Tohoku Math. J.
57 (2005), 303–319

COVARIANT HONDA THEORY

OLEG DEMCHENKO

(Received August 21, 2003, revised December 8, 2004)

Abstract. Honda's theory gives an explicit description up to strict isomorphism of formal groups over perfect fields of characteristic $p \neq 0$ and over their rings of Witt vectors by means of attaching a certain matrix, which is called its type, to every formal group. A dual notion of right type connected with the reduction of the formal group is introduced while Honda's original type becomes a left type. An analogue of the Dieudonné module is constructed and an equivalence between the categories of formal groups and right modules satisfying certain conditions, similar to the classical anti-equivalence between the categories of formal groups, and left modules satisfying certain conditions is established. As an application, the $\star$-isomorphism classes of the deformations of a formal group over and the action of its automorphism group on these classes are studied.

0. Introduction. Let k be a perfect field of characteristic $p \neq 0$ and $\mathcal{O}$ its ring of Witt vectors. Honda's theory [5] gives an explicit description of formal groups over $\mathcal{O}$ and k. It attaches to every n-dimensional formal group F a certain $n \times n$-matrix over the non-commutative twisted power series ring E, which is called a type of F. If we restrict our consideration to the p-typical formal groups we will not lose much: every formal group under consideration is strongly isomorphic to a p-typical group. In the present paper, we attach to every p-typical formal group another matrix over E, which we call a 'right type', while Honda's original type will be a 'left type'. The left type describes formal groups up to strict isomorphism and the right type is connected with the reduction of formal groups. In a sense, these notions are dual.

Fontaine [4] used Honda's technique to construct an anti-equivalence from the categories of formal groups over k and that over $\mathcal{O}$ to the category of left E-modules and the category of the pairs consisting of a left E-module and its $\mathcal{O}$-submodule satisfying certain conditions, respectively. Moreover, the reduction modulo p functor between the former categories corresponds to the forgetting of the second component functor between the latter ones. Employing the notion of right type, we obtain an equivalence from the categories of the formal groups over k and that over $\mathcal{O}$ to the category of right E-modules and the category of the pairs consisting of a right E-module and its $\mathcal{O}$-submodule satisfying certain conditions, respectively. In this construction, the reduction modulo p functor corresponds to the functor of factorization of the first component by the E-linear envelope of the second component.

2000 *Mathematics Subject Classification.* Primary 11S31; Secondary 14L05.

Key words and phrases. Formal group, Honda theory, Dieudonné module, p-adic period map.

This research was supported by Inoue Foundation. The author also thanks the Mathematical Institute of Tohoku University for its hospitality.

The presence of the two tools, one for the description of the isomorphisms of formal groups, another for their reductions, makes it easy to deal with problems where both subjects are involved. As an application, consider the $\star$-isomorphism classes of the deformations over $\mathcal{O}$ of a one-dimensional formal group over k. It is parameterized by the Lubin-Tate polydisk $p\mathcal{O} \times \cdots \times p\mathcal{O}$ (cf. [7]). We get an explicit formula for the logarithms of the deformations whose $\star$-isomorphism class corresponds to the given module. It enables us to get a simpler proof of the explicit expression for the right action of the automorphism group of the formal group on its moduli space (cf. [2] or [3]).

1. The bimodule of power series. Let k be a perfect field of characteristic $p \neq 0$. Denote the ring of Witt vectors $W(k)$ by $\mathcal{O}$, its fraction field by K and its Frobenius automorphism by $\triangle$. Then $a^p \equiv a^{\triangle} \bmod p$ for any $a \in \mathcal{O}$. The main object of our consideration will be a ring E, the non-commutative ring of formal power series with coefficients in $\mathcal{O}$ in the variable $\blacktriangle$ with multiplication rule $\blacktriangle a = a^{\triangle}\blacktriangle$, $a \in \mathcal{O}$, and two E-actions, left and right, on the additive group of power series

$$K[[t]]_p = \left\{ \sum_{i \geq 0} c_i t^{p^i},\ c_i \in K \right\}.$$

For $u = \sum u_j \blacktriangle^j$, $v = \sum v_j \blacktriangle^j$ and $f = \sum c_i t^{p^i}$, we define

$$u * f = \sum_i \left(\sum_{j \leq i} u_j c_{i-j}^{\triangle^j} \right) t^{p^i}, \quad f \cdot v = \sum_i \left(\sum_{j \leq i} c_j v_{i-j}^{\triangle^j} \right) t^{p^i}.$$

REMARK. The left action of E can be determined on the whole set of power series $K[[t]]_0$ with no constant term: if $f \in K[[t]]_0$, then $u * f = \sum_j u_j f^{\triangle^j}(t^{p^j})$ (see [5, 2.1]). The right action also can be extended on the whole set $K[[t]]_0$: if $f = \sum_{(r,p)=1} c_{rp^s} t^{rp^s}$, then $f \cdot v = \sum_{(r,p)=1} (\sum_{j \leq s} c_{rp^{s-j}} v_j^{\triangle^{s-j}}) t^{rp^s}$, but in this case many important properties fail to hold.

LEMMA 1. *The two actions define a torsion-free bimodule structure on $K[[t]]_p$.*

PROOF. If $v = v_j \blacktriangle^j$, $v' = v'_s \blacktriangle^s$ and $f = c_i t^{p^i}$, then

$$f \cdot v'v = (c_i t^{p^i}) \cdot (v'_s v_j^{\triangle^s} \blacktriangle^{s+j}) = c_i (v'_s v_j^{\triangle^s})^{\triangle^i} t^{p^{s+j+i}}$$

and

$$(f \cdot v') \cdot v = (c_i {v'_s}^{\triangle^i} t^{p^{i+s}}) \cdot (v_j \blacktriangle^j) = c_i {v_j}^{\triangle^{i+s}} {v'_s}^{\triangle^i} t^{p^{i+s+j}}.$$

This implies the equality $f \cdot v'v = (f \cdot v') \cdot v$ in this particular case. The general case is obvious. The equality $uu' * f = u * (u' * f)$ follows in a similar way.

Now let $u = u_j \blacktriangle^j$, $v = v_s \blacktriangle^s$ and $f = c_i t^{p^i}$. We have

$$u * (f \cdot v) = (u_j \blacktriangle^j) * (c_i v_s^{\triangle^i} t^{p^{i+s}}) = u_j (c_i v_s^{\triangle^i})^{\triangle^j} t^{p^{i+s+j}}$$

and

$$(u * f) \cdot v = (u_j c_i^{\triangle^j} t^{p^{i+j}}) \cdot (v_s \blacktriangle^s) = u_j c_i^{\triangle^j} v_s^{\triangle^{i+j}} t^{p^{i+j+s}}.$$

This implies that $u * (f \cdot v) = (u * f) \cdot v$ and the general case is obvious. □

In order to deal with formal power series in several variables we introduce the following notation. If A is a ring, then we denote the module of column vectors of dimension n with components in A by A^n and the full matrix ring of order n with entries in A by $M_n(A)$. As usual, $I_n \in M_n(A)$ is the identity matrix.

Let x be the set of n variables $x_1, \dots, x_n$ which sometimes will be treated as the column vector $(x_1, \dots, x_n)^{\mathrm{T}}$. Let $K[[x]]_p$ denote the module of formal power series

$$K[[x]]_p = \left\{ \sum_{i \geq 0} c_{i1} x_1^{p^i} + \cdots + \sum_{i \geq 0} c_{in} x_n^{p^i},\ c_{is} \in K \right\}.$$

Let $x' = (x'_1, \dots, x'_m)^{\mathrm{T}}$ be another set of variables. If $f \in K[[x]]_0^l$ and $\varphi \in K[[x']]_0^n$ then we define $f \circ \varphi \in K[[x']]_0^l$ in the following way. If $f = (f_1(x), \dots, f_l(x))^{\mathrm{T}}$ and $\varphi = (\varphi_1(x'), \dots, \varphi_n(x'))^{\mathrm{T}}$, then

$$f \circ \varphi = (f_1(\varphi_1(x'), \dots, \varphi_n(x')), \dots, f_l(\varphi_1(x'), \dots, \varphi_n(x')))^{\mathrm{T}}.$$

In the present paper we consider two categories of formal groups: formal groups over the unramified integer ring $\mathcal{O}$ and formal groups over its residue field k. We denote the reduction modulo p functor between these categories by an overbar. According to [5, Theorem 7], for every formal group Φ over k there is a formal group F over $\mathcal{O}$ such that $\Phi = \bar{F}$, i.e. this functor is surjective.

DEFINITION 1. An n-dimensional formal group F over $\mathcal{O}$ is called *p-typical* if its logarithm belongs to $K[[x]]_p^n$. A formal group Φ over k is called *p-typical* if there exists a p-typical formal group F over $\mathcal{O}$ such that $\Phi = \bar{F}$.

REMARK. These definitions differ from the conventional definition, but are equivalent to it in our situation (see [6] for details).

We restrict our consideration to p-typical formal groups. Then the reduction functor is also surjective for categories of p-typical formal groups over $\mathcal{O}$ and k. It is worth noting that our restriction does not lead to a considerable loss of generality, because any formal group is strictly isomorphic to a p-typical formal group (see [6, Theorem 15.2.9]). We also formulate all statements for this particular case while some of them are valid in a more general situation.

