. $J_1 \subset \tilde{\mathfrak{m}}_1 \cap \cdots \cap \tilde{\mathfrak{m}}_s$ and S is Noetherian.

Claim 1 is a consequence of the fact $\mathscr{L} = \mathfrak{m}\mathscr{O}_Y$ and the general finiteness property for proper morphism [EGA III, §5, Cor. 3.3.2] applied to the proper morphism $Y \to \mathrm{Spec}(R)$: we see that the graded $\oplus_{i\geq 0}\mathfrak{m}^i$-module

$$\oplus_{i\geq 0}\Gamma(Y,\mathfrak{m}^i\mathscr{O}_Y) = \oplus_{i\geq 0} J_i$$

is a finitely generated as a graded module, and claim 1 follows.

Claim 2 is the Artin–Rees lemma applied to the finite R-module S. Claim 3 is a formal consequence of claims 1 and 2, while claim 5 is a formal consequence of claims 3 and 4.

It remains to prove claim 4. Given an element $y \in S$ such that $y^a \in J_n$. For each $i = 1, \ldots, s$, let S_i be the localization of S at the generic point of the exceptional divisor E_i. Each E_i is a discrete valuation ring; let $\mathrm{ord}_{E_i}(\cdot)$ be associated normalized valuation with value group $\mathbb{Z}$. The assumption that $y^a \in J_n$ implies that $\mathrm{ord}_{E_i}(y^a) \geq n \cdot e_i$ for all i, therefore

$$\mathrm{ord}_{E_i}(y) \geq \tfrac{n e_i}{a} \geq \lfloor \tfrac{n}{a} \rfloor e_i$$

for $i = 1, \ldots, s$. Therefore there exists an open subset $U \subset Y$ which contains $Y \smallsetminus (E_1 \cup \cdots \cup E_s)$ and also the generic point of E_i for $i = 1, \ldots, s$, such that y defines a section of $\mathscr{L}^{\lfloor \frac{n}{a} \rfloor}$ over U. Because Y is normal and the codimension of U in Y is at least 2, y extends uniquely to a section of $\mathscr{L}^{\lfloor \frac{n}{a} \rfloor}$ over Y. We have proved claim 4 and proposition 4.2.2. □

(4.2.3) Corollary. *Let $(R, \mathfrak{m})$ be a complete Noetherian local domain of equi-characteristic $p > 0$, with perfect residue field κ.*

(i) *Let $A, b > 0$, $d \geq 0$ be real numbers. The linear topology on the ring $\big((R,\mathfrak{m})^{\mathrm{perf},\flat}_{A,b;d}\big)_{\mathrm{fin}}$ defined by the filtration on $\big((R,\mathfrak{m})^{\mathrm{perf},\flat}_{A,b;d}\big)_{\mathrm{fin}}$ induced by the filtration $\big(\mathrm{Fil}^u_{R^{\mathrm{perf}},\mathrm{deg}}\big)$ of R^{perf} is separated. Therefore the natural ring homomorphism*

$$\big((R,\mathfrak{m})^{\mathrm{perf},\flat}_{A,b;d}\big)_{\mathrm{fin}} \longrightarrow (R,\mathfrak{m})^{\mathrm{perf},\flat}_{A,b;d}$$

from $\big((R,\mathfrak{m})^{\mathrm{perf},\flat}_{A,b;d}\big)_{\mathrm{fin}}$ to its completion $(R,\mathfrak{m})^{\mathrm{perf},\flat}_{A,b;d}$ is an injection.

(ii) *Let r, s, n_0 be natural numbers, $0 < r < s$. The natural ring homomorphism*

$$\big((R,\mathfrak{m})^{\mathrm{perf},\#}_{s:\phi^r;[i_0]}\big)_{\mathrm{fin}} \longrightarrow (R,\mathfrak{m})^{\mathrm{perf},\#}_{s:\phi^r;[i_0]}$$

and

$$\big((R,\mathfrak{m})^{\mathrm{perf},\flat}_{s:\phi^r;[i_0]}\big)_{\mathrm{fin}} \longrightarrow (R,\mathfrak{m})^{\mathrm{perf},\flat}_{s:\phi^r;[i_0]}$$

are injections.

Proof. The statements (i) and (ii) are easy consequences of 4.2.2. We note that the statements (i) and (ii) are in fact equivalent. □

(4.2.4) Corollary. *Notation as in* 4.2.1. *In particular $h : (R_1, \mathfrak{m}_1) \to (R_2, \mathfrak{m}_2)$ is a ring homomorphism between equi-characteristic-p complete Noetherian local domains. Suppose that h is an injection. Then the induced homomorphisms $\tilde{h}$, $h^\#$ and $h^\flat$ in* 4.2.1 *are also injections.*

Proof. This statement is a corollary of 4.2.3. We explain the proof for $\tilde{h}$. The same argument in general topology also proves the statement for $h^\#$ and $h^\flat$.

The injective ring homomorphism $h : R_1 \to R_2$ induces a injective ring homomorphism

$$h' : \big((R_1,\mathfrak{m}_1)^{\mathrm{perf},\flat}_{A,b;d}\big)_{\mathrm{fin}} \longrightarrow \big((R_2,\mathfrak{m}_2)^{\mathrm{perf},\flat}_{A,b;d}\big)_{\mathrm{fin}}.$$

According to 4.2.3, we can identify $\big((R_2,\mathfrak{m}_2)^{\mathrm{perf},\flat}_{A,b;d}\big)_{\mathrm{fin}}$ as a subring of $(R_2,\mathfrak{m}_2)^{\mathrm{perf},\flat}_{A,b;d}$. The injection h' identifies $\big((R_1,\mathfrak{m}_1)^{\mathrm{perf},\flat}_{A,b;d}\big)_{\mathrm{fin}}$ also as a subring of $(R_2,\mathfrak{m}_2)^{\mathrm{perf},\flat}_{A,b;d}$. (It is actually contained in

$\big((R_2,\mathfrak{m}_2)^{\mathrm{perf},\flat}_{A,b;d}\big)_{\mathrm{fin}}$.) Let $\big((R_2,\mathfrak{m}_2)^{\mathrm{perf},\flat}_{A,b;d}\big)^{\wedge}_{\mathrm{fin}}$ be the closure of $\big((R_2,\mathfrak{m}_2)^{\mathrm{perf},\flat}_{A,b;d}\big)_{\mathrm{fin}}$ in the topological ring $(R_2,\mathfrak{m}_2)^{\mathrm{perf},\flat}_{A,b;d}$.

The topology on $\big((R_1,\mathfrak{m}_1)^{\mathrm{perf},\flat}_{A,b;d}\big)_{\mathrm{fin}}$ induced by the filtration $\big(\mathrm{Fil}^u_{R_1^{\mathrm{perf}},\deg}\big)$ is stronger than the topology $(R_2,\mathfrak{m}_2)^{\mathrm{perf},\flat}_{A,b;d}$. The closure of $\big((R_1,\mathfrak{m}_1)^{\mathrm{perf},\flat}_{A,b;d}\big)_{\mathrm{fin}}$ with respect to this stronger topology is naturally identified with a subset of $\big((R_2,\mathfrak{m}_2)^{\mathrm{perf},\flat}_{A,b;d}\big)^{\wedge}_{\mathrm{fin}}$. We have shown that $\tilde{h}$ is an injection. □

(4.3) Let κ be a perfect field. Denote by σ the Frobenius automorphism on κ, which sends every element $x\in\kappa$ to x^p. Let $u_1,\dots,u_a$ and $t_1,\dots,t_m$ be variables. Let $\kappa[u_1^{p^{-\infty}},\dots,u_a^{p^{-\infty}}]$ be the perfection of the polynomial ring $\kappa[u_1,\dots,u_m]$. Elements of $\kappa[u_1^{p^{-\infty}},\dots,u_a^{p^{-\infty}}]$ are finite sums of the form

$$\sum_{J\in\mathbb{N}[1/p]^a} b_J\,\underline{u}^J,$$

where $b_J\in\kappa$ for all $J\in\mathbb{N}[1/p]^a$, and all $b_J=0$ for all J outside of a finite subset of $\mathbb{N}[1/p]^a$.

We observe that for each element $i\in\mathbb{N}[1/p]$, the i-th power of an element

$$\sum_{J\in\mathbb{N}[1/p]^a} b_J\,\underline{u}^J \;\in\; \kappa[u_1^{p^{-\infty}},\dots,u_a^{p^{-\infty}}]$$

is well-defined: write $i=\frac{r}{p^s}$ with $r\in\mathbb{Z}$ and $s\in\mathbb{N}$, and define

$$\Big(\sum_{J\in\mathbb{N}[1/p]^a} b_J\,\underline{u}^J\Big)^{r/p^s} := \Big(\sum_{J\in\mathbb{N}[1/p]^a} b_J^{\sigma^{-s}}\cdot\underline{u}^{p^{-s}J}\Big)^r.$$

Therefore if $f\in\kappa[u_1^{p^{-\infty}},\dots,u_a^{p^{-\infty}}]$ and $g_1,\dots,g_a\in\kappa[t_1^{p^{-\infty}},\dots,t_m^{p^{-\infty}}]$, the composition $f(g_1,\dots,g_a)$ is a well-defined element of $\kappa[t_1^{p^{-\infty}},\dots,t_m^{p^{-\infty}}]$. It is not difficult to show that the operation of composition extends to complete restricted perfection of power series rings.

(4.3.1) Lemma. *Let $\kappa\supset\mathbb{F}_p$ be a perfect field. Let $u_1,\dots,u_a$ and $t_1,\dots,t_m$ be variables. Suppose that $f\in\kappa\langle\langle u_1^{p^{-\infty}},\dots,u_a^{p^{-\infty}}\rangle\rangle^{E_1,\flat}_{C_1;d_1}$, and $g_i\in\kappa\langle\langle t_1^{p^{-\infty}},\dots,t_m^{p^{-\infty}}\rangle\rangle^{E_2,\flat}_{C_2;d_2}$ for $i=1,\dots,a$. Assume for simplicity that $C_1,C_2,d_1,d_2\ge 1$. There exists a positive real number d_3 such that*

$$f(g_1(\underline{t}),\dots,g_a(\underline{t}))\in\kappa\langle\langle t_1^{p^{-\infty}},\dots,t_m^{p^{-\infty}}\rangle\rangle^{E_3,\flat}_{C_3;d_3}$$

where

- $E_3=E_1\cdot E_2+E_1+E_2$,
- $C_3=C_2\cdot C_1^{1+E_2}\cdot(\frac{1}{e_2})^{E_1(1+E_2)}$, *and*
- $e_2:=\mathrm{Min}\Big\{|J|_\sigma:\ J\neq 0\ \text{ and }\ \underline{t}^J\in\kappa\langle\langle t_1^{p^{-\infty}},\dots,t_m^{p^{-\infty}}\rangle\rangle^{E_2,\flat}_{C_2;d_2}\Big\}$.

A trivial lower bound for e_2 is

$$e_2\ge C_2^{-1}(1+d_2)^{-E_2}.$$

PROOF. Let $S_2 \subset \mathbb{N}[1/p]^m$ be the set of supports of all formal series in $\kappa\langle\langle t_1^{p^{-\infty}}, \dots, t_m^{p^{-\infty}}\rangle\rangle_{C_2;d_2}^{E_2,\flat}$ whose constant terms are 0. Similarly let $S_1 \subset \mathbb{N}[1/p]^a$ be the set of supports of all formal series in $\kappa\langle\langle u_1^{p^{-\infty}}, \dots, u_a^{p^{-\infty}}\rangle\rangle_{C_1;d_1}^{E_1,\flat}$ whose constant terms are 0. By definition $e_2 = \mathrm{Min}\{|J|_\sigma \colon J \in S_2\}$. Every non-zero element K in the support of $f(g_1(\underline{t}), \dots, g_a(\underline{t}))$ can be written in the following form

$$K = p^{-r}\,(J_{1,1} + \cdots + J_{1,i_1} + \cdots + J_{a,i} + \cdots + J_{a,i_a}),$$

where

- $(i_1, \dots, i_a) \in \mathbb{N}^a$, $r = \max(-\mathrm{ord}_p(i_1), \dots, -\mathrm{ord}_p(i_1), 0)$,
- $I := p^{-r}(i_1, \dots, i_a) \in S_1$, and
- $J_{\nu,\mu} \in S_2$ for all $\nu = 1, \dots, a$ and all $\mu = 1, \dots, i_a$.

Clearly the following inequalities hold.

(4.3.1.1) $$|K|_\sigma \geq e_2 \cdot p^{-r}(i_1\, e + \cdots + i_s\, e) = e_2 \cdot |I|_\sigma$$

(4.3.1.2) $$M_\sigma := \mathrm{Max}\left\{|J_{\nu,\mu}|_\sigma \colon\ 1 \leq \mu \leq i_\nu,\ 1 \leq \nu \leq a\right\} \leq p^r \cdot |K|_\sigma$$

(4.3.1.3) $$p^{-r} \cdot |K|_p \leq \mathrm{Max}\left\{|J_{\nu,\mu}|_p \colon\ 1 \leq \mu \leq i_\nu, 1 \leq \nu \leq a\right\} =: M_p$$

From the definitions of the rings $\kappa\langle\langle t_1^{p^{-\infty}}, \dots, t_m^{p^{-\infty}}\rangle\rangle_{C_2;d_2}^{E_2,\flat}$ and $\kappa\langle\langle u_1^{p^{-\infty}}, \dots, u_a^{p^{-\infty}}\rangle\rangle_{C_1;d_1}^{E_1,\flat}$ we know that

(4.3.1.4) $$p^r \leq C_1(|I|_\sigma + d_1)^{E_1} \leq C_1 \cdot (\tfrac{1}{e_2}\,|K|_\sigma + d_1)^{E_1}$$

(4.3.1.5) $$M_p \leq C_2(M_\sigma + d_2)^{E_2}$$

Combining the above inequalities, we see that

$$|K|_p \leq p^r \cdot C_2 \cdot (p^r\,|K|_\sigma + d_2)^{E_2} \leq C_1(e_2^{-1} \cdot |K|_\sigma + d_1)^{E_1} \cdot C_2\left(C_1(e_2^{-1} \cdot |K|_\sigma + d_1)^{E_1}|K|_\sigma + d_2\right)^{E_2}$$

The last term in the above displayed inequality is a polynomial in $|K|_\sigma$ of degree

$$E_3 := E_1 + E_2 + E_1 \cdot E_2$$

whose leading term is

$$C_3 := C_1^{1+E_2} \cdot C_2 \cdot (\tfrac{1}{e_2})^{E_1(1+E_2)}.$$

Hence for a sufficiently large constant d_3 it is bounded above by $C_3(|K|_\sigma + d_3)^{E_3}$ for all $|K|_\sigma \geq 0$. We have proved the main assertion of lemma 4.3.1.

To see the trivial lower bound for e_2, we only have to observe that if $J \in S_2$ and $|J|_\sigma \leq 1$ and $J \neq \mathbb{N}^m$, then

$$|J|_\sigma \geq |J|_p^{-1} \geq \left(C_2(1 + d_2)^{E_2}\right)^{-1}. \qquad \square$$

REMARK. Composition can be formulated for complete restricted perfections of general equi-characteristic-p complete Noetherian local rings.

(4.4) Let $\kappa \supset \mathbb{F}_p$ be a perfect field. We will generalize the Weierstrass preparation theorem to complete restricted perfections $\kappa\langle\langle t_1^{p^{-\infty}}, \ldots, t_m^{p^{-\infty}}\rangle\rangle_{C;d}^{E,\flat}$ of power series rings.

(4.4.1) Definition. Let $\kappa \supset \mathbb{F}_p$ be a perfect field of characteristic $p > 0$.

(i) Let $\kappa\langle\langle t_1^{p^{-\infty}}, \ldots, t_m^{p^{-\infty}}\rangle\rangle$ be the set of all formal series of the form

$$\sum_{i_1,\ldots,i_m \in \mathbb{N}[1/p]} b_{i_1,\ldots,i_m} t_1^{i_1} \cdots t_m^{i_m}$$

where $b_{i_1,\ldots,i_m} \in \kappa$ for all $(i_1, \ldots, i_m) \in \mathbb{N}[1/p]^m$. Note that $\kappa\langle\langle t_1^{p^{-\infty}}, \ldots, t_m^{p^{-\infty}}\rangle\rangle$ has a natural structure as a module over the perfection $\kappa[t_1^{p^{-\infty}}, \ldots, t_m^{p^{-\infty}}]$ of the polynomial ring $\kappa[t_1, \ldots, t_m]$.

(ii) Let $e \in \mathbb{Z}[1/p]_{>0}$ be a positive rational number whose denominator is a powere of p. An non-zero element $F(t_1, \ldots, t_m)$ in $\kappa\langle\langle t_1^{p^{-\infty}}, \ldots, t_m^{p^{-\infty}}\rangle\rangle$ is *regular of order e* in the variable t_m if the formal series $F(0, \ldots, 0, t_m)$ in one variable t_m has order e. In other words when $F(t_1, \ldots, t_m)$ is expanded in powers of t_m with coefficients in formal series of $t_1, \ldots, t_{m-1}$,

$$F(t_1, \ldots, t_m) = \sum_{j \in \mathbb{N}[1/p]} F_j(t_1, \ldots, t_{m-1})\, t_m^j$$

we have

$$F_j(0, \ldots, 0) = 0 \quad \forall\, j < e, \quad \text{and} \quad F_e(0, \ldots, 0) \in \kappa^{\times}.$$

(4.4.2) Proposition. *Let $F(t_1, \ldots, t_m)$ be a non-zero element of $\kappa\langle\langle t_1^{p^{-\infty}}, \ldots, t_m^{p^{-\infty}}\rangle\rangle_{C;d}^{E,\flat}$ which is regular of order $e > 0$ in the variable t_m.*

(1) *There exist constants $C' > 0, d' > 0$ depending only on the parameters C, d, E, m such that for every element $G \in \kappa\langle\langle t_1^{p^{-\infty}}, \ldots, t_m^{p^{-\infty}}\rangle\rangle_{C;d}^{E,\flat}$, there exists elements $U, R \in \kappa\langle\langle t_1^{p^{-\infty}}, \ldots, t_m^{p^{-\infty}}\rangle\rangle_{C';d'}^{E,\flat}$ such that*

$$G = U \cdot F + R$$

and for every element $I = (i_1, \ldots, i_m) \in \mathbb{N}[1/p]^m \in \mathrm{supp}(R)$ in the support of R, the inequalities

$$i_m < e, \quad i_1 + \cdots + i_{m-1} > 0$$

hold. Moreover the quotient U and the remainder R are uniquely determined by G and F. The constants C' and d' can be taken to be

$$C' = C \cdot (1 + \varepsilon_0^{-1})^E, \quad d' = \tfrac{d+e}{1+\varepsilon_0^{-1}},$$

where ε_0 is defined in 4.4.6.

(2) *Suppose that $e = \mathrm{Min}\{|I|_\sigma : I \in \mathrm{supp}(F)\}$. Then $U, R \in \kappa\langle\langle t_1^{p^{-\infty}}, \ldots, t_m^{p^{-\infty}}\rangle\rangle_{C;d+2e}^{E,\flat}$.*

(4.4.3) The uniqueness part 4.4.2 (1) is easy: suppose that

$$G = U' \cdot F + R'$$

with $U', R' \in \kappa\langle\langle t_1^{p^{-\infty}}, \ldots, t_m^{p^{-\infty}}\rangle\rangle_{C';d'}^{E,\flat}$ and R' satisfies the same condition as R. Then $(U' - U)\cdot F = R - R'$. Examine the degree in t_m of monomials appearing on both sides, we see that $R' - R = 0$. Therefore $(U' - U)\cdot F = 0$. Hence $U' - U = 0$ because $\kappa\langle\langle t_1^{p^{-\infty}}, \ldots, t_m^{p^{-\infty}}\rangle\rangle_{C';d'}^{E,\flat}$ is an integral domain.

