Math. Res. Lett.
Volume 21, Number 05, 1015–1045, 2014

On the moduli space of deformations of a p-divisible group

Oleg Demchenko and Alexander Gurevich

Let G be a connected p-divisible group of height h and dimension d over a perfect field k, and $\mathcal{O}$ denote the ring of Witt vectors over k. It is a well-known fact that the deformation functor $\mathcal{D}ef_G$ is representable by $\mathrm{Spf}_{\mathcal{O}}\mathcal{O}[[t_1, \dots, t_{d(h-d)}]]$. Following Hazewinkel's philosophy we construct explicitly a family of universal deformations of G.

Introduction

Deformation functor in the language of formal power series

Let $\mathcal{O}$ denote the ring of Witt vectors over a perfect field k of characteristic $p > 0$. Denote by $\mathcal{A}_{\mathcal{O}}$ the category of Artinian local $\mathcal{O}$-algebras with residue field k. For a p-divisible group G over k, the deformation functor $\mathcal{D}ef_G \colon \mathcal{A}_{\mathcal{O}} \to \mathcal{S}ets$ assigns to $R \in \mathrm{Ob}\mathcal{A}_{\mathcal{O}}$ the set of the isomorphism classes of the pairs $(G',\ i)$, where G' is a p-divisible group over R and $i : G' \otimes_R k \to G$ is an isomorphism. Grothendieck proved that $\mathcal{D}ef_G$ is representable by a smooth formal $\mathcal{O}$-scheme of relative dimension m (i.e., $\mathcal{D}ef_G \cong \mathrm{Spf}_{\mathcal{O}}\mathcal{O}[[t_1, \dots, t_m]]$), where $m = \dim G \cdot \dim G^t$, and G^t is the dual p-divisible group (see [7, Corollary 4.8]).

We essentially employ the coordinate point of view on both p-divisible groups and their deformation spaces. Any smooth d-dimensional connected formal scheme G over k is formally represented by the ring of formal power series in d variables with coefficients in k. If, in addition, G has a commutative group structure, then any choice of a coordinate system on G (i.e., an isomorphism $G \to \mathrm{Spf}_k k[[x_1, \dots x_d]]$) gives a commutative formal group law over k which we, following Honda [6], call a formal group.

Grothendieck's theorem can be formulated in terms of formal groups. Indeed, if a connected p-divisible group G over k is represented by a formal group Φ, the functor $\mathcal{D}ef_G$ can be identified with the functor which assigns to $R \in \mathrm{Ob}\mathcal{A}_{\mathcal{O}}$ the set of $\star$-isomorphism classes of R-deformations of Φ. Here R-deformation is a formal group over R with reduction equal to Φ, and $\star$-isomorphism is an isomorphism with identity reduction. Besides, if $\dim G = d$, then $\dim G^t = h - d$, where h is the height of G, i.e., the $\mathcal{O}$-rank of the Dieudonné module $\mathcal{D}(G)$. On the other hand, $\mathcal{D}(G)$ can be constructed through the logarithm of an $\mathcal{O}$-deformation of Φ (see for instance [4]).

The choice of a coordinate system on $\mathcal{D}ef_G$ (i.e., an isomorphism from $\mathcal{D}ef_G$ to $\mathrm{Spf}_{\mathcal{O}}\mathcal{O}[[t_1, \ldots, t_m]]$) is equivalent to the choice of a universal deformation of Φ. The latter is a formal group Γ over $\mathcal{O}[[t_1, \ldots, t_m]]$ satisfying the following condition: for any $R \in \mathrm{Ob}\mathcal{A}_{\mathcal{O}}$ and any R-deformation F of Φ there exists a unique $\mathcal{O}$-homomorphism $\mu : \mathcal{O}[[t_1, \ldots, t_m]] \to R$ such that $\mu_*\Gamma$ is $\star$-isomorphic to F.

We approach the deformation problem using Hazewinkel's universal multidimensional p-typical formal group and construct a family of explicit universal deformations of Φ as its specializations. In particular, it gives a new proof of Grothendieck's result. Note that Grothendieck's proof of the representability of $\mathcal{D}ef_G$ is based on the theory of obstructions, and it does not allow one to find a coordinate system on $\mathcal{D}ef_G$ explicitly.

Finally, we believe that our result can be applied to an explicit description of the natural action of $\mathrm{Aut}_k(G)$ on $\mathcal{D}ef_G$ defined by $\phi[(G', i)] = [(G', \phi \circ i)]$ for any $\phi \in \mathrm{Aut}_k(G)$, $[(G', i)] \in \mathcal{D}ef_G(R)$, $R \in \mathrm{Ob}\mathcal{A}_{\mathcal{O}}$. In the case where $\dim G = 1$, such a description was established in [2] with the aid of the universal deformation constructed by Hazewinkel. The universal deformation introduced in the present paper will hopefully allow us to treat similarly the action in the multidimensional case.

Historical review

Lubin and Tate [8] were the first to study the deformation functor in the case of dimension one. They considered the second cohomology group of Φ and proved that its deformation functor is isomorphic to $\mathrm{Spf}_{\mathcal{O}}\mathcal{O}[[t_1, \ldots, t_{h-1}]]$, where h is the height of Φ. For the case of arbitrary dimension, a similar consideration was given in [11], where the representability of the deformation functor was established by using Schlessinger's criterion. As in the case of Grothendieck's proof, this approach does not provide any explicit universal deformation.

A description of deformations of a p-divisible group can be obtained through the crystalline Dieudonné theory developed by Grothendieck and Messing [9]. Another approach to the deformation theory, due to Norman [10], includes an explicit construction of a universal deformation in terms of the Cartier module. Although only deformations over rings of finite characteristic were originally considered, Norman's ideas were later expanded by Zink to introduce the notion of $3n$-display. In his fundamental work [12], Zink described the universal deformation of a $\mathcal{3}n$-display and showed that the category of $\mathcal{3}n$-displays is equivalent to the category of p-divisible groups over excellent rings.

The result of Lubin and Tate was reproved by Hazewinkel [5]. He introduced the universal p-typical formal group F_V over a ring of formal power series such that any p-typical formal group over an arbitrary ring R can be obtained from F_V by specialization of the variables in R. Then, if the specialization for a one-dimensional p-typical formal group Φ over k of height h is given by a sequence of parameters, any lifting of all but the first $h-1$ parameters gives a universal deformation of Φ.

Outline of the paper

The present paper is organized as follows. Our main goal is to prove a generalization of Hazewinkel's theorem on deformations of a one-dimensional formal group [5, Theorem 22.4.4] to the multidimensional case. Following Hazewinkel, two distinct moduli problems are studied: one for deformations considered up to strict $\star$-isomorphism and the other for deformations considered up to $\star$-isomorphism. In the first case, all the proofs are much simpler, while the second case is more important, since it corresponds to the classical moduli problem on deformations of a p-divisible group. We state this theorem in the first case and sketch its proof.

For an infinite set V of independent variables, let F_V be a universal d-dimensional p-typical formal group over the polynomial ring $\mathbb{Z}[V]$. If a is a sequence of elements of a ring A, denote by $F_{V(a)}$ a formal group over A obtained by the specialization of F_V at $V = a$. Any p-typical formal group Φ over k is uniquely represented as $\Phi = F_{V(\Xi)}$, where Ξ is a sequence of elements from k. Fix any lifting Θ of Ξ to $\mathcal{O}$, then $F_{V(\Theta)}$ is a deformation of Φ over $\mathcal{O}$.

Our main result (Theorem 2) is that one can construct a finite set of indices Ψ such that for any local $\mathcal{O}$-algebra R with maximal ideal $\mathfrak{M}$ and for any deformation F of Φ over R, there exists a unique tuple $(\tau_\psi)_{\psi\in\Psi}$, $\tau_\psi \in \mathfrak{M}$, such that $F_{V(\Theta+\tau)}$ is strictly $\star$-isomorphic to F, where τ is a sequence whose elements are all zero except those corresponding to Ψ and equal to τ_ψ. The choice of Ψ is not necessarily unique and Proposition 9 provides some simple form for it. Moreover, it is shown that in this form Ψ behaves naturally with respect to direct sum of formal groups (Proposition 10). Finally, assuming k to be algebraically closed, Ψ is found explicitly for the standard representative of each isogeny class of formal groups over k (Example 3).

In the proof, Hazewinkel's strategy is followed. By induction, we construct a Cauchy sequence of parameters $Z(n)$ such that $F_{V(Z(1))}$ is strictly

$\star$-isomorphic to F, $F_{V(Z(n+1))}$ is strictly $\star$-isomorphic to $F_{V(Z(n))}$, and $Z(n)(v)$ converges to $\Theta(v)$ for any $v \in V \setminus \{v_\psi\}_{\psi\in\Psi}$. Then $Z = \lim Z(n)$ gives the required deformation $F_{V(Z)}$. To perform the induction step, we employ a universal strict isomorphism $\alpha_{V,T}\colon F_V \to F_{V,T}$ over $\mathbb{Z}[V,T]$, where T is another set of variables indexed by the same set as V. Since $F_{V,T}$ is p-typical, there exists $\kappa\colon \mathbb{Z}[V] \to \mathbb{Z}[V,T]$ such that $F_{V,T} = \kappa_* F_V$. Let $N(V,T)$ be the T-linear part of $V - \kappa(V)$ and $N_\Xi = N(\Xi,T)\colon \mathcal{T} \to \mathcal{T}$ denote the corresponding k-linear map for $\mathcal{T}$ being the vector space over k whose coordinates are indexed by T. In order to control the approximation error, a set of indices Ψ is chosen so that $\pi\, N_\Xi\colon \mathcal{T} \to \Pi_\Psi$ is surjective, where $\pi\colon \mathcal{T} \to \Pi_\Psi$ is the factorization map by the subspace of $\mathcal{T}$ consisting of vectors whose coordinates are non-zero only if the corresponding indices belong to Ψ. To prove the uniqueness of $F_{V(Z)}$, the injectivity of $\pi\, N_\Xi$ (Proposition 14) is needed. Thus Ψ must be such that $(v_\psi + \operatorname{Im} N_\Xi)_{\psi\in\Psi}$ form a basis in the cokernel of N_Ξ. It turns out that N_Ξ in this condition can be replaced by another linear operator Y_Ξ on $\mathcal{T}$ which has rather simple form (Proposition 4). In fact, there is a natural isomorphism of k-vector spaces between $\mathcal{T}$ and $\blacktriangle\mathrm{M}_d(\mathcal{E})$, where $\mathcal{E} = k[[\blacktriangle]]$ is a k-algebra with multiplication rule $\blacktriangle a = a^p \blacktriangle$, $a \in k$, so that Y_Ξ corresponds to the right multiplication by the element $U = \sum_{n=1}^{\infty} \Xi_n \blacktriangle^n \in \blacktriangle\mathrm{M}_d(\mathcal{E})$. Then it is easy to show that $\blacktriangle\mathrm{M}_d(\mathcal{E})/\blacktriangle\mathrm{M}_d(\mathcal{E})U$ is isomorphic as a k-vector space to the direct sum of d-copies of $\mathcal{D}(\Phi) \otimes_{\mathcal{O}} k$, where $\mathcal{D}(\Phi)$ is the Dieudonné module of Φ. Thus the codimension of Y_Ξ equals dh, which gives the number of elements in Ψ (Proposition 8).

The statement and the proof of the theorem in the second case are similar. We use the universal isomorphism with strict reduction $\gamma_{V,T'}\colon F_V \to F_{V,T'}$ defined over $\mathbb{Z}[V,T][[T_0]]$ (Theorem 1) instead of $\alpha_{V,T}$, and the linear operators N'_Ξ and Y'_Ξ (Proposition 7) instead of N_Ξ and Y_Ξ, respectively. Thus we obtain a condition on the set of indices Ψ^+ corresponding to variables which are allowed to vary, and calculate the number of its elements. The theorem proved implies that any choice of a deformation $F_{V(\Theta)}$ of Φ over $\mathcal{O}$ together with Ψ (resp. Ψ^+) provides a universal deformation of Φ in the first (resp. second) case.

1. Formal groups

Basic definitions

Let A be a ring. We denote by X the d-tuple of independent variables $(x_1, \dots, x_d)$ and write $X^q, q \in \mathbb{N}$, for the d-tuple $(x_1^q, \dots, x_d^q)$. We also consider the ring $A[[X]]_0$ of formal power series over A in variables $x_1, \dots, x_d$ without constant term.

A d-dimensional *formal group* over A is a d-tuple of formal power series $F \in A[[X,Y]]^d$ satisfying the following properties

(i) $F(X,0) = X$;

(ii) $F(X, F(Y,Z)) = F(F(X,Y),Z)$;

(iii) $F(X,Y) = F(Y,X)$.

The simplest examples are the one-dimensional additive and multiplicative formal groups $\mathbb{F}_a(X,Y) = X + Y$ and $\mathbb{F}_m(X,Y) = X + Y + XY$.

Let F and F' be d- and d'-dimensional formal groups over A. A d'-tuple of formal power series $g \in A[[X]]_0^{d'}$ is called a *homomorphism* from F to F', if $g(F(X,Y)) = F'(g(X), g(Y))$. The matrix $D \in \mathrm{M}_{d',d}(A)$ satisfying $g(X) \equiv DX \mod \deg 2$ is called the *linear coefficient* of g. It is easy to see that a homomorphism g is an isomorphism if and only if its linear coefficient is an invertible matrix. An isomorphism with identity linear coefficient is called a *strict isomorphism.*

Let R be a complete Noetherian local ring with residue field k, and Φ be a formal group law over k. A formal group F over R with reduction Φ is called a *deformation* of Φ over R. Let F, F' be deformations of Φ over R. An isomorphism from F to F' with identity reduction is called a $\star$*-isomorphism.*

If A is a $\mathbb{Q}$-algebra, then for any d-dimensional formal group F over A, there exists a unique strict isomorphism f from F to $\mathbb{F}_a^d$ (see for instance [6, Theorem 1]). This f is called the *logarithm* of F.

If A is a ring of characteristic 0 and F is a formal group over A, the logarithm of F is by definition the logarithm of $F_{A\otimes\mathbb{Q}}$. If, in addition, F' is another formal group over A and g is a homomorphism from F to F' with linear coefficient D, then $g = f'^{-1} \circ (Df)$, where f, f' are the logarithms of F, F', respectively (see [6, Proposition 1.6]).