We now extend the left action of E to $K[[x]]_p$ and the right action of E to $K[[t]]_p^n$. Let $u \in E$, $f \in K[[x]]_p$ and $f = \sum f^{(l)}(x_l)$ for $f^{(l)} \in K[[t]]_p$, $1 \leq l \leq n$, then $u * f = \sum u * f^{(l)}(x_l)$; if $v \in E$, $f \in K[[t]]_p^n$ and $f = (f_1, \dots, f_n)^{\mathrm{T}}$ for $f_j \in K[[t]]_p$, $1 \leq j \leq n$ we set $f \cdot v = (f_1 \cdot v, \dots, f_n \cdot v)^{\mathrm{T}}$.

We are ready to define left and right actions

$$M_{s,m}(E) \times K[[x]]_p^m \mapsto K[[x]]_p^s, \quad K[[x]]_p^m \times M_{n,r}(E) \mapsto K[[x']]_p^m,$$

where x is the set of n variables and x' is the set of r variables. Let $u \in M_{s,m}(E)$, $v \in M_{n,r}(E)$, $f \in K[[x]]_p^m$ and $u = \{u_{lj}\}$, $v = \{v_{ik}\}$, $f = (f_1, \dots, f_m)^{\mathrm{T}} = f^{(1)}(x_1) + \cdots + f^{(n)}(x_n)$, where $u_{lj}, v_{ik} \in E$ and $f_j \in K[[x]]_p$, $f^{(i)} \in K[[t]]_p^m$, $1 \leq j \leq m$, $1 \leq i \leq n$. We can also write $f_j = \sum f_{ji}(x_i)$ and $f^{(i)} = (f_{1i}, \dots, f_{mi})^{\mathrm{T}}$ for $f_{ji} \in K[[t]]_p$, $1 \le i \le n$, $1 \le j \le m$. Let us define

$$\begin{aligned} u * f &= \Big(\sum u_{1j} * f_j, \dots, \sum u_{sj} * f_j \Big)^{\mathrm{T}} \\ &= \left(\sum_{\substack{1 \le i \le n \\ 1 \le j \le m}} u_{1j} * f_{ji}(x_i), \dots, \sum_{\substack{1 \le i \le n \\ 1 \le j \le m}} u_{sj} * f_{ji}(x_i) \right)^{\mathrm{T}} \end{aligned}$$

and

$$\begin{aligned} f \cdot v &= \sum f^{(i)} \cdot v_{i1}(x_1) + \dots + \sum f^{(i)} \cdot v_{ir}(x_r) \\ &= \left(\sum_{\substack{1 \le i \le n \\ 1 \le k \le r}} f_{1i} \cdot v_{ik}(x_k), \dots, \sum_{\substack{1 \le i \le n \\ 1 \le k \le r}} f_{mi} \cdot v_{ik}(x_k) \right)^{\mathrm{T}} . \end{aligned}$$

In another notation, let $f \in K[[x]]_p^m$ be written in the form $f = \sum_{i \ge 0} C_i x^{p^i}$, where $C_i \in M_{m,n}(K)$ and $x^{p^i} = (x_1^{p^i}, \dots, x_n^{p^i})^{\mathrm{T}}$. Then for $u = \sum_{j \ge 0} U_j \blacktriangle^j$, $U_j \in M_{s,m}(\mathcal{O})$ and $v = \sum_{j \ge 0} V_j \blacktriangle^j$, $V_j \in M_{n,r}(\mathcal{O})$ we have

$$u * f = \sum_i \Big(\sum_{j \le i} U_j C_{i-j}^{\Delta^j} \Big) x^{p^i} , \quad f \cdot v = \sum_i \Big(\sum_{j \le i} C_j V_{i-j}^{\Delta^j} \Big) x^{p^i} .$$

REMARK. Let $\widetilde{E}$ be the non-commutative ring of formal power series with coefficients in K in the variable $\blacktriangle$ with multiplication rule $\blacktriangle a = a^{\Delta} \blacktriangle$. There is a natural group isomorphism between $K[[t]]_p$ and $\widetilde{E}$, $\sum c_i t^{p^i} \leftrightarrow \sum c_i \blacktriangle^i$, which can be extended to an isomorphism between $K[[x]]_p^m$ and $M_{m,n}(\widetilde{E})$. Under this isomorphism, the left and right actions defined above correspond to the left and right matrix multiplications.

PROPOSITION 1. (i) *For $f \in K[[x]]_p^m$ the following identities hold.*

$$\begin{aligned} (u * f) \cdot v = u * (f \cdot v) \quad &\text{for } u \in M_{s,m}(E) , \ v \in M_{n,r}(E) , \\ (u'u) * f = u' * (u * f) \quad &\text{for } u' \in M_{r,s}(E) , \ u \in M_{s,m}(E) , \\ f \cdot (vv') = (f \cdot v) \cdot v' \quad &\text{for } v \in M_{n,r}(E) , \ v' \in M_{r,s}(E) . \end{aligned}$$

In particular, the two actions define an $M_n(E)$-bimodule structure on $K[[x]]_p^n$.

(ii) *If $f \in K[[x]]_p^n$, $f \equiv x \bmod \deg 2$ and $u \in M_{m,n}(E)$ ($v \in M_{n,m}(E)$), then the equality $u * f = 0$ ($f \cdot v = 0$) implies $u = 0$ ($v = 0$).*

If $u \in M_m(E)$, $u \equiv pI_m \bmod \deg 1$ ($v \in M_n(E)$, $v \equiv pI_n \bmod \deg 1$) and $f \in K[[x]]_p^m$, then the equality $u * f = 0$ ($f \cdot v = 0$) implies $f = 0$.

(iii) *For $f \in K[[x]]_p^n$ and $u \in M_n(E)$, $u \equiv pI_n \bmod \deg 1$, the equalities $u * f = px$ and $f \cdot u = px$ are equivalent.*

(iv) *For any* $\varphi \in \mathcal{O}[[x]]_p^n, \varphi \equiv x \bmod \deg 2$ *and* $\psi \in \mathcal{O}[[x]]_p^m$ *there exists a unique* $w \in M_{m,n}(E)$ *such that* $\psi = w * \varphi$.

For any $\varphi \in \mathcal{O}[[x]]_p^n, \varphi \equiv x \bmod \deg 2$ *and* $\psi \in \mathcal{O}[[x']]_p^n$, *where* x' *is a set of* m *variables there exists a unique* $w \in M_{n,m}(E)$ *such that* $\psi = \varphi \cdot w$.

PROOF. Taking into account the correspondence of the actions to the matrix multiplications, the claims easily follow from the corresponding properties of the matrix multiplication. □

LEMMA 2. (i) *For any* $u \in M_n(E)$ *and* $f \in K[[x]]_p^n$ *such that* $u \equiv pI_n \bmod \deg 1$, $f \equiv x \bmod \deg 2$ *and* $u * f \equiv 0 \bmod p$ *there exists a unique* $v \in M_n(E)$ *such that* $v \equiv pI_n \bmod \deg 1$ *and* $f \cdot v = u * f$.

(ii) *For any* $v \in M_n(E)$ *and* $f \in K[[x]]_p^n$ *such that* $v \equiv pI_n \bmod \deg 1$, $f \equiv x \bmod \deg 2$ *and* $f \cdot v \equiv 0 \bmod p$ *there exists a unique* $u \in M_n(E)$ *such that* $u \equiv pI_n \bmod \deg 1$ *and* $u * f = f \cdot v$.

PROOF. We only prove (i). The uniqueness of v is obvious, and now we show its existence. Let $u * f = p\varphi$ where $\varphi \in \mathcal{O}[[x]]_p^n, \varphi \equiv x \bmod \deg 2$. Then Proposition 1(iv) implies that there exists $v \in M_n(E)$ such that $\varphi \cdot v = u * \varphi$. Therefore, $u * (f \cdot v) = p\varphi \cdot v = pu * \varphi = u * (u * f)$, which gives $f \cdot v = u * f$ as required. The condition $v \equiv pI_n \bmod \deg 1$ holds automatically. □

DEFINITION 2. Let $f \in K[[x]]_p^n$ and $f \equiv x \bmod \deg 2$. If there exists an element $u \in M_n(E)$ such that $u \equiv pI_n \bmod \deg 1$ and $u * f \equiv 0 \bmod p$, then u is called *a left type* of f. Similarly, we call an element $v \in M_n(E)$ such that $v \equiv pI_n \bmod \deg 1$ and $f \cdot v \equiv 0 \bmod p$ *a right type* of f.

Lemma 2 implies that the subsets of elements of $K[[x]]_p^n$ which have a left type and a right type coincide. We will denote this set by $\mathcal{H}_n$. So we have

$$\begin{aligned}\mathcal{H}_n &= \{f \in K[[x]]_p^n\, ;\, f \equiv x \bmod \deg 2 \text{ and } u * f \equiv 0 \bmod p \\ &\qquad \text{for some } u \in M_n(E),\ \ u \equiv pI_n \bmod \deg 1\} \\ &= \{f \in K[[x]]_p^n\, ;\, f \equiv x \bmod \deg 2 \text{ and } f \cdot v \equiv 0 \bmod p \\ &\qquad \text{for some } v \in M_n(E)\,,\ \ v \equiv pI_n \bmod \deg 1\}\,.\end{aligned}$$

DEFINITION 3. An element $u \in M_n(E), u \equiv pI_n \bmod \deg 1$ such that $u * f = f \cdot u = px$ is called *a canonical type* of f. Obviously, it is both a left and right type of f.