Our proof of the existence part of 4.4.2 is a generalization of the constructive proof of the Weierstrass preparation theorem in [7, p. 139]. The actual proof is in 4.4.5–4.4.8 below; the crucial estimates are in lemma 4.4.7. We will review the argument in [7, p. 139] after recalling the definition of the linear operators used in [7, p. 139].

(4.4.4) Definition. Let $\kappa \supset \mathbb{F}_p$ be a perfect field of characteristic p. Let $t_1, \ldots, t_m$ be variables. Let $e > 0$ be a positive rational number in $\mathbb{N}[1/p]$. Let $F \in \kappa\langle\langle t_1^{p^{-\infty}}, \ldots, t_m^{p^{-\infty}}\rangle\rangle$ be a formal series which is regular of order e in the variable t_m.

(i) Define κ-linear operators

$$\eta, \rho : \kappa\langle\langle t_1^{p^{-\infty}}, \ldots, t_m^{p^{-\infty}}\rangle\rangle \longrightarrow \kappa\langle\langle t_1^{p^{-\infty}}, \ldots, t_m^{p^{-\infty}}\rangle\rangle$$

depending on e, by

$$f = t_m^e \cdot \eta(f) + \rho(f)$$

for every element $f \in \kappa\langle\langle t_1^{p^{-\infty}}, \ldots, t_m^{p^{-\infty}}\rangle\rangle$. Clearly every monomial $t_1^{i_1}\cdots t_m^{i_m}$ with exponent $(i_1, \ldots, i_m) \in \mathbb{N}[1/p]^m$, $\eta(t_1^{i_1}\cdots t_m^{i_m})$ and $\rho(t_1^{i_1}\cdots t_m^{i_m})$ are given by

$$\eta(t_1^{i_1}\cdots t_m^{i_m}) = \begin{cases} t_1^{i_1}\cdots t_{m-1}^{i_{m-1}}\cdot t_m^{i_m - e} & \text{if } i_m \geq e \\ 0 & \text{if } i_m < e \end{cases} \tag{1}$$

$$\rho(t_1^{i_1}\cdots t_m^{i_m}) = \begin{cases} 0 & \text{if } i_m \geq e \\ t_1^{i_1}\cdots t_m^{i_m} & \text{if } i_m < e \end{cases}. \tag{2}$$

For a general element $f = \sum_{i_1,\ldots,i_m \in \mathbb{N}[1/p]} b_{i_1,\ldots,i_m} t_1^{i_1}\cdots t_m^{i_m} \in \kappa\langle\langle t_1^{p^{-\infty}}, \ldots, t_m^{p^{-\infty}}\rangle\rangle$, we have

$$\eta(f) = \sum_{i_1,\ldots,i_m \in \mathbb{N}[1/p]} b_{i_1,\ldots,i_m}\, \eta(t_1^{i_1}\cdots t_m^{i_m}) \tag{3}$$

$$\rho(f) = \sum_{i_1,\ldots,i_m \in \mathbb{N}[1/p]} b_{i_1,\ldots,i_m}\, \rho(t_1^{i_1}\cdots t_m^{i_m})). \tag{4}$$

Note that if $f \in \kappa\langle\langle t_1^{p^{-\infty}}, \ldots, t_m^{p^{-\infty}}\rangle\rangle_{C;d}^{E,\flat}$ for some parameter $E, C > 0$ and $d \geq 0$, then $\rho(f) \in \kappa\langle\langle t_1^{p^{-\infty}}, \ldots, t_m^{p^{-\infty}}\rangle\rangle_{C;d}^{E,\flat}$ and $\eta(f) \in \kappa\langle\langle t_1^{p^{-\infty}}, \ldots, t_m^{p^{-\infty}}\rangle\rangle_{C;d+e}^{E,\flat}$.

(ii) Suppose that formal series F is in $\kappa\langle\langle t_1^{p^{-\infty}}, \ldots, t_m^{p^{-\infty}}\rangle\rangle_{C;d}^{E,\flat}$ for some constants $E > 0$, $C > 0$, $d \geq 0$. Define a κ-linear operator

$$\mu : \bigcup_{C'',d''>0} \kappa\langle\langle t_1^{p^{-\infty}}, \ldots, t_m^{p^{-\infty}}\rangle\rangle_{C'';d''}^{E,\flat} \longrightarrow \kappa\langle\langle t_1^{p^{-\infty}}, \ldots, t_m^{p^{-\infty}}\rangle\rangle$$

depending on e and F, by

$$\mu(f) := \eta(-\eta(F)^{-1} \cdot \rho(F) \cdot f)$$

for all $C'', d'' > 0$ and every element $f \in \kappa\langle\langle t_1^{p^{-\infty}}, \ldots, t_m^{p^{-\infty}}\rangle\rangle_{C'';d''}^{E,\flat}$. Note that $\eta(F)$ is a formal series whose contant term is in $\kappa^\times$, therefore $\eta(F)^{-1} \in \kappa\langle\langle t_1^{p^{-\infty}}, \ldots, t_m^{p^{-\infty}}\rangle\rangle_{C;d+e}^{E,\flat}$ because $\eta(F) \in \kappa\langle\langle t_1^{p^{-\infty}}, \ldots, t_m^{p^{-\infty}}\rangle\rangle_{C;d+e}^{E,\flat}$. The product $\eta(F)^{-1} \cdot \rho(F) \cdot f$ on the right hand side of the above displayed formula makes sense because both formal series $\rho(F)$ is also an element of $\kappa\langle\langle t_1^{p^{-\infty}}, \ldots, t_m^{p^{-\infty}}\rangle\rangle_{C;d+e}^{E,\flat}$.

(4.4.5) The proof in [7, p. 139] is a fixed-point-theorem argument. Suppose that the equation

$$V = \eta(G) + \mu(V) \tag{4.4.5.1}$$

has a solution V in $\kappa\langle\langle t_1^{p^{-\infty}}, \ldots, t_m^{p^{-\infty}}\rangle\rangle_{C'';d''}^{E,\flat}$, and the parameters C'', d'' are such that $\eta(F)$ and $\rho(G)$ are also elements of $\kappa\langle\langle t_1^{p^{-\infty}}, \ldots, t_m^{p^{-\infty}}\rangle\rangle_{C'';d''}^{E,\flat}$. Let

$$U := \eta(F)^{-1} \cdot V. \tag{4.4.5.2}$$

Then we have

$$U \cdot \eta(F) = V = \eta(G) - \eta\big(\eta(F)^{-1} \cdot \rho(F) \cdot V\big) = \eta(G) - \eta\big(U \cdot \rho(F)\big). \tag{4.4.5.3}$$

By the definition of the operators η and ρ, we know that

$$U \cdot F = t_m^e \cdot U \cdot \eta(F) + U \cdot \rho(F),$$

hence

$$U \cdot \eta(F) = \eta(U \cdot F) - \eta\big(U \cdot \rho(F)\big). \tag{4.4.5.4}$$

From 4.4.5.3 and 4.4.5.4, we see that

$$\eta(G) = \eta(U \cdot F), \tag{4.4.5.5}$$

hence

$$G - \rho(G) = U \cdot F - \rho(U \cdot F). \tag{4.4.5.6}$$

In other words

$$G = U \cdot F + R,$$

where

$$R = \rho(G) - \rho(U \cdot F).$$

Note that $U = \eta(F)^{-1} \cdot V$ and R are both in $\kappa\langle\langle t_1^{p^{-\infty}}, \ldots, t_m^{p^{-\infty}}\rangle\rangle_{C'';d''}^{E,\flat}$ because we have assumed that $\eta(F)$ and $\rho(G)$ are both in $\kappa\langle\langle t_1^{p^{-\infty}}, \ldots, t_m^{p^{-\infty}}\rangle\rangle_{C'';d''}^{E,\flat}$.

(4.4.6) Definition. Suppose we are given parameters $e \in \mathbb{N}[1/p]_{>0}$, $E, C \in \mathbb{R}_{>0}$, and $d \in \mathbb{R}_{\geq 0}$. Let $T = T(m : e : E; C, d)$ be the subset of $\mathbb{N}[1/p]^m$ consisting of all m-tuples $(i_1, \ldots, i_m)$ in the support set $\mathrm{supp}(m : E; C, d+e)$ for $\kappa\langle\langle t_1^{p^{-\infty}}, \ldots, t_m^{p^{-\infty}}\rangle\rangle^{E,\flat}_{C;d+e}$ such that $(i_1, \ldots, i_{m-1}) \neq (0, \ldots, 0)$ $\mathbb{N}[1/p]^{m-1}$ and $i_m < e$. Define a positive constant ε_0 depending on parameters $m, e, E; C, d$ by

$$\varepsilon_0 = \varepsilon_0(m : e : E; C, d) := \min\left\{ \tfrac{i_1 + \ldots + i_{m-1}}{e} \,\middle|\, (i_1, \ldots, i_m) \in T(m : e : E; C, d) \right\}.$$

Note that this minimum is attained at some element of $T(m : e : E; C, d)$.

(4.4.7) Lemma. *Let $N \in \mathbb{N}$ be a positive integer. Consider the κ-linear operator*

$$\mu^n \colon \kappa\langle\langle t_1^{p^{-\infty}}, \ldots, t_m^{p^{-\infty}}\rangle\rangle^{E,\flat}_{C;d+e} \longrightarrow \kappa\langle\langle t_1^{p^{-\infty}}, \ldots, t_m^{p^{-\infty}}\rangle\rangle^{E,\flat}_{C;d+(N+1)\cdot e}.$$

defined in 4.4.4. *Let h be an element of $\kappa\langle\langle t_1^{p^{-\infty}}, \ldots, t_m^{p^{-\infty}}\rangle\rangle^{E,\flat}_{C;d+e}$. Let $J = (j_1, \ldots, j_{m-1}, j_m)$ be an exponent in the support* $\mathrm{supp}(\mu^N(h))$ *of the formal series $\mu^N(h)$.*

(i) $j_1 + \cdots + j_{m-1} \geq N \cdot \varepsilon_0 \cdot e.$

(ii) $|J|_p \leq C \cdot (1 + {\varepsilon_0}^{-1})^E \cdot \left(|J|_\sigma + \frac{d+e}{1+\varepsilon_0^{-1}} \right)^E$

(iii) *Suppose that* $e = \mathrm{Min}\{|I|_\sigma : I \in \mathrm{supp}(F)\}$. *Then*

$$|J|_p \leq C \cdot (|J|_\sigma + d + 2e)^E.$$

Proof. The statement (i) is obvious from the definition of the linear operator μ in 4.4.4. For statement (ii), we know that

$$|J|_p \leq C \cdot \big(|J|_\sigma + d + (N+1)e\big)^E$$

because $\mu^N\big(\langle\langle t_1^{p^{-\infty}}, \ldots, t_m^{p^{-\infty}}\rangle\rangle^{E,\flat}_{C;d+e}\big) \subseteq \kappa\langle\langle t_1^{p^{-\infty}}, \ldots, t_m^{p^{-\infty}}\rangle\rangle^{E,\flat}_{C;d+(N+1)e}$. We know from (i) that

$$N e \leq \varepsilon_0^{-1} \cdot (j_1 + \cdots + j_{m-1}) \leq \varepsilon_0^{-1} \cdot |J|_\sigma,$$

hence

$$|J|_p \leq C \cdot \big((1+\varepsilon_0)^{-1}) \cdot |J|_\sigma + d + e\big)^E \leq C \cdot (1 + \varepsilon_0^{-1})^E \cdot \left(|J|_\sigma + \frac{d+e}{1+\varepsilon_0^{-1}} \right)^E.$$

It remains to prove (iii). The assumption that $e = \mathrm{Min}\{|I|_\sigma : I \in \mathrm{supp}(F)\}$ implies that $|I'|_\sigma \geq e$ for every exponent $I' \in \mathrm{supp}(-\eta(F)^{-1} \cdot \rho(F))$. By the definition of the linear operator η, there exists exponents $I_0, \ldots, I_N$ with $I_0 \in \mathrm{supp}(h)$ and $I_j \in \mathrm{supp}(-\eta(F)^{-1} \cdot \rho(F))$ for $j = 1, \ldots, N$ such that

$$J = I_0 + I_1 + \ldots + I_N - (0, \ldots, 0, Ne).$$

So we have

$$|J|_p \leq \mathrm{Max}\left\{ |I_0|_p,\ |I_1|_p, \ldots, |I_N|_p,\ |e|_p \right\}$$

Because $(0,\ldots,0,e) \in \mathrm{supp}(F)$, we have

$$|e|_p \leq C \cdot (d+e)^E < C \cdot (|J|_\sigma + d + 2e)^E \,.$$

The assumption on e tells us that $|I_j|_\sigma \geq e$ for $j = 1,\ldots,N$, hence

$$|I_j|_\sigma \leq |J|_\sigma + e \quad \text{for} \;\; j = 0,1,\ldots,N.$$

From $I_0, I_1, \ldots, I_j \in \mathrm{supp}\big(\kappa\langle\langle t_1^{p^{-\infty}}, \ldots, t_m^{p^{-\infty}}\rangle\rangle^{E,\flat}_{C;d+e}\big)$, we get

$$|I_j|_p \leq C \cdot (|I_j|_\sigma + d + e)^E \leq C \cdot (|J|_\sigma + d + 2e)^E \quad \text{for} \;\; j = 0,1,\ldots,N.$$

It follows that

$$|J|_p \leq C \cdot (|J|_\sigma + d + 2e)^E.$$

We have proved statement (iii). □

(4.4.8) Proof of 4.4.2. The uniqueness part of 4.4.2 (1) has been settled. We will prove the existence part of 4.4.2 (1) with

$$C' = C \cdot (1 + \varepsilon_0^{-1})^E \quad \text{and} \quad d' = \tfrac{d+e}{1+\varepsilon_0^{-1}}.$$

As explained in 4.4.5, it suffices to show that there exists an element $V \kappa\langle\langle t_1^{p^{-\infty}}, \ldots, t_m^{p^{-\infty}}\rangle\rangle^{E,\flat}_{C';d'}$ such that

$$V = \eta(G) + \mu(V).$$

By lemma 4.4.7 (i), (ii), the limit of

$$\lim_{N\to\infty} \eta(G) + \mu(\eta(G)) + \mu^2(\eta(G)) + \cdots + \mu^N(\eta(G)) =: V$$

exists in $\kappa\langle\langle t_1^{p^{-\infty}}, \ldots, t_m^{p^{-\infty}}\rangle\rangle^{E,\flat}_{C';d'}$. Clearly the element V given by the above limit satisfies $V = \eta(G) + \mu(V)$. We have proved 4.4.2 (1).

Under the assumption that $e = \mathrm{Min}\big\{|I|_\sigma :\, I \in \mathrm{supp}(F)\big\}$, lemma 4.4.7 (iii) tells us that

$$\eta(G) + \mu(\eta(G)) + \mu^2(\eta(G)) + \cdots + \mu^N(\eta(G)) \in \kappa\langle\langle t_1^{p^{-\infty}}, \ldots, t_m^{p^{-\infty}}\rangle\rangle^{E,\flat}_{C;d+2e}$$

for all $N \in \mathbb{N}$, and the limit V exists in $\kappa\langle\langle t_1^{p^{-\infty}}, \ldots, t_m^{p^{-\infty}}\rangle\rangle^{E,\flat}_{C;d+2e}$. We have proved 4.4.2 (2). □

(4.5) Proposition. *Suppose that $E > 0$, $C \geq 1$ and $d \geq 1$. The integral closure of the local domain $\kappa\langle\langle t_1^{p^{-\infty}}, \ldots, t_m^{p^{-\infty}}\rangle\rangle^{E,\flat}_{C;d}$ in its own field of fractions is*

$$\bigcup_{d'>0} \kappa\langle\langle t_1^{p^{-\infty}}, \ldots, t_m^{p^{-\infty}}\rangle\rangle^{E,\flat}_{C;d'}.$$

(4.5.1) LEMMA. *Suppose that $\kappa \supset \mathbb{F}_p$ is an* infinite *field of characteristic p. Let $E, C > 0$ and $d \geq 0$ be real parameters. Let $F(t_1, \ldots, t_m)$ be an element of $\kappa\langle\langle t_1^{p^{-\infty}}, \ldots, t_m^{p^{-\infty}}\rangle\rangle_{C;d}^{E,\flat}$ whose constant term is* 0*; i.e. F is not a unit in $\kappa\langle\langle t_1^{p^{-\infty}}, \ldots, t_m^{p^{-\infty}}\rangle\rangle_{C;d}^{E,\flat}$. Let $e := \mathrm{Min}\{|I|_\sigma : I \in \mathrm{supp}(F)\}$. There exists an element $L \in \mathrm{GL}_m(\kappa)$ such that the automorphism L^* of $\kappa\langle\langle t_1^{p^{-\infty}}, \ldots, t_m^{p^{-\infty}}\rangle\rangle_{C;d}^{E,\flat}$ induced by L sends F to an t_m-regular element of order e in $\kappa\langle\langle t_1^{p^{-\infty}}, \ldots, t_m^{p^{-\infty}}\rangle\rangle_{C;d}^{E,\flat}$.*

PROOF. The usual/standard argument works; see the first paragraph of the proof of Lemma 3 on p. 147 of [7]. $\square$

(4.5.2) LEMMA. *Let $\kappa \supset \mathbb{F}_p$ be a field of characteristic p, and let $\tilde{\kappa}$ be an extension field of κ. Let $G, F \neq 0$ be element of $\kappa\langle\langle t_1^{p^{-\infty}}, \ldots, t_m^{p^{-\infty}}\rangle\rangle_{C;d}^{E,\flat}$, let H be an element of $\tilde{\kappa}\langle\langle t_1^{p^{-\infty}}, \ldots, t_m^{p^{-\infty}}\rangle\rangle_{C;d}^{E,\flat}$. Suppose that $G = F \cdot H$. Then $H \in \kappa\langle\langle t_1^{p^{-\infty}}, \ldots, t_m^{p^{-\infty}}\rangle\rangle_{C;d}^{E,\flat}$.*

PROOF. Define a well ordering on $\mathrm{supp}(m : E; C, d)$ by

$$(i_1, \ldots, i_m) \precneqq (j_1, \ldots, j_m) \iff \begin{array}{l} \text{either } i_1 + \cdots + i_m < j_1 + \cdots + j_m, \text{ or } i_1 + \cdots + i_m = j_1 + \cdots + j_m \\ \text{and } \exists\, a,\ 1 \leq a \leq m, \text{ s.t. } i_\lambda = j_\lambda \text{ for } \lambda = 1, \ldots, a-1 \text{ and } i_a < j_a. \end{array}$$

Write $H = \sum_{i_1, \ldots, i_m \in \mathrm{supp}(m:E;C,d)} b_{i_1, \ldots, i_m} t_1^{i_1} \cdots t_m^{i_m}$. An easy induction on $(i_1, \ldots, i_m)$ with respect to the above well ordering shows that $b_{i_1, \ldots, i_m} \in \kappa$ for all $(i_1, \ldots, i_m) \in \mathrm{supp}(m : E; C, d)$. $\square$

(4.5.3) DEFINITION. Let $\kappa \supset \mathbb{F}_p$ be a field of characteristic $p > 0$. Let $E, C > 0$, $d \geq 0$ be real numbers. Let $t_1, \ldots, t_m$ be variables. Define an $[0, \infty]$-valued function

$$\mathbf{o}_{t_m} : \kappa\langle\langle t_1^{p^{-\infty}}, \ldots, t_m^{p^{-\infty}}\rangle\rangle_{C;d}^{E,\flat} \longrightarrow [0, \infty]$$

by

$$\mathbf{o}_{t_m}(f) := \inf\{i_m \,|\, (i_1, \ldots, i_m) \in \mathrm{supp}(f)$$

for every formal series f in $\kappa\langle\langle t_1^{p^{-\infty}}, \ldots, t_m^{p^{-\infty}}\rangle\rangle_{C;d}^{E,\flat}$. We call $\mathbf{o}_{t_m}$ the *order* of f in the variable t_m. By definition $\mathbf{o}_{t_m}(0) = \infty$.

