

On the theory of commutative formal groups

By Taira HONDA

(Received Nov. 10, 1969)

The theory of (commutative) formal groups was initiated by M. Lazard and J. Dieudonné around 1954. Lazard [11], [12] studied commutative formal groups over an arbitrary commutative ring by treating the coefficients of power series explicitly. Whereas Dieudonné investigated formal groups over a field of characteristic $p > 0$ exclusively. He reduced in [4] the study of commutative formal groups over a perfect field of characteristic $p > 0$ to that of modules over a certain non-commutative ring, so-called Dieudonné modules, and obtained in [5] a complete classification of isogeny classes of commutative formal groups over an algebraically closed field of characteristic $p > 0$. Later Manin [16] studied isomorphism classes of simple formal groups. The study of one-dimensional formal groups over p -adic integer rings was begun by Lubin [13] and a number of interesting results were obtained by him and Tate.

In this paper we first construct a certain general family of commutative formal groups of arbitrary dimension over a p -adic integer ring. Over the ring $W(k)$ of Witt vectors over a perfect field of characteristic $p > 0$, this exhausts all the commutative formal groups. These are attached to a certain type of matrices with elements in the ring $W(k)_\sigma[[T]]$ of non-commutative power series, where σ is the Frobenius of $W(k)$, and homomorphisms of these formal groups are described in terms of matrices over $W(k)_\sigma[[T]]$. By reducing the coefficients of formal groups over $W(k) \bmod pW(k)$ we get formal groups over k . It is shown that all the commutative formal groups over k are obtained in this manner. Moreover homomorphisms of commutative formal groups over k are also described in terms of $W(k)_\sigma[[T]]$ -modules by lifting these homomorphisms to power series over $W(k)$. Thus we get the main results of Dieudonné [4] again by the method quite different from his. In [4] he used tools peculiar to characteristic $p > 0$ and his construction of formal groups was indirect, whereas in our method the relation between formal groups over $W(k)$ and those over k is transparent and the construction of formal groups is explicit and elementary.

We now explain briefly how to construct commutative formal groups over $W(k)$ in case of dimension one. Take an element u of $W(k)_\sigma[[T]]$ of the

form $p + \sum_{\nu=1}^{\infty} c_{\nu} T^{\nu}$ ($c_{\nu} \in W(k)$) and put $pu^{-1} = \sum_{\nu=0}^{\infty} b_{\nu} T^{\nu}$. The b_{ν} are elements of the fraction field of $W(k)$ and $b_0 = 1$. Form $f(x) = \sum_{\nu=0}^{\infty} b_{\nu} x^{\nu}$ and $F(x, y) = f^{-1}(f(x) + f(y))$. Then F is a formal group over $W(k)$. In some special case this fact can be proved by using the basic lemma of Lubin-Tate [14] (cf. [10]). In general case we have to adopt another idea. Any formal group over $W(k)$ is isomorphic to one obtained in this manner. Let v be another element of $W(k)_o[[T]]$ of the form mentioned above and let $g(x)$ and $G(x, y)$ be the corresponding power series and the formal group, respectively. It is known that any homomorphism of F to G is of the form $g^{-1}(cf(x))$ with $c \in W(k)$. We assert that $g^{-1}(cf(x))$ is in reality a homomorphism over $W(k)$, if and only if there is $t \in W(k)_o[[T]]$ such that $vc = tu$. All these results will be generalized and proved for an arbitrary dimension and for more general coefficient rings of characteristic 0 with discrete valuation.

Our results can be applied to construct and characterize formal groups over \mathbb{Z} corresponding to a certain type of Dirichlet series with matrix coefficients, thus generalizing the results of the last half of our previous paper [10]. In particular we get an interesting interpretation of the Dirichlet series obtained from a representation of Hecke operators in the space of cusp forms of dimension -2 with respect to a congruence unit group Γ_N of a maximal order of an indefinite quaternion algebra over \mathbb{Q} (Shimura [19]). There is an intimate connection between this Dirichlet series and a formal completion of the Jacobian J_N .

§1. Invariant differential forms on a formal group.

1.1. Let S be a ring. We denote by S^m the module consisting of all the column vectors of dimension m with components in S and by $M_m(S)$ the full matrix ring of order m with elements in S . I_m denotes the identity matrix of order m . For $a = {}^t(a_1, \dots, a_m) \in S^m$ we write a^{ν} for ${}^t(a_1^{\nu}, \dots, a_m^{\nu})$.