LEMMA 3. *For any* $f \in \mathcal{H}_n$ *there exists a unique canonical type.*

PROOF. If $u' * f = p\varphi$ for some left type $u' \in M_n(E)$ then $\varphi = w * x$ for some $w \in M_n(E), w \equiv I_n \bmod \deg 1$. We set $u = w^{-1}u'$ and Proposition 1(iii) proves the required property. The uniqueness of u is obvious. □

LEMMA 4. (i) *Let* $u \in M_n(E), u \equiv pI_n \bmod \deg 1$ *and* $f \in K[[x]]_p^n, f \equiv x \bmod \deg 2$. *Let* $u * f \equiv 0 \bmod p$. *Then* $u' * f \equiv 0 \bmod p$ *for* $u' \in M_{m,n}(E)$ *if and only if* $u' = wu$ *for some* $w \in M_{m,n}(E)$.

(ii) *Let* $v \in M_n(E), v \equiv pI_n \bmod \deg 1$ *and* $f \in K[[x]]_p^n$, $f \equiv x \bmod \deg 2$. *Let* $f \cdot v \equiv 0 \bmod p$. *Then* $f \cdot v' \equiv 0 \bmod p$ *for* $v' \in M_n(E)$ *if and only if* $v' = vw$ *for some* $w \in M_{n,m}(E)$.

PROOF. We only prove (ii) as (i) has a similar proof and follows directly from [5, Proposition 2.6]. If $v' = vw$, then $f \cdot v' = f \cdot vw \equiv 0 \bmod p$. If $f \cdot v' \equiv 0 \bmod p$, then by Proposition 1(iv) we can find $w \in M_{n,m}(E)$ such that $(1/p)f \cdot v' = ((1/p)f \cdot v) \cdot w$. This implies $f \cdot v' = f \cdot vw$, which gives $v' = vw$ as required. □

LEMMA 5. (i) *Let* $u \in M_n(E), u \equiv pI_n \bmod \deg 1$ *and* $f \in K[[x]]_p^n$, $f \equiv x \bmod \deg 2$. *Let* $u * f \equiv 0 \bmod p$. *Then* $u * g \equiv 0 \bmod p$ *for* $g \in K[[x']]_p^n$, *where* x' *is the set of* m *variables, if and only if* $g = f \cdot w$ *for some* $w \in M_{n,m}(E)$.

(ii) *Let* $v \in M_n(E), v \equiv pI_n \bmod \deg 1$ *and* $f \in K[[x]]_p^n$, $f \equiv x \bmod \deg 2$. *Let* $f \cdot v \equiv 0 \bmod p$. *Then* $g \cdot v \equiv 0 \bmod p$ *for* $g \in K[[x]]_p^m$ *if and only if* $g = w * f$ *for some* $w \in M_{m,n}(E)$.

PROOF. As usual we only prove (i). If $g = f \cdot w$, then $u * g = u * f \cdot w \equiv 0 \bmod p$. If $u * g \equiv 0 \bmod p$, then Proposition 1(iv) implies that there exists $w \in M_{n,m}(E)$ such that $(1/p)u * g = ((1/p)u * f) \cdot w$. This gives $u * g = u * (f \cdot w)$, i.e., $g = f \cdot w$. □

PROPOSITION 2. *Let* $f \in \mathcal{H}_n$ *be of left type* u *and right type* v. *Then* $v = \alpha u \beta$ *for some* $\alpha, \beta \in M_n(E)$ *such that* $\alpha \equiv \beta \equiv I_n \bmod \deg 1$.

PROOF. Let u' be the canonical type of f. Then, by Lemma 4, $u' = \alpha u$ and $v = u'\beta$ for some $\alpha \equiv \beta \equiv I_n \bmod \deg 1$. This gives $v = \alpha u \beta$. □

The following two lemmas of Honda, proven by direct computation, are our main tool for further investigation.

LEMMA 6 ([5, Lemma 2.3]). *Let* x' *be a finite set of variables. If* $f \in \mathcal{H}_n, \varphi \in \mathcal{O}[[x']]_0^n$ *and* $w \in M_{m,n}(E)$ *then* $w * (f \circ \varphi) \equiv (w * f) \circ \varphi \bmod p$.

LEMMA 7 ([5, Lemma 4.2]). *Let* x' *be a finite set of variables. If* $f \in \mathcal{H}_n, \varphi \in \mathcal{O}[[x']]_0^n$ *and* $\psi \in K[[x']]_0^n$ *then* $f \circ \varphi \equiv f \circ \psi \bmod p$ *if and only if* $\varphi \equiv \psi \bmod p$.

2. Modules associated with formal groups. The following proposition states that the set of the logarithms of p-typical formal groups over $\mathcal{O}$ and the set $\mathcal{H}_n$ coincide and gives the condition when such formal groups are strictly isomorphic.

PROPOSITION 3 ([5, Theorems 2 and 4]). (i) *If* $f \in \mathcal{H}_n$, *then* $F(x, y) = f^{-1}(f(x)+f(y))$ *is a* p*-typical formal group over* $\mathcal{O}$.

(ii) *If* F *is a* p*-typical formal group over* $\mathcal{O}$ *and* $f \in K[[x]]_p$ *is its logarithm, then* $f \in \mathcal{H}_n$.

(iii) $f, g \in \mathcal{H}_n$ *are of the same left type if and only if the formal groups* $F(x, y) = f^{-1}(f(x) + f(y))$ *and* $G(x, y) = g^{-1}(g(x) + g(y))$ *are strictly isomorphic.*

Let $f = (f_1, \dots, f_n)^{\mathrm{T}} = f^{(1)}(x_1) + \dots + f^{(n)}(x_n) \in \mathcal{H}_n$ and $F(x, y) = f^{-1}(f(x) + f(y))$ be the corresponding n-dimensional formal group over $\mathcal{O}$. Define a subgroup of the additive group $K[[x]]_p$

$$D_f = \{g \in K[[x]]_p\,;\, g \circ F(x, y) \equiv g(x) + g(y) \bmod p\}$$

and a subgroup of the additive group $K[[t]]_p^n$

$$Z_f = \{g \in K[[t]]_p^n\,;\, g = f \circ \varphi \text{ for some } \varphi \in \mathcal{O}[[t]]_0^n\}.$$

REMARK. D_f and Z_f are p-typical analogues for 'the module of quasilogarithms' (see [4]) and the 'invariant Cartier-Dieudonné module' (see [1, 5.2]), respectively.

Using the E-module structure on $K[[x]]_p$ and $K[[t]]_p^n$ we can give an explicit description of Z_f and D_f.

PROPOSITION 4. (i) $Z_f = \{\sum f^{(j)} \cdot w_j\,;\, w_1, \dots, w_n \in E\}$.

(ii) *If* $u = \{u_{ls}\}$ *is a left type of* f, *then* $Z_f = \{(g_1, \dots, g_n)^{\mathrm{T}} \in K[[t]]_p^n\,;\, \sum u_{ls} * g_s \equiv 0 \bmod p$ *for any* $1 \le l \le n\}$.

PROOF. (ii) If $\varphi \in \mathcal{O}[[t]]_0^n$ and $g = f \circ \varphi$ then $\sum u_{ls} * g_s = \sum u_{ls} * (f_s \circ \varphi) \equiv \sum (u_{ls} * f_s) \circ \varphi \equiv 0 \bmod p$ for any $1 \le l \le n$ by Lemma 6.

If $\sum u_{ls} * g_s \equiv 0 \bmod p$, then we construct a sequence $g_i = (g_{1i}, \dots, g_{ni})^{\mathrm{T}} \in K[[t]]_0^n$ such that: (1) $g_0 = g$; (2) $g_{i+1} = g_i - f \circ \varphi_i$ for some $\varphi_i \in \mathcal{O}[[t]]_0^n$; (3) $\sum u_{ls} * g_{si} \equiv 0 \bmod p$ for any $1 \le l \le n$; (4) $g_i \equiv 0 \bmod \deg i$. This implies that $\varphi_i \equiv 0 \bmod \deg i$, which allows us to set $\varphi = \varphi_0 +_F \varphi_1 +_F \cdots$, where $+_F$ is a formal addition given by the formal group $F(x, y) = f^{-1}(f(x) + f(y))$. For such φ we have $g = f \circ \varphi$ as required.

If g_i is defined, then $\sum u_{ls} * g_{si} = p\varphi_{li}$ for some $\varphi_i = (\varphi_{1i}, \dots, \varphi_{ni})^{\mathrm{T}} \in \mathcal{O}[[t]]_0^n$ and we put $g_{i+1} = g_i - f \circ \varphi_i$, which gives

$$\sum u_{ls} * g_{si+1} = \sum u_{ls} * (g_{si} - f_s \circ \varphi_i) \equiv \sum u_{ls} * g_{si} - \sum (u_{ls} * f_s) \circ \varphi_i \equiv 0 \bmod p$$

for any $1 \le l \le n$ by Lemma 6. If $g_{si} \equiv c_s x^i \bmod \deg i + 1$ for any $1 \le s \le n$, then $\varphi_{si} \equiv c_s x^i \bmod \deg i + 1$ and $g_{si+1} = g_{si} - f_s \circ \varphi_i \equiv c_s x^i - c_s x^i = 0 \bmod \deg i + 1$.