Formal groups over Witt vectors

Let k be a perfect field of characteristic $p \neq 0$, $\mathcal{O}$ be the ring of Witt vectors over k, $\mathcal{K}$ be the quotient field of $\mathcal{O}$, and $\Delta\colon \mathcal{K} \to \mathcal{K}$ be the Frobenius automorphism. Let E denote the set of formal power series over $\mathcal{O}$ in indeterminate $\blacktriangle$ with the usual addition and multiplication given by $\blacktriangle a = a^\Delta \blacktriangle$ for any $a \in \mathcal{O}$. Extend the $\mathcal{O}$-module structure on $\mathcal{K}[[X]]_0$ to a left E-module structure by the formula $\blacktriangle f(X) = f^\Delta(X^p)$. It determines a bilinear map $\mathrm{M}_{d',d}(E) \times \mathcal{K}[[X]]_0^d \to \mathcal{K}[[X]]_0^{d'}$. In particular, we obtain a left $\mathrm{M}_d(E)$-module structure on $\mathcal{K}[[X]]_0^d$.

Let $u \in \mathrm{M}_d(E)$ be such that $u \equiv pI \mod \blacktriangle$. We say that u is a *type* of $f \in \mathcal{K}[[X]]_0^d$ if $f(X) \equiv X \mod \deg 2$ and $uf \equiv 0 \mod p$, i.e., $uf \in p\mathcal{O}[[X]]$.

Honda theory [6] describes the logarithms of formal groups over $\mathcal{O}$ as formal power series of certain Honda type.

Theorem A1. *[6, Theorem 2 and Proposition 3.3]*

(1) *Let $u \in \mathrm{M}_d(E)$, $u \equiv pI \mod \blacktriangle$, $f \in \mathcal{K}[[X]]_0^d$ be of type u. Then f is the logarithm of a formal group over $\mathcal{O}$.*

(2) *Let F be a formal group over $\mathcal{O}$ with the logarithm $f \in \mathcal{K}[[X]]_0^d$. Then there exists $u \in \mathrm{M}_d(E)$, $u \equiv pI \mod \blacktriangle$, such that f is of type u.*

Proposition A1. *[6, Proposition 2.6] Let $u \in \mathrm{M}_d(E)$, $u \equiv pI \mod \blacktriangle$, $f \in \mathcal{K}[[X]]_0^d$ be of type u, $v \in \mathrm{M}_{d',d}(E)$. If $vf \equiv 0 \mod p$, then there exists $s \in \mathrm{M}_{d',d}(E)$ such that $v = su$.*

Formal groups over finite fields

With the aid of Honda theory, the category of formal groups over k can be also described and the Dieudonné module can be constructed. First, we formulate one more auxiliary statement.

Lemma A1. *[6, Lemma 4.2 and Lemma 4.3]*

(1) *Let $u \in \mathrm{M}_d(E)$, $u \equiv pI \mod \blacktriangle$, $f \in \mathcal{K}[[X]]_0^d$ be of type u, $\psi_1 \in \mathcal{K}[[X']]_0^d$ and $\psi_2 \in \mathcal{O}[[X']]_0^d$ for $X' = (x'_1, \dots, x'_{d'})$. Then $f \circ \psi_1 \equiv f \circ \psi_2 \mod p$ iff $\psi_1 \equiv \psi_2 \mod p$.*

(2) *Let F be a formal group over $\mathcal{O}$ with the logarithm $f \in \mathcal{K}[[X]]_0^d$ and $\psi \in \mathcal{K}[[X]]_0$. Then $\psi \circ F(X,Y) \equiv \psi(X) + \psi(Y) \mod p$ iff there exists $s \in \mathrm{M}_{1,d}(E)$ such that $\psi \equiv sf \mod p$.*

Proposition 1. *Let F,F' be formal groups over $\mathcal{O}$ with logarithms $f, f' \in \mathcal{K}[[X]]_0^d$, respectively. Then the reductions of F and F' modulo p are equal iff there exists $v \in \mathrm{GL}_d(E)$ such that $f \equiv vf' \mod p$.*

Proof. By Lemma A1 (2), $f \equiv vf' \mod p$ for some $v \in \mathrm{M}_d(E)$ iff $f \circ F'(X,Y) \equiv f(X) + f(Y) = f \circ F(X,Y) \mod p$. According to Theorem A1 (2), there exists $u \in \mathrm{M}_d(E)$, $u \equiv pI \mod \blacktriangle$, such that f is of type u. Then Lemma A1 (1) implies that $f \circ F' \equiv f \circ F \mod p$ iff $F' \equiv F \mod p$. □

Let F be a d-dimensional formal group over $\mathcal{O}$ with logarithm $f \in \mathcal{K}[[X]]_0^d$ of type $u \in \mathrm{M}_d(E)$, and Φ denote the reduction of F modulo p. The

E-module $\mathcal{D}(\Phi) = \mathrm{M}_{1,d}(E)f/p\mathcal{O}[[X]]_0$ is called the *Dieudonné module* of Φ. Proposition 1 implies that $\mathcal{D}(\Phi)$ depends only on Φ. Since $uf \in p\mathcal{O}[[X]]_0^d$, the E-linear map $\mathrm{M}_{1,d}(E) \to \mathcal{D}(\Phi)$ defined by $s \mapsto sf + p\mathcal{O}[[X]]_0$ induces a homomorphism $\mathrm{M}_{1,d}(E)/\mathrm{M}_{1,d}(E)u \to \mathcal{D}(\Phi)$ which is an isomorphism by Proposition A1. A formal group Φ is said to be of finite height if $\mathcal{D}(\Phi)$ is a free $\mathcal{O}$-module of finite rank (see [4, Proposition III.6.1]). In this case, the rank of $\mathcal{D}(\Phi)$ is called the *height* of Φ.

Proposition A2. *[6, Theorem 5] Let Φ, Φ' be formal groups over k of dimension d and d', respectively. Suppose that u, u' be types of logarithms of deformations of Φ, Φ'. Then there is a homomorphism from Φ to Φ' iff there exist $w, z \in \mathrm{M}_{d',d}(E)$ such that $u'w = zu$. The homomorphism is an isomorphism iff w is invertible.*

2. Universal formal groups and isomorphisms

Notation and conventions

Let $\mathrm{M}_d(A)$ and $\mathrm{GL}_d(A)$ denote the full matrix ring and the multiplicative group of invertible matrices of order d with entries in a ring A, respectively. Denote by $I \in \mathrm{M}_d(A)$ the identity matrix. An entry of a matrix M in the ith row and the jth column is denoted by $M(i,j)$. If M, M' are $d \times d$-matrices, along with standard matrix multiplication, we consider entry–by–entry multiplication $M * M'$, i.e., $(M * M')(i,j) = M(i,j)M'(i,j)$, $1 \le i,j \le d$. Similarly, the matrix obtained from M by raising all its entries to the qth power is denoted by $M^{(q)}$, i.e., $M^{(q)}(i,j) = M(i,j)^q$, $1 \le i,j \le d$.

If $\mu\colon A \to A'$ is a ring homomorphism and $f \in A[[X]]$, then $\mu_* f \in A'[[X]]$ stands for a power series obtained by applying μ to the coefficients of f. Besides, we consider polynomial rings with integer coefficients in an infinite number of variables, which are grouped together in matrices for convenience. Let V_n, S_n, $n \ge 1$ and T_n, $n \ge 0$ be $d \times d$-matrices of independent variables $V_n(i,j)$, $S_n(i,j)$ and $T_n(i,j)$, respectively. The sets of these matrices are denoted by $V = (V_1, V_2, \ldots)$, $\widehat{S} = (S_1, S_2, \ldots)$, $T = (T_1, T_2, \ldots)$ and $T' = (T_0, T_1, \ldots)$.

Let $P(f)$ denote the p-typical part of a power series f in variables $x_1, \ldots, x_d$, i.e., the power series obtained from f by removing all monomials except monomials of the form $ax_i^{p^n}$, $1 \le i \le d$, $n \ge 0$. If f_i, $1 \le i \le d$, are power series, we write $P(f_1, \ldots, f_d)$ for the d-tuple $(P(f_1), \ldots, P(f_d))$.

Let $\bar{\mathcal{P}}$ be the set of positive integers which are not p-powers.

Universal formal groups F_V and F_S

We state a special case of Hazewinkel's functional equation lemma and introduce some formal groups which play an important role in our paper.

Functional equation lemma. *[5, 10.2] Let p be a prime number, A be a subring of a ring K, σ be an endomorphism of K such that $\sigma(a) \equiv a^p \mod pA$ for all $a \in A$, and $s_1, s_2, \ldots \in \mathrm{M}_d(K)$ be such that $ps_n(i,j) \in A$ for $1 \le i,j \le d$, $n \ge 1$. Let $g \in A[[X]]_0^d$ be a d-tuple of power series with invertible Jacobian. Then the d-tuple of power series $f_g \in K[[X]]_0^d$ defined by the recursion formula*

$$f_g(X) = g(X) + \sum_{n=1}^{\infty} s_n \sigma_*^n f_g(X^{p^n})$$

is the logarithm of a d-dimensional formal group over A.

Apply the functional equation lemma for the following data:

(1) $K = \mathbb{Q}[V]$; $A = \mathbb{Z}[V]$; $\sigma(V_n(i,j)) = V_n(i,j)^p$; $s_n = p^{-1}V_n$; $g_V(X) = X$.

(2) $K = \mathbb{Q}[\widehat{S}]$; $A = \mathbb{Z}[\widehat{S}]$; $\sigma(S_n(i,j)) = S_n(i,j)^p$; $s_n = p^{-1}S_{p^n}$; $g_{\widehat{S}}(X) = X + \sum_{n\in\bar{\mathcal{P}}} S_n X^n$.

Then $f_V = f_{g_V}$ and $f_{\widehat{S}} = f_{g_{\widehat{S}}}$ are the logarithms of d-dimensional formal groups F_V and $F_{\widehat{S}}$ defined over $\mathbb{Z}[V]$ and $\mathbb{Z}[\widehat{S}]$, respectively.

Let $S = \widehat{S} \cup \{S_\omega\}_{\omega\in\Omega}$, where Ω is the set of multi-indices $\omega \in \mathbb{N}^d$ which have at least 2 non-zero components and S_ω are columns of independent variables with d entries. Denote $\xi(X) = X + \sum_{\omega\in\Omega} S_\omega X^\omega$, where $X^{(\omega_1,\ldots,\omega_d)} = x_1^{\omega_1} x_2^{\omega_2} \ldots x_d^{\omega_d}$.

Fix an embedding of $\mathbb{Q}[V]$ in $\mathbb{Q}[S]$ by identifying V_n and S_{p^n}, $n \ge 1$. Denote $f_S = f_{\widehat{S}} \circ \xi \in \mathbb{Q}[S][[X]]$ and $\varphi = f_S^{-1} \circ f_V \in \mathbb{Q}[S][[X]]$.

Theorem B1. *[5, Proposition 25.4.11 and Theorem 25.4.16]*

(1) *f_S is the logarithm of a d-dimensional formal group F_S over $\mathbb{Z}[S]$ which is strictly isomorphic to F_V over $\mathbb{Z}[S]$, i.e., $\varphi \in \mathbb{Z}[S][[X]]$.*

(2) *F_S is a universal formal group in the class of d-dimensional formal groups defined over $\mathbb{Z}_{(p)}$-algebras, i.e., for any $\mathbb{Z}_{(p)}$-algebra A and a d-dimensional formal group F over A, there exists a unique homomorphism $\mu\colon \mathbb{Z}[S] \to A$ such that $\mu_* F_S = F$.*

A formal group law F over a ring A is called *p-typical*, if there exists $\mu\colon \mathbb{Z}[V] \to A$ such that $\mu_* F_V = F$.

Proposition B1. *[5, Proposition 15.2.6] Let A be a ring of characteristic 0 and F be a formal group over A with logarithm f. Then F is p-typical iff $P(f) = f$, where $P(f)$ is a p-typical part of f.*

The following recurrence relation on the coefficients of f_V will be widely employed throughout the paper.

Proposition B2. *[5, 10.4.4 and 10.4.5] If $f_V = \sum_{n=1}^{\infty} a_n(V) X^{p^n}$, then $a_n(V) \in \mathbb{Q}[V_1, \ldots, V_n]$ and*

$$p\, a_n(V) = a_{n-1}(V) V_1^{(p^{n-1})} + \cdots + a_1(V) V_{n-1}^{(p)} + V_n, \qquad a_0(V) = I,$$
$$a_n(V) = \sum_{i_1 + \cdots + i_r = n} p^{-r} V_{i_1} V_{i_2}^{(p^{i_1})} \cdots V_{i_r}^{(p^{i_1 + \cdots + i_{r-1}})}.$$

Universal strict isomorphism of p-typical formal groups

Apply the functional equation lemma for the following data:
$K = \mathbb{Q}[V,T]$; $A = \mathbb{Z}[V,T]$; $\sigma(V_n(i,j)) = V_n(i,j)^p$; $\sigma(T_n(i,j)) = T_n(i,j)^p$; $s_n = p^{-1} V_n$; $g_{V,T}(X) = X + \sum_{n=1}^{\infty} T_n X^{p^n}$.
Then $f_{V,T} = f_{g_{V,T}}$ is the logarithm of a d-dimensional formal group $F_{V,T}$ over $\mathbb{Z}[V,T]$. Denote $\alpha_{V,T} = f_{V,T}^{-1} \circ f_V \in \mathbb{Q}[V,T][[X]]$.

Proposition B3. *[5, Theorem 10.3.5] $F_{V,T}$ and F_V are strictly isomorphic over $\mathbb{Z}[V,T]$, i.e., $\alpha_{V,T} \in \mathbb{Z}[V,T][[X]]$.*

Theorem B2. *[5, Theorem 19.2.6] The triple $(F_V, \alpha_{V,T}, F_{V,T})$ is universal in the class of triples (F, α, G) over $\mathbb{Z}_{(p)}$-algebras consisting of d-dimensional p-typical formal groups F, G and strict isomorphism $\alpha : F \to G$, i.e., for any $\mathbb{Z}_{(p)}$-algebra A, two d-dimensional p-typical formal groups F, G over A and a strict isomorphism $\alpha\colon F \to G$, there exists a unique homomorphism $\mu\colon \mathbb{Z}[V,T] \to A$ such that $\mu_* F_V = F$, $\mu_* F_{V,T} = G$ and $\mu_* \alpha_{V,T} = \alpha$.*

Universal isomorphism of p-typical formal groups with strict reduction

According to Theorem B1 (2), there exists a homomorphism $\lambda : \mathbb{Z}[S] \to \mathbb{Z}_{(p)}[V][[T_0]]$ such that $\lambda_* F_S = (I + T_0)^{-1} F_V((I + T_0)X, (I + T_0)Y)$. Denote $\widehat{V}_n = \lambda(V_n) \in \mathbb{Z}_{(p)}[V_1, \ldots, V_n][[T_0]]$.