(4.5.4) LEMMA. *The function $f \mapsto \mathbf{o}_{t_m}(f)$ defined in* 4.5.3 *satisfies the following properties.*

(i) $\mathbf{o}_{t_m}(f + g) \geq \min\{\mathbf{o}_{t_m}(f), \mathbf{o}_{t_m}(g)\}$ *for all* $f, g \in \kappa\langle\langle t_1^{p^{-\infty}}, \ldots, t_m^{p^{-\infty}}\rangle\rangle_{C;d}^{E,\flat}$.

(ii) $\mathbf{o}_{t_m}(f \cdot g) \geq \mathbf{o}_{t_m}(f) + \mathbf{o}_{t_m}(g)$ *for all* $f, g \in \kappa\langle\langle t_1^{p^{-\infty}}, \ldots, t_m^{p^{-\infty}}\rangle\rangle_{C;d}^{E,\flat}$.

(iii) $\mathbf{o}_{t_m}(f^n) = n \cdot \mathbf{o}(f)$ *for all $n \in \mathbb{N}$ and all non-zero formal series f in* $\kappa\langle\langle t_1^{p^{-\infty}}, \ldots, t_m^{p^{-\infty}}\rangle\rangle_{C;d}^{E,\flat}$.

PROOF. The statements (i) and (ii) are immediate from the definition. To prove (iii), note first that $\mathbf{o}_{t_m}(f^n) \geq n \cdot \mathbf{o}_{t_m}(f)$ by (ii). Again by (ii), if $\mathbf{o}_{t_m}(f^n) > n \cdot \mathbf{o}_{t_m}(f)$, then $\mathbf{o}_{t_m}(f^{n'}) > n' \cdot \mathbf{o}_{t_m}(f)$ for all integers $n' \geq n$. It is clear that $\mathbf{o}_{t_m}(f^{p^i}) = p^i \cdot \mathbf{o}_{t_m}(f)$ for every natural number i, because $\mathrm{supp}(f^{p^i}) = p^i \cdot \mathrm{supp}(f)$. The statement (iii) follow.

REMARK. We do not know whether the function $\mathbf{o}_{t_m}$ is a valuation on $\kappa\langle\langle t_1^{p^{-\infty}},\dots,t_m^{p^{-\infty}}\rangle\rangle_{C;d}^{E,\flat}$, i.e. whether the equality $\mathbf{o}_{t_m}(f\cdot g)=\mathbf{o}_{t_m}(f)+\mathbf{o}_{t_m}(g)$ holds for all $f,g\in\kappa\langle\langle t_1^{p^{-\infty}},\dots,t_m^{p^{-\infty}}\rangle\rangle_{C;d}^{E,\flat}$.

A related question is the following. Let I be the ideal of $\kappa\langle\langle t_1^{p^{-\infty}},\dots,t_m^{p^{-\infty}}\rangle\rangle_{C;d}^{E,\flat}$ consisting of all elements $f\in\kappa\langle\langle t_1^{p^{-\infty}},\dots,t_m^{p^{-\infty}}\rangle\rangle_{C;d}^{E,\flat}$ such that $\mathbf{o}_{t_m}(f)>0$. This ideal I is equal to its own radical, but we do not know whether it a prime ideal.

(4.5.5) PROOF OF 4.5.
1. Suppose that $f\in\kappa\langle\langle t_1^{p^{-\infty}},\dots,t_m^{p^{-\infty}}\rangle\rangle_{C;d'}^{E,\flat}$ for some $d'>0$. We show that f is in the fraction field L of $\kappa\langle\langle t_1^{p^{-\infty}},\dots,t_m^{p^{-\infty}}\rangle\rangle_{C;d}^{E,\flat}$ and is integral over $\kappa\langle\langle t_1^{p^{-\infty}},\dots,t_m^{p^{-\infty}}\rangle\rangle_{C;d}^{E,\flat}$.

Pick a natural number $N\geq d'-d$. Then $t_1^N\cdot f\in\kappa\langle\langle t_1^{p^{-\infty}},\dots,t_m^{p^{-\infty}}\rangle\rangle_{C;d}^{E,\flat}$, hence f is an element L. Consider a power f^{p^n} of f, where n is a natural number. The support subset of f^{p^n} consists of all elements of the form $p^n\cdot J$, where J is an exponent in the support subset of f. We have

$$|p^nJ|_p=p^{-n}|J|_p\leq p^{-n}\cdot C\cdot(|J|_\sigma+d')^E=p^{-n}\cdot C\cdot(p^{-n}|p^nJ|_\sigma+d')^E.$$

Let $\delta:=\mathrm{Min}\{|J|_\sigma\colon J\in\mathrm{supp}(f),\ J\neq 0\}$. Clearly $\delta>0$. Choose n_1 sufficiently large so that $(1-p^{-n_1}).\cdot p^{n_1}\cdot\delta>d'-d$. Then

$$|I|_p\leq C\cdot(|I|_\sigma+d)^E$$

for all $I\in\mathrm{supp}(f^{p^{n_1}})$, which implies that $f^{p^{n_1}}$ is an element of $\kappa\langle\langle t_1^{p^{-\infty}},\dots,t_m^{p^{-\infty}}\rangle\rangle_{C;d}^{E,\flat}$. Therefore f is integral over the ring $\kappa\langle\langle t_1^{p^{-\infty}},\dots,t_m^{p^{-\infty}}\rangle\rangle_{C;d}^{E,\flat}$.

2. By lemma 4.5.2, we may and do assume that κ is an infinite field. Let $f=\frac{G}{F}$ be an element of the fraction field L which is integral over the ring $\kappa\langle\langle t_1^{p^{-\infty}},\dots,t_m^{p^{-\infty}}\rangle\rangle_{C;d}^{E,\flat}$. If the constant term of F is a non-zero element of κ, then F is a unit of the ring $\kappa\langle\langle t_1^{p^{-\infty}},\dots,t_m^{p^{-\infty}}\rangle\rangle_{C;d}^{E,\flat}$ and there is nothing to prove. So we may and do assume that the constant term of F is zero.

Let $e:=\mathrm{Min}\big\{|I|_\sigma:\ I\in\mathrm{supp}(F)\big\}$. By lemma 4.5.1, after making a suitable linear change of coordinates, we may and do assume that F is t_m-regular of order e. By 4.4.2 (2), there exist elements $U,R\in\kappa\langle\langle t_1^{p^{-\infty}},\dots,t_m^{p^{-\infty}}\rangle\rangle_{C;d+2e}^{E,\flat}$ such that $G=U\cdot F+R$ and every exponent $I=(i_1,\dots,i_m)$ of the support subset $\mathrm{supp}(R)$ of R has the property that $i_m<e$. Because $f=F/G$ is integral over $\kappa\langle\langle t_1^{p^{-\infty}},\dots,t_m^{p^{-\infty}}\rangle\rangle_{C;d}^{E,\flat}$, the element R/F is also integral over $\kappa\langle\langle t_1^{p^{-\infty}},\dots,t_m^{p^{-\infty}}\rangle\rangle_{C;d}^{E,\flat}$. In other words there exist a positive integer $n_1>0$ and elements $H_1,\dots,H_n\in\kappa\langle\langle t_1^{p^{-\infty}},\dots,t_m^{p^{-\infty}}\rangle\rangle_{C;d}^{E,\flat}$ such that

$$(*)\qquad R^{n_1}+H_1\cdot R^{n_1-1}\cdot F+\cdots+H_{n_1-1}\cdot R\cdot F^{n_1-1}+H_{n_1}\cdot F^{n_1}=0$$

We may and do assume that $R\neq 0$. Let $e':=\mathbf{o}_{t_m}(R)$. Clearly $e'<e$. By 4.5.4, we know that $\mathbf{o}_{t_m}H_1\cdot R^{n_1-1}\cdot F+\cdots+H_{n_1-1}\cdot R\cdot F^{n_1-1}+H_{n_1}\cdot F^{n_1}\geq(n_1-1)e'+e$, while $\mathbf{o}_{t_m}(R^{n_1})=n_1\cdot e'<(n_1-1)+e$. This contradiction shows that $R=0$. In other words $f\in\kappa\langle\langle t_1^{p^{-\infty}},\dots,t_m^{p^{-\infty}}\rangle\rangle_{C;d+2e}^{E,\flat}$. We have proved that the integral closure of $\kappa\langle\langle t_1^{p^{-\infty}},\dots,t_m^{p^{-\infty}}\rangle\rangle_{C;d}^{E,\flat}$ in its fraction field L is contained in $\bigcup_{d'}\kappa\langle\langle t_1^{p^{-\infty}},\dots,t_m^{p^{-\infty}}\rangle\rangle_{C;d'}^{E,\flat}$ $\square$

§5. Action of a one-parameter subgroup on a biextension

In this section $k \supset \mathbb{F}_p$ is a perfect field, X, Y, Z are p-divisible *formal* groups over k, and $\pi : E \to X \times Y$ is a biextension of $X \times Y$ by Z.

(5.1) Suppose we have a one-dimensional p-adic Lie group Γ acting on a biextension E of $X \times Y$ by Z. We will extract from such an action a collection of congruence relations; see proposition 3.5.3. This collection of congruence relations comes from the "leading term" of the action of a sequence (γ_m) in Γ with $\lim_{m\to\infty} \gamma_m = 1$, and can be regarded as a substitute for the "derivative" of the action of Γ on E.[2]

We will need the following congruence estimate for the morphisms $\eta_n : \pi^{-1}(X[p^n] \times Y[p^n]) \to Z$ attached to a biextension $\pi : E \to X \times Y$ of p-divisible formal groups $X \times Y$ by Z.

(5.2) PROPOSITION. *Let $\mathfrak{m} = \mathfrak{m}_E$ be the maximal ideal of the coordinate ring $R = R_E$ of the smooth formal scheme E over k. Let $\left(\eta_n : \pi^{-1}(X[p^n] \times Y[p^n] \to Z\right)_{n\in\mathbb{N}}$ be the compatible family of morphisms defined in* 2.7.1. *Let $\mu = \mu_{Z,\min}$ be the maximum among the slopes of Z. There exist positive integers n_2, c_2 such that*

$$\eta_n \equiv 0 \pmod{\mathfrak{m}^{(p^{\lfloor n/\mu \rceil - c_2})}}$$

for all $n \geq n_2$.

(5.2.1) LEMMA. *Let R_1, R_2, S_1, S_2 be Noetherian local rings with maximal ideals $\mathfrak{m}_1, \mathfrak{m}_2, \mathfrak{n}_1, \mathfrak{n}_2$ respectively. Let $h_1 : R_1 \to S_1$ and $h_2 : R_2 \to S_2$ be injective local homomorphisms such that S_i is a finitely generated R_i-module via h_i for $i = 1, 2$. There exist positive integers C, d with the following property:*

> *Let $f, g : R_1 \to R_2$ and $f', g' : S_1 \to S_2$ be local homomorphisms such that $h_2 \circ f = f' \circ h_1$ and $h_2 \circ g = g' \circ h_1$. If $n \in \mathbb{N}$ and $f'(y) - g'(y) \equiv 0 \pmod{\mathfrak{n}_2^{Cn+d}}$ for all $y \in S_1$, then $f(x) - g(x) \equiv 0 \pmod{\mathfrak{n}_1^n}$ for all $x \in R_1$.*

PROOF. There exists a positive integer $a > 0$ such that $\mathfrak{n}_2^C \subset \mathfrak{n}_1 S_2$. By the Artin–Rees lemma, there exists a natural number e such that

$$S_1 \cap \mathfrak{n}_1^{m+e} S_2 \subseteq n_1^m \qquad \forall n \in \mathbb{N}.$$

Lemma 5.2.1 holds for $C = a$ and $d = ae$. □

---

[2]The challenge of finding a good notion of "derivative" can be seen in a simple example: the standard action of $\mathbb{Z}_p{}^\times$ on the formal completion $\widehat{\mathbb{G}_m} = \mathrm{Spf}(\overline{\mathbb{F}}_p[[t]])$ of $\mathbb{G}_m$ over $\overline{\mathbb{F}}_p$. The action of an element $a \in \mathbb{Z}_p{}^\times$ on $\widehat{\mathbb{G}_m}$ sends the coordinate t to $(1+t)^a - 1$.

(5.2.2) REDUCTION STEPS FOR THE PROOF OF PROPOSITION 5.2.

0. We may and do assume that the base field $k \supset \mathbb{F}_p$ is algebraically closed.

1. Suppose that there exists a biextension E' of p-divisible formal groups $X' \times Y'$ by Z' and an homomorphism $(\psi, \alpha, \beta, \gamma)$ from E to E' such that $\alpha : X \to X'$, $\beta : Y \to Y'$ and $\gamma : Z \to Z'$ are isogenies of p-divisible groups. It is easy to see from 2.6.3 that there exist isogenies $\alpha' : X' \to X$, $\beta' : Y' \to Y$, $\gamma' : Z' \to Z$ and a homomorphism $(\psi', \alpha', \beta', \gamma')$ from E' to E. By 5.2.1, proposition 5.2 holds for E if and only if it holds for E'. It suffices to prove 5.2 for a push-forward of the given biextension E by an isogeny $E \to E'$ of p-divisible groups. Therefore we may and do assume that the p-divisible group X is isomorphic to a product $X_1 \times \cdots \times X_a$ of isoclinic p-divisibles with distinct slopes, Y is isomorphic to a product $Y_1 \times \cdots \times Y_b$ os isoclinice p-divisibles with distinct slopes, and Z is isomorphic to a product $Z_1 \times \cdots Z_c$ of isoclinic p-divisible groups with distinct slopes.

2. In the situation at the end of step 1, the biextension E is decomposed into a product of biextensions E_{lmn}, $l = 1, \ldots, a$, $m = 1, \ldots, b$, $n = 1, \ldots, c$, where each E_{lmn} is a biextension of $X_l \times Y_m$ by Z_n. If 5.2 holds for all biextensions E_{lmn}, then it holds for E. Therefore we may and do assume that X, Y, Z are all isoclinic.

3. If $\mathrm{slope}(X) + \mathrm{slope}(Y) \neq \mathrm{slope}(Z)$, then the bilinear pairing $\Theta_E : \mathrm{M}_*(X) \times \mathrm{M}(Y) \to \mathrm{M}(Z)$ is zero and the biextension E splits canonically. In this case 5.2 holds for trivial reason. Therefore we may and do assume that $\mathrm{slope}(X) + \mathrm{slope}(Y) = \mathrm{slope}(Z)$.

4. Modifying Z by an isogeny if necessary, we may and do assume that there exist positive integers a, r, s, n_0 such that
   - $\mathrm{slope}(X) = \frac{a}{r}$,
   - $Z[p^a] = \mathrm{Ker}(\mathrm{Fr}^r_{Z/k})$,
   - $X[p^{na}] \supset \mathrm{Ker}(\mathrm{Fr}^{ns}_{X/k})$ and $Y[p^{na}] \supset \mathrm{Ker}(\mathrm{Fr}^{ns}_{Y/k})$ for all $n \geq n_0$,

5. Let $u_1, \ldots, u_b$ be a regular system of parameters of the coordinate ring of Z such that

$$[p^a]^*(u_j) = u_j^{p^r}, \qquad j = 1, \ldots, b.$$

   We have to show that there exist positive integers n_2, c_2 such that

$$\eta^*_{na}(u_j) \in \mathfrak{m}^{(p^{\lfloor n/\mu \rfloor - c_2})} \qquad \forall n \geq n_2,\ j = 1, \ldots, b.$$

6. It suffices to show that there exist positive integers n_3, c_3 such that

$$\eta^*_{na}(u_j) \in \mathfrak{m}^{(p^{rn-c_3})} \qquad \forall n \geq n_2,\ j = 1, \ldots, b.$$

(5.2.3) PROOF OF 5.2. We are in a position to apply results in 3.5. For each $j = 1, \ldots, b$ and each $n \geq n_0$, define

$$a_{j,n} = \eta_{na}^*(u_j) \mod \mathfrak{m}^{(p^{ns})}.$$

The sequence $\left(a_{j,n}\right)_{n \geq n_0}$ is ϕ^r-compatible.

Pick a regular system of parameters $t_1, \ldots, t_m$ of the coordinate ring of E. By 3.5.3, there exists a formal sequence

$$B_j = \sum_{I \in \mathbb{N}[1/p]^m} b_{j,I}\, \underline{t}^I$$

such that the inequality (ast) in 3.5.3 whenever $b_{j,I} \neq 0$, and

$$\eta_{na}^*(u_j) \equiv B_j^{p^n} \quad \left(\mathrm{mod} \left\{ \sum_{|I|_\infty \geq p^{sn}} r_I\, \underline{t}^I \right\}\right)$$

for all $n \geq n_0$. The above congruence is modulo terms of max-degree at least p^{sn}, i.e. modulo formal series of the form $\sum_{|I|_\infty \geq p^{sn}} r_I\, \underline{t}^I$. It is easily seen from the definition of the morphisms η_n that none of the $a_{j,n}$'s is a unit in $k[[\underline{t}]]/\mathfrak{m}^{(p^{ns})}$. So the constant term of B_j is zero for all $j = 1, \ldots, b$. The desired estimate for the $\eta_{na}^*(u_j)$'s follows immediately. □

(5.3) Recall from 2.6.4 that the Lie algebra of the compact p-adic Lie group $\mathrm{Aut}_{\mathrm{biext}}(E))$ consists of all triples (A, B, C) which kill the bilinear form Θ_E as in 2.6.4 (2).

(5.3.1) LEMMA. *Let $v = (A, B, C)$ be an element of the Lie algebra of $\mathrm{Aut}_{\mathrm{biext}}(E))$. Suppose that $A \in \mathrm{End}(X)$, $B \in \mathrm{End}(Y)$ and $C \in \mathrm{End}(Z)$. Then $\exp(p^2 t A) \in \mathrm{Aut}(X)$, $\exp(p^2 t B) \in \mathrm{Aut}(Y)$, $\exp(p^2 t C) \in \mathrm{Aut}(Z)$ and $\exp(p^2 t v) \in \mathrm{Aut}_{\mathrm{biext}}(E)$ for all $t \in \mathbb{Z}_p$.*

PROOF. The Taylor series for $\exp(p^2 t A) \in \mathrm{Aut}(X)$ converges p-adically and defines an element of $\mathrm{Aut}(X)$. Similarly $\exp(p^2 t B) \in \mathrm{Aut}(Y)$ and $\exp(p^2 t C) \in \mathrm{Aut}(Z)$. That $\exp(p^2 t v) \in \mathrm{Aut}_{\mathrm{biext}}(E)$ follows from 2.6.4. □

(5.3.2) PROPOSITION. *Let $v = (A, B, C)$ be an element of the Lie algebra of $\mathrm{Aut}_{\mathrm{biext}}(E))$ such that $A \in \mathrm{End}(X)$, $B \in \mathrm{End}(Y)$ and $C \in \mathrm{End}(Z)$.*

(i) *For every integer $n \geq 2$, the infinite series*

$$\sum_{j \geq 2} \frac{p^{n(j-1)}}{j!} C^j$$

converges to an element of $\mathrm{End}(Z)$.