Let R be a commutative ring with the identity. Let x be the set of n variables x_1, \dots, x_n . We denote by $R[[x]]$ the ring of formal power series on x_1, \dots, x_n . For basic properties of $R[[x]]$ we refer to Bourbaki [3]. We shall often regard x as the column vector ${}^t(x_1, \dots, x_n)$ in $R[[x]]^n$. Let f and g be power series in $R[[x]]$. We shall say that f is congruent to g modulo degree r , $f \equiv g \pmod{\deg r}$, if f and g differ only in terms of total degree $\geq r$. Let I be a submodule of R . f is said to be congruent to g modulo I , $f \equiv g \pmod{I}$, if all the coefficients of $f - g$ belong to I . We shall write $f \equiv g \pmod{\deg r, \pmod{I}}$, if there are $\varphi, \psi \in R[[x]]$ such that $f - g = \varphi + \psi$, $\varphi \equiv 0 \pmod{\deg r}$ and $\psi \equiv 0 \pmod{I}$. These definitions extend to $R[[x]]^m$. If $f = {}^t(f_1, \dots, f_m)$ and

$g = {}^t(g_1, \dots, g_m)$ are elements of $R[[x]]^m$, $f \equiv g \pmod{*}$ will mean $f_i \equiv g_i \pmod{*}$ for $1 \leq i \leq m$. We write $R[[x]]_0^m = \{f \in R[[x]]^m \mid f \equiv 0 \pmod{\deg 1}\}$.

Let $x' = {}^t(x'_1, \dots, x'_m)$ be another set of variables. If $f(x') = {}^t(f_1(x'), \dots, f_l(x'))$ ($f_i(x') = f_i(x'_1, \dots, x'_m)$) is in $R[[x']]^l$ and $\varphi(x) = {}^t(\varphi_1(x), \dots, \varphi_m(x))$ is in $R[[x]]^m$, the power series $f_i(\varphi(x)) = f_i(\varphi_1(x), \dots, \varphi_m(x))$ is well-defined and ${}^t(f_1(\varphi(x)), \dots, f_l(\varphi(x)))$ is an element of $R[[x]]^l$. We denote it by $f(\varphi(x))$ or simply by $f \circ \varphi$, if there is no fear of ambiguity. Define the identity function i of $R[[x]]_0^m$ by $i(x) = x$. If $\varphi(x)$ is an element of $R[[x]]_0^m$ such that $\varphi(x) \equiv Px \pmod{\deg 2}$ with an invertible matrix P in $M_n(R)$, there is a unique element $\psi(x)$ in $R[[x]]_0^m$ satisfying $\varphi \circ \psi = \psi \circ \varphi = i$. We shall call this ψ the inverse function of φ and denote it by φ^{-1} .

We adopt the classical definition of formal group.

DEFINITION. Let x and y be sets (or vectors) of n variables. An n -dimensional formal group over R is an element $F(x, y)$ of $R[[x, y]]_0^n$ satisfying:

- i) $F(x, y) \equiv x + y \pmod{\deg 2}$,
- ii) $F(F(x, y), z) = F(x, F(y, z))$.

If F satisfies $F(x, y) = F(y, x)$ moreover, F is said to be commutative.

It follows from (i) that there is a unique $i_F(x) \in R[[x]]_0^n$ such that $F(x, i_F(x)) = F(i_F(x), x) = 0$. Part (ii) shows that $F(x, 0) = x$ and $F(0, y) = y$.

DEFINITION. Let F and G be formal groups over R , of dimension n and m , respectively. An element φ of $R[[x]]_0^m$, where $x = {}^t(x_1, \dots, x_n)$, is said to be a homomorphism of F to G , if φ satisfies $\varphi \circ F = G \circ \varphi$, where $(G \circ \varphi)(x, y)$ stands for $G(\varphi(x), \varphi(y))$. If $m = n$ and φ is invertible, φ^{-1} is also a homomorphism of G to F . Such φ is called an isomorphism and G is said to be (weakly) isomorphic to F , $\varphi: F \sim G$ over R . If there is an isomorphism φ of F to G such that $\varphi(x) \equiv x \pmod{\deg 2}$, we shall say that G is strongly isomorphic to F and write $\varphi: F \approx G$ over R .

If G is commutative, the set $\text{Hom}_R(F, G)$ of all homomorphisms of F to G over R forms a module by defining $(\varphi_1 + \varphi_2)(x) = G(\varphi_1(x), \varphi_2(x))$ for $\varphi_1, \varphi_2 \in \text{Hom}_R(F, G)$. In particular $\text{End}_R G (= \text{Hom}_R(G, G))$ becomes a ring by defining the multiplication by composition of functions.