(i) For $\hat{g} = g(x_1) + \dots + g(x_n) \in K[[x]]_p^n$ the conditions $g = \sum f^{(j)} \cdot w_j$ for some $w_1, \dots, w_n \in E$ and $\hat{g} = f \cdot w$ for some $w \in M_n(E)$ are equivalent. The conditions $\sum u_{ls} * g_s \equiv 0 \bmod p$ for any $1 \le l \le n$ and $u \cdot \hat{g} \equiv 0 \bmod p$ are also equivalent. It remains to apply Lemma 5. □

PROPOSITION 5. (i) $D_f = \{\sum w_j * f_j\,;\, w_1, \dots, w_n \in E\}$.

(ii) *If* $v = \{v_{ls}\}$ *is a right type of* f, *then* $D_f = \{g^{(1)}(x_1) + \dots + g^{(n)}(x_n) \in K[[x]]_p\,;\, \sum g^{(l)} \cdot v_{ls} \equiv 0 \bmod p$ *for any* $1 \le s \le n\}$.

PROOF. (i) If $g = \sum w_j * f_j$ for some $w_j \in E$, $1 \le j \le n$ then

$$\begin{aligned} g \circ F(x, y) &= \sum (w_j * f_j) \circ F(x, y) \equiv \sum w_j * (f_j \circ F(x, y)) \\ &= \sum w_j * (f_j(x) + f_j(y)) = g(x) + g(y) \bmod p \end{aligned}$$

by Lemma 6.

To prove the opposite inclusion we construct a sequence $g_i \in K[[x]]_p$ such that: (1) $g_0 = g$; (2) $g_{i+1} = g_i - \sum_{j=1}^n c_{ij}\blacktriangle^i * f_j$ for some $c_{ij} \in \mathcal{O}$; (3) $g_i \circ F(x, y) \equiv g_i(x) + g_i(y) \bmod p$; (4) $g_i \equiv 0 \bmod \deg p^i$. This implies that $g = \sum w_j * f_j$ for $w_j = \sum c_{ij}\blacktriangle^i$.

If g_i is defined, then $g_i \equiv \sum_{j=1}^n c_{ij} x_j^{p^i} \bmod \deg p^i + 1$ for some $c_{ij} \in K$. The congruence $g_i \circ F(x, y) \equiv g_i(x) + g_i(y) \bmod p$ implies that $c_{ij}(x_j + y_j)^{p^i} \equiv c_{ij} x_j^{p^i} + c_{ij} y_j^{p^i} \bmod p$, which gives $c_{ij} \in \mathcal{O}$.

Now $g_{i+1} = g_i - \sum_{j=1}^n c_{ij}\blacktriangle^i * f_j \equiv 0 \bmod \deg p^i + 1$ whence $g_{i+1} \equiv 0 \bmod \deg p^{i+1}$. Finally

$$\begin{aligned} g_{i+1} \circ F(x, y) &= \Big(g_i - \sum c_{ij}\blacktriangle^i * f_j\Big) \circ F(x, y) \\ &\equiv g_i(x) + g_i(y) - \sum c_{ij}\blacktriangle^i * (f_j \circ F(x, y)) \\ &= g_i(x) + g_i(y) - \sum c_{ij}\blacktriangle^i * (f_j(x) + f_j(y)) \\ &= g_{i+1}(x) + g_{i+1}(y) \bmod p\,. \end{aligned}$$

(ii) For $\tilde{g} = (g, \dots, g)^{\mathrm{T}} \in K[[x]]_p^n$, the conditions $g = \sum w_j * f_j$ for some $w_1, \dots, w_n \in E$ and $\tilde{g} = w * f$ for some $w \in M_n(E)$ are equivalent. On the other hand, the conditions $\sum g^{(l)} \cdot v_{ls} \equiv 0 \bmod p$ for any $1 \le s \le n$ and $\tilde{g} \cdot v \equiv 0 \bmod p$ are equivalent. Lemma 5 completes the proof. □

Propositions 4 and 5 imply that D_f is a left E-submodule of $K[[x]]_p$ and Z_f is a right E-submodule of $K[[t]]_p^n$.

Given two left types, Honda described homomorphisms between formal groups with logarithms of these types.

PROPOSITION 6 ([5, Theorem 3]). *Let $f \in \mathcal{H}_n$, $g \in \mathcal{H}_m$ be of left type u and u', respectively. Then $[a]_{F,G} := g^{-1} \circ (af) \in \mathrm{Hom}_{\mathcal{O}}(F, G)$ for $a \in M_{m,n}(\mathcal{O})$, if and only if $u'a = wu$ for some $w \in M_{m,n}(E)$.*

Now we can prove that for the logarithm f of F, the module Z_f is connected with the strong isomorphism class of F and D_f with the reduction of F.

PROPOSITION 7. *Let $f, g \in \mathcal{H}_n$ be of left type u and u', respectively. Then the following properties are equivalent.*

(i) *$u' = wu$ for some $w \in M_n(E)$.*

(ii) *$Z_f = Z_g$.*

(iii) *$Z_f \subseteq Z_g$.*

(iv) *The formal groups $F(x, y) = f^{-1}(f(x) + f(y))$ and $G(x, y) = g^{-1}(g(x) + g(y))$ are strongly isomorphic.*

PROOF. Let $f = f^{(1)}(x_1) + \dots + f^{(n)}(x_n)$. Then $Z_f \subseteq Z_g \Leftrightarrow f^{(l)}(x_l) \in Z_g$ for any $1 \le l \le n \Leftrightarrow u' * f \equiv 0 \bmod p$ (Proposition 4) $\Leftrightarrow u' = wu$ for some $w \in M_n(E)$ (Lemma 4).

This implies the equivalence of properties (i) and (iii). As property (i) is symmetric, it is also equivalent to (ii). Proposition 3(ii) proves the equivalence of (iv) with the other properties. □

PROPOSITION 8. *Let $f, g \in \mathcal{H}_n$ be of right type v and v', respectively, and let $F(x, y) = f^{-1}(f(x) + f(y))$ and $G(x, y) = g^{-1}(g(x) + g(y))$ be the corresponding formal groups. Then the following properties are equivalent.*

(i) *$v' = vw$ for some $w \in M_n(E)$.*

(ii) *$D_f = D_g$.*

(iii) *$D_f \subseteq D_g$.*

(iv) *$\bar{F} = \bar{G}$.*

PROOF. The proof of the equivalence of (i), (ii) and (iii) is analogous to that in Proposition 7. Furthermore, $g \circ F(x, y) \equiv g(x) + g(y) = g \circ G \bmod p \Leftrightarrow F \equiv G \bmod p$ by Lemma 7, which proves the equivalence of (ii) and (iv). □

3. Formal groups over finite fields. The following proposition explicitly describes homomorphisms between $\bar{F}$ and $\bar{G}$.

PROPOSITION 9 ([5, Theorems 5 and 6]). *Let $w \in M_{m,n}(E)$ and $f \in \mathcal{H}_n$, $g \in \mathcal{H}_m$ be of left type u and u', respectively. Then we have the following.*

(i) *$\varphi_w := g^{-1} \circ (w * f)$ has integral coefficients if and only if $u'w = zu$ for some $z \in M_{m,n}(E)$.*

(ii) *$\bar{\varphi}_w$ is a homomorphism from $\bar{F}$ to $\bar{G}$ if φ_w has integral coefficients.*

(iii) *Any homomorphism from $\bar{F}$ to $\bar{G}$ is of the form described in* (ii).

(iv) *Let $w' \in M_{l,m}(E)$ and $h \in \mathcal{H}_l$. If φ_w and $\varphi_{w'} = h^{-1} \circ (w' * g)$ have integral coefficients, then $\varphi_{w'w} = h^{-1} \circ (w'w * f)$ also has integral coefficients and $\bar{\varphi}_{w'} \circ \bar{\varphi}_w = \bar{\varphi}_{w'w}$.*

We prove the theorem which can be considered as dual to Proposition 9.

THEOREM 1. *Let $z \in M_{m,n}(E)$ and $f, g \in \mathcal{H}_n$ be of right type v and v', respectively*; *let $F(x, y) = f^{-1}(f(x) + f(y))$ and $G(x, y) = g^{-1}(g(x) + g(y))$ be the corresponding formal groups. Then we have the following.*

(i) *$\psi_z := g^{-1} \circ (g \cdot z)$ has integral coefficients.*

(ii) *$\bar{\psi}_z$ is a homomorphism from $\bar{F}$ to $\bar{G}$ if and only if $zv = v'w$ for some $w \in M_{m,n}(E)$.*

(iii) *Any homomorphism from $\bar{F}$ to $\bar{G}$ is of the form described in* (ii).