(ii) *The restriction of the automorphism* $\exp(p^n t v)$ *to $E_n = \pi^{-1}(X[p^n] \times Y[p^n])$ is equal to*

$$\left(C \circ \eta_n + \sum_{j \geq 2} \frac{p^{n(j-1)}}{j!} C^j \circ \eta_n \right) * \mathrm{id}_{E_n}$$

PROOF. The statement (i) follows from the easy estimate

$$\mathrm{ord}_p(j!) < \frac{j}{p-1} \leq j,$$

which implies that

$$\mathrm{ord}_p\Big(\frac{p^{2(j-1)}}{j!}\Big) \geq (n-1)(j-1)-1.$$

Clearly $(n-1)(j-1)-1 \geq 0$ for all $j \geq 2$ and $(n-1)(j-1)-1 \to 0$ as $j \to \infty$. The statement (i) follows.

For (ii), we note that the automorphism $\exp(p^n C) \times \exp(p^n A) \times \exp(p^n B)$ of $Z \times X[p^n] \times Y[p^{2n}]$ descents to the restriction to E_n of the automorphism $\exp(p^n v)$ of E, according to 2.5.1 (iv) and 2.5.4. The statement (ii) follows from the definition of η_n in 2.7.1 and the Taylor expansion of $\exp(p^n C)$. □

(5.4) We adopt the following assumptions and notation. They are compatible with the assumptions and notation in 2.7.

(i) Let $v = (A,B,C)$ be an element of the Lie algebra of $\mathrm{Aut}_{\mathrm{biext}}(E))$. Assume that $A \in \mathrm{End}(X)$, $B \in \mathrm{End}(Y)$ and $C \in \mathrm{End}(Z)$.

(ii) Assume that a, s, r are three positive integers such that

- $0 < r < s$, and $\frac{a}{r}$ is the largest slope of Z
- $\frac{a}{s}$ is strictly bigger than every slope of X and every slope of Y.

From general properties of slopes of p-divisible groups we know that there exist natural numbers $n_0, c_0 \in \mathbb{N}$ with $n_0 \geq \min(2, c_0/r)$ such that

$$X[p^{na}] \supset \mathrm{Ker}(\mathrm{Fr}_X^{ns}) \quad \text{and} \quad Y[p^{na}] \supset \mathrm{Ker}(\mathrm{Fr}_Y^{ns})$$

and

$$Z[p^{na}] \supset \mathrm{Ker}(\mathrm{Fr}_Z^{nr-c_0})$$

for all $n \geq n_0$, where $\mathrm{Fr}_X^{ns} : X \to X^{(p^{ns})}$ (respectively Fr_Y^{ns}) is the (ns)-th iterate of the relative Frobenius for X (respectively Y). Similarly for $\mathrm{Fr}_Z^{nr-c_0}$.

(iii) Let $R = R_E$ be the affine coordinate ring of the smooth formal scheme E, so that $E = \mathrm{Spf}(R)$ and R is non-canonically isomorphic to a formal power series ring in d variables, where $d = \dim(E)$. Let $\mathfrak{m} = \mathfrak{m}_E$ be the maximal ideal of R. Let $\phi = \phi_R$ be the absolute Frobenius endomorphism of R, which sends every element $x \in R$ to x^p.

For every natural number j, define an ideal of R by

$$\mathfrak{m}^{(p^j)} := \phi^j(\mathfrak{m})R.$$

Note that

$$\mathfrak{m}^{\lceil p^j/d \rceil} \subseteq \mathfrak{m}^{(p^j)} \subseteq \mathfrak{m}^{p^j}.$$

Denote by $E \bmod \mathfrak{m}^{(j)}$ the Artinian scheme

$$E \bmod \mathfrak{m}^{(j)} := \operatorname{Spec}(R/\mathfrak{m}^{(j)})$$

(5.5) Proposition. *We use the notation and assumption in* 5.4 *and* 5.3.2. *There exist positive integers n_3, c_3 such that the congruence*

$$\psi(\exp(p^{na}v)) \equiv (C \circ \eta_{na}) * \mathrm{id}_{E_{na}} \pmod{\mathfrak{m}^{(p^{\min(ns, 2nr-c_3)})}}$$

for the action $\psi(\exp(p^{na}v))$ of the element $\exp(p^{na}v) \in G$ on E holds for all integers $n \geq n_3$. In other words, the restrictions to the Artinian scheme $E \bmod \mathfrak{m}^{(p^{dn})}$ of the two automorphisms $\psi(\exp(p^{na}v))$ and $(C \circ \eta_{na}) * \mathrm{id}_{E_{na}}$ of the formal scheme E coincide. Here $E_{na} = \pi^{-1}(X[p^{na}] \times Y[p^{na}])$ as before.

Proof. This proposition is a straight-forward consequence of 5.2 and 5.3.2.

1. The assumption 5.4 (ii) tells us that. $E_{na} \supset \operatorname{Spec}\big(R/\mathfrak{m}^{(p^{ns})}\big)$ for all $n \geq n_0$.
2. We know from 5.3.2 that the restriction of $\psi(\exp(p^{na}\,v))$ to E_{na} is equal to

$$\Big(C \circ \eta_{na} + \sum_{j \geq 2} \frac{p^{na(j-1)}}{j!} C^j \circ \eta_{na}\Big) * \mathrm{id}_{E_{na}}.$$

3. We know from 5.2 that there exist positive integers n_2, c_2 such that

$$\eta_{na} \equiv 0 \left(\bmod\ \mathfrak{m}^{(p^{nr-c_2})}\right)$$

   for all $n \geq \frac{n_2}{a}$.
4. An elementary calculation shows that

$$\operatorname{ord}_p \tfrac{p^{na(j-1)}}{j!} > na(j-1) - \tfrac{j}{p-1} \geq na - 2 \qquad \forall j \geq 2$$

Let $n_3 := \operatorname{Min}(n_0, \lceil n_2/a \rceil)$. Combining 3 and 4 above we get an estimate of the typical "error term" $\frac{p^{na(j-1)}}{j!} C^j \circ \eta_{na}$:

$$\frac{p^{na(j-1)}}{j!} C^j \circ \eta_{na} \equiv 0 \left(\bmod\ \mathfrak{m}^{(p^{2nr-c_3})}\right)$$

where $c_3 := 2c_0 + c_2$, for all $n \geq n_3$ and all $j \geq 2$. □

(5.6) The following corollary 5.7 is a variant of 5.5 and will be convenient for our purpose. We will follow the general notation scheme in 5.4 and 5.5: X, Y, Z are p-divisible groups over a perfect field $k \supset \mathbb{F}_p$, $\pi : E \to X \times Y$ is a biextension of $X \times Y$ by Z. Let $(R, \mathfrak{m}) = (R_E, \mathfrak{m}_E)$ be the coordinate ring of E.

(i) Assume that X, Y, Z are p-divisible formal groups, i.e. every slope of X, Y, Z is strictly positive.

(ii) Let $v = (A,B,C)$ be an element of the Lie algebra of $\mathrm{Aut}_{\mathrm{biext}}(E \to X \times Y)$, $A \in \mathrm{End}(X)$, $B \in \mathrm{End}(Y)$ and $C \in \mathrm{End}(Z)$.

(iii) Assume that Z is a product of isoclinic p-divisible groups; write Z as a product of isoclinic p-divisible subgroups with distinct slopes: $Z = \prod Z_l$, where each Z_l is isoclinic, the slopes of the Z_l are mutually distinct, and the slope of Z_l is the biggest among slopes of Z. Assume that the slope of Z_1 is strictly bigger than every slope of $X \times Y$.

(iv) Choose positive integers a, r, s, n_3 with $r < s$ such that the following conditions hold.

- $\mathrm{slope}(Z_1) = \frac{a}{r}$
- $X[p^{na}] \supset \mathrm{Ker}(\mathrm{Fr}_X^{ns})$ and for all $n \geq n_3$.
- $Z_l[p^{na}] \supset \mathrm{Ker}(\mathrm{Fr}_{Z_l}^{ns})$ for all $l \neq 1$ and all $n \geq n_3$.

(v) For every $n \geq n_3$, define a morphism

$$\rho_{na} : \pi^{-1}\big(\mathrm{Ker}(\mathrm{Fr}_X^{ns}) \times \mathrm{Ker}(\mathrm{Fr}_Y^{ns})\big) \longrightarrow Z_1$$

to be the restriction to $\pi^{-1}\big(\mathrm{Ker}(\mathrm{Fr}_X^{ns}) \times \mathrm{Ker}(\mathrm{Fr}_Y^{ns}\big)$ of the composition of η_{na} with the projection $\mathrm{pr}_{Z_l} : Z \to Z_l$ from Z to its l-th factor:

$$\rho_{na} = \left(\mathrm{pr}_{Z_l} \circ \eta_{na}\right)\big|_{\pi^{-1}(\mathrm{Ker}(\mathrm{Fr}_X^{ns} \times \mathrm{Ker}(\mathrm{Fr}_Y^{ns}))} .$$

(5.7) Corollary. *Notation and assumptions as in* 5.6. *In particular a, r, s are positive integers, $r < s$, $\frac{a}{r}$ is the largest slope of Z, $\frac{a}{s}$ is strictly bigger than any slope of $X \times Y$ and any other slope of Z, Z_1 is the maximal p-divisible subgroup of Z with slope $\frac{a}{r}$, and $Z_1[p^a] = \mathrm{Ker}(\mathrm{Fr}^r_{Z_1/k})$. There exist positive integers n_4, c_4 such that*

$$\psi(\exp(p^{na}v)) \equiv (C|_{Z_1} \circ \rho_{na}) * \mathrm{id}_{E \bmod \mathfrak{m}} \pmod{\mathfrak{m}^{(p^{\min(ns, 2nr - c_4)})}}$$

for all $n \geq n_4$, where $C|_{Z_1} \in \mathrm{End}(Z_1)$ is the restriction to the factor Z_1 of Z of the endomorphism $C \in \mathrm{End}(Z)$.

Corollary 5.7 is an easy consequence of 5.5.

§6. How to prove identities using powers of Frobenius

(6.1) The main technical tool for proving local rigidity for p-divisible formal groups with respect to non-trivial actions of compact p-adic Lie groups is the statement [3, Prop. 3.1], about power series, which looks like a mess at first sight. A slightly different form, stated in [3, 3.1.1], is reproduced in 6.1.1 below for the convenience of the readers. A weak rigidity statement 6.2 for a section of a biextension stable under the action of a p-adic Lie group is presented as an application of 6.1.1.

(6.1.1) Proposition. *Let $k \supset \mathbb{F}_p$ be a field. Let $\mathbf{u} = (u_1, \ldots, u_a)$, $\mathbf{v} = (v_1, \ldots, v_b)$ be two tuples of variables. Let $f(\mathbf{u}, \mathbf{v}) \in k[[\mathbf{u}, \mathbf{v}]]$ be a formal power series in the variables $u_1, \ldots, u_a, v_1, \ldots, v_b$ with coefficients in k. Let $\mathbf{x} = (x_1, \ldots, x_m)$, $\mathbf{y} = (y_1, \ldots, y_m)$ be two new sets of variables. Let*

$(g_1(\mathbf{x}),\ldots,g_a(\mathbf{x}))$ *be an a-tuple of power series such that* $g_i(\mathbf{x}) \in (\mathbf{x})k[[\mathbf{x}]]$ *for* $i = 1,\ldots,a$. *Let* $(h_1(\mathbf{y}),\ldots,h_b(\mathbf{y}))$ *be a b-tuple of power series with* $h_j(\mathbf{y}) \in (\mathbf{y})k[[\mathbf{y}]]$ *for* $j = 1,\ldots,b$. *Let* $q = p^r$ *be a power of p for some positive integer r. Let* $n_0 \in \mathbb{N}$ *be a natural number. Let* $(d_n)_{n\in\mathbb{N},n\geq n_0}$ *be a sequence of natural numbers such that* $\lim_{n\to\infty} \frac{q^n}{d_n} = 0$. *Suppose we are given power series* $\phi_{j,n}(\mathbf{v}) \in k[[\mathbf{v}]]$ *for all* $j = 1,\ldots,b$ *and all* $n \geq n_0$ *such that*

$$R_{j,n}(\mathbf{v}) := \phi_{j,n} - v_j^{q^n} \equiv 0 \pmod{(\mathbf{v})^{d_n}} \quad \forall\, j = 1,\ldots,b,\ \forall n \geq n_0.$$

and

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

in $k[[\mathbf{x}]]$, *for all* $n \geq n_0$. *Then*

$$f(g_1(\mathbf{x}),\ldots,g_a(\mathbf{x}),h_1(\mathbf{y}),\ldots,h_b(\mathbf{y})) = 0 \text{ in } k[[\mathbf{x},\mathbf{y}]].$$

(6.1.2) REMARK. As noted in [3, 3.1.1], the proof of [3, 3.1] also proves 6.1.1. We will not reproduce the proof of 6.1.1 here. However we would like to remark here that the argument in [3] also works if the power series rings in the statement of 6.1.1 are replaced by complete restricted perfections of power series rings. This "easy exercise" will be carried out in 6.4.

(6.1.3) REMARK. Readers who looked up [3, 3.1.1] may find it somewhat different from the statement of 6.1.1. There it is assumed that there exists an natural number b' with $0 \leq b' \leq b$ such that $\phi_{j,n} - v_j^{q^n} \equiv 0 \pmod{(\mathbf{v})^{d_n}}$ $\forall\, j = 1,\ldots,b'$, $\forall n \geq n_0$, and $\phi_{j,n} \equiv 0 \pmod{(\mathbf{v})^{d_n}}$ $\forall\, j = b'+1,\ldots,$ $\forall n \geq n_0$. So the condition in [3, 3.1.1] that

$$f\left(g_1(\mathbf{x}),\ldots,g_a(\mathbf{x}),\phi_{1,n}(h(\mathbf{x})),\ldots,\phi_{b,n}(h(\mathbf{x}))\right) \equiv 0 \pmod{(\mathbf{x})^{d_n}} \ \forall n \geq n_0$$

is equivalent to the assumption that

$$f'\left(g_1(\mathbf{x}),\ldots,g_a(\mathbf{x}),\phi_{1,n}(h(\mathbf{x})),\ldots,\phi_{b',n}(h(\mathbf{x}))\right) \equiv 0 \pmod{(\mathbf{x})^{d_n}} \ \forall n \geq n_0,$$

where $f'(u_1,\ldots,u_a,v_1,\ldots v_{b'}) := f(u_1,\ldots,u_a,v_1,\ldots,v_{b'},0,\ldots,0)$. The conclusion of [3, 3.1.1] is that $f'(g_1(\mathbf{x}),\ldots,g_a(\mathbf{x}),h_1(\mathbf{y}),\ldots,h_{b'}(\mathbf{y})) = 0$, which is the conclusion of 6.1.1 (with b replaced by b' and f replaced by b'). So the statements of 6.1.1 is really the same as that of [3, 3.1].

Proposition 6.2 can be reformulated as follows. We will use the following notation.

- Let $k \supset \mathbb{F}_p$ be a field.
- Let U,V and X be local formal schemes over k which are isomorphic to the formal spectrum of a power seriers ring over k in a finite number of variables.
- For each positive integer m, let U_m,V_m,X_m be the m-th infinitesimal neighborhood of the local formal schemes U,V,X respectively.
- Let $U \times V$ be the fiber product of U and V over k in the category of formal schemes over k.
- Let $q = p^r$ be a positive power of p.

- Let $\mathrm{Fr}^q_{Y/k} : V \to V^{(q)}$ be the r-th iterate of the relative Frobenius for V/k.
- Let $\delta : V^{(q)} \xrightarrow{\sim} V$ be an isomorphism over k and let $\Phi = \delta \circ \mathrm{Fr}^q_{V/k}$.
- For each $n \in \mathbb{N}$, let
$$(g, \Phi^n \circ h) : X \to U \times V$$
be the morphism from X to the fiber product $U \times V$ with components g and $\Phi^n \circ h$. For each $m \in \mathbb{N}$, let
$$(g, \Phi^n \circ h)_m : X_m \to (U \times V)_m$$
be the morphism from the m-th infinitesimal neighborhood of X to the m-th infinitesimal neighborhood of $U \times V$ induced by $(g, \Phi^n \circ h)$.

(6.1.4) PROPOSITION. *We use notations in the preceding paragraph. Let $(d_n)_{n \geq n_0}$ be a sequence of positive integers such that*
$$\lim_{n\to\infty} \frac{q^n}{d_n} = 0.$$
Let $f \in \Gamma(U \times V, \mathscr{O}_{UxV})$ be a regular function on the formal scheme $U \times V$. Suppose for each $n \geq n_0$, the function $f \circ (g, \Phi^n \circ h)_{X_{d_n}}$ on the d_n-th infinitesimal neighborhood X_{d_n} of the closed point of X induced by the morphism $(g, \Phi^n \circ h)_{d_n} : X_{d_n} \longrightarrow (U \times V)_{d_n}$ and f is zero. Then the composition of f with $g \times h : X \times X \to U \times V$ is zero. In other words f vanishes on the schematic closure of the morphism $g \times h : X \times X \to U \times V$.

(6.1.5) REMARK. Suppose that the base field $k \supset \mathbb{F}_p$ in is algebraically closed field. Then the schematic closure of $g \times h : X \times X \to U \times V$ is equal to the product of the schematic closures of $g : X \to U$ and $h : X \to V$. So 6.1.4 simplifies to: the schematic closure of (the union of) the family of morphisms
$$(g, \Phi^n \circ h)_{d_n} : X_{d_n} \to (U \times V)_{d_n} \hookrightarrow U \times V$$
contains the product of the schematic closure of $g : X \to U$ with the schematic closure of $h : X \to V$. The universal case of the last statment is when $U = V = X$ and g, h are both equal to id_X, and the family of morphisms in the statement is induced by the family of Frobenius-twisted diagonal maps
$$(\mathrm{id}_{X_{d_n}}, \Phi^n \circ \mathrm{id}_{X_{d_n}}) : X_{d_n} \to X_{d_n} \times X_{d_n}.$$
Note that $(X \times X)_{d_n}$ is naturally identified with $(X_{d_n} \times X_{d_n})_{d_n}$, the d_n-th infinitesimal neighborhood of the closed point of $X_{d_n} \times X_{d_n}$.

(6.2) PROPOSITION. *Let $k \supset \mathbb{F}_p$ be a field. Let X, Y, Z be p-divisible formal groups over k. Let $\pi : E \to X \times_{\mathrm{Spec}(k)} Y$ be a biextension of $X \times_{\mathrm{Spec}(k)} Y$ by Z. Let $s : X \times_{\mathrm{Spec}(k)} Y \to E$ be a section of π, i.e. $\pi \circ s = \mathrm{id}_{X \times_{\mathrm{Spec}(k)} Y}$. Let G be a compact p-adic Lie group action on the biextension $E \to X \times Y$.*

(i) *Suppose that Z is isoclinic, and the slope of Z is strictly bigger than every slope of X and every slope of Y.*

(ii) *Assume that the induced action of G on Z is strongly non-trivial.*

(iii) *Assume moreover that the graph of the section s is stable under the action of G on E.*

Then the biextension $\pi : E \to X \times_{\mathrm{Spec}(k)} Y$ is trivial, and the section s is its canonical splitting.

PROOF. There are two preliminary reduction steps before the main argument

REDUCTION STEP 1. According to the last paragraph of 2.4.1, it suffice to verify the assertion in the last sentence of 6.2 after extending the base field from k to an algebraic closure of k. So we may and do assume that k is algebraically closed.