Lemma 1. $P(f_S) = f_V$.

Proof. The definition of ξ implies that $P(f_S) = P(f_{\widehat{S}})$ and the one of $g_{\widehat{S}}$ that $P(f_{\widehat{S}}) = f_V$. □

Proposition 2. *For any* $n \geq 1$,

$$\widehat{V}_n = (I + T_0)^{-1} V_n (I + T_0)^{(p^n)} + (I + T_0)^{-1} \sum_{j=1}^{n-1} a_j(V) \left(V_{n-j}^{(p^j)} (I + T_0)^{(p^n)} - (I + T_0)^{(p^j)} \widehat{V}_{n-j}^{(p^j)} \right).$$

Proof. Denote $D = I + T_0$. The logarithm of $D^{-1} F_V(DX, DY)$ equals $D^{-1} f_V(DX) = \sum_{n=0}^{\infty} D^{-1} a_n(V)(DX)^{p^n}$. By Lemma 1 we obtain $\lambda_* f_V = \lambda_* P(f_S) = P(\lambda_* f_S)$. Since $P(\sum D^{-1} a_n(V)(DX)^{p^n}) = \sum D^{-1} a_n(V) D^{(p^n)} X^{p^n}$, we deduce that

$$\sum D^{-1} a_n(V) D^{(p^n)} X^{p^n} = \sum a_n(\widehat{V}) X^{p^n}.$$

Hence by Proposition B2

$$\begin{aligned} \widehat{V}_n + \sum_{j=1}^{n-1} D^{-1} a_j(V) D^{(p^j)} \widehat{V}_{n-j}^{(p^j)} &= \widehat{V}_n + \sum_{j=1}^{n-1} a_j(\widehat{V}) \widehat{V}_{n-j}^{(p^j)} = p\, a_n(\widehat{V}) \\ &= D^{-1} p\, a_n(V) D^{(p^n)} \\ &= D^{-1} V_n D^{(p^n)} + D^{-1} \sum_{j=1}^{n-1} a_j(V) V_{n-j}^{(p^j)} D^{(p^n)}, \end{aligned}$$

which implies

$$\widehat{V}_n = D^{-1} V_n D^{(p^n)} + D^{-1} \sum_{j=1}^{n-1} a_j(V) \left(V_{n-j}^{(p^j)} D^{(p^n)} - D^{(p^j)} \widehat{V}_{n-j}^{(p^j)} \right).$$

□

Corollary. $\widehat{V}_n \in \mathbb{Z}[V_1, \ldots, V_n][[T_0]]$.

Proposition 3. *Let* A *be a ring of characteristic* 0, G *be a formal group over* A *with logarithm* λ, *and* $\mu : \mathbb{Z}[S] \to A \otimes \mathbb{Z}_{(p)}$ *be the homomorphism provided by Theorem B1 (2) such that* $\mu_* F_S = G$.

(1) *If the components of* λ *have zero coefficients at all the monomials* x_i^m, *where* $1 \le i \le d$ *and* $m \in \bar{\mathcal{P}}$, *then* $\mu(S_n) = 0$ *for all* $n \in \bar{\mathcal{P}}$.

(2) *If* $\mu(S_m) \in A$ *for all* $m \ge 1$, *then* $\mu(S_\omega) \in A$ *for all* $\omega \in \Omega$.

Proof. (1) Denote by $\mathcal{X}$ the ideal of $\mathbb{Q}[V][[T_0]][[X]]$ generated by the elements $X^\omega, \omega \in \Omega$. Then $\xi(X) \equiv X \mod \mathcal{X}$ and $f_S \equiv f_{\widehat{S}} \mod \mathcal{X}$. Let $n \in \bar{\mathcal{P}}$ be the least number such that $\mu(S_n) \ne 0$. In the equivalence $\lambda \equiv \mu_* f_{\widehat{S}} \mod \mathcal{X}$, the coefficient of $(0, \dots, 0, x_j^n, 0 \dots, 0)$, where x_j^n appears at ith position, on the left-hand side is 0 and on the right-hand side is $\lambda(S_n(i,j))$, a contradiction.

(2) Let $B_n(X,Y) = X^n + Y^n - (X+Y)^n$, and let $\nu_p(n) = 1$ if $n \in \bar{\mathcal{P}}$ and $\nu(n) = p$ otherwise. Then $\nu_p(n)^{-1} B_n(X,Y)$ has integer coefficients. The definition of F_S implies that for any $n \ge 1$

$$F_S(X,Y) \equiv X + Y + \nu(n)^{-1} B_n(X,Y) + \mathcal{L}_n(X) + \mathcal{L}_n(Y) - \mathcal{L}_n(X+Y) \mod \{S_2, \dots, S_{n-1}\} \cup \{S_\omega\}_{\omega \in \Omega, |\omega| < n},$$

where $\mathcal{L}_n(X) = \sum_{\omega \in \Omega, |\omega| = n} S_\omega X^\omega$. Let n be the least number such that there exists $\omega \in \Omega$ with $|\omega| = n$ and $\mu(S_\omega) \notin \mathbb{Z}[V][[T_0]]$. Then the previous equivalence implies that the coefficients of $\mu_* \mathcal{L}_n(X) + \mu_* \mathcal{L}_n(Y) - \mu_* \mathcal{L}_n(X + Y)$ belong to $Z[V][[T_0]]$. If $\omega = (\omega_1, \dots, \omega_d)$ and $1 \le i, j \le d$ are such that $\omega_i, \omega_j \ne 0$, $i \ne j$, then the coefficient of $x_i^{\omega_i} y_j^{\omega_j}$ in the above expression is equal to $\mu(S_\omega)$, a contradiction. □

Corollary. *The image of* λ *is contained in* $\mathbb{Z}[V][[T_0]]$.

Taking tensor product of $\lambda \colon \mathbb{Z}[S] \to \mathbb{Z}[V][[T_0]]$ with the identity isomorphism on $\mathbb{Z}[T]$ we get a homomorphism $\mathbb{Z}[S,T] \to \mathbb{Z}[V,T][[T_0]]$ which we also denote by λ by abuse of notations. Denote $F_{V,T'} = \lambda_* F_{V,T}$.

Define an isomorphism $\varepsilon_{V,T_0} \colon F_V \to \lambda_* F_V$ over $\mathbb{Z}[V][[T_0]]$ as the composition

$$F_V \xrightarrow{(I+T_0)^{-1}X} (I+T_0)^{-1} F_V((I+T_0)X, (I+T_0)Y) = \lambda_* F_S \xrightarrow{\lambda_* \varphi^{-1}} \lambda_* F_V,$$

and an isomorphism $\gamma_{V,T'} \colon F_V \to F_{V,T'}$ over $\mathbb{Z}[V,T][[T_0]]$ as the composition

$$F_V \xrightarrow{\varepsilon_{V,T_0}} \lambda_* F_V \xrightarrow{\lambda_* \alpha_{V,T}} \lambda_* F_{V,T} = F_{V,T'}.$$

Theorem 1. *The triple* $(F_V, \gamma_{V,T'}, F_{V,T'})$ *is universal in the class of triples* (F, γ, G) *over complete Noetherian local rings with residue fields of characteristic* $p \ne 0$ *consisting of* p*-typical* d*-dimensional formal groups* F, G

and an isomorphism $\gamma : F \to G$ *with strict reduction, i.e., for any complete Noetherian local ring* R *with residue field* $R/\mathfrak{M}$ *of characteristic* $p \neq 0$, *two* d*-dimensional* p*-typical formal groups* F, G *over* R *and an isomorphism* $\gamma : F \to G$ *whose reduction modulo* $\mathfrak{M}$ *is strict, there is a unique homomorphism* $\mu : \mathbb{Z}[V, T'] \to R$ *such that* $\mu(T_0) \in \mathfrak{M}$ *and* $\mu_* F_V = F$, $\mu_* F_{V,T'} = G$, $\mu_* \gamma_{V,T'} = \gamma$.

Proof. Let $\gamma : F \to G$ be an isomorphism with strict reduction and $\gamma(X) \equiv D^{-1}X \mod \deg 2$ for some $D \equiv I \mod \mathfrak{M}$. Since R is complete, we can take $\tau : \mathbb{Z}[[T_0]] \to R$ such that $\tau(T_0) = D - I$. Then for the isomorphism $\tau_* \varepsilon_{V,T_0} : F_V \to (\tau\lambda)_* F_V$ over $R[V]$, we have $\tau_* \varepsilon_{V,T_0}(X) \equiv D^{-1}X \mod \deg 2$.

Let $\rho : \mathbb{Z}[[V]] \to R$ be such that $\rho_* F_V = F$. Then $(\rho\tau)_* \varepsilon_{V,T_0} : \rho_* F_V \to (\rho\tau\lambda)_* F_V$ is an isomorphism and $(\rho\tau)_* \varepsilon_{V,T_0}(X) \equiv D^{-1}X \mod \deg 2$. Hence there exists a strict isomorphism $\alpha : (\rho\tau\lambda)_* F_V \to G$ such that $\alpha \circ (\rho\tau)_* \varepsilon_{V,T_0} = \gamma$. By Theorem B2, there exists a homomorphism $\sigma : \mathbb{Z}[V, T] \to R$ such that $\sigma_* F_V = (\rho\tau\lambda)_* F_V$, $\sigma_* F_{V,T} = G$ and $\sigma_* \alpha_{V,T} = \alpha$. The first condition implies $\sigma\big|_{\mathbb{Z}[V]} = \rho\tau\lambda\big|_{\mathbb{Z}[V]}$.

Now let $\mu : \mathbb{Z}[V, T'] \to R$ be given by its restrictions $\mu\big|_{\mathbb{Z}[V]} = \rho$, $\mu\big|_{\mathbb{Z}[T]} = \sigma\big|_{\mathbb{Z}[T]}$ and $\mu\big|_{\mathbb{Z}[[T_0]]} = \tau$. Then $\mu_* F_V = \rho_* F_V = F$ and $\mu_* F_{V,T'} = (\mu\lambda)_* F_{V,T} = \sigma_* F_{V,T} = G$, since $\mu\lambda\big|_{\mathbb{Z}[T]} = \mu\big|_{\mathbb{Z}[T]} = \sigma\big|_{\mathbb{Z}[T]}$ and $\mu\lambda\big|_{\mathbb{Z}[V]} = \mu\big|_{\mathbb{Z}[V][[T_0]]} \lambda\big|_{\mathbb{Z}[V]} = \rho\tau\lambda\big|_{\mathbb{Z}[V]} = \sigma\big|_{\mathbb{Z}[V]}$. In a similar way, we get $\mu_* \gamma_{V,T'} = (\mu\lambda)_* \alpha_{V,T} \circ \mu_* \varepsilon_{V,T_0} = \sigma_* \alpha_{V,T} \circ (\mu\big|_{\mathbb{Z}[V][[T_0]]})_* \varepsilon_{V,T_0} = \gamma$.

In order to prove the uniqueness, suppose that there are $\mu, \mu' : \mathbb{Z}[V, T'] \to R$ such that $\mu_* F_V = \mu'_* F_V$, $\mu_* F_{V,T'} = \mu'_* F_{V,T'}$ and $\mu_* \gamma_{V,T'} = \mu'_* \gamma_{V,T'}$. Then the first condition implies $\mu\big|_{\mathbb{Z}[V]} = \mu'\big|_{\mathbb{Z}[V]}$ and the third condition implies $\mu\big|_{\mathbb{Z}[[T_0]]} = \mu'\big|_{\mathbb{Z}[[T_0]]}$, since $\gamma_{V,T'}(X) \equiv (I + T_0)^{-1}X \mod \deg 2$. It gives $\mu_* \varepsilon_{V,T_0} = \mu'_* \varepsilon_{V,T_0}$ and $(\mu\lambda)_* \alpha_{V,T} \circ \mu_* \varepsilon_{V,T_0} = \mu_* \gamma_{V,T'} = \mu'_* \gamma_{V,T'} = (\mu'\lambda)_* \alpha_{V,T} \circ \mu'_* \varepsilon_{V,T_0}$ which yields $(\mu\lambda)_* \alpha_{V,T} = (\mu'\lambda)_* \alpha_{V,T}$. Taking into account the equalities $(\mu\lambda)_* F_V = (\mu\big|_{\mathbb{Z}[V][[T_0]]})_* \lambda_* F_V = (\mu'\big|_{\mathbb{Z}[V][[T_0]]})_* \lambda_* F_V = (\mu'\lambda)_* F_V$ and $(\mu\lambda)_* F_{V,T} = \mu_* F_{V,T'} = \mu'_* F_{V,T'} = (\mu'\lambda)_* F_{V,T}$, the universality property of $\alpha_{V,T}$ implies that $\mu\lambda = \mu'\lambda$, hence $\mu\big|_{\mathbb{Z}[T]} = \mu'\big|_{\mathbb{Z}[T]}$. □

3. Some recurrence relations

Recurrence relation for the universal strict isomorphism

The definition of $F_{V,T}$ and Proposition B1 imply that $F_{V,T}$ is p-typical, i.e., there exists a homomorphism $\kappa : \mathbb{Z}[V] \to \mathbb{Z}[V, T]$ such that $\kappa_* F_V = F_{V,T}$. Denote $\bar{V}_n = \kappa(V_n) \in \mathbb{Z}[V_1, \ldots, V_n; T_1, \ldots, T_n]$ for $n \geq 1$.

Let $\mathfrak{T}$ be the ideal of $\mathbb{Z}[V,T]$ generated by $T_n(i,j)$ for $1 \leq i,j \leq d$, $n \geq 1$. Let $N_n(V,T)$ denote the linear part of $V_n - \bar{V}_n$, i.e., $N_n(V,T) \equiv V_n - \bar{V}_n \mod \mathfrak{T}^2$ and $N_n(V,T) \in \sum_{k=1}^{n} \sum_{i,j=1}^{d} \mathbb{Z}[V] T_k(i,j)$.