(iv) *Let $z' \in M_{l,m}(E)$, $h \in \mathcal{H}_l$ and $H(x, y) = h^{-1}(h(x) + h(y))$ be the corresponding formal groups. If $\psi_{z'} = h^{-1} \circ (h \cdot z')$ and $\bar{\psi}_{z'}$ is a homomorphism from $\bar{G}$ to $\bar{H}$, then $\bar{\psi}_{z'} \circ \bar{\psi}_z = \bar{\psi}_{z'z}$, where $\psi_{z'z} = h^{-1} \circ (h \cdot z'z)$.*

PROOF. (i) Let u' be a left type of g. Then $u' * (g \cdot z) = (u' * g) \cdot z \equiv 0 \bmod p$, which implies by Proposition 4 that for $g \cdot z = \sum_{l=1}^{n} (g \cdot z)^{(l)}(x_l)$, $(g \cdot z)^{(l)} \in K[[t]]_p^m$ we have $(g \cdot z)^{(l)} \in Z_g$, i.e., $\psi_z^{(l)} = g^{-1} \circ (g \cdot z)^{(l)}$ has integral coefficients for any $1 \leq l \leq n$.

(ii) If $zv = v'w$ for some $w \in M_{m,n}(E)$, then $(g \cdot z) \cdot v = (g \cdot v') \cdot w \equiv 0 \bmod p$, i.e., $g \cdot z = w' * f$ for some $w' \in M_{m,n}(E)$ by Lemma 5. Then Proposition 9 implies that $\bar{\psi}_z = \bar{\varphi}_{w'}$ is a homomorphism from $\bar{F}$ to $\bar{G}$.

Conversely, if $\bar{\psi}_z$ is a homomorphism from $\bar{F}$ to $\bar{G}$, then $\bar{\psi}_z = \bar{\varphi}_{w'}$ for some $w' \in M_{m,n}(E)$ by Proposition 9. This means that $g^{-1} \circ (g \cdot z) \equiv g^{-1} \circ (w' * f) \bmod p$, which is equivalent to $g \cdot z \equiv w' * f \bmod p$ by Lemma 7. Hence, $g \cdot zv \equiv w' * f \cdot v \equiv 0 \bmod p$, which gives $zv = v'w$ for some $w \in M_{m,n}(E)$ by Lemma 4.

(iii) By Proposition 9 any homomorphism from $\bar{F}$ to $\bar{G}$ is of the form $\bar{\varphi}_w$ for some $w \in M_{m,n}(E)$ such that $u'w = ru$, where u, u' are left types of f, g, respectively, and $r \in M_{m,n}(E)$. We have $u' * (w * f) = r * (u * f) \equiv 0 \bmod p \Rightarrow w * f = g \cdot z$ for some $z \in M_{m,n}(E)$ by Lemma 5. Thus, $g \cdot zv = w * f \cdot v \equiv 0 \bmod p$, i.e., $zv = v'w$ for some $w \in M_{m,n}(E)$ by Lemma 4.

(iv) As $\bar{\psi}_{z'}$ is a homomorphism from $\bar{G}$ to $\bar{H}$, we know from (ii) that $h \cdot z' = w * g$ for some $w \in M_{l,m}(E)$. Then $(h \cdot z') \circ \psi_z = (w * g) \circ \psi_z \equiv w * (g \circ \psi_z) = w * g \cdot z = h \cdot z'z \bmod p$ by Lemma 6. Hence $\psi_{z'} \circ \psi_z = h^{-1} \circ ((h \cdot z') \circ \psi_z) \equiv h^{-1} \circ (h \cdot z'z) = \psi_{z'z} \bmod p$ by Lemma 7. □

DEFINITION 4. Let $u \in M_n(E), u \equiv pI_n \bmod \deg 1$ and $u' \in M_m(E), u' \equiv pI_m \bmod \deg 1$. We say that u' is *weakly associated with* u, if there are $w, z \in M_{m,n}(E)$ such that $u'w = zu$ and $w \neq tu$ for any $t \in M_{m,n}(E)$ (or, equivalently, $z \neq u's$ for any $s \in M_{m,n}(E)$). We say that u and u' are *associated* if $m = n$ and there are invertible $w, z \in M_n(E)$ such that $u'w = zu$.

One can see easily that the submodule $p\,\mathcal{O}[[x]]_p$ is contained in D_f and the submodule $p\,\mathcal{O}[[t]]_p^n$ is contained in Z_f. Consider the factor modules

$$\bar{D}_f = D_f / p\,\mathcal{O}[[x]]_p\,, \quad \bar{Z}_f = Z_f / p\,\mathcal{O}[[t]]_p^n\,.$$

If f is of left type $u = \{u_{ij}\}$ and of right type $v = \{v_{ij}\}$, then by Propositions 4 and 5 we have the following E-module isomorphisms. Denote $u_i = (u_{i1}, \dots, u_{in}), v_j = (v_{1j}, \dots, v_{nj}) \in E \times \cdots \times E$ for $1 \leq 1, j \leq n$. Then

$$\bar{D}_f \cong E \times \cdots \times E/(Eu_1 + \cdots + Eu_n)\,, \quad \bar{Z}_f \cong E \times \cdots \times E/(v_1E + \cdots + v_nE)\,.$$

REMARK. $\bar{D}_f$ is isomorphic to the classical Dieudonné-Honda module (see [4]).

THEOREM 2. *Let $f \in \mathcal{H}_n, g \in \mathcal{H}_m$ and $F(x, y) = f^{-1}(f(x) + f(y)), G(x, y) = g^{-1}(g(x)+g(y))$ be the corresponding formal groups. Let u, u' be left types and v, v' be right types of f and g, respectively. Then there are the following canonical group isomorphisms*

$$\mathrm{Hom}(\bar{F}, \bar{G}) \cong \{w \in M_{m,n}(E)\,;\, u'w = zu, z \in M_{m,n}(E)\}/M_{m,n}(E)u \cong \mathrm{Hom}(\bar{D}_g, \bar{D}_f)$$
$$\mathrm{Hom}(\bar{F}, \bar{G}) \cong \{z \in M_{m,n}(E)\,;\, zv = v'w, w \in M_{m,n}(E)\}/v'M_{m,n}(E) \cong \mathrm{Hom}(\bar{Z}_f, \bar{Z}_g)$$

and ring isomorphisms

$$\mathrm{End}(\bar{F}) \cong \{w \in M_n(E)\,;\, uw = zu, z \in M_n(E)\}/M_n(E)u \cong \mathrm{End}(\bar{D}_f)$$
$$\mathrm{End}(\bar{F}) \cong \{z \in M_n(E)\,;\, zv = vw, w \in M_n(E)\}/vM_n(E) \cong \mathrm{End}(\bar{Z}_f).$$

PROOF. We construct the chain of canonical isomorphisms

$$\mathrm{Hom}(\bar{F},\bar{G}) \to \{z \in M_{m,n}(E)\,;\, zv = v'w\}/v'M_{m,n}(E) \to \mathrm{Hom}(\bar{Z}_f,\bar{Z}_g)\,.$$

According to Theorem 1, the mapping $z \mapsto \bar{\psi}_z$, where $\psi_z = g^{-1} \circ (g \cdot z)$, provides an epimorphism from the group $\{z \in M_{m,n}(E)\,;\, zv = v'w\}$ to $\mathrm{Hom}(\bar{F},\bar{G})$. We have $\bar{\psi}_z = 0 \Leftrightarrow g^{-1} \circ (g \cdot z) \equiv 0 \bmod p \Leftrightarrow g \cdot z \equiv 0 \bmod p$ (Lemma 7) $\Leftrightarrow z \in v'M_{m,n}(E)$ (Lemma 4). This gives the first isomorphism.

Since $\bar{Z}_f \cong E \times \cdots \times E/(v_1E + \cdots + v_nE)$ for $v_j = (v_{1j},\ldots,v_{nj})$, $1 \le j \le n$ and $v = \{v_{ij}\}$, the second isomorphism is obvious: $z \mapsto$ 'homomorphism taking $f^{(l)}$, $1 \le l \le n$ to $g^{(1)} \cdot z_{1l} + \cdots + g^{(m)} \cdot z_{ml}$', where $f = f^{(1)}(x_1) + \cdots + f^{(n)}(x_n)$, $g = g^{(1)}(x_1) + \cdots + g^{(m)}(x_m)$ and $f^{(l)} \in K[[t]]_p^n$, $g^{(i)} \in K[[t]]_p^m$.