REDUCTION STEP 2. Let ν be the slope of Z. We know that there exists an isogeny $\xi : Z \to Z_1$ such that Z_1 is completely slope divisible in the sense that there exist positive integers a_1, r_1 with $a_1 = r_1 \cdot \nu$ such that the kernel of the N-th iterate

$$\mathrm{Fr}_{Z/k}^{(p^{a_1})} : Z \to Z^{(p^N)}$$

of the relative Frobenius is equal to $Z[p^{a_1}]$. Let $E_1 \to X \times_{\mathrm{Spec}(k)} Y$ be the push forward by ξ of the biextension E, and let $\tilde{\xi} : E \to E_1$ be the canonical biextension homomorphism from E to E_1. For each element $g \in G$, let $\alpha(g)$, $\beta(g)$ and $\gamma(g)$ be the automorphism of X, Y and Z induced by the action of g on the biextension E. There exists an open subgroup G_1 of G such that the isogeny $\xi \circ \alpha(g) \circ \xi^{-1}$ is an automorphism of Z. One verifies without difficulty that there exists a continuous homomorphism $\rho_1 : G_1 \to \mathrm{Aut}_{\mathrm{biext}}(E_1)$ such that $\rho_1(g) \circ \tilde{\xi} = \tilde{\xi} \circ \rho(g)$ for every $g \in G_1$. From the last paragraph of 2.4.4, to show that the biextension E of $X \times_{\mathrm{Spec}(k)} Y$ by Z is trivial, it suffices to show that the biextension E_1 of $X \times_{\mathrm{Spec}(k):} Y$ by Z_1 is trivial. In this case the composition of the canonical splitting of E_1 is the unique section of $E \to X \times_{\mathrm{Spec}(k)} Y$ whose composition with $\tilde{\xi}$ is equal to the canonical splitting of the biextension $E_1 \to X \times_{\mathrm{Spec}(k)} Y$. So we may and do assume that $Z[p^{a_1}] = \mathrm{Ker}(\mathrm{Fr}_Z^{r_1})$.

By [3, Thm. 4.3], the graph of the restriction of s to $X \times 0_Y$ is a p-divisible subgroup of $\pi^{-1}(X \times 0_Y) \cong X \times_{\mathrm{Spec}(k)} Z$, meaning that the restriction of s to $X \times 0_Y$ is a group homomorphism from $X \to \pi^{-1}(X \times 0_Y)$. Because X and Z does not have common slope, s coincides with ε_2 on $X \times 0_Y$. Similarly s coincides with ε_1 on $0_X \times Y$. Let $\tau : (X \times X) \times Y \to Z$ and $\sigma : X \times (Y \times Y) \to Z$ be defined by formulas (a), (b) in 2.2.1. To prove 6.2, it suffices to show that both τ and σ are zero, in the sense that each is equal to the composition of the zero section 0_Z of Z with the projection of its source to $\mathrm{Spec}(k)$.

The assumption that the graph of the section s is stable under the action of G means that the map $\mu_{\rho(g)} : X \times Y \to Z$ in 2.3.4 is identically 0 for each $g \in G$. Therefore

$$\gamma(g)(\tau(x_1, x_2; y)) - \tau(\alpha(g)(x_1), \alpha(g)(x_2); \beta(g)(y)) = 0 \tag{6.2.1}$$

$$\gamma(g)(\sigma(x; y_1, y_2)) - \sigma(\alpha(g)(x); \beta(g)(y_1), \beta(g)(y_2)) = 0 \tag{6.2.2}$$

for all $x, x_1, x_2 \in X$ and all $y, y_1, y_2 \in Y$.

The key observation here is that equations (1), (2) above for elements $g \in G$ close to the identity element of G, under the assumption that the slope of Z is strictly bigger than all slopes of X and Y, produces a large number of identities which are increasingly close to equations of the form

$$d\gamma(C) \cdot \tau = 0_Z = d\gamma(C) \cdot \sigma$$

in the sensse specified in 6.1.1, so that the identity principle with Frobenius powers 6.1.1 is applicable. Here C is any element of $\mathrm{Lie}(G)$ such that $d\gamma(C)$, a priori an element of $\mathrm{End}(Z)\otimes_{\mathbb{Z}}\mathbb{Q}$, is actually an endomorphism of Z. The limit equations resulting from the identity principle is the following.

($*$) *If v is an element of $\mathrm{Lie}(G)$ such that the image of v under the representation*

$$(d\alpha, d\beta, d\gamma) : \mathrm{Lie}(G) \to \mathrm{End}(Z)\otimes_{\mathbb{Z}}\mathbb{Q}$$

lies in $\mathrm{End}(X)\oplus\mathrm{End}(Y)\oplus\mathrm{End}(Z)$, then $d\gamma(v)$ kills both Z-valued functions τ and σ from $X\times Y$ to Z.

Since the action of G on Z is assumed to be strongly non-trivial, the statement ($*$) above implies that the maps $\tau : (X\times X)\times Y \to Z$ and $\sigma : X\times(Y\times Y)\to Z$ are both identically zero and 6.2 follows.

It remains to prove ($*$). Let $\mu = \mathrm{slope}(Z)$. After extending the base field k, we may and do assume that k is algebraically closed. Changing Z by an isogeny, we may and do assume that there exist positive integers a_1, r_1 such that $Z[p^{a_1}] = \mathrm{Ker}(\mathrm{Fr}^{r_1}_{Z/k})$.

Let v be an element of $\mathrm{Lie}(G)$ such that $A = d\alpha(v)$ is an endomorphism of Z, $B = d\beta(v)$ is an endomorphism of Y and $C = d\gamma(v)$ is an endomorphism of Z. There exists positive integers a, r, s, c, n_0 such that (i)–(iv) below hold for all integers $n \geq n_0$.

(i) a, r are multiples of a_1, r_1 respectively, $r < s$, and a/s is strictly bigger than every slope of X and every slope of Y,

(ii) $\gamma(\exp(p^{na}C)) \equiv \mathrm{id}_Z + p^{na}C \pmod{\mathrm{Ker}(\mathrm{Fr}^{ns-c}_{Z/k})}$,

(iii) $\alpha(\exp(p^{na}A)) \in \mathrm{End}(X)$, $\beta(\exp(p^{na}B)) \in \mathrm{End}(Y)$,

(iv) $\alpha(\exp(p^{na}A)) \equiv \mathrm{id}_X \pmod{\mathrm{Ker}(\mathrm{Fr}^{as-c}_{X/k})}$, and $\beta(\exp(p^{na}B)) \equiv \mathrm{id}_Y \pmod{\mathrm{Ker}(\mathrm{Fr}^{as-c}_{Y/k})}$.

The equations (6.2.1), (6.2.2 with $g = \exp(p^{na}A$ and the congruences (ii) and (iv) above implies that

$$(p^{na}C)\cdot\tau(x_1, x_2; y) \equiv 0 \pmod{\mathrm{Ker}(\mathrm{Fr}^{as-c}_{Y/k})}$$

and

$$(p^{na}C)\cdot\sigma(x; y_1, y_2) \equiv 0 \pmod{\mathrm{Ker}(\mathrm{Fr}^{as-c}_{Y/k})}$$

for all $n \geq n_0$. Applying proposition 6.1.1, we conclude that

$$C\cdot\tau(x_1, x_2; y) = 0 \ \text{ and } \ C\cdot\sigma(x; y_1, y_2) = 0\,.$$

We have proved the statement ($*$) and proposition 6.2. $\square$

(6.3) We make some preparations before stating proposition 6.4. The latter is a generalization of 6.1.1 to the context of complete restricted perfections of power series rings.

(6.3.1) Definition. Let $E > 0$, $C, d \geq 1$ be real numbers. Define the support subset

$$\mathrm{supp}(m : E; C, d) \subset \mathbb{N}[1/p]^m$$

with parameters $(E; C, d)$ by

$$\mathrm{supp}(m : E; C, d) = \left\{ I \in \mathbb{N}[1/p]^m \colon |I|_p \leq C \cdot (|I|_\sigma + d)^E \right\}$$

(6.3.2) Definition. Let $\underline{x} = (x_1, \ldots, x_m)$ be a tuple of variables,

(i) The total degree of monomials in $\underline{x}$ gives rise to a decreasing filtration

$$\mathrm{Fil}^{\geq \bullet}_{\mathrm{t.deg}}$$

on $k\langle\langle x_1, \ldots, x_m \rangle\rangle^{E,\flat}_{C;d}$, indexed by real numbers:

$$\mathrm{Fil}^{\geq u}_{\mathrm{t.deg}}\big(k\langle\langle x_1, \ldots, x_m \rangle\rangle^{E,\flat}_{C;d}\big) := \left\{ \sum_{I \in \mathrm{supp}(m:E;C,d)} a_I \cdot \underline{x}^I \;\middle|\; a_J \in k \;\; \forall I, \;\; a_I = 0 \;\text{ if }\; |I|_\sigma < u \right\}$$

for every $u \in \mathbb{R}$.

(ii) For every real number u, define $\mathrm{Fil}^{>u}_{\mathrm{t.deg}}$ by

$$\mathrm{Fil}^{>u}_{\mathrm{t.deg}}\big(k\langle\langle x_1, \ldots, x_m \rangle\rangle^{E,\flat}_{C;d}\big) := \left\{ \sum_{I \in \mathrm{supp}(m:E;C,d)} a_I \cdot \underline{x}^I \;\middle|\; a_J \in k \;\; \forall I, \;\; a_I = 0 \;\text{ if }\; |I|_\sigma \leq u \right\}.$$

The following lemma deals with the perfection $k[x_1^{p^{-\infty}}, \ldots, x_m^{p^{-\infty}}] = \cup_{n \in \mathbb{N}} k[x_1^{p^{-n}}, \ldots, x_m^{p^{-n}}]$ of the polynomial ring $k[x_1, \ldots, x_m]$ over the perfect base field k. Notice that one can evaluate any element of $k[x_1^{p^{-\infty}}, \ldots, x_m^{p^{-\infty}}]$ at any m-tuple $(c_1, \ldots, c_m) \in k^m$. Lemma 6.3.3 provides a dichotomy when an element $F(x_1, \ldots, x_m) \in k[x_1^{p^{-\infty}}, \ldots, x_m^{p^{-\infty}}]$ is evaluated at all Fr_q-powers

$$\{ (c_1^{q^n}, \ldots, c_m^{q^n}) \;:\; n \in \mathbb{N}$$

of a gien m-tuple $(c_1, \ldots, c_m)$, where $q = p^r$ is a power of p, $r \in \mathbb{N}_{>0}$:

- either $F(c_1^{q^n}, \ldots, c_m^{q^n}) = 0$ for infinitely many natural numbers,
- or $F(c_1^{q^n}, \ldots, c_m^{q^n}) = 0$ for all $n \in \mathbb{Z}$.

(6.3.3) Lemma. *Let r be a positive integer, and let $q = p^r$. Let $F(x_1, \ldots, x_m)$ be an element of $k[x_1^{p^{-\infty}}, \ldots, x_m^{p^{-\infty}}]$. Suppose that $(c_1, \ldots, c_m) \in k^m$ is an element of k^m and n_0 is a natural number such that*

$$F(c_1^{q^n}, \ldots, c_n^{q^n}) = 0$$

for all integers $n \geq n_0$. Then $F(c_1^{q^n}, \ldots, c_n^{q^n}) = 0$ for all $n \in \mathbb{Z}$. In particular $F(c_1, \ldots, c_n) = 0$.

Proof. When $F(x_1, \ldots, x_n) \in k[x_1, \ldots, x_n]$, this statement was proved in [3, 2.2]. The general case follows because there exists a positive integer i such that $F(x_1, \ldots, x_m)^{p^i} \in k[x_1, \ldots, x_m]$. $\square$

(6.4) PROPOSITION. *Let $\underline{x} = (x_1, \dots, x_m)$, $\underline{y} = (y_1, \dots, y_m)$, $\underline{u} = (u_1, \dots, a)$ and $\underline{v} = (v_1, \dots, v_b)$ be four tuples of variables. Let $(E_1; C_1, d_1)$ and $(E_2; C_2, d_2)$ be two triples of real parameters with $E_1, E_2 > 0$ and $C_1, C_2, d_1, d_2 \geq 1$. Let*

$$f(\underline{u}, \underline{v}) \in k\langle\langle u_1^{p^{-\infty}}, \dots, u_a^{p^{-\infty}}, v_1^{p^{-\infty}}, \dots, v_b^{p^{-\infty}}\rangle\rangle_{C_1; d_1}^{E_1, \flat}$$

be an element of $k\langle\langle u_1^{p^{-\infty}}, \dots, u_a^{p^{-\infty}}, v_1^{p^{-\infty}}, \dots, v_b^{p^{-\infty}}\rangle\rangle_{C_1; d_1}^{E_1, \flat}$ such that the support set $\mathrm{supp}(f)$ of f is contained in the product $\mathrm{supp}(a : E_1; C_1, d_1) \times \mathrm{supp}(b : E_1; C_1, d_1)$:

(6.4.1) $$\mathrm{supp}(f) \subseteq \mathrm{supp}(a : E_1; C_1, d_1) \times \mathrm{supp}(b : E_1; C_1, d_1).$$

In other words f lies in the closure in $k\langle\langle u_1^{p^{-\infty}}, \dots, u_a^{p^{-\infty}}, v_1^{p^{-\infty}}, \dots, v_b^{p^{-\infty}}\rangle\rangle_{C_1; d_1}^{E_1, \flat}$ of the subring

$$k\langle\langle u_1^{p^{-\infty}}, \dots, u_a^{p^{-\infty}}\rangle\rangle_{C_1; d_1}^{E_1, \flat} \otimes_k k\langle\langle v_1^{p^{-\infty}}, \dots, v_b^{p^{-\infty}}\rangle\rangle_{C_1; d_1}^{E_1, \flat}.$$

Let

$$(g_1(\underline{x}), \dots, g_a(\underline{x})) \in \left(\mathrm{Fil}_{\mathrm{t.deg}}^{>0} k\langle\langle x_1^{p^{-\infty}}, \dots, x_m^{p^{-\infty}}\rangle\rangle_{C_2; d_2}^{E_2, \flat}\right)^a$$

be an a-tuple of elements in $k\langle\langle x_1^{p^{-\infty}}, \dots, x_m^{p^{-\infty}}\rangle\rangle_{C_2; d_2}^{E_2, \flat}$ whose constant terms are 0. Let

$$(h_1(\underline{y}), \dots, h_b(\underline{y})) \in \left(\mathrm{Fil}_{\mathrm{t.deg}}^{>0} k\langle\langle y_1^{p^{-\infty}}, \dots, y_m^{p^{-\infty}}\rangle\rangle_{C_2; d_2}^{E_2, \flat}\right)^b$$

be a b-tuple of elements in $k\langle\langle y_1^{p^{-\infty}}, \dots, y_m^{p^{-\infty}}\rangle\rangle_{C_2; d_2}^{E_2, \flat}$ whose constant terms are 0. Let $q = p^r$ be a power of p, where $r > 0$ is a positive integer. Let n_0 be a natural number. Suppose that there exists a sequence $(d_n)_{n \geq n_0}$ of natural numbers such that

(6.4.2) $$\lim_{n \to \infty} \frac{q^n}{d_n} = 0$$

and

(6.4.3) $$f(g_1(\underline{x}), \dots, g_a(\underline{x}), h_1(\underline{x})^{q^n}, \dots, h_b(\underline{x})^{q^n}) \equiv 0 \pmod{\mathrm{Fil}_{\mathrm{t.deg}}^{d_n}} \qquad \forall n \geq n_0.$$

Then

(6.4.4) $$f(g_1(\underline{x}), \dots, g_a(\underline{x}), h_1(\underline{y}), \dots, h_b(\underline{y})) = 0.$$

In the above the congruence relation 6.4.3 takes place in $k\langle\langle x_1^{p^{-\infty}}, \dots, x_m^{p^{-\infty}}\rangle\rangle_{C_3; d_3}^{E_3, \flat}$, and the equation 6.4.4 holds in the ring $k\langle\langle x_1^{p^{-\infty}}, \dots, x_m^{p^{-\infty}}, y_1^{p^{-\infty}}, \dots, y_m^{p^{-\infty}}\rangle\rangle_{C_3; d_3}^{E_3, \flat}$, where

- *$E_3 = E_1 + E_2 + E_1 E_2$,*
- *$C_3 = C_1^{1+E_2} \cdot C_2^{1+E_1+E_1E_2} \cdot (1+d)^{E_1 E_2 (1+E_2)}$, and*
- *d_3 is a sufficiently large constant depending on $(E_1; C_1, d_1)$ and $(E_2; C_2, d_2)$.*

See 4.3.1 and the trivial lower bound for e_2 there.

REMARK. For application to rigidity of biextensions of p-divisible formal groups, we will need only the special case of 6.4 when $f(\underline{u}, \underline{v}) \in\in k[[u_1, \dots, u_a, v_1, \dots, v_b]]$, i.e. $f(\underline{u}, \underline{v})$ is a usual power series. It is interesting to know whether 6.4 holds without the assumption 6.4.1 on $f(\underline{u}, \underline{v})$. We do not know the answer.

(6.5) PROOF OF PROPOSITION 6.4. Let

$$\underline{t} = \big(t_{i,j}\big)_{(i,j)\in\{1,\ldots,b\}\times(\mathrm{supp}(m:E_2;C_2,d_2)\smallsetminus\underline{0})}$$

be an infinite array of variables indexed by $\{1,\ldots,b\}\times\big(\mathrm{supp}(m:E_2;C_2,d_2)\smallsetminus\{\underline{0}\}\big)$, where $\underline{0}$ is the zero element of the support subset $\mathrm{supp}(m:E_2;C_2,d_2)\subset\mathbb{N}[1/p]^m$ defined in 6.3.1. For each $i=1,\ldots,b$,

$$h_i(\underline{y}) = \sum_{\underline{0}\neq K\in\mathrm{supp}(m:E_2;C_2,d_2)} c_{i,K}\,\underline{y}^J$$

with $c_{i,K}\in k$ for all $J\in S(m:E_2;C_2,d_2)\smallsetminus\{\underline{0}\}$. Let

$$H_i(\underline{t};\underline{y}) := \sum_{\underline{0}\neq K\in\mathrm{supp}(m:E_2;C_2,d_2)} \underline{t}_{i,K}\,\underline{y}^K$$

The assumption 6.4.1 implies that the composition

$$f\big(g_1(\underline{x}),\ldots,g_a(\underline{x}),H_1(\underline{t};\underline{y}),\ldots,H_1(\underline{t};\underline{y})\big)$$

is a well-defined formal series $k\langle\langle x_1^{p^{-\infty}},\ldots,x_m^{p^{-\infty}},y_1^{p^{-\infty}},\ldots,y_m^{p^{-\infty}}\rangle\rangle_{C_3;d_3}^{E_3,\flat}$ whose support is contained in the product $\mathrm{supp}(m:E_3;C_3,d_3)\times\mathrm{supp}(m:E_3;C_3,d_3)$:

(6.5.1) $$f\big(\underline{g}(\underline{x}),\underline{H}(\underline{t};\underline{y})\big) = \sum_{(I,J)\in\mathrm{supp}(m:E_3;C_3,d_3)\times\mathrm{supp}(m:E_3;C_3,d_3)} A_{I,J}(\underline{t})\,\underline{x}^I\underline{y}^J$$

Moreover each coefficient $A_{I,J}(\underline{t})$ is an element in the perfection

$$k[\underline{t}^{p^{\infty}}] = k\big[t_{i,K}^{p^{-\infty}}\big]_{i\in\{1,\ldots,b\},\,K\in\mathrm{supp}(m:E_2;C_2,d_2)\smallsetminus\{\underline{0}\}}$$

of the polynomial ring

$$k[\underline{t}^{p^{-\infty}}] = k[t_{i,K}]_{i\in\{1,\ldots,b\},\,K\in\mathrm{supp}(m:E_2;C_2,d_2)\smallsetminus\{\underline{0}\}}$$

in infinitely many variables $t_{i,K}$. Clearly For every $n\in\mathbb{N}$, we have

(6.5.2) $$f\big(\underline{g}_1(\underline{x}),\ldots,\underline{g}_a(\underline{x}),\underline{h}_1(\underline{x})^{q^n},\ldots,\underline{h}_b(\underline{x})^{q^n}\big) = \sum_{I,J} A_{I,J}(\underline{c}^{q^n})\,\underline{x}^{I+q^nJ}\,.$$

In particular

(6.5.3) $$f\big(\underline{g}_1(\underline{x}),\ldots,\underline{g}_a(\underline{x}),\underline{h}_1(\underline{x}),\ldots,\underline{h}_b(\underline{x})\big) = \sum_{I,J} A_{I,J}(\underline{c})\,\underline{x}^{I+J}\,.$$

By assumption 6.4.2, we get

(6.5.4) $$\sum_{(I,J)\ \text{s.t.}\ |I+q^nJ|_\sigma<d_n} A_{I,J}(\underline{c}^{q^n})\,\underline{x}^{I+q^nJ} = 0 \qquad \forall n\geq n_0\,.$$

We want to show that $A_{I,J}(\underline{c})=0$ for all $(I,J)\in\mathrm{supp}(m:E_3;C_3,d_3)\times\mathrm{supp}(m:E_3;C_3,d_3)$. Suppose to the contrary that $A_{I_0,J_0}(\underline{c})\neq 0$ for some $(I_0,J_0)\in\mathrm{supp}(m:E_3;C_3,d_3)\times\mathrm{supp}(m:E_3;C_3,d_3)$.