In order to study $N_n(V,T)$, we introduce

$$Y_n(V,T) = T_1 V_{n-1}^{(p)} + \cdots + T_{n-1} V_1^{(p^{n-1})}$$

for $n \geq 2$ and $Y_1(V,T) = 0$. We will get a recurrence relation which expresses $N_n(V,T)$ modulo p via $Y_n(V,T)$ and $N_k(V,T)$ with $k < n$.

Proposition B4. *[5, Theorem 19.3.7] For any $n \geq 1$,*

$$\begin{aligned} \bar{V}_n = V_n + p\,T_n &+ \sum_{\substack{i+j=n \\ i,j\geq 1}} \left(V_i T_j^{(p^i)} - T_j \bar{V}_i^{(p^j)} \right) \\ &+ \sum_{k=1}^{n-1} a_{n-k}(V) \left(V_k^{(p^{n-k})} - \bar{V}_k^{(p^{n-k})} \right) \\ &+ \sum_{k=2}^{n-1} a_{n-k}(V) \left(\sum_{\substack{i+j=k \\ i,j\geq 1}} \left(V_i^{(p^{n-k})} T_j^{(p^{n-j})} - T_j^{(p^{n-k})} V_i^{(p^{n-i})} \right) \right). \end{aligned}$$

Lemma 2. *Let $\mathcal{J}$ be an ideal in a ring A. If $U_1 \equiv U_2 + U_3 \mod \mathcal{J}^2$ for some matrices $U_1, U_2 \in \mathrm{M}_d(A)$ and $U_3 \equiv 0 \mod \mathcal{J}$ then*

$$U_1^{(p^k)} \equiv U_2^{(p^k)} + p^k U_2^{(p^k-1)} * U_3 \mod \mathcal{J}^2.$$

Proof. For $1 \leq i,j \leq d$

$$\begin{aligned} U_1(i,j)^{p^k} &\equiv (U_2(i,j) + U_3(i,j))^{p^k} \\ &\equiv U_2(i,j)^{p^k} + p^k U_2(i,j)^{p^k-1} U_3(i,j) \mod \mathcal{J}^2. \end{aligned}$$

□

Denote $V_1^{\langle n \rangle} = V_1 V_1^{(p)} \cdots V_1^{(p^{n-1})} \in \mathbb{Z}[V]$.

Proposition 4. *For any $n \geq 1$,*

$$N_n(V,T) \equiv Y_n(V,T) - \sum_{k=1}^{n-1} V_1^{\langle n-k \rangle} \left(V_k^{(p^{n-k}-1)} * N_k(V,T) \right) \mod p.$$

Proof. We proceed by induction on n. The case $n = 1$ is trivial as $\bar{V}_1 = V_1 + pT_1$. Assume that the equivalence is satisfied for any $1 \le k \le n-1$ and consider the linear part of the recurrence formula of Proposition B4. The contribution of the third sum modulo $\mathfrak{T}^2$ is equal to 0. The contribution of the first sum is

$$-T_1\bar{V}_{n-1}^{(p)} - \cdots - T_{n-1}\bar{V}_1^{(p^{n-1})} \equiv -Y_n(V,T) \mod \mathfrak{T}^2,$$

since by the induction assumption $\bar{V}_l \equiv V_l \mod \mathfrak{T}$, $1 \le l \le n-1$.

Now consider the contribution of the second sum. By the induction assumption and Lemma 2 for $1 \le k \le n-1$, we have

$$V_k^{(p^{n-k})} - \bar{V}_k^{(p^{n-k})} \equiv p^{n-k}V_k^{(p^{n-k}-1)} * N_k(V,T) \mod \mathfrak{T}^2.$$

Proposition B2 implies that $p^k a_k(V) \equiv V_1^{\langle k\rangle} \mod p$ which gives the desired equivalence. □

Recurrence relation for the universal isomorphism with strict reduction

Remind that $(\lambda \circ \kappa)_* F_V = F_{V,T'}$. Denote for $n \ge 1$

$$\widetilde{V}_n = \lambda(\bar{V}_n) = (\lambda \circ \kappa)(V_n) \in \mathbb{Z}[V_1, \ldots, V_n; T_1, \ldots, T_n][[T_0]].$$

Let $\mathfrak{T}'$ be the ideal of $\mathbb{Z}[V,T][[T_0]]$ generated by $T_n(i,j)$ for $1 \le i,j \le d$, $n \ge 0$. Denote by $N'_n(V,T')$ the linear part of $V_n - \widetilde{V}_n$, i.e., $N'_n(V,T') \equiv V_n - \widetilde{V}_n \mod \mathfrak{T}'$ and $N'_n(V,T') \in \sum_{k=0}^n \sum_{i,j=1}^d \mathbb{Z}[V]T_k(i,j)$.

As a first step in studying $N'_n(V,T)$, we relate $N'_n(V,T)$ and $N_n(V,T)$ through a certain linear form $H_n(V,T_0)$.

Let $\mathfrak{T}_0$ be the ideal of $\mathbb{Z}[V][[T_0]]$ generated by $T_0(i,j)$ for $1 \le i,j \le d$. Denote by $H_n(V,T_0)$ the linear part of $\widehat{V}_n - V_n + T_0V_n$, i.e., $H_n(V,T_0) \equiv \widehat{V}_n - V_n + T_0V_n \mod \mathfrak{T}_0^2$ and $H_n(V,T_0) \in \sum_{i,j=1}^d \mathbb{Z}[V]T_0(i,j)$.

Proposition 5. *For any $n \ge 1$,*

$$\begin{aligned} H_n(V,T_0) \equiv &-\sum_{k=1}^{n-1} V_1^{\langle k\rangle}\left(V_{n-k}^{(p^k-1)} * H_{n-k}(V,T_0)\right) \\ &+\sum_{k=1}^{n-1} V_1^{\langle k\rangle}\left(V_{n-k}^{(p^k-1)} * (T_0V_{n-k}) - (I * T_0)V_{n-k}^{(p^k)}\right) \mod p. \end{aligned}$$

Proof. Using Proposition 2, Lemma 2 and the fact that $p^k a_k(V) \in \mathbb{Z}[V]$ we obtain

$$\begin{aligned}
\widehat{V}_n - (I - T_0)V_n &\equiv (I - T_0)\sum_{k=1}^{n-1} a_k(V)\big(V_{n-k}^{(p^k)}(I + T_0)^{(p^n)} - (I + T_0)^{(p^k)}\widehat{V}_{n-k}^{(p^k)}\big) \\
&\equiv (I - T_0)\sum_{k=1}^{n-1} a_k(V)\Big(V_{n-k}^{(p^k)} - \big(I + p^k(I * T_0)\big)\big(V_{n-k}^{(p^k)} \\
&\quad + p^k V_{n-k}^{(p^k-1)} * (\widehat{V}_{n-k} - V_{n-k})\big)\Big) \\
&\equiv (I - T_0)\sum_{k=1}^{n-1} p^k a_k(V)\Big(V_{n-k}^{(p^k-1)} * (V_{n-k} - \widehat{V}_{n-k}) \\
&\quad - (I * T_0)V_{n-k}^{(p^k)}\Big) \mod p\,\mathfrak{T}_0 + \mathfrak{T}_0^2
\end{aligned}$$

Proposition B2 implies that $p^k a_k(V) \equiv V_1^{\langle k\rangle} \mod p$. Then we have

$$\begin{aligned}
\widehat{V}_n - V_n + T_0 V_n &\equiv (I - T_0)\sum_{k=1}^{n-1} V_1^{\langle k\rangle}\left(V_{n-k}^{(p^k-1)} * (V_{n-k} - \widehat{V}_{n-k} - T_0 V_{n-k})\right) \\
&\quad + \sum_{k=1}^{n-1} V_1^{\langle k\rangle}\Big(V_{n-k}^{(p^k-1)} * (T_0 V_{n-k}) \\
&\quad - (I * T_0)V_{n-k}^{(p^k)}\Big) \mod p\,\mathfrak{T}_0 + \mathfrak{T}_0^2
\end{aligned}$$

Finally, if we assume that the required statement holds for any $n < n'$, the last formula shows that it holds also for n'. □

Proposition 6. *For any $n \geq 1$,*

$$N'_n(V, T') = T_0 V_n + N_n(V, T) - H_n(V, T_0).$$

Proof. Proposition 5 implies that $\widehat{V}_n \equiv V_n \mod \mathfrak{T}'$. Then we have

$$\begin{aligned}
\widetilde{V}_n = \lambda(\bar{V}_n) &\equiv \lambda(V_n) - \lambda(N_n(V, T)) \equiv \widehat{V}_n - N_n(V, T) \\
&\equiv V_n - T_0 V_n + H_n(V, T_0) - N_n(V, T) \mod \mathfrak{T}'^2.
\end{aligned}$$

□

For further investigation of $N'_n(V,T)$, we introduce

$$Y'_n(V,T') = T_0V_n + Y_n(V,T) + \sum_{k=1}^{n-1} V_1^{\langle n-k\rangle}(I * T_0)V_k^{(p^{n-k})}.$$

We will prove a recurrence relation which expresses $N'_n(V,T)$ modulo p through $Y'_n(V,T)$ and $N'_k(V,T)$ with $k < n$.

Proposition 7. *For any $n \geq 1$,*

$$N'_n(V,T') \equiv Y'(V,T') - \sum_{k=1}^{n-1} V_1^{\langle n-k\rangle}\left(V_k^{(p^{n-k}-1)} * N'_k(V,T')\right) \mod p.$$

Proof. Using Propositions 4, 5 and 6 we obtain

$$\begin{aligned}
N'_n(V,T') &= T_0V_n + Y_n(V,T) - Y_n(V,T) + N_n(V,T) - H_n(V,T_0)\\
&\equiv Y'_n(V,T') - \sum_{k=1}^{n-1} V_1^{\langle n-k\rangle}(I * T_0)V_k^{(p^{n-k})}\\
&\quad - \sum_{k=1}^{n-1} V_1^{\langle n-k\rangle}\left(V_k^{(p^{n-k}-1)} * N_k(V,T)\right)\\
&\quad + \sum_{k=1}^{n-1} V_1^{\langle n-k\rangle}\left(V_k^{(p^{n-k}-1)} * H_k(V,T_0)\right)\\
&\quad - \sum_{k=1}^{n-1} V_1^{\langle n-k\rangle}\left(V_k^{(p^{n-k}-1)} * (T_0V_k) - (I * T_0)V_k^{(p^{n-k})}\right)\\
&= Y'(V,T') - \sum_{k=1}^{n-1} V_1^{\langle n-k\rangle}\left(V_k^{(p^{n-k}-1)} * N'_k(V,T')\right) \mod p.
\end{aligned}$$

□

4. Basis of the deformation space

Relation between the image of Y_Ξ and the height of $F_{V(\Xi)}$

For a module M over a ring A, denote by M^∞ the A-module consisting of all infinite sequences of elements of M indexed by all positive integers. Then M^∞_m is the submodule of M^∞ consisting of the sequences starting with m zeros.

Let $a = (a_1, a_2, \ldots)$ be a sequence of $d \times d$-matrices with entries in a ring R. Denote by $F_{V(a)}$ the formal group $\mu_* F_V$ over R, where the homomorphism $\mu : \mathbb{Z}[V] \to R$ is given by $\mu(V_n(i,j)) = a_n(i,j)$, $n \geq 1$, $1 \leq i, j \leq d$. A similar notation will be used also for $F_{V,T}$ and $\alpha_{V,T}$.

Let k, $\mathcal{O}$, E be as in Section 1. Let Φ be a d-dimensional formal group over k. According to Theorem B1, Φ is isomorphic to a p-typical formal group over k. Thus without loss of generality we can suppose that Φ is p-typical, i.e., there exists $\Xi = (\Xi_1, \Xi_2, \ldots) \in \mathrm{M}_d(k)^\infty$ such that $\Phi = F_{V(\Xi)}$. Let $\widehat{\Xi} = (\widehat{\Xi}_1, \widehat{\Xi}_2, \ldots) \in \mathrm{M}_d(\mathcal{O})^\infty$ be the sequence of matrices which are composed of the Teichmüller representatives in $\mathcal{O}$ of the entries of the matrices Ξ_n. Then $\widehat{F} = F_{V(\widehat{\Xi})}$ is a deformation of Φ over $\mathcal{O}$, and $\widehat{f} = f_{V(\widehat{\Xi})}$ is its logarithm. Denote $u = pI - \sum_{n=1}^\infty \widehat{\Xi}_n \blacktriangle^n \in \mathrm{M}_d(E)$.

Lemma 3. $u\widehat{f} = pX$.

Proof. Since $\widehat{\Xi}_i^\Delta = \widehat{\Xi}_i^{(p)}$, we get $\blacktriangle^n \widehat{f} = \widetilde{f}^{(n)}_{V(\widehat{\Xi})}$, where $\widetilde{f}^{(n)}_V = \sigma^n_* f_V$ and $\sigma \colon \mathbb{Q}[V] \to \mathbb{Q}[V]$ is defined by $\sigma(V_i) = V_i^{(p)}$ for $i \geq 1$. Then according to the definition of f_V, we obtain $u\widehat{f} = pf_{V(\widehat{\Xi})} - \sum_{n=1}^\infty \widehat{\Xi}_n \widetilde{f}^{(n)}_{V(\widehat{\Xi})} = pX$. □

Remind that $Y_1(V,T) = 0$ and $Y_n(V,T) = T_1 V_{n-1}^{(p)} + \cdots + T_{n-1} V_1^{(p^{n-1})}$ for $n \geq 2$. Put $Y_n^+(V,T') = T_0 V_n + Y_n(V,T)$ for $n \geq 1$. Let Y_Ξ be a k-linear operator on $\mathrm{M}_d(k)^\infty$ defined by $Y_\Xi(T) = (Y_1(\Xi,T), Y_2(\Xi,T), \ldots)$. A k-linear operator Y_Ξ^+ on $\mathrm{M}_d(k)^\infty$ is introduced in a similar way.

Let $\mathcal{E} = E \otimes_{\mathcal{O}} k$ be a non-commutative ring with multiplication given by $\blacktriangle\alpha = \alpha^p \blacktriangle$ for any $\alpha \in k$. Define $\iota : \blacktriangle \mathrm{M}_d(\mathcal{E}) \to \mathrm{M}_d(k)^\infty$ as follows $\iota(\sum_{n=1}^\infty \Theta_n \blacktriangle^n) = (\Theta_1, \Theta_2, \ldots)$. Evidently, ι is a k-isomorphism, $\iota^{-1} \circ Y_\Xi \circ \iota$ is the right multiplication by $U = \sum_{i=1}^\infty \Xi_i \blacktriangle^i \in \blacktriangle \mathrm{M}_d(\mathcal{E})$, and $\iota^{-1} \circ Y_\Xi^+ \circ \iota$ is the right multiplication by $\blacktriangle^{-1} U$.