The claims concerning left types and modules $\bar{D}_f$ are well-known and have similar proofs. □

COROLLARY 1. *Let $f \in \mathcal{H}_n$, $g \in \mathcal{H}_m$. Let u, u' be left types and let v, v' be right types of f and g, respectively. Then the following properties are equivalent*:

(i) *u' is weakly associated with u.*

(ii) *v' is weakly associated with v.*

(iii) *There exists a non-zero homomorphism from $\bar{F}$ to $\bar{G}$, where $F(x,y) = f^{-1}(f(x) + f(y))$ and $G(x,y) = g^{-1}(g(x) + g(y))$.*

(iv) *There exists a non-zero E-module homomorphism from $\bar{Z}_f$ to $\bar{Z}_g$.*

(v) *There exists a non-zero E-module homomorphism from $\bar{D}_g$ to $\bar{D}_f$.*

COROLLARY 2. *Let $f, g \in \mathcal{H}_n$. Let u, u' be left types and let v, v' be right types of f and g, respectively. Then the following properties are equivalent*:

(i) *u and u' are associated.*

(ii) *v and v' are associated.*

(iii) *$\bar{F}$ and $\bar{G}$ are isomorphic, where $F(x,y) = f^{-1}(f(x) + f(y))$ and $G(x,y) = g^{-1}(g(x) + g(y))$.*

(iv) *The right E-modules $\bar{Z}_f$ and $\bar{Z}_g$ are isomorphic.*

(v) *The left E-modules $\bar{D}_f$ and $\bar{D}_g$ are isomorphic.*

4. Classification results.

LEMMA 8. *Let $\mathcal{E}$ be an integral domain satisfying both left and right Ore conditions. Then any linear system of $n-1$ equations in n variables with coefficients in $\mathcal{E}$*

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = 0 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = 0 \\ \qquad\qquad\qquad \vdots \\ a_{n-11}x_1 + a_{n-12}x_2 + \cdots + a_{n-1n}x_n = 0 \end{cases}$$

has a non-zero solution in $\mathcal{E}$.

PROOF. We proceed by induction on n; the case $n = 2$ follows from the right Ore condition. If $a_{11} = \cdots = a_{n-11} = 0$, we can assume that $x_1 = 1$, $x_2 = \cdots = x_n = 0$. Let $a_{11} \neq 0$. Then by the left Ore condition there exist $\lambda_i, \mu_i \in \mathcal{E}$, $2 \leq i \leq n$ such that $\lambda_i a_{11} = \mu_i a_{i1}$ and $\mu_i \neq 0$. This gives the system

$$\begin{cases} (\lambda_2 a_{12} - \mu_2 a_{22})x_2 + \cdots + (\lambda_2 a_{1n} - \mu_2 a_{2n})x_n = 0 \\ \qquad\qquad\qquad\qquad \vdots \\ (\lambda_{n-1} a_{12} - \mu_{n-1} a_{n-12})x_2 + \cdots + (\lambda_{n-1} a_{1n} - \mu_{n-1} a_{n-1n})x_n = 0 \end{cases}$$

which has a non-zero solution $x_2 = \xi_2, \ldots, x_n = \xi_n$ by the induction assumption. The right Ore condition implies that there are $\xi_1, b \in \mathcal{E}$, $b \neq 0$ such that $a_{11}\xi_1 + (a_{12}\xi_2 + \cdots + a_{1n}\xi_n)b = 0$. Check that $x_1 = \xi_1, x_2 = \xi_2 b, \ldots, x_n = \xi_n b$ give a non-zero solution of the initial system. For $2 \leq i \leq n-1$

$$\mu_i(a_{i1}\xi_1 + (a_{i2}\xi_2 + \cdots + a_{in}\xi_n)b) = \lambda_i(a_{11}\xi_1 + (a_{12}\xi_2 + \cdots + a_{1n}\xi_n)b) = 0\,,$$

whence $a_{i1}\xi_1 + a_{i2}\xi_2 b + \cdots + a_{in}\xi_n b = 0$ as required. □

PROPOSITION 10. *For $u \in M_n(E)$ the following conditions are equivalent.*

(i) *There exist $w \in M_n(E)$ and an integer h such that $wu \equiv \blacktriangle^h I_n \bmod p$.*

(ii) *There exist $w \in M_n(E)$ and an integer h such that $uw \equiv \blacktriangle^h I_n \bmod p$.*

(iii) *pI_n is not weakly associated with u, i.e., if $su \equiv 0 \bmod p$ for $s \in M_n(E)$, then $s \equiv 0 \bmod p$.*

(iv) *u is not weakly associated with pI_n, i.e., if $us \equiv 0 \bmod p$ for $s \in M_n(E)$, then $s \equiv 0 \bmod p$.*

PROOF. Let $\mathcal{E}$ be the non-commutative ring of formal power series with coefficients in k in the variable $\blacktriangle$ with multiplication rule $\blacktriangle\alpha = \alpha^p\blacktriangle$, $\alpha \in k$. The reduction mapping from $M_n(E)$ to $M_n(\mathcal{E})$ is denoted by overline. Notice that the ring $\mathcal{E}$ satisfies both left and right Ore conditions.

(ii) $\Rightarrow$ (iii) Let $w \in M_n(E)$ be such that $\bar{u}\bar{w} = \blacktriangle^h I_n$ in $M_n(\mathcal{E})$. If $\bar{s}\bar{u} = 0$ then $\bar{s}\blacktriangle^h = \bar{s}\bar{u}\bar{w} = 0$, which implies $\bar{s} = 0$.

(iv) $\Rightarrow$ (ii) By Lemma 8, for any $1 \leq i \leq n$ there exists a non-zero column vector $\sigma_i \in \mathcal{E}^n$ such that $\bar{u}\sigma_i$ is a column vector with all components except the ith one equal to zero. The ith component is non-zero since otherwise the non-zero matrix $\sigma \in M_n(\mathcal{E})$ with columns all equal to σ_i satisfies $\bar{u}\sigma = 0$. Let $\omega \in M_n(\mathcal{E})$ be such that its ith column is σ_i, $1 \leq i \leq n$. Then $\bar{u}\omega$ is a diagonal matrix with no zero entries on the main diagonal and we can assume $\bar{u}\omega = \blacktriangle^h I_n$.

Implications (i) $\Rightarrow$ (vi) and (iii) $\Rightarrow$ (i) have similar proofs, so we are done. □

REMARK. Corollary 1 implies that the above conditions are also equivalent to the following conditions:

(i) $\mathrm{Hom}(\bar{F}, F_a) = \{0\}$;

(ii) $\mathrm{Hom}(F_a, \bar{F}) = \{0\}$;

(iii) $\mathrm{Hom}(\bar{Z}_f, E^n/pE^n) = \{0\}$;

(iv) $\operatorname{Hom}(E^n/pE^n, \bar{Z}_f) = \{0\}$;

where F is the formal group with the logarithm f of canonical type u and F_a is the additive formal group.

DEFINITION 5. We say that $u \in M_n(E)$ is *of finite height* if u satisfies one of the equivalent conditions listed above. A formal group over $\mathcal{O}$ is *of finite height* if its logarithm f has the canonical type of finite height. A formal group over k is *of finite height* if it is equal to the reduction of a formal group over $\mathcal{O}$ of finite height.

REMARK. (1) If f is the logarithm of a formal group over $\mathcal{O}$ of finite height, then Lemma 4 implies that any left or right type of f is also of finite height.

(2) Any lifting of a formal group over k of finite height is of finite height by Proposition 8.

Provide the ring E with $\blacktriangle$-adic topology. Let $\bar{\mathcal{Z}}$ be the category of right topological E-modules $\bar{Z}$ such that:

(a) the action of $\blacktriangle$ on $\bar{Z}$ is injective;

(b) $\bar{Z}p \subseteq \bar{Z}\blacktriangle$;

(c) $\bar{Z}/\bar{Z}\blacktriangle$ is a finite dimensional vector space over k;

and the morphisms of $\bar{\mathcal{Z}}$ are the E-linear mappings.

Let $\bar{\mathcal{Z}}^o$ be the full subcategory of $\bar{\mathcal{Z}}$ of objects $\bar{Z}$ such that $\bar{Z}$ is a free $\mathcal{O}$-module of finite rank.

THEOREM 3. *The correspondence $\bar{F} \mapsto \bar{Z}_f$, where f is the logarithm of F, establishes an equivalence between the category of p-typical formal groups over k and the category $\bar{\mathcal{Z}}$; in particular, the subcategory of p-typical formal groups over k of finite height is equivalent to the subcategory $\bar{\mathcal{Z}}^o$.*

PROOF. It is easy to see that $\bar{Z}_f \in \bar{\mathcal{Z}}$. Theorem 1(iv) and Theorem 2 prove that the correspondence $\bar{F} \mapsto \bar{Z}_f$ is functorial and fully faithful. It remains to check that for every object $\bar{Z} \in \bar{\mathcal{Z}}$ there exists $f \in \mathcal{H}_n$ such that $\bar{Z}$ and $\bar{Z}_f$ are isomorphic as E-modules.

Let $d_1 + \bar{Z}\blacktriangle, \dots, d_n + \bar{Z}\blacktriangle$ form a basis of $\bar{Z}/\bar{Z}\blacktriangle$. Then for every $d' \in \bar{Z}$ there exist $c_{01}, \dots, c_{0n} \in \mathcal{O}$ and $d'' \in \bar{Z}$ such that $d' = \sum d_j c_{0j} + d''\blacktriangle$. For any $N > 0$ that gives $d' - \sum d_j(c_{0j} + \cdots + c_{Nj}\blacktriangle^N) \in \bar{Z}\blacktriangle^{N+1}$ for some $c_{ij} \in \mathcal{O}$, whence $d' = \sum d_i w_i$ for some $w_1, \dots, w_n \in E$.