By lemma 6.3.3, there exists infinitely many natural numbers n such that $A_{I_0,J_0}(\underline{c}^{q^n}) \neq 0$. Define a subset $T \subseteq \mathrm{supp}(m:E_3;C_3,d_3) \times \mathrm{supp}(m:E_3;C_3,d_3)$ by

$$T := \left\{ (I,J) \ : \ I,J \in \mathrm{supp}(m:E_3;C_3,d_3),\ A_{I,J}(\underline{c}^{q^n}) \neq 0 \ \text{ for infinitely many } n \in \mathbb{N} \right\}.$$

This set T is non-empty because it contains (I_0,J_0). Again by lemma 6.3.3 we know that

$$A_{I,J}(\underline{c}^{q^n}) = 0 \qquad \forall n \in \mathbb{Z} \ \text{ if } \ (I,J) \notin T\,,$$

and equation 6.5.5 becomes

$$\sum_{(I,J)\in T \ \text{s.t.}\ |I+q^nJ|_\sigma < d_n} A_{I,J}(\underline{c}^{q^n})\, \underline{x}^{I+q^nJ} = 0 \qquad \forall n \geq n_0\,. \tag{6.5.5}$$

Let

$$M_2 := \min\{\, |J|_\sigma : \ (I,J) \in T\}$$

and let

$$M_1 := \min\{\, |I|_\sigma : \ (I,J) \in T \ \text{ and } \ |J|_\sigma = M_2\}\,.$$

The minimum defining M_2 (respectively M_1) exists because every subset $\mathrm{supp}(m:E_3;C_3,d_3)$ whose archimedean norm is bounded above is a finite set. This finiteness property for $\mathrm{supp}(m:E_3;C_3,d_3)$ also implies that there exists a positive number $\varepsilon_2 > 0$ such that

$$J \in \mathrm{supp}(m:E_3;C_3,d_3) \ \text{ and } \ |J|_\sigma > M_2 \implies |J|_\sigma > M_2 + \varepsilon_2. \tag{6.5.6}$$

The subset

$$T_1 := \{(I,J) \in T \ : \ |J|_\sigma = M_2,\ |I|_\sigma = M_1\}$$

is a non-empty finite set. There exists a natural number $n_1 \geq n_0$ such that properties 6.5.7–6.5.9 below hold.

$$M_1 + q^n M_2 < d_n - 2 \quad \forall\, n \geq n_1,\ n \in \mathbb{N} \tag{6.5.7}$$

$$q^n \cdot \varepsilon_2 > M_1 \quad \forall n \geq n_1,\ n \in \mathbb{N} \tag{6.5.8}$$

$$(I_1,J_1),(I_2,J_2) \in T_1,\ \ I_1 + q^nJ_1 = I_2 + q^nJ_2 \ \text{ and } \ n \geq n_1 \implies (I_1,J_1) = (I_2,J_2) \tag{6.5.9}$$

Consider the set

$$S_n := \left\{ (I,J) \in T \ : \ |I+q^nJ|_\sigma = M_1 + q^nM_2 \right\}.$$

The property 6.5.8 and the inequality 6.5.6 implies that $S_n = T_1$ for all $n \geq n_1$. Because $S_n = T_1$, when we examine terms of total degree $M_1 + q^nM_2$ in equation 6.5.5, we find that

$$\sum_{(I,J)\in T_1} A_{I,J}(\underline{c}^{q^n})\, \underline{x}^{I+q^nJ} = 0 \qquad \forall n \geq n_1\,. \tag{6.5.10}$$

By property 6.5.9 and equation 6.5.9, we see that

$$A_{I,J}(\underline{c}^{q^n}) = 0$$

for all $(I,J) \in T_1$ and all $n \geq n_1$, therefore T_1 is the empty set. This is a contradiction. We have proved proposition 6.4. □

REMARK. (a) The assumption 6.4.1 on the support of $f(\underline{u},\underline{v})$ implies the uniform bound 6.5.1 on the support of the composition $f\big(g_1(\underline{x}),\dots,g_a(\underline{x}),H_1(\underline{t};\underline{y}),\dots,H_b(\underline{t};\underline{y})\big)$. This observation allows us to take advantage of the finiteness property of the support set $\operatorname{supp}(m;E_3;C_3,d_3)$. The rest of the argument in the proof of 6.4 is identical with the proof of [3, 3.1].

(b) Our proof is not strong enough to show that 6.4 holds for every element f in $k\langle\langle \underline{u}^{p^{-\infty}},\underline{u}^{p^{-\infty}}\rangle\rangle^{E_1,\flat}_{C_1;d_1}$. But we don't have a counter-example either. It will be interesting if one can find a larger class of formal series $f(\underline{u},\underline{v})$ in $k\langle\langle \underline{u}^{p^{-\infty}},\underline{u}^{p^{-\infty}}\rangle\rangle^{E_1,\flat}_{C_1;d_1}$ for which the statement 6.4 holds.

§7. Rigidity results for biextensions

(7.1) Notation and basic setup. In this section k is a perfect field of characteristic $p>0$.

(i) Let X,Y,Z be p-divisible formal groups, and $\pi: E\to X\times_{\operatorname{Spec}(k)} Y$ is a biextension of $X\times_{\operatorname{Spec}(k)} Y$ by Z.

(ii) Let G be a compact p-adic Lie group. Let $(\rho,\alpha,\beta,\gamma)$ be an action of G on the biextension $E\to X\times Y$, where $\rho: G\to \operatorname{Aut}_{\text{biext}}(E\to X\times Y)$ is a continuous homomorphism, and $\alpha: G\to \operatorname{Aut}(X)$ (respectively $\beta: G\to\operatorname{Aut}(Y)$, $\gamma: G\to\operatorname{Aut}(Z)$) is the action of G on X (respectively Y, Z) underlying ρ. We know from 2.6.4 that the group homomorphism

$$(\alpha,\beta,\gamma)\colon\, G\longrightarrow \operatorname{Aut}(X)\times\operatorname{Aut}(Y)\times\operatorname{Aut}(Z)$$

is a closed embedding of compact p-adic Lie groups, and the induced map

$$(d\alpha,d\beta,d\gamma)\colon\,\longrightarrow \operatorname{Lie}(G)\operatorname{End}(X)_{\mathbb{Q}}\oplus\operatorname{End}(Y)_{\mathbb{Q}}\oplus\operatorname{End}(Z)_{\mathbb{Q}}$$

is an injection of finite dimensional vector spaces over $\mathbb{Q}_p$. We often use the map (α,β,γ) to G with a subgroup of $\operatorname{Aut}(X)\times\operatorname{Aut}(Y)\times\operatorname{Aut}(Z)$, and regard $\operatorname{Lie}(G)$ as a $\mathbb{Q}_p$-vector subspace of $\operatorname{Lie}(G)\operatorname{End}(X)_{\mathbb{Q}}\oplus\operatorname{End}(Y)_{\mathbb{Q}}\oplus\operatorname{End}(Z)_{\mathbb{Q}}$.

(iii) Let $W\subset E$ be a formal subvariety of E, in the sense that there exists a prime ideal I_W of the coordinate ring R_E of E such that $W=\operatorname{Spf}(R_E/I_W)$. Assume that W is stable under the action of G.

(iv) The formal subvariety $V=\operatorname{Spf}\big(R_{X\times_{\operatorname{Spec}(k)}Y}/(I_W\cap R_{X\times Y})\big)\subseteq X\times_{\operatorname{Spec}(k)} Y$ will be said to be the *image* of W in $X\times_{\operatorname{Spec}(k)} Y$.

(7.2) THEOREM. *Let W be a formal subvariety of E stable under the action of G. Let μ_1 be the largest slope of Z. Let Z_1 be the maximal p-divisible subgroup of Z which is isoclinic of slope μ_1. Let Z_2 be the largest among all isoclinic p-divisible subgroups of Z with slope μ_1 which are contained in W. Let $\Upsilon_{Z_2}: Z_2\times E\to E$ be the morphism*

$$\Upsilon: Z_2\times E\to E \qquad (z_2,e)\mapsto z_2 * e\,,$$

corresponding to the restriction to Z_2 of the action of Z on E. Let $v=(A,B,C)\in\operatorname{Lie}(G)$ be an element of the Lie algebra of G such that $A\in\operatorname{End}(X)$, $B\in\operatorname{End}(Y)$ and $C\in\operatorname{End}(Z)$.

(1) *Assume that* μ_1 *is strictly bigger than every slope of* X *and every slope of* Y*. Then*

$$\big(\Upsilon\circ(C|_{Z_2}\times \mathrm{id}_W)\big)(Z_2\times W)\subseteq W.$$

In other words the formal subvariety $W\subset E$ *is stable under translation by the p-divisible subgroup* $C(Z_2)$ *of* Z*.*

(2) *Assume in addition that the action of* G *on* Z_2 *is strongly non-trivial. Then*

$$\Upsilon(Z_2\times W)\subseteq W\,.$$

(7.2.1) 7.2 (1) $\Longrightarrow$ 7.2 (2).

The assumption that the action of G on Z_2 is strongly non-trivial implies that there exists elements $v_{ij}=(A_{ij},B_{ij},C_{ij})\in\mathrm{Lie}(G)$, indexed by a finite subset

$$\big\{(i,j)\in\mathbb{N}^2:\ i\in\{1,\ldots,m\},\ j\in\{1,\ldots,n_i\}\big\}\,,$$

where $n_i\in\mathbb{N}_{\geq 1}$ for each $i=1,\ldots,m$, such that

$$\sum_{1\leq i\leq m} C_{i,1}|_{Z_2}\circ\cdots\circ C_{i,n_i}|_{Z_2}\in\mathrm{End}(Z_2)_{\mathbb{Q}}^{\times}.$$

Here $C_{i,j}\in\mathrm{End}(Z_2)_{\mathbb{Q}}$ stands for the restriction to Z_2 of the element $C_{i,j}\in\mathrm{End}(Z)_{\mathbb{Q}}=\mathrm{End}(Z)\otimes_{\mathbb{Z}}\mathbb{Q}$. See [3, 4.1.1] for this lemma on representation theory. The statement (2) follows from statement (1) and the above linear algebra consequence of the assumption that G operates strongly non-trivially on Z_2. The statement (1) will be proved in 7.2.3.

(7.2.2) The main ingredients in the proof of the statement (1) have been developed in previous sections. Here is a brief summary of how these ingredients come into the proof

(i) The analysis of the action on E of $\psi(\exp(p^{na}v)$ for elements $\exp(p^{na}v)\in G$ close to the identity element of G in 5.7, where $v=(A,B,C)=(d\alpha(v),d\beta(v),d\gamma(v))$ is an element of the Lie algebra $\mathrm{Lie}(G)$ of G. This analysis says that the difference between $\psi(\exp(p^{na}v))$ is represented modulo $\mathfrak{m}^{p^{ns}}$ by a linearized "main term"

$$C|_{Z_1}\circ\rho_{na}\qquad(\mathrm{mod}\ \mathfrak{m}_E^{p^{ns}})$$

for natural numbers $n\gg 0$. The map

$$\rho_{na}:E\ \mathrm{mod}\,\mathfrak{m}_E^{p^{ns}}\to Z_1\ \mathrm{mod}\,\mathfrak{m}_E^{p^{ns}}$$

comes from the composition of the map

$$\eta_{na}\ \mathrm{mod}\,\mathfrak{m}_E^{p^{ns}}:E\ \mathrm{mod}\,\mathfrak{m}_E^{p^{ns}}\to Z\ \mathrm{mod}\,\mathfrak{m}_Z^{p^{ns}}$$

defined in 2.7 with the projection $\mathrm{pr}_{Z_1}:Z\to Z_1$ from Z to its factor Z_1. The phenomenon is that the main term shows up already at the level of $\mathfrak{m}_E^{c\cdot p^{nr}}$, where $\frac{a}{r}=\mu_1$ and $s>r$, while the error term lies in $\mathfrak{m}_E^{p^{ns}}$. Thus the error term goes to 0 at a rate much faster than the rate at which the main term does. It is tempting to replace "much faster" by "doubly exponential" in the preceding sentence in order to better convey the comparison. At any rate, this family of congruences relations for $\psi(\exp(p^{na}v))$ can be regarded as a reasonable substitute in the attempt to differentiate the function $t\mapsto\psi(\exp(tv))$ for t in a small neighborhood of 0 in $\mathbb{Z}_p$.

(ii) In order to analyse the compatible family of maps ρ_n defined in 3.3.2, one is naturally led to the notion of complete restricted perfection of equi-characteristic-p complete Noetherian local domains in §3. When applied to the coordinate ring $(R_E, \mathfrak{m}_E)$ of a biextension E, this procedure produces many of mutually related of rings, depending on parameters; each one is a completion of some suitable subring of the perfection of R_E. After picking a good regular system of parameters $(z_1, \ldots, z_d)$ for the coordinate ring of Z_1, the compatible family of maps ρ_n's is controlled by a b-tuple $h_1, \ldots, h_b$ of elements of a suitable complete restricted perfection $\widetilde{R_E}$ of R_E, so that ρ_{na} is represented by $(h_1^{p^{nr}}, \ldots, h_b^{p^{nr}})$ for all large n's. Restricting to a formal subvariety W of E, one gets a d-tuple of elements of $\widetilde{R_W}$, where $\widetilde{R_W}$ is a complete restricted perfection of the coordinate ring R_W of W.

(iii) Let $\Delta_2 : R_E \to R_{Z_2} \widehat{\otimes} R_E$ be the ring homomorphism corresponding to the translation action $Z_2 \times E \to E$ of Z_2 on E, and let $C|_{Z_2}^* : R_{Z_2} \to R_{Z_2}$ be the ring endomorphism corresponding to the restriction to Z_2 of $C \in \mathrm{End}(Z)$.

To show that a G-invariant formal subvariety W is stable under translation by $C|_{Z_2}^*(Z_2)$, one needs to show that every element f in the prime ideal I_W for W is sent to an element of $R_{Z_2} \cdot I_W$ under $(C|_{Z_2}^* \otimes 1_{R_E}) \circ \Delta_2$, or equivalently, the element $(C|_{Z_2}^* \otimes 1_{R_E})(\Delta_2(f))$ is mapped to 0 under the natural surjection $R_{Z_2} \widehat{\otimes} R_E \twoheadrightarrow R_{Z_1} \widehat{\otimes} R_E$. Following [3], our strategy is to try to show that a suitable element $\tilde{f} \in \widetilde{R_W} \widehat{\otimes} \widetilde{R_W}$ attached to $\Delta(f_1)$ is zero.

(iv) To simplify the algebra involved, one deploys an easy form of local uniformization and embed R_W in a formal power series ring S. The situation then is that we have an element $f(u_1, \ldots, u_a, v_1, \ldots, v_b) \in \widetilde{S} \widehat{\otimes} \widetilde{S}$ attached to f_1, and all we have going for us is a family of congruences of the form

$$f\big(g_1(\underline{x}), \ldots, g_a(\underline{x}), h_1(\underline{x})^{p^{rn}}, \ldots, h_b(\underline{x})^{p^{rn}}\big) \equiv 0 \pmod{(\underline{x}) p^{n(s-\varepsilon)-c}}$$

for all $n \gg 0$, with integer constants $s > r > 0$, $c > 0$, where $\underline{x} = (x_1, \ldots, x_m)$ are variables for the power series ring S. These congruences are consequences of the analysis of $\psi(\exp(p^{na} v))$ in (i) above.

At this point the identity principle 6.4 comes to the rescue. It says that the above family of congruences implies that the function $f\big(g_1(\underline{x}), \ldots, g_a(\underline{x}), h_1(\underline{y}), \ldots, h_b(\underline{y})$ in two sets of variables $x_1, \ldots, x_m, y_1, \ldots, y_m$ is identically equal to 0.

(7.2.3) PROOF OF THEOREM 7.2.
1. Preliminary reduction steps.

(a) It suffices to verify the statement of 7.2 after extending the base field k to an algebraic closure of k. So we may and do assume that k is algebraically closed.

(b) If $E \to E'$ is an isogeny of biextensions, the statement of 7.2 holds for E if and only if it holds for E'. Modifying E by suitable isogenies, we may and do assume that X, Y, Z are product of isoclinic p-divisible groups. Moreover may and do assume that there exist positive integers a, r such that $\mu_1 = \frac{a}{r}$ and $Z_1[p^a] = \mathrm{Fr}_{Z_1}^r$.

(c) Choose a suitable regular system of parameters $(u_1, \ldots, u_b)$ for the coordinate ring Z_1 such that $Z_1 = \mathrm{Spf}(k[[u_1, \ldots, u_b]])$ and

$$[p^a]^*(u_i) = u_i^{p^r}$$

for $i = 1, \ldots, b$.

(d) The largest slope μ_1 of Z is assumed to be bigger than every slope appearing in $X \times Y$. Multiplying a, r by a suitable positive integer, we may and do assume that there exists positive intergers s, n_0 such that $s > r$ and $\frac{a}{s}$ is strictly bigger than every slope of $X \times Y$, and

$$X[p^{na}] \supset \mathrm{Ker}(\mathrm{Fr}^{ns}_{X/k}) \quad \text{and} \quad Y[p^{na}] \supset \mathrm{Ker}(\mathrm{Fr}^{ns}_{Y/k})$$

for all $n \geq n_0$.

(e) Let $R_W = R_E/I_W$ be the coordinate ring of W, where I_W is the prime ideal of R_E corresponding to W. By [3, 2.1], there exists a k-linear injective local homomorphism

$$\iota : R_W = R_E/I_W \hookrightarrow k[[t_1, \ldots, t_m]]$$

from R_W to a formal power series ring in m variables, where $m = \dim(R_W)$.