Proposition 8.

(1) *The following claims are equivalent:*
  (i) Φ *is of finite height;*
  (ii) $\mathrm{M}_d(k)^\infty_m \subset \operatorname{Im} Y_\Xi$ *for some positive integer* m*;*
  (iii) $\mathrm{M}_d(k)^\infty_{m'} \subset \operatorname{Im} Y_\Xi^+$ *for some positive integer* m'*;*
  (iv) Y_Ξ *is a monomorphism;*
  (v) Y_Ξ^+ *is a monomorphism;*

(2) *If* Φ *is of height* h*, then* $\dim \operatorname{Coker} Y_\Xi = dh$ *and* $\dim \operatorname{Coker} Y_\Xi^+ = d(h-d)$.

Proof. (1) We can restate the claims as follows:

(ii) there exist $W \in \blacktriangle \mathrm{M}_d(\mathcal{E})$, $m \geq 1$ such that $WU = I\blacktriangle^m$;

(iii) there exist $W' \in \blacktriangle \mathrm{M}_d(\mathcal{E})$, $m' \geq 1$ such that $W'\blacktriangle^{-1}U = I\blacktriangle^{m'}$;

(iv) if $CU = 0$ for some $C \in \blacktriangle \mathrm{M}_d(\mathcal{E})$, then $C = 0$;

(v) if $C'\blacktriangle^{-1}U = 0$ for some $C' \in \blacktriangle \mathrm{M}_d(\mathcal{E})$, then $C' = 0$;

Obviously, (ii) is equivalent to (iii), and (iv) is equivalent to (v). By [1, Proposition 10], (ii) and (iv) are equivalent.

Assume that (i) is satisfied. Then for any $1 \leq i \leq d$, the system $\{\blacktriangle^n \widehat{f_i}\}_{n\geq 1} \subset \mathcal{D}(\Phi)$ is not linear independent over $\mathcal{O}$, i.e., there exists $z_i \in E$ such that $z_i\widehat{f_i} \equiv 0 \mod p$. Since $\mathcal{D}(\Phi)$ is a free $\mathcal{O}$-module, we can suppose that one of the coefficients of z_i is invertible in $\mathcal{O}$. Weierstrass preparation lemma implies that there exists a monic polynomial $v_i \in E$ of degree m_i such that $v_i \equiv \blacktriangle^{m_i} \mod p$ for some integer m_i, and $v_i\widehat{f_i} \equiv 0 \mod p$. Put $m = \max m_i$. Define $v \in \mathrm{M}_d(E)$ as follows: $v(i,j) = \delta_i^j \blacktriangle^{m-m_i} v_i$. Then $v \equiv I\blacktriangle^m \mod p$ and $v\widehat{f} \equiv 0 \mod p$. By Lemma 3 and Proposition A1, there exists $w \in \mathrm{M}_d(E)$ such that $v = wu$, which implies (ii).

Assume that (ii) is satisfied. Then $\{\blacktriangle^n \widehat{f_i}\}_{0\leq n\leq m, 1\leq i\leq d}$ generates $\mathcal{D}(\Phi)$ as an $\mathcal{O}$-module. If $f = v\widehat{f}$, $v \in \mathrm{M}_{1,d}(E)$, is such that $pf \equiv 0 \mod p$, then by Proposition A1, there exists $c \in \mathrm{M}_{1,d}(E)$ such that $pv = cu$. According to (iv), $c = pb$ for some $b \in \mathrm{M}_{1,d}(E)$, and hence, $f = bu\widehat{f} \equiv 0 \mod p$. It implies that $\mathrm{M}_{1,d}(E)\widehat{f}/p\mathcal{O}[[X]]_0 = \mathcal{D}(\Phi)$ is p-torsion free, and thus we obtain (i).

(2) Taking into account the above observation, we have to prove the following: $\dim_k \blacktriangle \mathrm{M}_d(\mathcal{E})/\blacktriangle \mathrm{M}_d(\mathcal{E})U = dh$; $\dim_k \blacktriangle \mathrm{M}_d(\mathcal{E})/\blacktriangle \mathrm{M}_d(\mathcal{E})\blacktriangle^{-1}U = d(h-d)$. Since the reduction of u is equal to $-U$, we have

$$\blacktriangle \mathrm{M}_d(\mathcal{E})/\blacktriangle \mathrm{M}_d(\mathcal{E})U \cong \mathrm{M}_d(\mathcal{E})/\mathrm{M}_d(\mathcal{E})U \cong (\mathrm{M}_d(E)/\mathrm{M}_d(E)u) \otimes_{\mathcal{O}} k.$$

The factor module $\mathrm{M}_d(E)/\mathrm{M}_d(E)u$ is isomorphic as an $\mathcal{O}$-module to the direct sum of d copies of $M_{1,d}(E)/M_{1,d}(E)u \cong \mathcal{D}(\Phi)$, and hence, it is a free $\mathcal{O}$-module of rank dh. That implies the first claim. Finally, $\blacktriangle \mathrm{M}_d(\mathcal{E})/\blacktriangle \mathrm{M}_d(\mathcal{E})\, \blacktriangle^{-1}U = \blacktriangle \mathrm{M}_d(\mathcal{E})/\mathrm{M}_d(\mathcal{E})U$. Using the above argument, one obtains $\dim_k \mathrm{M}_d\, (\mathcal{E})/\mathrm{M}_d(\mathcal{E})U = dh$, and moreover, $\dim_k \mathrm{M}_d(\mathcal{E})/\blacktriangle \mathrm{M}_d(\mathcal{E}) = d^2$. That implies the second claim. □

Basis of the cokernel of Y_Ξ

From now on, Φ is supposed to be of height h. For $n \geq 1$, $1 \leq i,j \leq d$, denote by $B_{(n,i,j)} \in \mathrm{M}_d(k)^\infty$ the sequence of matrices with the only nonzero entry which equals $1 \in k$ and appears in the nth matrix at the (i,j)th position. By Proposition 8, $\mathrm{M}_d(k)^\infty_m \subset \operatorname{Im} Y_\Xi$ for some integer $m > 0$, i.e., the set $\Lambda = \{(n,i,j) \mid 1 \le n, 1 \le i,j \le d, B_{(n,i,j)} \notin \operatorname{Im} Y_\Xi\}$ is finite. One can pick a set $\Psi \subset \Lambda$ so that $\{B_\psi + \operatorname{Im} Y_\Xi \mid \psi \in \Psi\}$ is a basis of $\operatorname{Coker} Y_\Xi$. In this case, we say that Ψ specifies a basis of $\operatorname{Coker} Y_\Xi$.

There is an alternative description of Ψ. The coordinates of Y_Ξ are linear k-functions on $\mathrm{M}_d(k)^\infty$. Choose those of them which form a basis of their span. Then Ψ is the set of the coordinates not included in the basis.

We will show that the set Ψ can always be chosen in a rather simple form. For a d-tuple of positive integers $(k_1, \ldots, k_d)$ define

$$\Gamma_{k_1,\ldots,k_d} = \{(n,i,j) 1 \le i,j \le d, 1 \le n \le k_j\}.$$

Clearly $\Gamma_{k_1,\ldots,k_d}$ contains $(k_1 + \cdots + k_d)d$ elements. We say that a d-tuple $(k_1, \ldots, k_d)$ specifies a basis of $\operatorname{Coker} Y_\Xi$ if $\Gamma_{k_1,\ldots,k_d}$ does so.

Proposition 9. *There exists a d-tuple specifying a basis of* $\operatorname{Coker} Y_\Xi$.

Proof. It suffices to prove two facts:

I. The d-tuple $(1, \ldots, 1)$ specifies a linear independent system in $\operatorname{Coker} Y_\Xi$.

II. If $(k_1, \ldots, k_d)$ specifies a linear independent system and for any $1 \le s \le d$ the system specified by $(k_1, \ldots, k_s + 1, \ldots, k_d)$ is linear dependent in $\operatorname{Coker} Y_\Xi$, then $(k_1, \ldots, k_d)$ specifies a basis of $\operatorname{Coker} Y_\Xi$.

Since $Y_1(\Xi, T) = 0$, we have $\operatorname{Im} Y_\Xi \subset \mathrm{M}_d(k)_1^\infty$ which implies I.

Denote by J the set $\iota^{-1}(\operatorname{Im} Y_\Xi) = \{CU \mid C \in \blacktriangle\mathrm{M}_d(\mathcal{E})\}$ which is a left $\mathrm{M}_d(\mathcal{E})$-submodule of $\blacktriangle\mathrm{M}_d(\mathcal{E})$. Denote by $E_{i,j}$ the $d \times d$-matrix with the only non-zero entry which equals $1 \in k$ and appears at the (i,j)th position. In order to prove II, one has to show that for any $1 \le s,t \le d$ and $m \ge 1$ the element $E_{t,s}\blacktriangle^m + J$ of $\blacktriangle\mathrm{M}_d(\mathcal{E})/J$ belongs to the span of $\{E_{i,j}\blacktriangle^n + J \mid (n,i,j) \in \Gamma_{k_1,\ldots,k_d}\}$. We use induction by $m - k_s$. If $m \le k_s$, the claim is trivial. Consider any $m \ge k_s + 1$. There are $a_{(n,i,j)} \in k$, $(n,i,j) \in \Gamma_{k_1,\ldots,k_d}$ and $b_1, \ldots, b_d \in k$ not all equal 0 such that $\sum_r b_r E_{r,s}\blacktriangle^{k_s+1} \equiv \sum_{n,i,j} a_{(n,i,j)} E_{i,j}\blacktriangle^n \bmod J$. Let $b'_1, \ldots, b'_d \in k$ satisfy $\sum_{r=1}^d b_r b'_r = 1$. Multiplying by $\sum_r b'_r E_{t,r} \;\; \blacktriangle^{m-k_s-1}$ on the left one gets $E_{t,s}\blacktriangle^m \equiv \sum_{n,i,j} b'_i a_{(n,i,j)}^{p^{m-k_s-1}} E_{t,j}\blacktriangle^{n+m-k_s-1} \bmod J$. Since $(n+m-k_s-1) - k_j < m - k_s$, the induction assumption yields the desired result. □

Let $F_{V^{(1)}}$, $F_{V^{(2)}}$ and $F_{V^{(3)}}$ denote the formal group F_V in the case where $d = d_1$, d_2 and $d_1 + d_2$, respectively. For $i = 1, 2$, let $\Xi^{(i)} = (\Xi_1^{(i)}, \Xi_2^{(i)}, \ldots) \in \mathrm{M}_{d_i}(k)^\infty$, $\Phi^{(i)} = F_{V^{(i)}(\Xi^{(i)})}$, and $Y_{\Xi^{(i)}}^{(i)}$ be the corresponding operator on

$\mathrm{M}_{d_i}(k)^\infty$. It is clear that $\Phi^{(1)}\oplus\Phi^{(2)}=F_{V^{(3)}(\Xi^{(1)}\oplus\Xi^{(2)})}$ where

$$\Xi^{(1)}\oplus\Xi^{(2)}=\left(\begin{pmatrix}\Xi_1^{(1)} & 0\\ 0 & \Xi_1^{(2)}\end{pmatrix},\begin{pmatrix}\Xi_2^{(1)} & 0\\ 0 & \Xi_2^{(2)}\end{pmatrix},\dots\right).$$

Denote the corresponding operator on $\mathrm{M}_{d_1+d_2}(k)^\infty$ by $Y^{(3)}_{\Xi^{(1)}\oplus\Xi^{(2)}}$.

Proposition 10. *The d_i-tuple $(k_1^{(i)},\dots,k_{d_i}^{(i)})$ specifies a basis of* $\operatorname{Coker} Y^{(i)}_{\Xi^{(i)}}$ *for $i=1,2$ iff the (d_1+d_2)-tuple $(k_1^{(1)},\dots,k_{d_1}^{(1)},k_1^{(2)},\dots,k_{d_2}^{(2)})$ specifies a basis of* $\operatorname{Coker} Y^{(3)}_{\Xi^{(1)}\oplus\Xi^{(2)}}$.

Proof. Fix a positive integer e. Let ${}_eT_n$, $n\ge 0$ be an $e\times d$-matrix of independent variables and ${}_eT=({}_eT_1,{}_eT_2,\dots)$, ${}_eT'=({}_eT_0,{}_eT_1,\dots)$.

Put ${}_eY_1(V,{}_eT)=0$ and ${}_eY_n(V,{}_eT)={}_eT_1V_{n-1}^{(p)}+\dots+{}_eT_{n-1}V_1^{(p^{n-1})}$ for $n\ge 2$. Introduce a k-linear operator ${}_eY_\Xi$ on $\mathrm{M}_{e,d}(k)^\infty$ by ${}_eY_\Xi({}_eT)=({}_eY_1(\Xi,{}_eT),{}_eY_2(\Xi,{}_eT),\dots)$. Obviously, ${}_dY_\Xi$ coincides with Y_Ξ.

For a d-tuple of positive integers $(k_1,\dots,k_d)$, define

$${}_e\Gamma_{k_1,\dots,k_d}=\{(n,i,j)\mid 1\le i\le e, 1\le j\le d, 1\le n\le k_j\}.$$

For $n\ge 1$, $1\le i\le e$, $1\le j\le d$, denote by $B^e_{(n,i,j)}\in\mathrm{M}_{e,d}(k)^\infty$ the sequence of matrices with the only non-zero entry which equals $1\in k$ and appears in the nth matrix at the (i,j)th position.

Define $\iota_e:\blacktriangle\mathrm{M}_{e,d}(\mathcal{E})\to\mathrm{M}_{e,d}(k)^\infty$ by $\iota_e(\sum_{n=1}^\infty\Theta_n\blacktriangle^n)=(\Theta_1,\Theta_2,\dots)$. Denote by J_e the set $\iota_e^{-1}(\operatorname{Im}{}_eY_\Xi)=\{CU\mid C\in\blacktriangle\mathrm{M}_{e,d}(\mathcal{E})\}$ which is a left $\mathrm{M}_e(\mathcal{E})$-submodule of $\blacktriangle\mathrm{M}_{e,d}(\mathcal{E})$. Denote by $E^{n,m}_{i,j}$ the $(n\times m)$-matrix with the only non-zero entry which equals $1\in k$ and appears at the (i,j)th position.