1.2. Let $A = R[[x]]$ be as in 1.1. We denote by $\mathfrak{D}(A; R)$ the space of derivations of A over R . It is a free left A -module with a base D_1, \dots, D_n , where $D_i = \partial/\partial x_i$ (cf. [3]). Denote by $\mathfrak{D}^*(A; R)$ the dual A -module of $\mathfrak{D}(A; R)$, the space of differentials of A over R . For $f \in A$ the map $D \mapsto Df$ of $\mathfrak{D}(A; R)$ into A defines a differential, which we denote by df . A differential of this form is called exact. It is well-known that $dx = {}^t(dx_1, \dots, dx_n)$ is an A -base of $\mathfrak{D}^*(A; R)$ and $df = \sum_{i=1}^n (D_i f) dx_i$ for any $f \in A$.

Let $B = R[[x']]$ be another ring of power series on m variables and let $\omega = \sum_{j=1}^m \phi_j(x') dx'_j$ be a differential in $\mathfrak{D}^*(B; R)$. If $\varphi \in R[[x]]^m$, $\sum_{j=1}^m \phi_j(\varphi(x)) d\varphi_j(x)$ is a differential in $\mathfrak{D}^*(A; R)$. We denote it by $\varphi^*(\omega)$. φ^* is an R -homomorphism of $\mathfrak{D}^*(B; R)$ into $\mathfrak{D}^*(A; R)$.

Let F be an n -dimensional formal group over R . Introducing a new set $t = (t_1, \dots, t_n)$ of variables we may consider that F is also defined over $R_t = R[[t]]$.

DEFINITION. The *right translation* T_t on F is an element of $R_t[[x]]^m$ defined by $T_t(x) = F(x, t)$. A differential ω in $\mathfrak{D}^*(A; R)$ is said to be a *right invariant differential* on F if $T_t^*(\omega) = \omega$.

We denote by $\mathfrak{D}^*(F; R)$ the space consisting of all right invariant differentials on F . As in the case of a Lie group or an algebraic group, we have:

PROPOSITION 1.1. *If F is an n -dimensional formal group over R , $\mathfrak{D}^*(F; R)$ is a free R -module of rank n . More precisely, $(\phi_{ij}(z))$ denoting the inverse matrix of $((\partial/\partial x_j)F_i(0, z))$, we have $\phi_{ij}(0) = \delta_{ij}$ and $\omega_i = \sum_{j=1}^n \phi_{ij}(x) dx_j$ ($1 \leq i \leq n$) form an R -basis of $\mathfrak{D}^*(F; R)$. Moreover the base $\{\omega_1, \dots, \omega_n\}$ is characterized by these two properties.*

PROOF. Differentiating $F_i(u, F(v, w)) = F_i(F(u, v), w)$ relative to u_j , we get

$$(\partial/\partial x_j)F_i(u, F(v, w)) = \sum_{k=1}^n (\partial/\partial x_k)F_i(F(u, v), w)(\partial/\partial x_j)F_k(u, v),$$

so that

$$(\partial/\partial x_j)F_i(0, F(v, w)) = \sum_{k=1}^n (\partial/\partial x_k)F_i(v, w)(\partial/\partial x_j)F_k(0, v)$$

or by matrix notation

$$(1.1) \quad ((\partial/\partial x_j)F_i(0, F(v, w))) = ((\partial/\partial x_j)F_i(v, w))((\partial/\partial x_j)F_k(0, v)).$$

Since $(\partial/\partial x_j)F_i(0, z) \equiv \delta_{ij} \pmod{\deg 1}$, the matrix $((\partial/\partial x_j)F_i(0, z))$ is invertible, $\phi_{ij}(z) \in R[[z]]$ and $\phi_{ij}(0) = \delta_{ij}$. Hence (1.1) is equivalent to

$$(1.2) \quad (T_t \phi_{ij}(z))((\partial/\partial x_j)F_i(z, t)) = (\phi_{ij}(z)).$$

Now a differential $\omega = \sum_{i=1}^n \phi_i(x) dx_i$ in $\mathfrak{D}^*(A; R)$ is right invariant on F , if and only if

$$(1.3) \quad \phi_j(x) = \sum_{k=1}^n \phi_k(F(x, t))(\partial/\partial x_j)F_k(x, t).$$

This shows $\omega_1, \dots, \omega_n \in \mathfrak{D}^*(F; R)$ by (1.2). On the other hand we get from (1.3)

$$\phi_j(0) = \sum_{k=1}^n \phi_k(t)(\partial/\partial x_j)F_k(0, t),$$

which implies that, if $\omega \in \mathfrak{D}^*(F; R)$, $\omega = 0 \Leftrightarrow \phi_i(0) = 0$ for $1 \leq i \leq n$. Therefore the map $\Phi: \omega \mapsto (\phi_1(0), \dots, \phi_n(0))$ defines an R -isomorphism of $\mathfrak{D}^*(F; R)$ into R^n . Since the $\Phi(\omega_i)$ ($1 \leq i \leq n$) are the unit vectors of R^n , the map Φ is surjective and $\{\omega_1, \dots, \omega_n\}$ is a base of $\mathfrak{D}^*(F; R)$.