As $\bar{Z}p \subseteq \bar{Z}\blacktriangle$, there exist $v_{ij} \in E, 1 \le i, j \le n$ such that $v_{ii} \equiv p \operatorname{mod} \operatorname{deg} 1$, $v_{ij} \equiv 0 \operatorname{mod} \operatorname{deg} 1$ for $i \neq j$ and $\sum d_i v_{ij} = 0$ for any $1 \le j \le n$. Take $f \in \mathcal{H}_n$ of right type $v = \{v_{ij}\}$. We know that as E-module $\bar{Z}_f \cong E \times \cdots \times E/(v_1 E + \cdots + v_n E)$ for $v_j = (v_{1j}, \dots, v_{nj})$ and now we only have to prove that the equality $\sum d_j z_j = 0$ for $z_1, \dots, z_n \in E$ implies $z_j = \sum v_{jl} w_l$ for some $w_1, \dots, w_n \in E$.

To this end we construct n sequences $z_{ij} \in E, 1 \le j \le n$ such that: (1) $z_{0j} = z_j$; (2) $\sum d_j z_{ij} = 0$; (3) $z_{i+1j} = z_{ij} - \sum_{l=1}^{n} v_{jl} a_{il} \blacktriangle^i$ for some $a_{il} \in \mathcal{O}$; (4) $z_{ij} \equiv 0 \operatorname{mod} \operatorname{deg} i$. If $z_{ij}, 1 \le j \le n$ are already defined, we know that $z_{ij} \equiv b_{ij}\blacktriangle^i \operatorname{mod} \operatorname{deg} i+1$ for some $b_{ij} \in \mathcal{O}$. The injectivity of $\blacktriangle$ implies $\sum d_j b_{ij} \in \bar{Z}\blacktriangle$, which gives $b_{ij} = pa_{ij}$ for some $a_{ij} \in \mathcal{O}$ and we set $z_{i+1j} = z_{ij} - \sum_{l=1}^{n} v_{jl} a_{il} \blacktriangle^{i}$. Then $\sum d_j z_{i+1j} = \sum d_j z_{ij} - \sum d_j v_{jl} a_{il} \blacktriangle^{i} = 0$ and $z_{i+1j} \equiv p a_{ij} \blacktriangle^{i} - p a_{ij} \blacktriangle^{i} = 0 \bmod \deg i + 1$. Now we have $z_j = \sum v_{jl}(a_{0l} + a_{1l}\blacktriangle + \cdots)$ as required.

Let $f \in \mathcal{H}_n$ be the logarithm of a p-typical formal group of finite height. Then $f \cdot \blacktriangle^{h} I_n \equiv f \cdot pz \bmod p$ for some $z \in E$ and integer h, which implies $f^{(l)} \cdot \blacktriangle^{h} \in p\bar{Z}_f$, $1 \leq l \leq n$ for $f = f^{(1)}(x_1) + \cdots + f^{(n)}(x_n)$. Then $\{f^{(l)} \cdot \blacktriangle^{j} \; ; \; 1 \leq l \leq n, 0 \leq j < h\}$ gives a system of generators of $\bar{Z}_f$. It remains to check that $\bar{Z}_f$ has no p-torsion. Let $p \sum d_j z_j = 0$, then $pz = vw$ for some $w \in M_n(E)$, where $z = \{z_j\}_{i,j=1}^{n}$. Since f is the logarithm of a formal group of finite height, we have $w = pw'$ for some $w' \in M_n(E)$. Thus $z = vw'$ and $\sum d_j z_j = 0$.

Conversely, if $\bar{Z}_f \in \bar{\mathcal{Z}}^{o}$, then for every component of $f = f^{(1)}(x_1) + \cdots + f^{(n)}(x_n)$ there exists a polynomial $z_l \in E$ such that $f^{(l)} \cdot z_l \equiv 0 \bmod p$, $1 \leq l \leq n$. Since $\bar{Z}_f$ is a free $\mathcal{O}$-module, z_l is not divisible by p. Then we can assume $z_l \equiv \blacktriangle^{h} \bmod p$ for some integer h and $1 \leq l \leq n$. By Lemma 4, f is the logarithm of a formal group of finite height. □

Let $\mathcal{Z}Y$ be the category consisting of the pairs (Z, Y) such that:

(a) Z is a free right E-module of finite rank;

(b) Y is a free right $\mathcal{O}$-submodule of Z of the same rank;

(c) $(Y + Z\blacktriangle)/Z\blacktriangle = (Zp + Z\blacktriangle)/Z\blacktriangle$;

and the morphisms from (Z_1, Y_1) to (Z_2, Y_2) be E-linear mappings $\xi \colon Z_1 \to Z_2$ such that $\xi(Y_1) \subseteq Y_2$.

Let $\mathcal{Z}Y^{o}$ be the full subcategory of $\mathcal{Z}Y$ of objects (Z, Y) such that $Z/\langle Y \rangle$ is a free $\mathcal{O}$-module of finite rank, where $\langle Y \rangle$ denotes the minimal right E-submodule containing Y.

For $f \in \mathcal{H}_n$ and $F(x, y) = f^{-1}(f(x) + f(y))$ being the corresponding formal group, we define an $\mathcal{O}$-submodule of Z_f

$$Y_0 = \{(a_1 t, \ldots, a_n t)^{\mathrm{T}} \; ; \; a_i \in p\mathcal{O}\}\,.$$

THEOREM 4. *The correspondence $F \mapsto (Z_f, Y_0)$, where f is the logarithm of F, establishes an equivalence between the category of p-typical formal groups over $\mathcal{O}$ and the category $\mathcal{Z}Y$; in particular, the subcategory of p-typical formal groups over $\mathcal{O}$ of finite height is equivalent to the subcategory $\mathcal{Z}Y^{o}$.*

PROOF. If we fix $f^{(1)}, \ldots, f^{(n)}$ as generators of Z_f, we have $Y_0 = \{\sum_{j,l=1}^{n} f^{(j)} \cdot u_{jl} b_l \; ; \; b_l \in \mathcal{O}\}$, where $u = \{u_{jl}\} \in M_n(E)$ is the canonical type of f. This implies

$$(Y_0 + Z_f\blacktriangle)/Z_f\blacktriangle = \left\{ \sum f^{(j)} \cdot pb_j + Z_f\blacktriangle \; ; \; b_j \in \mathcal{O} \right\} = (Z_f p + Z_f\blacktriangle)/Z_f\blacktriangle\,,$$

whence $(Z_f, Y_0) \in \mathcal{Z}Y$.

Let G be another m-dimensional formal group over $\mathcal{O}$ with logarithm g of canonical type $v = \{v_{ij}\}$. If $\varphi = [a]_{F,G} \in \mathrm{Hom}_{\mathcal{O}}(F, G)$, we have $va = wu$ for some $w = \{w_{ij}\} \in M_n(E)$ by Proposition 6. This allows us to define the image of φ to be equal to the E-linear mapping from Z_f to Z_g, which sends $f^{(j)} \mapsto \sum g^{(i)} \cdot w_{ij}$, $1 \leq j \leq n$. Then $\sum f^{(j)} \cdot u_{jl} b_l \mapsto \sum g^{(i)} \cdot w_{ij} u_{jl} b_l = \sum g^{(i)} \cdot v_{ij} a_{jl} b_l = \sum g^{(i)} \cdot v_{ij} (\sum a_{jl} b_l)$, therefore the image of Y_0 is in Y_0. The correspondence is functorial and fully faithful; if $\xi : Z_f \to Z_g$ is an E-linear mapping such that $\xi(Y_0) \subseteq Y_0$ then $\sum \xi(f^{(j)}) \cdot u_{jl} = \sum (g^{(i)} \cdot v_{il}) \cdot a_{jl}$ for any $1 \leq j \leq n$ and some $a_{jl} \in \mathcal{O}$. This implies $va = wu$ for $a = \{a_{jl}\} \in M_n(\mathcal{O})$ and $w = \{w_{ij}\} \in M_n(E)$ such that $\xi(f^{(j)}) = \sum g^{(i)} \cdot w_{ij}$. Hence, $[a]_{F,G} \in \mathrm{Hom}_{\mathcal{O}}(F, G)$ by Proposition 6.

It remains to prove that for every object $(Z, Y) \in \mathcal{Z}Y$ there exists $f \in \mathcal{H}_n$ such that (Z, Y) is isomorphic to (Z_f, Y_0). Let $d_1, \dots, d_n$ be free E-generators of Z and let $\sum d_j u_{j1}, \dots, \sum d_j u_{jn}$ be free $\mathcal{O}$-generators of Y. If $u^o_{jl} \in \mathcal{O}$ is the constant term of u_{jl} and $u^o = \{u^o_{jl}\}$ then the equality

$$\left\{ \sum d_j b_j p + Z\blacktriangle \, ; \; b_j \in \mathcal{O} \right\} = (Zp + Z\blacktriangle)/Z\blacktriangle = (Y + Z\blacktriangle)/Z\blacktriangle$$
$$= \left\{ \sum d_i u^o_{il} b_l + Z\blacktriangle \, ; \; b_l \in \mathcal{O} \right\}$$

implies that $u^o_{jl} \equiv 0 \bmod p$ and $u^o \varepsilon = pI_n$ for $\varepsilon \in M_n(\mathcal{O})$. Therefore, ε is invertible and we can assume $u^o = pI_n$. Now choose $f \in \mathcal{H}_n$ of canonical type u. Then the E-linear mapping from Z_f to Z, which sends $f^{(j)} \mapsto d_j$, $1 \leq j \leq n$, induces an isomorphism between (Z_f, Y_0) and (Z, Y).