2. By 5.7, there exist positive integers $n_4 \geq n_0$ and c_4 such that

$$\psi(\exp(p^{na}v)) \equiv (C|_{Z_1} \circ \rho_{na}) * \mathrm{id}_{E \bmod \mathfrak{m}} \pmod{\mathfrak{m}^{(p^{\min(ns, 2nr - c_4)})}} \tag{7.2.3.1}$$

for all $n \geq n_4$, where

$$\rho_{na} = \left(\mathrm{pr}_{Z_l} \circ \eta_{na}\right)\big|_{\pi^{-1}(\mathrm{Ker}(\mathrm{Fr}^{ns}_X \times \mathrm{Ker}(\mathrm{Fr}^{ns}_Y))} : \pi^{-1}\big(\mathrm{Ker}(\mathrm{Fr}^{ns}_X) \times \mathrm{Ker}(\mathrm{Fr}^{ns}_Y)\big) \longrightarrow Z_1$$

is the restriction to $\pi^{-1}\big(\mathrm{Ker}(\mathrm{Fr}^{ns}_X) \times \mathrm{Ker}(\mathrm{Fr}^{ns}_Y)\big)$ of the composition of η_{na} with the projection

$$\mathrm{pr}_{Z_l} : Z \to Z_l.$$

For each $j = 1, \ldots, b$, defined a ϕ^r-compatible sequence $(a_{j,n})_{n \geq n_4}$ by

$$a_{j,n} := \rho_{na}^*(u_j) \in R_E/\mathfrak{m}_E^{(p^{ns})}$$

for all $n \geq n_4$. Let $i_1 := \max\big(s - r, \lceil \frac{n_4}{r} \rceil\big)$. For each $j = 1, \ldots, b$, let

$$\tilde{a}_j \in (R_E, \mathfrak{m}_E)^{\mathrm{perf}, \#}_{s:\phi^r;[i_1]}$$

be the formal series corresponding to the ϕ^r compatible sequence $(a_{j,n})_{n \geq n_4}$.

Although $(R_E, \mathfrak{m}_E)^{\mathrm{perf}, \#}_{s:\phi^r;[i_1]}$ is more tightly related to ϕ^r-compatible sequences through the construction in 3.5, we will pass to the larger ring $(R_E, \mathfrak{m}_E)^{\mathrm{perf}, \flat}_{s:\phi^r;[i_1]}$, and consider the $\tilde{a}_j$'s as elements of $(R_E, \mathfrak{m}_E)^{\mathrm{perf}, \flat}_{s:\phi^r;[i_1]}$ in the rest of the proof.

3. The elements $\tilde{a}_1,\dots,\tilde{a}_b \in (R_E,\mathfrak{m}_E)^{\mathrm{perf},\#}_{s:\phi^r;[i_1]}$ defines a ring homomorphism

$$\tilde{\eta}: R_{Z_1} = k[[u_1,\dots,u_b]] \longrightarrow (R_E,\mathfrak{m}_E)^{\mathrm{perf},\#}_{s:\phi^r;[i_1]}\,.$$

Let

$$\omega_1:\ (R_E,\mathfrak{m}_E)^{\mathrm{perf},\flat}_{s:\phi^r;[i_1]} \longrightarrow (R_{Z_1},\mathfrak{m}_{Z_1})^{\mathrm{perf},\flat}_{s:\phi^r;[i_1]}$$

be the ring homomorphism induced by the inclusion $Z_1 \hookrightarrow E$. Because the restriction to Z of the morphism $\eta_n : \pi^{-1}(X[p^n]\times Y[p^n]) \to Z$ is equal to $[p^n]_Z$ for every $n\in\mathbb{N}$, We see that

$$\omega_1\circ\tilde{\eta} = j_{R_{Z_1}} \tag{7.2.3.2}$$

where $j_{R_{Z_1}}: R_{Z_1} \hookrightarrow (R_{Z_1},\mathfrak{m}_{Z_1})^{\mathrm{perf},\flat}_{s:\phi^r;[i_1]}$ is the natural injection from R_{Z_1} to its complete restricted perfection $(R_{Z_1},\mathfrak{m}_{Z_1})^{\mathrm{perf},\flat}_{s:\phi^r;[i_1]}$.

5. We also have the following ring homomorphisms.

(a) The canonical homomorphism $R_E \to R_E/I_W = R_W$ gives rise to a homomorphism

$$\tau : (R_E,\mathfrak{m}_E)^{\mathrm{perf},\flat}_{s:\phi^r;[i_1]} \longrightarrow (R_W,\mathfrak{m}_W)^{\mathrm{perf},\flat}_{s:\phi^r;[i_1]}\,.$$

(b) The injective local homomorphism $\iota : R_W \to k[[t_1,\dots,t_m]]$ induces a injective continuous homomorphism

$$\tilde{\iota} : (R_W,\mathfrak{m}_W)^{\mathrm{perf},\flat}_{s:\phi^r;[i_1]} \longrightarrow k\langle\langle t_1^{p^{-\infty}},\dots,t_m^{p^{-\infty}}\rangle\rangle^{\flat}_{s:\phi^r;[i_1]}\,.$$

(c) Continuous ring homomorphisms

$$\Delta_1 : R_E \to R_{Z_1}\widehat{\otimes} R_E \quad\text{and}\quad \Delta_2 : R_E \to R_{Z_2}\widehat{\otimes} R_E$$

corresponding to the actions $Z_1\times E\to E$ and $Z_2\times E\to E$ of Z_1 and Z_2 on E.

(d) The ring homomorphism

$$\omega_2 : (R_W,\mathfrak{m}_W)^{\mathrm{perf},\flat}_{s:\phi^r;[i_1]} \longrightarrow (R_{Z_2},\mathfrak{m}_{Z_2})^{\mathrm{perf},\flat}_{s:\phi^r;[i_1]}\,.$$

induced by the surjective ring homomorphism $R_W \twoheadrightarrow R_{Z_2}$ which corresponds to the inclusion $Z_2 \hookrightarrow W$.

(e) The ring endomorphisms $C|_{Z_1}^{*} : R_{Z_1} \to R_{Z_1}$ and $C|_{Z_2}^{*} : R_{Z_2}\to R_{Z_2}$ corresponding to the endomorphisms $C|_{Z_1}$ (respectively $C|_{Z_2}$) of the p-divisible group Z_1 (respectively Z_2).

(f) The ring homomorphism

$$\tilde{q} : (R_{Z_1},\mathfrak{m}_{Z_1})^{\mathrm{perf},\flat}_{s:\phi^r;[i_1]} \longrightarrow (R_{Z_2},\mathfrak{m}_{Z_2})^{\mathrm{perf},\flat}_{s:\phi^r;[i_1]}$$

induced by the canonical surjection $q : R_{Z_1} \twoheadrightarrow R_{Z_2}$

Clearly we have

(7.2.3.3) $$\omega_2 \circ \tau = \tilde{q} \circ \omega_1 \quad \text{and} \quad C|_{Z_2}^* \circ q = q \circ C|_{Z_1}^*$$

The following diagram

(7.2.3.4)
$$\begin{tikzcd}
R_{Z_1} \arrow[r, "\tilde{\eta}"] \arrow[d, "="'] & (R_E, \mathfrak{m}_E)^{\mathrm{perf},\flat}_{s:\phi^r;[i_1]} \arrow[r, "\tau"] \arrow[d, "\omega_1"'] & (R_W, \mathfrak{m}_W)^{\mathrm{perf},\flat}_{s:\phi^r;[i_1]} \arrow[d, "\omega_2"'] \\
R_{Z_1} \arrow[r, "j_{R_{Z_1}}"'] & (R_{Z_1}, \mathfrak{m}_{Z_1})^{\mathrm{perf},\flat}_{s:\phi^r;[i_1]} \arrow[r, "\tilde{q}"'] & (R_{Z_2}, \mathfrak{m}_{Z_2})^{\mathrm{perf},\flat}_{s:\phi^r;[i_1]}
\end{tikzcd}$$

commutes by 7.2.3.2. It follows that the diagram

(7.2.3.5)
$$\begin{tikzcd}
R_E \arrow[r, "="] \arrow[d, "\Delta_1"'] & R_E \arrow[d, "\Delta_2"'] & \\
R_{Z_1}\hat{\otimes}R_E \arrow[r, "q\otimes 1"] \arrow[d, "C|_{Z_1}^*\otimes 1"'] & R_{Z_2}\hat{\otimes}R_W \arrow[d, "C|_{Z_2}^*\otimes 1"'] & \\
R_{Z_1}\hat{\otimes}R_E \arrow[r, "q\otimes 1"] \arrow[d, "\tilde{\eta}\otimes 1"'] & R_{Z_2}\hat{\otimes}R_W \arrow[r, "j_{R_{Z_2}}\otimes j_{R_W}"] & (R_{Z_2}, \mathfrak{m}_{Z_2})^{\mathrm{perf},\flat}_{s:\phi^r;[i_1]} \hat{\otimes} (R_W, \mathfrak{m}_W)^{\mathrm{perf},\flat}_{s:\phi^r;[i_1]} \\
(R_E, \mathfrak{m}_E)^{\mathrm{perf},\flat}_{s:\phi^r;[i_1]} \hat{\otimes} (R_E, \mathfrak{m}_E)^{\mathrm{perf},\flat}_{s:\phi^r;[i_1]} \arrow[rr, "\omega_1\otimes\tau"] \arrow[d, "\tau\otimes\tau"'] & & (R_{Z_1}, \mathfrak{m}_{Z_1})^{\mathrm{perf},\flat}_{s:\phi^r;[i_1]} \hat{\otimes} (R_W, \mathfrak{m}_W)^{\mathrm{perf},\flat}_{s:\phi^r;[i_1]} \arrow[u, "\tilde{q}\otimes 1"'] \arrow[d, "\tilde{q}\otimes 1"] \\
(R_W, \mathfrak{m}_W)^{\mathrm{perf},\flat}_{s:\phi^r;[i_1]} \hat{\otimes} (R_W, \mathfrak{m}_W)^{\mathrm{perf},\flat}_{s:\phi^r;[i_1]} \arrow[rr, "\omega_2\otimes 1"] & & (R_{Z_2}, \mathfrak{m}_{Z_2})^{\mathrm{perf},\flat}_{s:\phi^r;[i_1]} \hat{\otimes} (R_W, \mathfrak{m}_W)^{\mathrm{perf},\flat}_{s:\phi^r;[i_1]}
\end{tikzcd}$$

also commutes.

6. Recall that I_W is the prime ideal of the coordinate ring of E consisting of all functions on E which vanishes on the G-invariant formal subvariety $W \subset E$. We want to show that

(A) $$(C|_{Z_2}^* \times 1_{R_E}) \circ \Delta_2(f) = 0 \quad \forall f \in I_W$$

We know from 7.2.3.5 that

$$(C|_{Z_2}^* \times 1_{R_E}) \circ \Delta_2(f) = \big((q \otimes 1) \circ (C|_{Z_1}^* \times 1_{R_E}) \circ \Delta_1\big)(f).$$

Because $j_{R_{Z_2}}$ and j_{R_W} are both injective, our goal 6A is to equivalent to

(B) $$\big((j_{R_{Z_2}} \otimes j_{R_W}) \circ (q \otimes 1) \circ (C|_{Z_1}^* \times 1_{R_E}) \circ \Delta_1\big)(f) = 0 \quad \forall f \in I_W$$

What we will show is a stronger statement

(C) $$\big((\tau \otimes \tau)(\tilde{\eta} \otimes) \circ (C|_{Z_1}^* \times 1_{R_E}) \circ \Delta_1\big)(f) = 0 \quad \forall f \in I_W$$

In other words, the composition of the four vertical arrows at the left edge of the diagram 7.2.3.5 kills every element of the prime ideal I_W. It follows immediately from the commutative diagram 7.2.3.5 that

$$(C) \implies (B) \iff (A).$$

It remains to prove (C).

7. Suppose that f is an element of I_W. Define an element $\tilde{f} \in (R_W,\mathfrak{m}_W)^{\mathrm{perf},\flat}_{s:\phi^r;[i_1]} \hat{\otimes} (R_W,\mathfrak{m}_W)^{\mathrm{perf},\flat}_{s:\phi^r;[i_1]}$ by

$$\tilde{f} := \big((j_{R_{Z_2}} \otimes j_{R_W}) \circ (q \otimes 1) \circ (C|^*_{Z_1} \times 1_{R_E}) \circ \Delta_1\big)(f).$$

Let ϕ be the Frobenius endomorphism $x \mapsto x^p$ on $(R_W,\mathfrak{m}_W)^{\mathrm{perf},\flat}_{s:\phi^r;[i_1]}$, Let

$$\nu_W\colon\ (R_W,\mathfrak{m}_W)^{\mathrm{perf},\flat}_{s:\phi^r;[i_1]} \hat{\otimes} (R_W,\mathfrak{m}_W)^{\mathrm{perf},\flat}_{s:\phi^r;[i_1]} \longrightarrow (R_W,\mathfrak{m}_W)^{\mathrm{perf},\flat}_{s:\phi^r;[i_1]}$$

be map which defines multiplication for the ring $(R_W,\mathfrak{m}_W)^{\mathrm{perf},\flat}_{s:\phi^r;[i_1]}$. Geometrically ν_W corresponds to the diagonal morphism from $\mathrm{Spec}((R_W,\mathfrak{m}_W)^{\mathrm{perf},\flat}_{s:\phi^r;[i_1]}$ to its self-product.

Because the formal subvariety $W \subset E$ is assumed to be stable under G, therefore stable under $\psi(\exp p^{na} v$ for all $n \geq n_4$. Hence the congruence property 7.2.3.1 implies that under the homomorphism

$$\phi^{nr} \otimes 1\colon\ (R_W,\mathfrak{m}_W)^{\mathrm{perf},\flat}_{s:\phi^r;[i_1]} \hat{\otimes} (R_W,\mathfrak{m}_W)^{\mathrm{perf},\flat}_{s:\phi^r;[i_1]} \longrightarrow (R_W,\mathfrak{m}_W)^{\mathrm{perf},\flat}_{s:\phi^r;[i_1]} \hat{\otimes} (R_W,\mathfrak{m}_W)^{\mathrm{perf},\flat}_{s:\phi^r;[i_1]},;$$

we have

$$(\phi^{nr} \otimes 1)(\tilde{f}) \equiv 0 \pmod{\mathrm{Fil}_\flat^{ns-i_1}} \qquad \forall n \geq n_4. \tag{7.2.3.6}$$

8. We claim that the family of congruence conditions 7.2.3.6 satisfied by $\tilde{f}$ implies that $\tilde{f} = 0$. By 4.2.4, the homomorphism $\tilde{\iota} : (R_W,\mathfrak{m}_W)^{\mathrm{perf},\flat}_{s:\phi^r;[i_1]} \to k\langle\langle t_1^{p^{-\infty}},\dots,t_m^{p^{-\infty}}\rangle\rangle^\flat_{s:\phi^r;[i_1]}$ induced by $\iota : R_W \hookrightarrow k[[t_1,\dots,t_m]]$ is also an injection. Therefore it suffices to show that the injective map

$$\tilde{\iota} \otimes \tilde{\iota}\colon\ (R_W,\mathfrak{m}_W)^{\mathrm{perf},\flat}_{s:\phi^r;[i_1]} \hat{\otimes} (R_W,\mathfrak{m}_W)^{\mathrm{perf},\flat}_{s:\phi^r;[i_1]} \longrightarrow k[[t_1,\dots,t_m]]\hat{\otimes}k[[t_1,\dots,t_m]]$$

sends $\tilde{f}$ to 0. Under the ring homomorphism $\tilde{\iota} \otimes \tilde{\iota}$ the family of congruence conditions 7.2.3.6 for $\tilde{f}$ is transformed into a similar family of congruence conditions for the element $(\tilde{\iota} \otimes \tilde{\iota})(\tilde{f}) \in k[[t_1,\dots,t_m]]\hat{\otimes}k[[t_1,\dots,t_m]]$. Let $E = \frac{r}{s-r}$, choose suitable parameters $C > 1$, $d \geq 0$ so that the ring $k\langle\langle t_1^{p^{-\infty}},\dots,t_m^{p^{-\infty}}\rangle\rangle^\flat_{s:\phi^r;[i_1]}$ is contained in $k\langle\langle t_1^{p^{-\infty}},\dots,t_m^{p^{-\infty}}\rangle\rangle^{E,\flat}_{C;d}$. Apply the identity principle 6.4, we conclude that $(\tilde{\iota} \otimes \tilde{\iota})(\tilde{f}) = 0$. Hence $\tilde{f} = 0$. We have proved the claim and concludes the proof of the statement (C). We have seen the (C) implies (A), which is exactly the statement of 7.2. □

(7.2.4) Corollary. *Let W be a formal subvariety of E stable under the action of G. Let Z_1 be the largest p-divisible subgroup of Z contained in W. Let*

$$\Upsilon_{Z_1} : Z_1 \times_{\mathrm{Spec}(k)} E \to E$$

be the translation action of Z_1 on E. Assume that every slople of Z_1 is strictly larger then every slope of $X \times Y$ and the action of G on Z_1 is strongly non-trivial. Then

$$\Upsilon_{Z_1}(Z \times_{\mathrm{Spec}(k)} W) \subset W.$$

PROOF. We may and do assume that $X_1 = X$ and $Y_1 = Y$. We prove 7.2.4 by induction on $\dim(Z_1)$. If Z_1 is isoclinic, then $Z_2 = Z_1$ and 7.2.4 follows immediate from 7.2. Let $\zeta : Z \twoheadrightarrow Z/Z_2$ be the canonical map from Z to the quotient p-divisible group Z/Z_2. Let $\tilde{\zeta} : E \to \zeta_* E =: \overline{E}$ be the canonical map from E to its push-forward by ζ, which is naturally identified with the map "quotient by the p-divisible group Z_2". Let $\overline{W}$ be the image of W in $\overline{E}$ under $\tilde{\zeta}$. By induction, the formal subvariety $\overline{W}$ in $\overline{E}$ is stable under the natural action of Z_1/Z_2. It follows that W is stable under the action of Z_1. □

(7.3) PROPOSITION. *Let W be a formal subvariety of E stable under the action of G. Let Z_1 be the largest p-divisible subgroup of Z contained in W We make the following assumptions.*

(i) *The p-divisible groups X and Y have no slope in common.*

(ii) *Every slope of the p-divisible group Z_1 is strictly bigger every slope of $X \times Y$.*

(iii) *The action of G on E is strictly non-trivial.*

Then W is a sub-biextension of E. In other words there exists a p-divisible subgroup X_1 of X, a p-divisible subgroup Y_1 of Y, a p-divisible subgroup Z_1 of Z, such that

- $\pi(W) \subset X_1 \times Y_1$,
- *W is stable under the two relative group laws $+_1$ and $+_2$,*
- *W is stable under translation by Z_1,*
- *the morphism $\pi|_W : W \to X_1 \times Y_1$ is formally smooth,*
- *$\pi|_W : W \to X_1 \times$ gives W a natural structure as a Z_1-torsor over $X_1 \times Y_1$.*

PROOF. The image V of W in $X \times_{\mathrm{Spec}(k)} Y$ is a p-divisible subgroup of $X \times_{\mathrm{Spec}(k)}$, by local rigidity for p-divisible groups [3, Thm. 4.3]. Because the p-divisible formal groups X and Y do not have common slopes, there exists p-divisible subgroups $X_1 \subset X$ and $Y_1 \subset Y$ such that $V = X_1 \times_{\mathrm{Spec}(k)} Y_1$. Again by local rigidity for p-divisible groups, the intersection $(W \cap Z)$ with reduced structure is a p-divisible subgroup Z_3 of Z. We also know that

$$\dim(Z_3) \geq \dim(W) - \dim(X_1) - \dim(Y_1)$$

from basic commutative algebra.