We shall call this $\{\omega_1, \dots, \omega_n\}$ the *canonical base* of $\mathfrak{D}^*(F; R)$.

PROPOSITION 1.2. *Let F, G be formal groups over R and $\varphi \in \text{Hom}_R(F, G)$. If $\eta \in \mathfrak{D}^*(G; R)$, then $\varphi^*(\eta) \in \mathfrak{D}^*(F; R)$.*

PROOF. Write $\eta = \sum_{i=1}^m \phi_i(x') dx'_i$ where m is the dimension of G . Then

$$\begin{aligned} T_i(\varphi^*(\eta)) &= T_i\left(\sum_{i=1}^m \phi_i(\varphi(x)) d\varphi_i(x)\right) \\ &= \sum_{i=1}^m \phi_i(\varphi(F(x, t))) d\varphi_i(F(x, t)) \\ &= \sum_{i=1}^m \phi_i(G(\varphi(x), \varphi(t))) dG(\varphi_i(x), \varphi_i(t)) \\ &= \sum_{i=1}^m \phi_i(\varphi(x)) d\varphi_i(x) \\ &= \varphi^*(\eta). \end{aligned}$$

1.3. We now study invariant differential forms on a commutative formal group.

PROPOSITION 1.3. *Let F be a commutative formal group over R . Then every differential in $\mathfrak{D}^*(F; R)$ is closed.*

PROOF. Let $\omega_i = \sum_{j=1}^n \phi_{ij}(x) dx_j$ ($1 \leq i \leq n$) be the canonical base of $\mathfrak{D}^*(F; R)$. We shall prove $d\omega_i = 0$ for $1 \leq i \leq n$. First $d\omega_i$ is a right invariant 2-form, since

$$\begin{aligned} T_i^*(d\omega_i) &= T_i^*\left(\sum_{j=1}^n d\phi_{ij}(x) \wedge dx_j\right) \\ &= \sum_j d\phi_{ij}(F(x, t)) \wedge dF_j(x, t) \\ &= d(T_i^*(\omega_i)) \\ &= d\omega_i. \end{aligned}$$

Now differentiating

$$\sum_{k=1}^n (\partial/\partial x_k) F_i(0, z) \phi_{kj}(z) = \delta_{ij}$$

relative to z_l and putting $z = 0$, we get

$$\sum_k (\partial^2/\partial x_k \partial y_l) F_i(0, 0) \phi_{kj}(0) + \sum_k (\partial/\partial x_k) F_i(0, 0) (\partial/\partial x_l) \phi_{kj}(0) = 0,$$

which is reduced to

$$(\partial^2/\partial x_j \partial y_l)F_i(0, 0) + (\partial/\partial x_l)\phi_{ij}(0) = 0,$$

since

$$\phi_{kj}(0) = \delta_{kj} \quad \text{and} \quad (\partial/\partial x_k)F_i(0, 0) = \delta_{ik}.$$

Hence, by the commutativity of F we get

$$\begin{aligned} (\partial/\partial x_l)\phi_{ij}(0) &= -(\partial^2/\partial x_j \partial y_l)F_i(0, 0) \\ &= -(\partial^2/\partial x_l \partial y_j)F_i(0, 0) \\ &= (\partial/\partial x_j)\phi_{il}(0). \end{aligned}$$

Since

$$\begin{aligned} d\omega_i &= \sum_{j,l} (\partial/\partial x_l)\phi_{ij}(x) dx_l \wedge dx_j \\ &= \sum_{j < l} ((\partial/\partial x_l)\phi_{ij}(x) - (\partial/\partial x_j)\phi_{il}(x)) dx_l \wedge dx_j, \end{aligned}$$

the coefficients of $dx_l \wedge dx_j$ in $d\omega_i$ have no constant term. So we have only to prove that, if $\eta = \sum_{i < j} \lambda_{ij}(x) dx_i \wedge dx_j$ is right invariant on F and $\lambda_{ij}(0) = 0$ for all $1 \leq i < j \leq n$, η must be equal to 0. An easy computation shows that $T_i^*(\eta) = \eta$ is equivalent to

$$\lambda_{ki}(x) = \sum_{i < j} \lambda_{ij}(F(x, t)) \begin{vmatrix} (\partial/\partial x_k)F_i(x, t) & (\partial/\partial x_l)F_i(x, t) \\ (\partial/\partial x_k)F_j(x, t) & (\partial/\partial x_l)F_j(x, t) \end{vmatrix},$$

which implies

$$\lambda_{ki}(0) = \sum_{i < j} \lambda_{ij}(t) \begin{vmatrix} (\partial/\partial x_k)F_i(0, t) & (\partial/\partial x_l)F_i(0, t) \\ (\partial/\partial x_k)F_j(0, t) & (\partial/\partial x_l)F_j(0, t) \end{vmatrix}$$

for $1 \leq k < l \leq n$. Since the matrix $((\partial/\partial x_j)F_i(0, t))$ is regular, this shows in fact $\lambda_{ij}(0) = 0$ for all $i < j \Rightarrow \lambda_{ij}(t) = 0$ for all $i < j$.