Let ${}_{e_1}Y_\Xi$ and ${}_{e_2}Y_\Xi$ be operators on $\mathrm{M}_{e_1,d}(k)^\infty$ and $\mathrm{M}_{e_2,d}(k)^\infty$, respectively. If positive integers $k_1,\dots,k_d$ are such that $\{B^{e_1}\psi+\operatorname{Im}{}_{e_1}Y_\Xi\mid\psi\in{}_{e_1}\Gamma_{k_1,\dots,k_d}\}$ is a basis of $\operatorname{Coker}{}_{e_1}Y_\Xi$, prove that $\{B^{e_2}_\psi+\operatorname{Im}{}_{e_2}Y_\Xi\mid\psi\in{}_{e_2}\Gamma_{k_1,\dots,k_d}\}$ is a basis of $\operatorname{Coker}{}_{e_2}Y_\Xi$.

In order to show it, assume that $\sum_{n,i,j}a_{(n,i,j)}E^{e_2,d}_{i,j}\blacktriangle^n\in J_{e_2}$ for some $a_{(n,i,j)}\in k$, $(n,i,j)\in{}_{e_2}\Gamma_{k_1,\dots,k_d}$. For any $1\le r\le e_2$, multiply by $E^{e_1,e_2}_{1,r}$ on the left and get $\sum_{n,j}a_{(n,r,j)}E^{e_1,d}_{1,j}\blacktriangle^n\in J_{e_1}$, whence $a_{(n,r,j)}=0$ for any $1\le j\le d$, $1\le n\le k_j$.

Furthermore, for any $1 \leq s \leq d$ there are $a_{(n,i,j)} \in k$, $(n,i,j) \in {}_{e_2}\Gamma_{k_1,\ldots,k_d}$ such that $E^{e_1,d}_{1,s}\blacktriangle^m \equiv \sum_{n,i,j} a_{(n,i,j)} E^{e_1,d}_{i,j}\blacktriangle^n \mod J_{e_1}$. For any $1 \leq t \leq e_2$ multiplying by $E^{e_2,e_1}_{t,1}$ on the left, one gets $E^{e_2,d}_{t,s}\blacktriangle^m \equiv \sum_{n,j} a_{(n,1,j)} E^{e_2,d}_{t,j}\blacktriangle^n \mod J_{e_2}$ and we are done.

Thus one can restate the main claim: the d_1- and d_2-tuples $(k^{(1)}_1, \ldots, k^{(1)}_{d_1})$ and $(k^{(2)}_1, \ldots, k^{(2)}_{d_2})$ specify bases of $\mathrm{Coker}\, {}_{d_1+d_2}Y^{(1)}_{\Xi^{(1)}}$ and $\mathrm{Coker}\, {}_{d_1+d_2}Y^{(2)}_{\Xi^{(2)}}$, respectively, iff the (d_1+d_2)-tuple $(k^{(1)}_1, \ldots, k^{(1)}_{d_1}, k^{(2)}_1, \ldots, k^{(2)}_{d_2})$ specifies a basis of $\mathrm{Coker}\, Y^{(3)}_{\Xi^{(1)}\oplus\Xi^{(2)}}$. We are now in a position to prove it. Use the notation $T = (T_1, T_2, \ldots)$ for $(d_1 + d_2) \times (d_1 + d_2)$- matrices of independent variables. For $n \geq 1$, let $T_n = (T^{(1)}_n, T^{(2)}_n)$ where $T^{(i)}_n$ are $(d_1 + d_2) \times d_i$-matrices, $i = 1, 2$. Denote $T^{(i)} = (T^{(i)}_1, T^{(i)}_2, \ldots)$. Then

$$Y^{(3)}_{\Xi^{(1)}\oplus\Xi^{(2)}}(T) = \big({}_{d_1+d_2}Y^{(1)}_{\Xi^{(1)}}(T^{(1)}), {}_{d_1+d_2}Y^{(2)}_{\Xi^{(2)}}(T^{(2)})\big).$$

Since

$$\Gamma_{k^{(1)}_1,\ldots,k^{(1)}_{d_1},k^{(2)}_1,\ldots,k^{(2)}_{d_2}} = {}_{d_1+d_2}\Gamma_{k^{(1)}_1,\ldots,k^{(1)}_{d_1}} \cup \Big\{(n,i,j) \mid (n,i,j-d_1) \in {}_{d_1+d_2}\Gamma_{k^{(2)}_1,\ldots,k^{(2)}_{d_2}}\Big\},$$

the proposition follows. □

Formal groups with unique Ψ

Proposition 11. *The following conditions are equivalent*

(i) $|\Lambda| = \dim \mathrm{Coker}\, Y_\Xi$;

(ii) Ψ *specifying a basis of* $\mathrm{Coker}\, Y_\Xi$ *is unique;*

(iii) *A d-tuple specifying a basis of* $\mathrm{Coker}\, Y_\Xi$ *is unique.*

Proof. If $|\Lambda| = \dim \mathrm{Coker}\, Y_\Xi$, then Ψ is unique and equal to Λ. Clearly, (ii) implies (iii) and it remains to prove (iii) $\Rightarrow$ (i). Suppose that $|\Lambda| > \dim \mathrm{Coker}\, Y_\Xi$ and show that there are more than one d-tuple specifying a basis of $\mathrm{Coker}\, Y_\Xi$.

We say that that a subset C of Λ is a chain if there exists $(a_\psi)_{\psi\in C}$, $a_\psi \in k \setminus \{0\}$, such that $\sum_{\psi\in C} a_\psi B_\psi \in \mathrm{Im}\, Y_\Xi$. If C is a chain, then $(1,i,j) \notin C$. Since $\{B_\psi + \mathrm{Im}\, Y_\Xi \mid \psi \in \Lambda\}$ is linear dependent, there exists at least one chain. Define a partial order on the set of all chains as follows: we say that $C < C'$ if

(1) for any $(n,i,j)\in C$ there is $(n',i',j)\in C'$ with $n'\ge n$;

(2) there exists $(n',i',j')\in C'$ such that $n'>n$ for any $(n,i,j')\in C$.

Let C_0 be a minimal chain and $A_j=\{n|(n,i,j)\in C_0 \text{ for some } 1\le i\le d\}$. We will show that there are at least two different indices with non-empty A_j. Indeed, otherwise $\sum_{(n,i)} a_{(n,i)}B_{(n,i,j_0)}\in \operatorname{Im} Y_\Xi$, $a_{(n,i)}\ne 0$. Using the notation of the proof of Proposition 9, one can write $\sum_{(n,i)} a_{(n,i)}E_{i,j_0}\blacktriangle^n\in J$. Let n^* be the minimal index appearing in the pairs (n,i). There is $N\ge n^*$ such that $E_{i_0,j_0}\blacktriangle^N\notin J$ and $E_{i_0,j_0}\blacktriangle^{N+1}\in J$ for some $1\le i_0\le d$. If $\sum_i b_i a_{(n^*,i)}^{p^{N-n^*}}=1$ for some $b_1,\dots,b_d\in k$, multiplication by $\sum_i b_iE_{i_0,i}\blacktriangle^{N-n^*}$ yields the contradiction.

Define a d-tuple $(k_1,\dots,k_d)$ by

$$k_j=\begin{cases}1, & \text{if } A_j=\varnothing,\\ \max A_j, & \text{if } A_j\ne\varnothing\end{cases}$$

and let $j_1\ne j_2$ be such that $k_{j_1}>1$ and $k_{j_2}>1$. Then $\Gamma_{k_1,\dots,k_{j_1}-1,\dots,k_d}$ and $\Gamma_{k_1,\dots,k_{j_2}-1,\dots,k_d}$ contain no chain and thus specify linear independent systems in $\operatorname{Coker} Y_\Xi$. According to the proof of Proposition 9, each of them can be extended to a basis given by a d-tuple. If such a basis is unique, it should contain both of them and hence their union $\Gamma_{k_1,\dots,k_d}$, which is impossible since $\Gamma_{k_1,\dots,k_d}$ contains the chain C_0. Thus there is more than one basis given by a d-tuple, as required. □

Proposition 12. *In the notation of Proposition 10, d_1- and d_2-tuples specifying bases of* $\operatorname{Coker} Y^{(1)}_{\Xi^{(1)}}$ *and* $\operatorname{Coker} Y^{(2)}_{\Xi^{(2)}}$ *are unique iff a (d_1+d_2)-tuple specifying a basis of* $\operatorname{Coker} Y^{(3)}_{\Xi^{(1)}\oplus\Xi^{(2)}}$ *is also unique.*

Proof. Follows from Proposition 10. □

Let $\Phi^{(1)}=F_{V(\Xi^{(1)})}$ and $\Phi^{(2)}=F_{V(\Xi^{(2)})}$ be p-typical formal groups. Denote by $\widehat{\Xi}^{(i)}\in \mathrm{M}_d(\mathcal{O})^\infty$, the sequences of matrices composed of the Teichmüller representatives of the entries of the corresponding matrices in the sequence $\Xi^{(i)}$, $i=1,2$. Then $\widehat{F}^{(1)}=F_{V(\widehat{\Xi}^{(1)})}$, $\widehat{F}^{(2)}=F_{V(\widehat{\Xi}^{(2)})}$ are deformations of $\Phi^{(1)}$, $\Phi^{(2)}$ over $\mathcal{O}$ with logarithms of types $u^{(1)}=pI-\sum_{n=1}^\infty \widehat{\Xi}^{(1)}_n\blacktriangle^n$, $u^{(2)}=pI-\sum_{n=1}^\infty \widehat{\Xi}^{(2)}_n\blacktriangle^n$, respectively. If $\Phi^{(1)}$ and $\Phi^{(2)}$ are isomorphic then by Proposition A2 there exist invertible $w,z\in \mathrm{M}_d(E)$ such that $u^{(2)}w=zu^{(1)}$. Suppose, in addition, that there exists a unique $\Psi^{(2)}$ specifying a basis of $\operatorname{Coker} Y_{\Xi^{(2)}}$. Then $\Psi^{(2)}$ and w allow one to determine all possible choices of $\Psi^{(1)}$ specifying a basis of $\operatorname{Coker} Y_{\Xi^{(1)}}$. Indeed, $U^{(2)}W=ZU^{(1)}$, where $U^{(1)}=\sum_{n=1}^\infty \Xi^{(1)}_n\blacktriangle^n\in$

$\blacktriangle \mathrm{M}_d(\mathcal{E})$, $U^{(2)} = \sum_{n=1}^{\infty} \Xi_n^{(2)} \blacktriangle^n \in \blacktriangle \mathrm{M}_d(\mathcal{E})$ and $Z, W \in \mathrm{M}_d(\mathcal{E})$ are the reductions of z,w to k. Since $\iota^{-1} \circ Y_{\Xi^{(i)}} \circ \iota$ is the right multiplication by $U^{(i)}$ for $i = 1, 2$, one has $\mathrm{Im}\, Y_{\Xi^{(i)}} = \iota(\blacktriangle \mathrm{M}_d(\mathcal{E}) U^{(i)})$ and $\mathrm{Im}\, Y_{\Xi^{(1)}} = \iota((\iota^{-1} \mathrm{Im}\, Y_{\Xi^{(2)}}) W)$ since Z is invertible. Finally, since $\Psi^{(2)}$ is unique, $\mathrm{Im}\, Y_{\Xi^{(1)}} = \iota((\iota^{-1} \langle \{B_{(n,i,j)}\}_{(n,i,j) \notin \Psi^{(2)}} \rangle) W)$. As soon as $\mathrm{Im}\, Y_{\Xi^{(1)}}$ is given, all possible choices of $\Psi^{(1)}$ can be calculated.

Examples

(1) Let the first non-zero Ξ_n be invertible. This is always the case when $d = 1$. If $\Xi_n = 0$ for $1 \le n \le m-1$ and Ξ_m is invertible, then the height of $F_{V(\Xi)}$ is equal to dm, $\mathrm{Im}\, Y_\Xi = \mathrm{M}_d(k)_m^\infty$, $\Lambda = \Gamma_{m,\ldots,m}$, $|\Lambda| = d^2 m = \dim \mathrm{Coker}\, Y_\Xi$, and $\Psi = \Lambda$ is unique.

(2) Let $\Xi_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \Xi_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \Xi_3 = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$ and $\Xi_n = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ for $n \ge 4$.

The height of $F_{V(\Xi)}$ is equal to 5. For $T_n = \begin{pmatrix} x_n & y_n \\ z_n & t_n \end{pmatrix}$, $n \ge 1$, we get

$$\begin{aligned}
Y_1(\Xi, T) &= \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \\
Y_2(\Xi, T) &= \begin{pmatrix} x_1 & 0 \\ z_1 & 0 \end{pmatrix}, \\
Y_3(\Xi, T) &= \begin{pmatrix} x_2 + y_1 & x_1 \\ z_2 + t_1 & z_1 \end{pmatrix}, \\
Y_4(\Xi, T) &= \begin{pmatrix} x_3 + y_2 & x_1 + x_2 + y_1 \\ z_3 + t_2 & z_1 + z_2 + t_1 \end{pmatrix}, \\
Y_5(\Xi, T) &= \begin{pmatrix} x_4 + y_3 & x_2 + x_3 + y_2 \\ z_4 + t_3 & z_2 + z_3 + t_2 \end{pmatrix}.
\end{aligned}$$

Then $\Lambda = \Gamma_{3,4}$, $|\Lambda| = 14 > 10 = \dim \mathrm{Coker}\, Y_\Xi$. Clearly, Ψ can be chosen among $\Gamma_{1,4}$, $\Gamma_{2,3}$, $\Gamma_{3,2}$, and these are all the possibilities in the form of Proposition 9. In fact, there are many other possible choices of Ψ.