By 7.2.4, W is stable under the action of Z_3. The quotient $\overline{E} := E/Z_3$ has a natural structure as a biextension of $X \times_{\mathrm{Spec}(k)} Y$ by $\overline{Z} := Z/Z_3$. The quotient $\overline{W} := W/Z_3$ is a formal subvariety of $\overline{E}$, stable under the action of G. Its dimension $\dim(\overline{W})$ is equal to $\dim(W) - \dim(Z_3)$. The image over $\overline{W}$ in $X \times_{\mathrm{Spec}(k)} Y$ is $X_1 \times_{\mathrm{Spec}(k)} Y_1$, hence $\dim(\overline{W}) \geq \dim_{X_1} + \dim(Y_1)$. Combined with the displayed inequality in the previous paragraph, we see that $\dim(\overline{W}) = \dim(X_1 \times Y_1)$. On the other hand the closed fiber of the morphism $\overline{q} : \overline{W} \to X_1 \times Y_1$ is zero-dimensional with exactly one point. Hence the morphism $\overline{q}$ of formal schemes, which corresponds to a local homomorphism between complete noetherian k-algebras, is finite and purely inseparable.

Let $\overline{\pi}_1 : \overline{E}_1 \to X_1 \times Y_1$ be the restriction to $X_1 \times Y_1$ of the biextension $\overline{E} \to X \times Y$. Because X_1 and Y_1 are both p-divisible formal groups, the purely inseparable map $\bar{q}$ is dominated by suitable isogenies: There exists an isogeny $u : X_2 \to X_1$, an isogeny $v : Y_2 \to Y_1$ and a morphism $\xi : X_2 \times Y_2 \to \overline{W}$ such that $\overline{q} \circ \xi = u \times v$.

Consider the pull-back
$$\overline{E}_2 := (u \times v)^* \overline{E}_1 \longrightarrow X_2 \times Y_2$$
of the biextension $\overline{\pi}_1 : \overline{E}_1 \to X_1 \times Y_1$. We know that the compact p-adic Lie group G operates on the biextension $\overline{E}_1$, and $\overline{W}$ is stable under the action of G. There exists a compact open subgroup $G_2 \subset G$ which operates on the biextension $\overline{E}_2$, and the natural map $h : \overline{E}_2 \to \overline{E}_1$ is equivariant with respect to the inclusion $G_2 \hookrightarrow G$. The morphism $\xi : X_2 \times Y_2 \to \overline{W}$ defines a morphism $\xi_2 : X_2 \times Y_2 \to \overline{E}_2$ such that $h \circ \xi_2 = \xi_1$. It follows that

$$(u \times v) \circ \overline{\pi}_2 \circ \xi_2 = \overline{\pi}_1 \circ h \circ \xi_2 = \overline{\pi}_1 \circ \xi_1 = u \times v .$$

Therefore
$$\overline{\pi}_2 \circ \xi_2 = \mathrm{id}_{X_2 \times Y_2} .$$
In other words ξ_2 is a section of the biextension $\overline{E}_2$ of $X_2 \times Y_2$ by $\overline{Z}$. Moreover ξ_2 is equivariant with respect to the action of G_2 on $\overline{E}_2$.

Because every slope of $\overline{Z}$ is strictly bigger than every slope of $X_2 \times Y_2$, we know by 6.2 that the biextension $\overline{E}_2$ splits, and ξ_2 is its canonical splitting. So the biextension $\overline{E}_1$ also splits. The inverse image of the canonical splitting of $\overline{E}_1$ in $\pi^{-1}(X_1 \times Y_1)$ is a biextension E' of $X_1 \times Y_1$ by Z_1, which is a sub-biextension of E. This sub-biextension E' is contained in W and has the same dimension as W, hence W is equal to E'. □

(7.4) PROPOSITION. *Let W be a formal subvariety of E stable under the action of G. Assume that the slope of X, Y are mutually distinct, Z is isoclinic, and the slope of Z is strictly bigger than every slope of $X \times Y$. Assume also that the action of G on E is strongly non-trivial in the sense of 2.6.5. Then W is a sub-biextension of E.*

PROOF. We will first perform some reduction steps.

Reduction step 1. Being a sub-biextension means that W is stable under the two relative group laws $+_1$ and $+_2$, which can be verified after extending the base field k to an algebraic closure of k. So we may and do assume that k is algebraically closed.

Reduction step 2. It is easy to see that the statement 7.4 does not change under isogeny: if $E' \to E$ and $E \to E''$ are isogenies of biextensions, then the statement 7.4 for E is equivalent to the statement for E' and also equivalent to the statement for E''. Changing X, Y, Z by isogeny if necessary, we may and do assume that both X and Y are product of isoclinic p-divisible subgroups. Moreover if U is the maximal isoclinic p-divisible subgroup for a given slope in one of the three p-divisible groups X, Y, or Z, then there exists positive integers $c, d > 0$ such that $U[p^c] = \mathrm{Ker}[\mathrm{Fr}^d_{U/k}]$.

Reduction step 3. We may and do assume that the image of W in $X \times Y$ is equal to $X \times Y$.

Claim. The statement 7.4 holds under the additional assumptions in reduction steps 1–3.

We have seen that 7.4 follows from the claim. We will prove the claim by induction on the number of slopes of $X \times Y$. Denote this number by #slopes$(X \times Y)$

THE CASE WHEN #slopes$(X \times Y) = 2$, namely both X and Y are isoclinic. This is the initial step of the induction.

Suppose first that $\mathrm{slope}(X) + \mathrm{slope}(Y) \neq \mathrm{slope}(Z)$, then the $W(k)$-bilinear pairing

$$\Theta_E : \mathrm{M}_*(X) \times \mathrm{M}_*(Y) \to \mathrm{M}_*(Z)$$

is identically zero. Then the biextension $E \to X \times Y$ splits by 2.6.3, and the canonical splitting of E induces a natural isomorphism h from E to the trivial biextension $X \times Y \times Z$. The trivial biextension $X \times Y \times Z$ has a natural structure as a p-divisible group, and every automorphism of this trivial biextension is also an automorphism for the p-divisible group structure. Apply the local rigidity for p-divisible formal groups [3, 4.3], we conclude that the G-stable formal subvariety W of $E \cong X \times Y \times Z$ is of the form $Z_1 \times X \times Y$ for a p-divisible subgroup of Z. Therefore W is a sub-biextension of E.

Assume now that $\mathrm{slope}(X) + \mathrm{slope}(Y) = \mathrm{slope}(Z)$. Recall that both X and Y are p-divisible formal groups, hence $\mathrm{slope}(X) > 0$ and $\mathrm{slope} = 0$ and 7.2.4 applies. We have proved the claim when both X and Y are isoclinic.

THE INDUCTION STEP. Suppose that #slopes$(X \times Y) = m_0$, $m_0 \geq 3$, and that the claim holds whenever #slopes$(X \times Y) \leq m_0 - 1$. By symmetry may assume that the largest slope of X, μ_1, is bigger than the largest slope of Y. Let X_1 be the largest p-divisible subgroup of X with slope μ_1. According to the assumption in reduction step 2, the p-divisible group X is isomorphic to a product $X_1 \times X_2$, where X_2 is a p-divisible subgroup such that every slope of X_2 is strictly smaller than μ_1.

There are two cases to consider. If $\mu_1 < \mathrm{slope}(Z)$, then the claim holds for the biextension E by 7.2.4. It remains to treat the case when $\mu_1 > \mathrm{slope}(Z)$.

Suppose now that $\mu_1 > \mathrm{slope}(Z)$. Let $E_1 := \pi^{-1}(X_1 \times Y)$ and $E_2 := \pi^{-1}(X_2 \times Y)$. We have

$$E \xrightarrow{\sim} (+_Z : Z \times Z \to Z)_*(E_1 \times_Y E_2)\,,$$

where $+Z : Z \times Z \to Z$ is the group law for Z, and the push-out by $+_Z$ of the fiber product $E_1 \times_Y E_2$ is an analog of the familiar Baer sum construction for extensions of commutative groups; we will call it the Y-Baer sum of E_1 and E_2 Notice that the Y-Baer sum $(+_Z)_*(E_1 \times_Y E_2)$ of two biextensions of $X \times Y$ by the same p-divisible group Z has a natural structure as a biextension, and the above isomorphism is compatible with the biextension structures on both sides of the arrow. The biextension $E_1 \to X_1 \times Y$ of $X_1 \times Y_1$ by Z splits, and we have a canonical G-equivariant isomorphism $\upsilon : E_1 \xrightarrow{\sim} X_1 \times Y \times Z$. Let $\mathrm{pr}_{X_1} : E \to X_1$ be the composition of $\pi : E \to X \times Y = X_1 \times X_2 \times Y$ with the projection $\mathrm{pr}_{X_1} : X_1 \times X_2 \times Y \to X_1$. The splitting of the biextension E_1 and the partial group law $+_1$ defines a natural translation action

$$T\colon X_1 \times_{\mathrm{Spec}(k)} E \to E \qquad (x_1, e) \mapsto x_1 *_{X_1} e := T(x_1, e) \;\; x_1 \in X_1,\; e \in E$$

of X_1 on E, which is compatible with the composition $\mathrm{pr}_{X_2 \times Y} \circ \pi$, where $\pi : E \to X \times Y = X_1 \times X_2 \times Y$ is the structural map of the biextension E and $\mathrm{pr}_{X_2 \times Y}$ is the projection $\mathrm{pr}_{X_2 \times Y} : X_1 \times X_2 \times Y \to X_2 \times Y$. By local rigidity of p-divisible formal groups, we know that $W \supset \upsilon^{-1}(X_1)$.

It is important to obverse that because the slope of X_1 is strictly bigger than every slope appearing in Z, X_2 or Y, for every element $v = (A, B, C) \in \mathrm{Lie}(G)$ such that $A \in \mathrm{End}(X)$, $B \in \mathrm{End}(Y)$, and $C \in \mathrm{End}(Z)$, the action of $\exp(p^n v)$ on E is essentially translation by $p^n C \circ \mathrm{pr}_{X_1}$ for all sufficiently large natural numbers $n \in \mathbb{N}$. More precisely, there exist positive integers r_1, s_2, a_1, n_1 such that

- $0 < r_1 < s_1$, $a_1 > 0$, $n_1 \geq 2$,
- $\mathrm{slope}(X_1) = \frac{a_1}{r_1}$, and $X_1[p^{a_1}] = \mathrm{Ker}(\mathrm{Fr}^{r_1}_{X_1/k})$,
- $\psi(\exp(p^{na_1} v)) \equiv \left(p^{na_1} C \circ \mathrm{pr}_{X_1}\right) *_{X_1} \mathrm{id}_E \pmod{\mathfrak{m}_E^{p^{ns_1}}}$ for all $n \geq n_1$.

The above properties allows us to apply the identity principle 6.1.1 as in the proof of 7.2 to conclude that for the morphism

$$T_{X_1} \circ \left((C \circ \mathrm{pr}_{X_1}) \times \mathrm{id}_E\right) : E \times E \longrightarrow E, \quad (e_1, e_2) \mapsto T_{X_1}\left(C \circ \mathrm{pr}_{X_1}(e_1), e_2\right), \;\; e_1, e_2 \in E$$

we have

$$\left(T_{X_1} \circ \left((C \circ \mathrm{pr}_{X_1}) \times \mathrm{id}_E\right)\right)(W \times W) \subseteq W.$$

Note that the above proof that the formal variety W is stable under translation by $(C \circ \mathrm{pr}_{X_1})$ is the same as the argument in step 1 of the proof of [3, 4.3]; complete restricted perfection of power series rings are not used.

The rest of the proof is quite formal. Because the action of G on X is strongly non-trivial, we deduce that

$$\left(T_{X_1} \circ \left(\mathrm{pr}_{X_1} \times \mathrm{id}_E\right)\right)(W \times W) \subseteq W.$$

In particular W is stable under translation by X_1. The quotient of E by X_1 is canonically isomorphic to E_2. Under this canonical isomorphism W/X_1 becomes a formal subvariety of E_2. By induction W/X_1 is sub-biextension of E_2, which is a biextension of $X_2 \times Y$ by the p-divisible subgroup $W \cap Z \subseteq Z$ of Z. It follows that W itself is a sub-biextension of E. $\square$

(7.5) THEOREM. *Let W be a formal subvariety of E stable under the action of G. Assume that the slope of X, Y, Z are mutually distint, i.e. no two of the p-divisible formal groups X, Y, Z share any common slope. Assume also that the action of G on E is strongly non-trivial in the sense of 2.6.5. Then W is a sub-biextension of E.*

PROOF. As in the proof of 7.4, we may and do assume that the assumption in the reduction steps 1–3 in the proof of 7.4 hold. We will use induction on the pair

$$\mathrm{inv}_E := (\#\mathrm{slopes}(Z), \#\mathrm{slopes}(X \times Y))$$

under the lexicographic ordering. The case when $\#\mathrm{slopes}(Z) = 1$ has been treated in 7.4.

Suppose that $\#\mathrm{slopes}(Z) = m_2 \geq 2$, $\#\mathrm{slopes}(X \times Y) = m_3 \geq 2$, and assume that the statement of 7.5 holds whenever $\mathrm{inv}_E < (m_2, m_3)$ in the lexicographic order. Let ν_2 be the largest slope of Z, and let ν_3 be the largest slope of $X \times Y$. We may and do assume that ν_3 is a slope of X. Write $X = X_3 \times X_4$, where X_3 is isoclinic of slope ν_3, and ν_3 is not a slope of X_4. Similarly $Z = Z_2 \times Z_4$, where Z is isoclinic of slope ν_2, and ν_2 is not a slope of Z_4.

There are two cases to consider.

CASE 1. Suppose first that $\nu_2 > \nu_3$.

Let $E_2 := (\mathrm{pr}_{Z_2} : Z \to Z_2)_* E$, $E_4 := (\mathrm{pr}_{Z_2} : Z \to Z_4)_* E$. We have a natural isomorphism

$$E \xrightarrow{\sim} E_2 \times_{(X\times Y)} E_4$$

over $X \times Y$. Let W_2 be the image of W in E_2, and let W_4 be the image of W in E_4. By induction, we know that W_2 is an sub-biextension E_2' of $X \times Y$ by a p-divisible subgroup Z_2' of Z_2. Clearly $Z_2' = Z_2 \cap W$, where we have regarded Z_2 as a formal subvariety of $Z = \pi^{-1}(0,0) \subset E$. Again by induction we know that W_4 is a sub-biextension E_4' of $X \times Y$ by a p-divisible subgroup Z_4' of Z_4.

Modifying Z by an isogeny, we may and do assume that there exists a p-divisible subgroup Z'' of Z such that $Z \cong Z_2' \times Z_2''$. Let E_2' and E_2'' be the push-out of the biextension E_2 by the projections from E_2 to E_2' and E_2'' respectively. We have a natural isomorphism

$$E_2 \xrightarrow{\sim} E_1' \times_{(X\times Y)} E_2''.$$

Clearly the formal subvariety W of E is contained in the sub-biextenion $E_2' \times_{(X\times Y)} E_4$ of E. If $Z'' \neq (0)$, we are done by induction. So we may and do assume that $Z_2' = Z$.

By 7.2 we know that W is stable under translation by Z_2. Under the natural isomorphism $E/Z_2 \xrightarrow{\sim} E_4$ the quotient W/Z_2 corresponds to a G-invariant formal subvariety of the biextension $E_4 \to X \times Y$. By induction, this G-invariant formal subvariety W/Z_2 of E_4 is a sub-biextension of $E_4 \cong E/Z_2$. It follows that W itself is a sub-biextension of E. We have finished the case when the largest slope ν_2 of Z is bigger then every slope of $X \times Y$.

CASE 2. $\nu_2 < \nu_3$. There exists a p-divisible subgroups X_3, X_4 of X such that X_3 is isoclinic of slope ν_3, and every slope of X_4 is strictly smaller than ν_3. Let E_3, E_4 be the pull-back of E to $X_3 \times Y$ and $X_4 \times Y$ respectively. The biextension E is naturally isomorphic to the "Y-Baer sum" $(+_Z : Z \times Z \to Z)_*(E_3 \times_Y E_4)$ of the biextensions E_3 and E_4:

$$E \xrightarrow{\sim} (+_Z : Z \times Z \to Z)_*(E_3 \times_Y E_4)$$

Because the slope ν_3 of X_3 is strictly bigger than every slope of Z, the biextension $E_3 \to X_3 \times Y$ of $X_3 \times Y$ by Z splits:

$$E_3 \xrightarrow{\sim} X_3 \times Y \times Z.$$

As in the proof of 7.4, the condition that $\nu_3 > \nu_2$ implies that for every element $v = (A,B,C) \in \mathrm{Lie}(G)$ such that $A \in \mathrm{End}(X)$, $B \in \mathrm{End}(Y)$ and $C \in \mathrm{End}(Z)$, the action of $\psi(\exp(p^m)v)$ on E has a "main term" corresponding to translation by the composition of the endomorphism $p^n C|_{X_3}$ of X_3 with the projection $\mathrm{pr}_{X_3} : E \to X_3$. More precisely the automorphism $\psi(\exp(p^m)v)$ of E satisfies a congruence relation

$$\left(p^m C \circ \mathrm{pr}_{X_3}\right) *_{X_3} \mathrm{id}_E \mod \mathfrak{m}^{p^{\lfloor m/(\nu_2+\varepsilon_2)\rfloor}}$$

for a suitably small real number $\varepsilon_2 < \nu_3 - \nu_2$, and for all natural numbers $m \geq m_0$, where m_0 is a natural number which depends on the biextension $E \to X \times Y$ and ε_2. Applying the identity principle 6.1.1 for power series, we deduce that

$$\left(T_{X_3} \circ \left((C \circ \mathrm{pr}_{X_3}) \times \mathrm{id}_E\right)\right)(W \times W) \subseteq W,$$

where

- $\mathrm{pr}_{X_3} : E \to X_3$ is the composition of $\pi : E \to X \times Y = X_3 \times X_4 \times Y$ with the projection $X_3 \times X_4 \times Y \to X_3$,

- $T_{X_3} : X_3 \times E \to E$ is the translation action of X_3 on E induced by the action of X_3 on the trivial biextension $E_3 \xrightarrow{\sim} X_3 \times Y \times Z$ and the trivial action of X_3 on E_4, through the natural isomorphism $E \cong (+_Z : Z \times Z \to Z)_* E_3 \times_{(X \times Y)} E_4$.

Because the action of G on X is strictly non-trivial, it follows that W is stable under translation by X_3 in the following sense:

$$\left(T_{X_3} \circ (\mathrm{pr}_{X_3} \times \mathrm{id}_E)\right)(W \times W) \subseteq W.$$

The quotient W/X_3 is a formal subvariety of $E/X_3 \xrightarrow{\sim} E_4$. The induction hypothesis implies that W/X_3 is a sub-biextension of E_4, which in turn implies that W is a sub-biextension of E. We have finished the induction step. $\square$

References

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

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

[3] C.-L. Chai. A rigidigy result for p-divisible formal groups, *Asian J. Math.* **12** (2008), 193–202.

[4] H. Hida. The Iwasawa μ-invariant of p-adic Hecke L-functions. *Ann. Math.* **172** (2010) 41–137.

[5] (SGA 7 I) *Groupes de Monodromie en Géométrie Algébrique*, dirigé par A. Grothendieck, Lecture Notes in Math. 288, Springer-Verlag 1972.

[6] D. Mumford. Bi-extensions of formal groups. In *Algebraic Geometry* (Internat. Colloq. Tata Inst. Fund. Res., Bombay, 1968), Oxford Univ. Press, 1969, 307–322.

[7] O. Zariski and P. Samuel. *Commutative Algebra* volume *II*, Van Nostrand, 1960.