We now consider the case where R is a \mathbf{Q} -algebra. In this case every power series in $R[[x]]$ is termwise integrable with respect to x_i . The following lemma is essentially well-known in elementary analysis and the proof is easy.

LEMMA 1.4. *If R is a \mathbf{Q} -algebra, a closed differential in $\mathfrak{D}^*(A; R)$ is exact.*

The following theorem, mentioned in [10], was also proved in [7] in a slightly different manner.

THEOREM 1. *Let F be an n -dimensional commutative formal group over a \mathbf{Q} -algebra R and let $\omega = {}^t(\omega_1, \dots, \omega_n)$ be the canonical base of $\mathfrak{D}^*(F; R)$. Then there exists a unique element f of $R[[x]]_0^{\mathfrak{g}}$ such that $\omega = df$. This f satisfies*

$$f(x) \equiv x \pmod{\text{deg } 2}$$

and

$$F(x, y) = f^{-1}(f(x) + f(y)).$$

In particular $F(x, y) \approx x + y$ over R .

PROOF. The existence of f follows from Proposition 1.3 and Lemma 1.4. The uniqueness follows from the fact that $d\varphi=0$ for $\varphi \in R[[x]]$, if and only if φ is a constant. Since $\phi_{ij}(0)=\delta_{ij}$, we have $f(x)\equiv x \pmod{\text{deg } 2}$. Now, $df(x)$ being right invariant, we have

$$df(F(x, t))=df(x),$$

which implies

$$f(F(x, t))-f(x) \in R[[t]].$$

Writing $g(t)=f(F(x, t))-f(x)$ and putting $x=0$ we get

$$g(t)=f(t).$$

Thus we have

$$f(F(x, t))=f(x)+f(t)$$

or

$$F(x, t)=f^{-1}(f(x)+f(t)).$$

This completes the proof of our theorem.

1.4. Let R be an integral domain of characteristic 0 and K its fraction field.

LEMMA 1.5. Let $x={}^t(x_1, \dots, x_n)$ and $y={}^t(y_1, \dots, y_n)$ be sets of n variables. If $\phi \in K[[x]]^m$ satisfies

$$\phi(x+y)=\phi(x)+\phi(y),$$

ϕ must be linear, i. e. there is an $m \times n$ matrix C over K such that $\phi(x)=Cx$.

PROOF. We have only to consider the case where $m=1$ and ϕ is a homogeneous polynomial. Then our assertion is verified by a simple computation. (See the proof of Lemma 3.2).

Let F be a commutative formal group over R , of dimension n . By Theorem 1 there is $f(x) \in K[[x]]_0^n$ such that $f \equiv i \pmod{\text{deg } 2}$ and $F(x, y)=f^{-1}(f(x)+f(y))$. If there is another element h of $K[[x]]_0^n$ satisfying $h \equiv i \pmod{\text{deg } 2}$ and $F(x, y)=h^{-1}(h(x)+h(y))$, we have

$$f \circ h^{-1} \equiv i \pmod{\text{deg } 2},$$

$$(f \circ h^{-1})(x+y)=(f \circ h^{-1})(x)+(f \circ h^{-1})(y).$$

Hence we get $f \circ h^{-1}=i$ or $f=h$ by Lemma 1.5.

DEFINITION. Let R and K be as above; let F be an n -dimensional commutative formal group over R . The unique element f of $K[[x]]_0^n$, such that $f \equiv i \pmod{\text{deg } 2}$ and $F(x, y)=f^{-1}(f(x)+f(y))$, is called the *transformer* of F .

Let G be another commutative formal group over R , of dimension m and with the transformer g . If $\varphi \in \text{Hom}_R(F, G)$, we have

$$\varphi(f^{-1}(f(x)+f(y)))=g^{-1}(g(\varphi(x))+g(\varphi(y))).$$

Substituting x, y by $f^{-1}(x), f^{-1}(y)$, respectively, we get

$$(g \circ \varphi \circ f^{-1})(x+y)=(g \circ \varphi \circ f^{-1})(x)+(g \circ \varphi \circ f^{-1})(y).$$

Hence by Lemma 1.5 there is an $m \times n$ matrix C over K such that $(g \circ \varphi \circ f^{-1})(x) = Cx$. This implies $\varphi(x) = g^{-1}(Cf(x))$. As $\varphi(x) \equiv Cx \pmod{\text{deg } 2}$, C is a matrix with elements in R .