(3) Fix a positive integer r. Let $\Xi_n = 0 \in \mathrm{M}_d(k)$ for any $n \ne 1, r+1$ and

$$\Xi_1 = \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 \\ 1 & 0 & & 0 & 0 \\ 0 & 1 & & 0 & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & & 1 & 0 \end{pmatrix}, \quad \Xi_{r+1} = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & & 0 & 0 \\ 0 & 0 & & 0 & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & & 0 & 0 \end{pmatrix}.$$

The height of $F_{V(\Xi)}$ is equal to $d+r$. A direct calculation shows that $Y_1(\Xi,T)=0$, $Y_n(\Xi,T)=\{y_n(i,j)\}_{1\le i,j\le d}$ where $y_n(i,j)=T_{n-1}(i,j+1)$ for $2\le n$, $1\le j\le d-1$, $y_n(i,d)=0$ for $2\le n\le r+1$, and $y_n(i,d)=T_{n-r-1}\,(i,1)$ for $r+2\le n$. Hence $B_{(n,i,j)}\in \operatorname{Im} Y_\Xi$ iff $n>1$ and either $j<d$ or $n>r+1$. Thus $\Lambda=\Gamma_{1,\dots,1,r+1}$, $|\Lambda|=d^2+dr=\dim \operatorname{Coker} Y_\Xi$, and $\Psi=\Lambda$ is unique.

Notice that the formal group from Example 3 is isomorphic to the formal group $G_{d,0,r}$ introduced in [3]. Dieudonné proved that in the case where k is algebraically closed, any formal group of finite height is isogenous to a direct sum of simple formal groups of finite height, and any simple formal group of finite height is isogenous either to $\mathbb{F}_m$ (simple formal group of slope 1) or to $G_{d,0,r}$ for some coprime d,r (simple formal group of slope $d/(d+r)$). For instance, if Ξ_1 is invertible, the formal group is isogenous to $\mathbb{F}_m^d$. A direct computation of the localized Dieudonné module over the Laurent power series ring shows that the formal group from Example 2 is isogenous to $\mathbb{F}_m\oplus G_{1,0,3}$.

Proposition 13. *If k is algebraically closed, and $\tilde\Phi$ is a formal group over k of finite height with slopes $(d_1/h_1),\dots,(d_s/h_s)$ with $(d_i,h_i)=1$ for any $1\le i\le s$, there exists a p-typical formal group $\Phi=F_{V(\Xi)}$ isogenous to $\tilde\Phi$ such that a tuple specifying a basis of* $\operatorname{Coker} Y_\Xi$ *is unique and equal to*

$$(1,\dots,1,h_1-d_1+1,1,\dots,1,h_2-d_2+1,\dots,1,\dots,1,h_s-d_s+1)$$

with the element h_i-d_i+1 appearing at $\left(\sum_{j=1}^i d_j\right)$-th position, $1\le i\le s$.

Proof. Follows from the arguments above, Propositions 10 and 12. □

As it was explained above, if $\Phi^{(1)}$ is isomorphic to $\Phi^{(2)}$ and $\Phi^{(2)}$ possesses a unique $\Psi^{(2)}$ specifying a basis of $\operatorname{Coker} Y_{\Xi^{(2)}}$, one can determine all possible choices of $\Psi^{(1)}$ provided the set $\Psi^{(2)}$ and the isomorphism are given. This can be illustrated with the following example.

Let $\Phi^{(1)}=F_{V(\Xi^{(1)})}$ with $\Xi_1^{(1)}=\begin{pmatrix}1&-1\\1&-1\end{pmatrix}$, $\Xi_2^{(1)}=\begin{pmatrix}0&1\\0&0\end{pmatrix}$ and $\Xi_n^{(1)}=\begin{pmatrix}0&0\\0&0\end{pmatrix}$ for $n\ge 3$. Take $\Phi^{(2)}$ to be the formal group from Example 3 for $d=2$, $r=1$.

Since $u^{(2)}\begin{pmatrix}1 & -1\\ 0 & 1\end{pmatrix}=\begin{pmatrix}1 & -1\\ 0 & 1\end{pmatrix}u^{(1)}$, the formal groups $\Phi^{(1)}$ and $\Phi^{(2)}$ are isomorphic. The unique possible choice of $\Psi^{(2)}$ is $\Gamma_{1,2}$. Then

$$\begin{aligned}\operatorname{Im} Y_{\Xi^{(1)}} &= \iota\left(\left(\iota^{-1}\langle B_{(2,1,1)}, B_{(2,2,1)}, \{B_{(n,i,j)}\}_{n\geq 3, 1\leq i,j\leq 2}\rangle\right)\begin{pmatrix}1 & -1\\ 0 & 1\end{pmatrix}\right)\\ &= \langle B_{(2,1,1)} - B_{(2,1,2)}, B_{(2,2,1)} - B_{(2,2,2)}, \{B_{(n,i,j)}\}_{n\geq 3, 1\leq i,j\leq 2}\rangle.\end{aligned}$$

Thus $\Lambda^{(1)}=\Gamma_{2,2}$, and there are four options for $\Psi^{(1)}$, among them two ($\Gamma_{1,2}$ and $\Gamma_{2,1}$) are of the form of Proposition 9.

Infinite dimensional linear operators

Lemma 4. *Let A be a ring and $L: A^\infty \to A^\infty$ be an A-module homomorphism such that $L(A^\infty_m)\subset A^\infty_m$ for any $m>m^*$. Then for every $m>m^*$, there exists a unique homomorphisms $L_m: A^m\to A^m$ such that $L_m \mathrm{pr}_m = \mathrm{pr}_m L$, where $\mathrm{pr}_m: A^\infty = A^m\oplus A^\infty_m \to A^m$ is the projection to the first summand. Moreover, if L_m is an isomorphism for any $m>m^*$, then L is an isomorphism.*

Proof. Since $L(A^\infty_m)\subset A^\infty_m$, the homomorphisms L_m are well defined. If $\alpha\in A^\infty$ and $L(\alpha)=0$ then $L_m(\mathrm{pr}_m(\alpha))=0$, whence $\mathrm{pr}_m(\alpha)=0$ for any $m>m^*$ and $\alpha=0$. If $\beta\in A^\infty$ then for any $m>m^*$ there is $\alpha^{(m)}\in A^\infty$ such that $\mathrm{pr}_m(L(\alpha^{(m)}))=L_m(\mathrm{pr}_m(\alpha^{(m)}))=\mathrm{pr}_m(\beta)$. Obviously, it implies the existence of $\alpha\in A^\infty$ such that $L(\alpha)=\beta$. □

Let R be a complete Noetherian local ring with maximal ideal $\mathfrak{M}$ and residue field k.

Lemma 5.

(1) *Let $l: k^\infty\to k^\infty$ be a linear operator such that $(l-\mathrm{id}_{k^\infty})(k^\infty_m)\subset k^\infty_{m+1}$ for any $m>m^*$. Then l is an isomorphism.*

(2) *Let $L: R^\infty\to R^\infty$ be an R-module homomorphism such that $L(R^\infty_m)\subset R^\infty_m$ for any $m>m^*$, and $L\otimes_R \mathrm{id}_k: k^\infty\to k^\infty$ is an isomorphism. Then L is an isomorphism.*

Proof. (1) By Lemma 4, it is sufficient to check that $l_m: k^m\to k^m$ is an isomorphism for any $m>m^*$. The matrix of l_m in the corresponding basis is triangular with units on its main diagonal, so we are done.

(2) Since $L(R_m^\infty) \subset R_m^\infty$, the homomorphisms $L_m : R^m \to R^m$ are well defined for any $m > m^*$. Then $L_m \otimes_R \mathrm{id}_k : k^m \to k^m$ is a surjection and, therefore, an isomorphism. Since R is complete, it implies that L_m is an isomorphism, and applying Lemma 4 we obtain the required statement. □

Relation between Ψ and N_Ξ

Fix a certain Ψ (not necessarily in the form of Proposition 9) to the rest of the paper. It is clear that the set

$$\begin{aligned}\Lambda^+ &= \{(n,i,j) \mid n \geq 1, 1 \leq i \leq e, 1 \leq j \leq d, B_{(n,i,j)} \notin \operatorname{Im} Y_\Xi^+\} \\ &= \{(n,i,j) \mid (n+1,i,j) \in \Lambda\}\end{aligned}$$

is finite, and the set $\Psi^+ = \{(n,i,j) \mid (n+1,i,j) \in \Psi\}$ is a subset of Λ^+ such that $\{B_\psi + \operatorname{Im} Y_\Xi^+ \mid \psi \in \Psi^+\}$ is a basis of $\operatorname{Coker} Y_\Xi^+$. The coordinates of Y_Ξ^+ which do not belong to Ψ^+ form a basis of the span of all the coordinates of Y_Ξ^+. Finally, if $\Psi = \Gamma_{k_1,\dots,k_d}$ then $\Psi^+ = \Gamma_{k_1-1,\dots,k_d-1}$.

Let $N_n(V,T)$, $N'_n(V,T')$ and $Y'_n(V,T')$ be as in Section 3. Then k-linear operators N_Ξ, N'_Ξ and Y'_Ξ on $\mathrm{M}_d(k)^\infty$ can be introduced similarly to Y_Ξ.

Denote $\Pi_\Psi = \mathrm{M}_d(k)^\infty/\langle B_\psi|\psi \in \Psi\rangle$, $\Pi_\Psi^+ = \mathrm{M}_d(k)^\infty/\langle B_\psi|\psi \in \Psi^+\rangle$, and let π, π^+ be the corresponding factorization maps.

Proposition 14. *$\pi N_\Xi : \mathrm{M}_d(k)^\infty \to \Pi_\Psi$ and $\pi^+ N'_\Xi : \mathrm{M}_d(k)^\infty \to \Pi_\Psi^+$ are isomorphisms.*

Proof. The restriction of π to $\operatorname{Im} Y_\Xi$ is a bijection. According to Proposition 8, Y_Ξ is a monomorphism, and hence, $\pi Y_\Xi : \mathrm{M}_d(k)^\infty \to \Pi_\Psi$ is an isomorphism. Denote $C = Y_\Xi \circ (\pi Y_\Xi)^{-1} : \Pi_\Psi \to \mathrm{M}_d(k)^\infty$. Obviously, $\pi C = \mathrm{id}_{\Pi_\Psi}$. Proposition 4 implies that $N_\Xi = LY_\Xi$ for a linear operator $L = \mathrm{id} + U$ on $\mathrm{M}_d(k)^\infty$ such that $U(\mathrm{M}_d(k)_n^\infty) \subset \mathrm{M}_d(k)_{n+1}^\infty$ for any integer n. Then we have $\pi N_\Xi = \pi LC\pi Y_\Xi = (\mathrm{id}_{\Pi_\Psi} + \pi UC)\pi Y_\Xi$. Since $\pi|_{\mathrm{M}_d(k)_m^\infty} = \mathrm{id}$, the operator $\mathrm{id}_{\Pi_\Psi} + \pi UC$ satisfies the condition of Lemma 5, 1), and hence, is an isomorphism which gives the first claim.

The restriction of π^+ to $\operatorname{Im} Y_\Xi^+$ is a bijection. By Proposition 8, Y_Ξ^+ is monomorphism, and hence, $\pi^+ Y_\Xi^+ : \mathrm{M}_d(k)^\infty \to \Pi_\Psi^+$ is an isomorphism. Notice that $Y'_\Xi = Y_\Xi^+ W$, where W is the linear operator on $M_d(k)^\infty$ defined by the formula $W_n(T) = T_n + \Xi_1^{\langle n\rangle}(I * T_0)$, $n \geq 1$. Since W is an isomorphism, $\pi^+ Y'_\Xi : \mathrm{M}_d(k)^\infty \to \Pi_\Psi^+$ is also an isomorphism. To complete the proof, we proceed exactly as in the first part using Proposition 7 instead of Proposition 4. □

5. Construction of universal deformations

We keep the notation of the previous sections. Denote by $\mathfrak{T}_n$ the ideal of $\mathbb{Z}[V,T]$ generated by $T_k(i,j)$ for $1 \le i,j \le d$, $1 \le k \le n$.

Lemma 6.

(1) $\alpha_{V,T}(X) \equiv X - T_n X^{p^n} \mod (\mathfrak{T}_{n-1}, \deg p^n + 1)$. *In particular,* $\alpha_{V,T}(X) \equiv X \mod \mathfrak{T}$.

(2) $\varphi(X) \equiv X \mod \{S_n\}_{n\in\bar{\mathcal{P}}} \cup \{S_\omega\}_{\omega\in\Omega}$.

(3) $\varepsilon_{V,T_0}(X) \equiv X \mod \mathfrak{T}_0$.

(4) $\gamma_{V,T'}(X) \equiv X \mod \mathfrak{T}'$.

Proof. (1) We have $g_{V,T}(X) \equiv g_V(X) + T_n X^{p^n} \mod (\mathfrak{T}_{n-1}, \deg p^n + 1)$ which gives $f_{V,T}(X) \equiv f_V(X) + T_n X^{p^n} \mod (\mathfrak{T}_{n-1}, \deg p^n + 1)$ and $\alpha_{V,T}(X) = f_{V,T}^{-1} \circ f_V \equiv X - T_n X^{p^n} \mod (\mathfrak{T}_{n-1}, \deg p^n + 1)$.

(2) Since $f_{\widehat{S}} \equiv f_V \mod \{S_n\}_{n\in\bar{\mathcal{P}}}$ and $\xi(X) \equiv X \mod \{S_\omega\}_{\omega\in\Omega}$, one gets $f_S = f_{\widehat{S}} \circ \xi \equiv f_V \mod \{S_n\}_{n\in\bar{\mathcal{P}}} \cup \{S_\omega\}_{\omega\in\Omega}$.

(3) It suffices to check that $(\mathrm{red}_{T_0})_* \lambda_* \varphi(X) = X$, where red_{T_0} is the reduction modulo T_0. Since $\mathrm{red}_{T_0}\lambda : \mathbb{Z}[S] \to \mathbb{Z}[V]$ is given as $S_{p^k} \mapsto V_k$; $S_n \mapsto 0$, $n \in \bar{\mathcal{P}}$; $S_\omega \mapsto 0$, $\omega \in \Omega$, the required identity follows from 2).

(4) Follows from (1) and (3).

□

Let R be a ring with unit. Similarly to $B_{(n,i,j)}$, where $n \ge 1$, $1 \le i,j \le d$, denote by $\hat{B}_{(n,i,j)} \in \mathrm{M}_d(R)^\infty$ the sequence of matrices with the only non-zero entry equal to $1 \in R$ and appearing in the nth matrix at the (i,j)th position.