Since $Z_f/\langle Y_0 \rangle = Z_f/p\mathcal{O}[[t]]^n_p = \bar{Z}_f$, we have that $(Z_f, Y_0) \in \mathcal{Z}Y^o \Leftrightarrow Z_f/\langle Y_0 \rangle = \bar{Z}_f$ is a free $\mathcal{O}$-module of finite rank $\Leftrightarrow \bar{Z}_f \in \bar{\mathcal{Z}}^o \Leftrightarrow f$ is the logarithm of a formal groups of finite height. □

5. Applications. We illustrate the application of our approach by considering the Lubin-Tate polydisk, which parameterizes the $\star$-isomorphism classes of deformations of a one-dimensional formal group over a perfect field of characteristic $p \neq 0$ (see [7]).

Let Φ be a one-dimensional finite height formal group over k in normal form and A a complete Noetherian local $\mathcal{O}$-algebra with maximal ideal $\mathcal{M} \supseteq pA$ and residue field $A/\mathcal{M} \supseteq k$. Two formal groups over A are called $\star$-isomorphic if there exists an isomorphism between them with identity reduction. Lubin and Tate constructed a moduli space for $\star$-isomorphism classes of deformations of Φ. More precisely, they proved the existence of a formal group Γ over $\mathcal{O}[[t_1, \dots, t_{h-1}]]$ such that for any deformation F of Φ over A there is a unique $(h-1)$-tuple $(\tau_1, \dots, \tau_{h-1})$, $\tau_i \in \mathcal{M}$, such that F is $\star$-isomorphic to $\Gamma(\tau_1, \dots, \tau_{h-1})$ over A and the $\star$-isomorphism is uniquely defined. The formal group Γ is not unique and Hazewinkel's universal p-typical formal group [6] gives the explicit construction for one of them.

The choice of a p-typical formal group Φ of height h corresponds to the choice of multiplicative representative $r_h, r_{h+1}, \dots \in \mathcal{O}$. Let the sequence $a_i \in K[t_1, \dots, t_{h-1}]$ be given by the recursive relation

$$pa_i = \sum_{j=1}^{\min(i,h-1)} t_j^{p^{i-j}} a_{i-j} + \sum_{j=h}^{i} r_j^{\Delta^{i-j}} a_{i-j} \, , \quad a_0 = 1 \, .$$

The power series $f = \sum a_i x^{p^i}$ is the logarithm of a formal group $\varGamma$ over $\mathcal{O}[[t_1, \dots, t_{h-1}]]$, which parametrizes the $\star$-isomorphism classes of deformations of $\varPhi$ (cf. [6, Theorem 22.4.4]).

Now consider the case $A = \mathcal{O}$. For any modulus $(\tau_1, \dots, \tau_{h-1}) \in p\mathcal{O} \times \cdots \times p\mathcal{O}$ we denote by $f_\tau(x) = \sum a_i(\tau) x^{p^i}$ the logarithm of the corresponding p-typical deformation over $\mathcal{O}$. Proposition 8 implies that $f_\tau = w_\tau * f_0$ for some $w_\tau \in E$. We find w_τ explicitly, namely we prove that

$$w_\tau = 1 + \sum_{i \geq 1} \left(\frac{1}{p} \sum_{j=1}^{\min(i,h-1)} \tau_j^{p^{i-j}} a_{i-j}(\tau) \right) \blacktriangle^i .$$

The recursive relation for a_i and $t = \tau$ can be written in our notation as $f_\tau \cdot u_0 = (px) \cdot w_\tau$, where $u_0 = p - r_h \blacktriangle^h - r_{h+1} \blacktriangle^{h+1} - \cdots$. Since $w_0 = 1$, we get $f_0 \cdot u_0 = px$ and $w_\tau * f_0 \cdot u_0 = w_\tau * (px) = (px) \cdot w_\tau = f_\tau \cdot u_0$, which gives the desired result.

The formula obtained allows us to give an explicit description of the right action of the automorphism group $\mathrm{Aut}_k \varPhi$ on the moduli space (see [2, 3] for details). If $\xi \in \mathrm{Aut}_k \varPhi$ and $[F]$ is the $\star$-isomorphism class of a deformation F of $\varPhi$ over $\mathcal{O}$, then by definition $[F]\xi = [\varphi^{-1} \circ F \circ \varphi]$, where $\varphi \in \mathcal{O}[[x]]_0$ and $\bar{\varphi} = \xi$.

By Proposition 9 any $\xi \in \mathrm{Aut}_k \varPhi$ is equal to $\bar{\varphi}_w$, where $\varphi_w = f_0^{-1} \circ (w * f_0)$ and $w \in E$ satisfies $u_0 w = z u_0$ for some $z \in E$. By the Weierstrass preparation theorem for the ring E, there is a unique $s \in E^*$ such that $u_0' := s u_0$ is a monic polynomial of degree h. Thus we can only consider polynomials $w = 1 + \sum_{i=1}^{h-1} \beta_i \blacktriangle^i$, $\beta_i \in \mathcal{O}$ with $u_0 \varepsilon w = z u_0$ for some $z \in E$ and $\varepsilon \in \mathcal{O}^*$. Our aim is to find an explicit relation between the coefficients of such polynomials and the corresponding Lubin-Tate's parameters.

Let $u_0' = \sum_{i=1}^h \pi_i \blacktriangle^i$ where $\pi_h = 1$ and $\pi_i \in pO$ for $1 \leq i \leq h-1$. Define the sequence $\zeta_n \in O$ as follows: $\zeta_0 = 1$, $\zeta_j = 0$ for $1 \leq j \leq h-1$ and

$$\zeta_j = -\sum_{i=0}^{h-1} \pi_i^{\Delta^{-h}} \zeta_{j+i-h}^{\Delta^{i-h}}, \quad j \geq h .$$

Let $\mathcal{O}\{y\}_p$ denote the $\mathcal{O}$-submodule of $\mathcal{O}[[y]]_p$ consisting of the formal power series $\sum_{j=0}^\infty c_j y^{p^j}$ such that $\lim c_j = 0$. Let $\blacktriangle$ operate on $A\{y\}_p$ by the formula

$$\blacktriangle \sum_{j=0}^\infty c_j y^{p^j} = \sum_{j=0}^\infty c_{j+1}^\Delta y^{p^j} .$$

This determines a left E-module structure on $\mathcal{O}\{y\}_p$. One can see that $\sum \zeta_j y^{p^j} \in \mathcal{O}\{y\}_p$ and $u_0' \sum \zeta_j y^{p^j} = 0$. Define the sequence of rigid analytic functions

$$\rho_n(t_1, \dots, t_{h-1}) = p\zeta_n + \sum_{i=1}^\infty \sum_{j=1}^{\min(i,h-1)} \zeta_{i+n}^{\Delta^i} t_j^{p^{i-j}} a_{i-j}, \quad n \geq 0 .$$

Denote the coefficients of w_τ by b_i, i.e., $w_\tau = \sum_{i=0}^{\infty} b_i \blacktriangle^i$, $b_0 = 1$. Then $\rho_n(\tau_1, \dots, \tau_{h-1}) = p \sum_{i=0}^{\infty} \zeta_{i+n}^{\Delta^i} b_i$. Since $w_\tau = s_1 u_0' + \varepsilon(1 + \sum_{i=1}^{h-1} \beta_i \blacktriangle^i)$ for some $s_1 \in E$, we get

$$\sum_{n=0}^{\infty} \rho_n y^{p^n} = p w_\tau \sum_{j=0}^{\infty} \zeta_j y^{p^j} = p\varepsilon \left(1 + \sum_{i=1}^{h-1} \beta_i \blacktriangle^i \right) \sum_{j=0}^{\infty} \zeta_j y^{p^j} ,$$

which implies $\beta_i = ((\rho_0, \dots, \rho_{h-1}) Z^{-1})_i / \rho_0$, where $Z = \{\zeta_{i+j}^{\Delta^i}\}_{i,j=0}^{h-1}$. This is Theorem 6.5 of [3].

References

[1] M. Bondarko and S. Vostokov, Explicit classification of formal groups over local fields, Tr. Mat. Inst. Steklova 241 (2003), 43–67.

[2] O. Demchenko and A. Gurevich, Explicit formula for the action of the automorphism group of a formal group on the moduli space of its deformations, MPIM Preprint Series 101, 2002.

[3] 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.

[4] J.-M. Fontaine, Sur la construction du module de Dieudonné d'un groupe formel, C. R. Acad. Sci. Paris Sér. A-B 280 (1975), 1273–1276.

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

[6] M. Hazewinkel, Formal groups and applications, Pure Appl. Math. 78, Academic Press, New York, 1978.

[7] J. Lubin and J. Tate, Formal moduli for one-parameter formal Lie group, Bull. Soc. Math. France 94 (1966), 49–60.

Department of Mathematics and Mechanics
St. Petersburg State University
Universitetski pr. 28, Staryj Petergof
198504 St. Petersburg
Russia

E-mail address: vasja@eu.spb.ru