PROPOSITION 1.6. *Let F, f, G, g be as above. Every element φ of $\text{Hom}_R(F, G)$ has the form $g^{-1} \circ (Cf)$, where C is an $m \times n$ matrix over R . Conversely, C being an $m \times n$ matrix over R , $g^{-1} \circ (Cf) \in \text{Hom}_R(F, G)$, if and only if $g^{-1} \circ (Cf)$ has coefficients in R . The map $\varphi \rightarrow C$ yields an isomorphism of $\text{Hom}_R(F, G)$ into the module of $m \times n$ matrices over R . If $F = G$ in particular, this map is a ring isomorphism of $\text{End}_R F$ into $M_n(R)$.*

PROOF. The first assertion has already been proved. The second follows from

$$(g^{-1} \circ (Cf)) \circ F = G \circ (g^{-1} \circ (Cf)).$$

The rests follow from the definitions.

§ 2. Formal groups over a p -adic integer ring.

Throughout the rest of this paper we exclusively deal with commutative formal groups. By a formal group we always mean a commutative one.

Let K be a discrete valuation field of characteristic 0 and let \mathfrak{o} and \mathfrak{p} be the ring of integers in K and the maximal ideal of \mathfrak{o} , respectively. We assume that the residue class field $k = \mathfrak{o}/\mathfrak{p}$ is of characteristic $p > 0$. Consider the following condition on K :

(F) There are an endomorphism σ of K and a power q of p such that

$$\alpha^\sigma \equiv \alpha^q \pmod{\mathfrak{p}} \quad \text{for any } \alpha \in \mathfrak{o}.$$

We note $\mathfrak{p}^\sigma = \mathfrak{p}$, since σ sends a unit of \mathfrak{o} to \mathfrak{o} and $p^\sigma = p$. In this section we study formal groups over \mathfrak{o} , when K satisfies (F). We do not assume the completeness of K .

Let K_0 be a finite extension of the p -adic number field \mathbf{Q}_p and let q be the cardinal of its residue field. Then it is well-known that an unramified extension of K_0 (of finite or infinite degree) or its completion satisfies (F) with a Frobenius σ .

2.1. Let $K_\sigma[[T]]$ be the non-commutative power series ring on T with the multiplication rule: $T\alpha = \alpha^\sigma T$ for $\alpha \in K$. We denote by $\mathfrak{B}_{m,n}$ (resp. $\mathfrak{A}_{m,n}$) the module consisting of all $m \times n$ matrices over $K_\sigma[[T]]$ (resp. $\mathfrak{o}_\sigma[[T]]$).

Let $x = {}^t(x_1, \dots, x_n)$ be a set of n variables. For $f \in K[[x]]_0^m$ and $u = \sum_{\nu=0}^{\infty} C_\nu T^\nu \in \mathfrak{B}_{l,m}$ (where the C_ν are matrices over K), we define an element $u * f$ of $K[[x]]_0^l$ by

$$(u * f)(x) = \sum_{\nu=0}^{\infty} C_\nu f^{\sigma^\nu}(x^{q^\nu}).$$

This is well-defined, since $f(x)$ has no constant term. If $v = \sum_{\nu=0}^{\infty} D_{\nu}T^{\nu}$ is in $\mathfrak{B}_{k,l}$, we have

$$(2.1) \quad (vu) * f = v * (u * f),$$

since

$$\begin{aligned} (v * (u * f))(x) &= \sum_{\nu=0}^{\infty} D_{\nu} \sum_{\mu=0}^{\infty} C_{\mu}^{\sigma^{\nu}} f^{\sigma^{\mu+\nu}}(x^{q^{\mu+\nu}}) \\ &= \sum_{\lambda=0}^{\infty} \sum_{\mu+\nu=\lambda} D_{\nu} C_{\mu}^{\sigma^{\nu}} f^{\sigma^{\lambda}}(x^{q^{\lambda}}) \\ &= ((vu) * f)(x). \end{aligned}$$

From now on we fix a prime element π of \mathfrak{o} .

LEMMA 2.1. For any rational integers $\nu \geq 0$, $a \geq 1$ and $m \geq 1$ we have

$$\pi^{-\nu}(X + \pi Y)^{m p^{a\nu}} \equiv \pi^{-\nu} X^{m p^{a\nu}} \pmod{\mathfrak{p}}.$$

In particular we have

$$m^{-1}(X + pY)^m \equiv m^{-1}X^m \pmod{pZ_p}$$

for $m \geq 1$.

This is Lemma 4 of [10]. As the proof is elementary and easy, we omit it here.

We write \mathfrak{A}_n (resp. \mathfrak{B}_n) for $\mathfrak{A}_{n,n}$ (resp. $\mathfrak{B}_{n,n}$).