Theorem 2. *Let $\Phi = F_{V(\Xi)}$ and $\Theta \in \mathrm{M}_d(\mathcal{O})^\infty$ be such that the reduction of Θ is equal to Ξ. Then for any complete Noetherian local $\mathcal{O}$-algebra R with maximal ideal $\mathfrak{M}$ containing p and residue field k, and for any deformation F of Φ over R*

(1) *there exists a unique dh-tuple $(\tau_\psi)_{\psi\in\Psi}$, $\tau_\psi \in \mathfrak{M}$, such that F is strictly $\star$-isomorphic to the formal group $F_{V(Z)}$, where $Z = \Theta + \sum_{\psi\in\Psi} \tau_\psi \hat{B}_\psi \in \mathrm{M}_d(R)^\infty$.*

(2) *there exists a unique $d(h-d)$-tuple $(\tau_\psi)_{\psi\in\Psi^+}$, $\tau_\psi \in \mathfrak{M}$, such that F is $\star$-isomorphic to the formal group $F_{V(Z)}$, where $Z = \Theta + \sum_{\psi\in\Psi^+} \tau_\psi \hat{B}_\psi \in \mathrm{M}_d(R)^\infty$.*

Proof. (1) *Uniqueness.* Let $\rho : F_{V(Z)} \to F_{V(Z^*)}$ be a strict $\star$-isomorphism, where $Z^* = \Theta + \sum_{\psi\in\Psi} \tau^*_\psi \hat{B}_\psi \in \mathrm{M}_d(R)^\infty$ and $\tau^*_\psi \in \mathfrak{M}$. Then Theorem B2 implies that there exists $Q \in \mathrm{M}_d(R)^\infty$ such that $Z^* = \bar{V}(Z, Q)$ and $\rho = \alpha_{V(Z),T(Q)}$. Since $\alpha_{V(Z),T(Q)}$ is a $\star$-isomorphism, Lemma 6 (1) implies that $Q \in \mathrm{M}_d(\mathfrak{M})^\infty$. Now assume that $Q \in \mathrm{M}_d(\mathfrak{M}^n)^\infty$. Since $\bar{V}_i \equiv V_i - N_i(V, T)$ mod $\mathfrak{T}^2$, we have $Z^* \equiv Z - N(Z, Q) \mod \mathfrak{M}^{n+1}$. Therefore $\pi\, N(Z, Q) \equiv 0$ mod $\mathfrak{M}^{n+1}$. On the other hand, $\pi\, N(Z, T) \otimes_R \mathrm{id}_k = \pi\, N_\Xi$ is an isomorphism by Proposition 14. Then Lemma 5 (2) implies that $Q \in \mathrm{M}_d(\mathfrak{M}^{n+1})^\infty$. Thus $Q = 0$ and $\rho(X) = X$.

Existence. Let F be a deformation of Φ over R and $\delta : \mathbb{Z}[S] \to R$ a unique ring homomorphism such that $\delta_* F_S = F$. Since Φ is p-typical, the composition $\mathbb{Z}[S] \xrightarrow{\delta} R \to k$ factors through the projection $\mathbb{Z}[S] \to \mathbb{Z}[V]$ ($S_{p^k} \mapsto V_k$; $S_n \mapsto 0$, $n \in \bar{\mathcal{P}}$; $S_\omega \mapsto 0$). Then $\delta(S_n), \delta(S_\omega) \in \mathfrak{M}$ for $n \in \bar{\mathcal{P}}$, $\omega \in \Omega$, and the strict isomorphism $\delta_*\varphi : \delta_* F_V \to F$ is a strict $\star$-isomorphism by Lemma 6 (2). Thus one can assume $F = F_{V(Z^*)}$ for some $Z^* \in \mathrm{M}_d(R)^\infty$ such that $Z^* \equiv \Theta$ mod $\mathfrak{M}$.

By induction on n, we construct $Z(n) \in \mathrm{M}_d(R)^\infty$ and $\zeta_n \in R[[X]]^d_0$ such that

(i) $\zeta_n : F_{V(Z(n))} \to F_{V(Z(n+1))}$ is a strict isomorphism;

(ii) $\zeta_n(X) \equiv X \mod \mathfrak{M}^n$;

(iii) $Z(1) = Z^*$, $Z(n) \equiv Z(n+1) \mod \mathfrak{M}^n$;

(iv) $\pi Z(n) \equiv \pi\Theta \mod \mathfrak{M}^n$.

Assume that $Z(n)$ and ζ_{n-1} are already constructed. According to Proposition 14, $\pi\, N(Z(n), T) \otimes_R \mathrm{id}_k = \pi\, N_\Xi$ is an isomorphism. Then there exists $Q \in \mathrm{M}_d(R)^\infty$ such that $\pi\, N(Z(n), Q) = \pi\, Z(n) - \pi\,\Theta$. Therefore $Q \equiv 0$ mod $\mathfrak{M}^n$ by Lemma 5 (2).

Let $\zeta_n = \alpha_{V(Z(n)),T(Q)}$ and $Z(n+1) = \bar{V}(Z(n), Q)$. Then

$$\zeta_n : F_{V(Z(n))} \to F_{V(Z(n)),T(Q)} = F_{V(Z(n+1))}$$

is a strict isomorphism. Lemma 6 (1) implies that $\zeta_n(X) \equiv X \mod \mathfrak{M}^n$.

Since $\bar{V}_i \equiv V_i - N_i(V, T) \mod \mathfrak{T}^2$, $i \geq 1$, one obtains

$$Z(n+1) \equiv Z(n) - N(Z(n), Q) \mod \mathfrak{M}^{n+1}.$$

It follows that $Z(n+1) \equiv Z(n) \mod \mathfrak{M}^n$ and

$$\pi\, Z(n+1) \equiv \pi\, Z(n) - \pi\, N(Z(n), Q) = \pi\,\Theta \mod \mathfrak{M}^{n+1}.$$

Now take $Z = \lim_{n\to\infty} Z(n) \in \mathrm{M}_d(R)^\infty$ and $\zeta = \cdots \circ \zeta_2 \circ \zeta_1$. Then $Z \equiv \Theta \mod \mathfrak{M}$, $\pi Z = \pi\Theta$ and ζ is a strict $\star$-isomorphism from F to $F_{V(Z)}$. This yields $(\tau_\psi)_{\psi\in\Psi}$, as required.

(2) *Uniqueness.* Let $\rho : F_{V(Z)} \to F_{V(Z^*)}$ be a $\star$-isomorphism, where $Z^* = \Theta + \sum_{\psi\in\Psi^+} \tau^*_\psi \hat{B}_\psi \in \mathrm{M}_d(R)^\infty$ and $\tau^*_\psi \in \mathfrak{M}$.

By Theorem 1, there exists a sequence $Q' = (Q_0, Q_1, \ldots) \in \mathrm{M}_d(R)^\infty$ such that $Q_0 \in \mathrm{M}_d(\mathfrak{M})$, $Z^* = \widetilde{V}(Z, Q')$ and $\rho = \gamma_{V(Z),T'(Q')}$. Since $\gamma_{V(Z),T'(Q')}$ is a $\star$-isomorphism and $\varepsilon_{V(Z),T_0(Q_0)}$ is also a $\star$-isomorphism by Lemma 6 (3), we deduce that $\widetilde{\alpha}_{V(Z),T'(Q')}$ is a $\star$-isomorphism, where $\widetilde{\alpha}_{V,T'} = \lambda_* \alpha_{V,T}$. By Lemma 6 (1), $\lambda_*\alpha_{V,T}(X) \equiv X - T_i X^{p^i} \mod (\mathfrak{T}_{i-1}, \deg p^i + 1)$, which gives $Q_i \in \mathrm{M}_d(\mathfrak{M})$ for $i \geq 1$.

Assume that $Q' \in \mathrm{M}_d(\mathfrak{M}^n)^\infty$. Since $\widetilde{V}_i \equiv V_i - N'_i(V, T') \mod \mathfrak{T}'^2$, we have $Z^* \equiv Z - N'(Z, Q') \mod \mathfrak{M}^{n+1}$. Therefore, $\pi^+ N'(Z, Q') \equiv 0 \mod \mathfrak{M}^{n+1}$. By Proposition 14, $\pi^+ N'(Z, T') \otimes_k 1 = \pi^+ N'_\Xi$ is an isomorphism. Then Lemma 5 (2) implies that $Q' \in \mathrm{M}_d(\mathfrak{M}^{n+1})^\infty$. Therefore $Q' = 0$ and $\rho(X) = X$.

Existence. One can assume $F = F_{V(Z^*)}$ for some $Z^* \in \mathrm{M}_d(R)^\infty$ such that $Z^* \equiv \Theta \mod \mathfrak{M}$. By induction on n, we construct $Z(n) \in \mathrm{M}_d(R)^\infty$ and $\zeta_n \in R[[X]]^d_0$ such that

(i) $\zeta_n : F_{V(Z(n))} \to F_{V(Z(n+1))}$ is an isomorphism;

(ii) $\zeta_n(X) \equiv X \mod \mathfrak{M}^n$;

(iii) $Z(1) = Z^*$, $Z(n) \equiv Z(n+1) \mod \mathfrak{M}^n$;

(iv) $\pi^+ Z(n) \equiv \pi^+\Theta \mod \mathfrak{M}^n$.

Assume that $Z(n)$ and ζ_{n-1} are already constructed. According to Proposition 14, $\pi^+ N'(Z(n), T') \otimes_R \mathrm{id}_k = \pi^+ N'_\Xi$ is an isomorphism. Therefore, there is a sequence $Q' = (Q_0, Q_1, \ldots) \in \mathrm{M}_d(R)^\infty$ such that $\pi^+ N'(Z(n), Q') = \pi^+ Z(n) - \pi^+ \Theta$. Then by Lemma 5 (2), we obtain $Q' \equiv 0 \mod \mathfrak{M}^n$.

Let $\zeta_n = \gamma_{V(Z(n)),T'(Q')}$ and $Z(n+1) = \widetilde{V}(Z(n), Q')$. Then

$$\zeta_n : F_{V(Z(n))} \to F_{V(Z(n)),T'(Q')} = F_{V(Z(n+1))}$$

is an isomorphism, and $\zeta_n(X) = \varepsilon_{V(Z(n)),T_0(Q_0)} \circ \widetilde{\alpha}_{V(Z(n)),T'(Q')}$, where $\widetilde{\alpha}_{V,T} = \lambda_*\alpha_{V,T}$. Lemma 6 (4) implies that $\zeta_n(X) \equiv X \mod \mathfrak{M}^n$.

Since $\widetilde{V}_i \equiv V_i - N_i(V, T') \mod \mathfrak{T}'^2$, $i \geq 1$, we obtain

$$Z(n+1) \equiv Z(n) - N'(Z(n), Q') \mod \mathfrak{M}^{n+1}.$$

It follows that $Z_i(n+1) \equiv Z_i(n) \mod \mathfrak{M}^n$ and

$$\pi^+ Z(n+1) \equiv \pi^+ Z(n) - \pi^+ N'(Z(n), Q') = \pi^+ \Theta \mod \mathfrak{M}^{n+1}.$$

Now take $Z = \lim_{n\to\infty} Z(n) \in \mathrm{M}_d(R)^\infty$ and $\zeta = \cdots \circ \zeta_2 \circ \zeta_1$. Then we have $Z \equiv \Theta \mod \mathfrak{M}$, $\pi^+ Z = \pi^+\Theta$ and ζ is a $\star$-isomorphism from F to $F_{V(Z)}$. This gives $(\tau_\psi)_{\psi\in\Psi^+}$, as required. □

If $d = 1$ then Ψ and Ψ^+ are uniquely defined, namely $\Psi = \{1, \dots, h\}$, $\Psi^+ = \{1, \dots, h-1\}$, where $h = \min\{i \mid \Xi_i \neq 0\}$, and Theorem 2 gives Hazewinkel's result [5, Proposition 22.4.4].

Corollary. *If Θ is as in Theorem 2 and a homomorphism $\gamma\colon \mathbb{Z}[V] \to \mathcal{O}[[t_\psi]]_{\psi\in\Psi^+}$ is defined by $\gamma(V) = \Theta + \sum_{\psi\in\Psi^+} \tau_\psi \hat{B}_\psi$, then $\Gamma = \gamma_* F_V$ is a universal deformation of Φ, i.e., for any complete Noetherian local $\mathcal{O}$-algebra R with residue field k and for any deformation F of Φ over R there exists a unique $\mathcal{O}$-homomorphism $\mu\colon \mathcal{O}[[t_\psi]]_{\psi\in\Psi^+} \to R$ such that $\mu_*\Gamma$ is $\star$-isomorphic to F.*

Acknowledgment

The authors thank the referee for a careful reading and several helpful suggestions. The first author acknowledges partial support by RFBR grant 14-01-00393a and the hospitality of Hokkaido University where this work was completed.

References

[1] O. Demchenko, *Covariant Honda theory*, Tohoku Math. J. **57** (2005), 303–319.

[2] O. Demchenko and A. Gurevich, *p-adic period map for the moduli space of deformations of a formal group*, J. Algebra **288** (2005), 445–462.

[3] J. Diedonné, *Groupes de Lie et hyperalgébres de Lie sur un corps de caractéristique $p > 0$ (VII)*, Math. Ann. **134** (1957), 114–133.

[4] J.-M. Fontaine, *Groupes p-divisibles sur les corps locaux*, Astérisque **47–48** (1977).

[5] M. Hazewinkel, Formal groups and applications, Academic Press (1978).

[6] T. Honda, *On the theory of commutative formal groups*, J. Math. Soc. Japan **22** (1970), 213–246.

[7] L. Illusie, *Déformations de groupes de Barsotti-Tate*, Astérisque **127** (1985), 151–198.

[8] J. Lubin and J. Tate, *Formal moduli for one-parameter formal Lie group*, Bull. Soc. Math. France **99** (1966), 49–60.

[9] W. Messing, *The crystals associated to Barsotti-Tate groups*, Vol. 264 of Lecture Notes in Mathematics, Springer (1972).

[10] P. Norman, *An algorithm for computing local moduli of abelian varieties*, Ann. Math. **101** (1975), 499–509.

[11] H. Umemura, *Formal moduli for p-divisible groups*, Nagoya Math. J. **42** (1971), 1–7.

[12] T. Zink, *The display of a formal p-divisible group*, Astérisque **278** (2002), 127–248.

Department of Mathematics and Mechanics
St. Petersburg State University
Universitetsky pr. 28, Stary Petergof
St.Petersburg 198504
Russia
E-mail address: vasja@eu.spb.ru

Einstein Institute of Mathematics
Hebrew University of Jerusalem
Givat Ram, Jerusalem, 91904
Israel
E-mail address: gurevich@math.huji.ac.il

Received November 17, 2011