DEFINITION. An element u of \mathfrak{A}_n is said to be *special*, if $u \equiv \pi I_n \pmod{\text{deg } 1}$. Let P be an invertible matrix in $M_n(\mathfrak{o})$ and let u be a special element of \mathfrak{A}_n . An element f of $K[[x]]^{\#}$ is said to be of *type* $(P; u)$, if f satisfies the following two conditions:

- i) $f(x) \equiv Px \pmod{\text{deg } 2}$,
- ii) $(u * f)(x) \equiv 0 \pmod{\mathfrak{p}}$.

If f is of type $(I_n; u)$, we shall simply say that f is of *type* u .

Let $u \in \mathfrak{A}_n$ be special and put $w = u^{-1}\pi (\in \mathfrak{B}_n)$. Then, i being the identity function,

$$(u * (w * i))(x) = ((uw) * i)(x) = \pi x \equiv 0 \pmod{\mathfrak{p}}.$$

This implies that $(u^{-1}\pi) * i$ is of type u .

LEMMA 2.2. Let $u \in \mathfrak{A}_n$ be special and put $u^{-1}\pi = I_n + \sum_{\nu=1}^{\infty} B_{\nu}T^{\nu}$. Then we have $\pi^{\nu}B_{\nu} \in M_n(\mathfrak{o})$ for $\nu \geq 0$.

PROOF. Write $u = \pi I_n + \sum_{\nu=1}^{\infty} C_{\nu}T^{\nu}$ and replace T by πT in the equality

$$\left(\pi I_n + \sum_{\nu=1}^{\infty} C_{\nu}T^{\nu} \right) \left(I_n + \sum_{\nu=1}^{\infty} B_{\nu}T^{\nu} \right) = \pi I_n.$$

Then we get

$$\left(I_n + \sum_{\nu=1}^{\infty} \pi^{\sigma+\dots+\sigma^{\nu-1}} C_{\nu} T^{\nu}\right) \left(I_n + \sum_{\nu=1}^{\infty} \pi^{1+\sigma+\dots+\sigma^{\nu-1}} B_{\nu} T^{\nu}\right) = I_n.$$

This implies $\pi^{\nu} B_{\nu} \in M_n(0)$, since $\pi^{\sigma^{\mu}}$ is also a prime element of \mathfrak{o} .

2.2. The following two lemmas play crucial roles in our further investigation and will be used repeatedly.

LEMMA 2.3. *Let $f \in K[[x]]_{\mathfrak{o}}^n$ be of type $(P; u)$ and let v be an element of $\mathfrak{A}_{m,n}$. Let ϕ be an element of $K[[x']]_{\mathfrak{o}}^n$, x' being a finite set of variables. If the coefficients (of components) of ϕ , of terms of (total) degree $\leq r-1$, belong to \mathfrak{o} for some $r \geq 2$, we have*

$$v*(f \circ \phi) \equiv (v*f) \circ \phi \pmod{\deg(r+1), \text{ mod } \mathfrak{p}}.$$

If $\phi \in \mathfrak{o}[[x']]_{\mathfrak{o}}^n$ in particular, we have

$$v*(f \circ \phi) \equiv (v*f) \circ \phi \pmod{\mathfrak{p}}.$$

LEMMA 2.4. *If f (resp. g) $\in K[[x]]_{\mathfrak{o}}^n$ is of type $(P; u)$ (resp. of type $(Q; u)$), then $g^{-1} \circ f \in \mathfrak{o}[[x]]_{\mathfrak{o}}^n$.*

Put $h = (u^{-1}\pi)*i$. First we will prove the first assertion of Lemma 2.3 for $f=h$. Write

$$u^{-1}\pi = I_n + \sum_{\nu=1}^{\infty} B_{\nu} T^{\nu}, \quad v = \sum_{\nu=0}^{\infty} A_{\nu} T^{\nu}.$$

We have

$$\begin{aligned} (2.2) \quad ((v*h) \circ \phi)(x') &= (((vu^{-1}\pi)*i) \circ \phi)(x') \\ &= \sum_{\mu, \nu} A_{\nu} B_{\mu}^{\sigma^{\nu}} \phi(x')^{q^{\mu+\nu}}. \end{aligned}$$

Now

$$(2.3) \quad B_{\mu}^{\sigma^{\nu}} \phi(x')^{q^{\mu+\nu}} = \pi^{\mu} B_{\mu}^{\sigma^{\nu}} \pi^{-\mu} \phi(x')^{q^{\mu+\nu}}$$

and $\pi^{\mu} B_{\mu}^{\sigma^{\nu}} \in M_n(0)$ by Lemma 2.2. We will prove

$$(2.4) \quad \pi^{-\mu} \phi(x')^{q^{\mu+\nu}} \equiv \pi^{-\mu} (\phi^{\sigma^{\nu}}(x'^{q^{\nu}}))^{q^{\mu}} \pmod{\deg(r+1), \text{ mod } \mathfrak{p}}.$$

If $\mu = \nu = 0$, (2.4) is trivial. If $\mu = 0$ and $\nu \geq 1$, we have

$$\phi(x')^{q^{\nu}} \equiv \phi^{\sigma^{\nu}}(x'^{q^{\nu}}) \pmod{\deg(r+1), \text{ mod } \mathfrak{p}},$$

since terms of ϕ of degree $\geq r$ do not affect this congruence. (Note $\phi(0) = 0$.)

Assume $\mu \geq 1$. Because

$$\phi(x')^{q^{\nu}} \equiv \phi^{\sigma^{\nu}}(x'^{q^{\nu}}) \pmod{\deg r, \text{ mod } \mathfrak{p}},$$

we get (2.4) by Lemma 2.1 and by the fact $\phi(0) = 0$. This completes the proof of (2.4). Thus we get from (2.2), (2.3) and (2.4)

$$\begin{aligned} ((v*h) \circ \phi)(x') &\equiv \sum_{\mu, \nu} A_{\nu} B_{\mu}^{\sigma^{\nu}} (\phi^{\sigma^{\nu}}(x'^{q^{\nu}}))^{q^{\mu}} \pmod{\deg(r+1), \text{ mod } \mathfrak{p}} \\ &= (v*(h \circ \phi))(x'). \end{aligned}$$

PROOF OF LEMMA 2.4. Since $g^{-1} \circ f = (g^{-1} \circ h) \circ (h^{-1} \circ f) = (h^{-1} \circ g)^{-1} \circ (h^{-1} \circ f)$ and $(h^{-1} \circ g)(x) \equiv Qx \pmod{\text{deg } 2}$, we have only to prove $h^{-1} \circ f \in \mathfrak{o}[[x]]_{\mathfrak{p}}^{\#}$. Put $h^{-1} \circ f = \varphi$ or $f = h \circ \varphi$. The first-degree coefficients of φ are in \mathfrak{o} . Assume that the coefficients of φ , of (total) degree $\leq r-1$, are integers for some $r \geq 2$. By Lemma 2.3 for $f = h$ we have

$$\begin{aligned} \pi\varphi &= (u * h) \circ \varphi \equiv u * (h \circ \varphi) \pmod{\text{deg } (r+1), \text{ mod } \mathfrak{p}} \\ &= u * f \equiv 0 \pmod{\mathfrak{p}}. \end{aligned}$$

This implies that the r -th degree coefficients of φ are also integers. This completes our proof by induction.

PROOF OF LEMMA 2.3. We have only to prove the first assertion. Notations being as above,

$$\begin{aligned} v * (f \circ \phi) &= v * ((h \circ \varphi) \circ \phi) = v * (h \circ (\varphi \circ \phi)) \\ &\equiv (v * h) \circ (\varphi \circ \phi) \pmod{\text{deg } (r+1), \text{ mod } \mathfrak{p}} \\ &= ((v * h) \circ \varphi) \circ \phi. \end{aligned}$$

Since $\varphi(x) \equiv Px \pmod{\text{deg } 2}$, we have

$$((v * h) \circ \varphi)(x) \equiv A_0 Px \equiv (v * (h \circ \varphi))(x) \pmod{\text{deg } 2}.$$

Put $\lambda_1(x) = ((v * h) \circ \varphi)(x) - A_0 Px$ and $\lambda_2(x) = (v * (h \circ \varphi))(x) - A_0 Px$. Then $\lambda_1 \equiv \lambda_2 \equiv 0 \pmod{\text{deg } 2}$ and $\lambda_1 \equiv \lambda_2 \pmod{\mathfrak{p}}$ by what we have proved. It follows from this

$$\lambda_1 \circ \phi \equiv \lambda_2 \circ \phi \pmod{\text{deg } (r+1), \text{ mod } \mathfrak{p}},$$

since the terms of ϕ of degree r do not affect this congruence. Hence we get

$$\begin{aligned} v * (f \circ \phi) &\equiv ((v * h) \circ \varphi) \circ \phi \pmod{\text{deg } (r+1), \text{ mod } \mathfrak{p}} \\ &= A_0 P\phi + \lambda_1 \circ \phi \\ &\equiv A_0 P\phi + \lambda_2 \circ \phi \pmod{\text{deg } (r+1), \text{ mod } \mathfrak{p}} \\ &= (v * (h \circ \varphi)) \circ \phi \\ &= (v * f) \circ \phi. \end{aligned}$$

This completes the proof of our lemma.

2.3. The results of 2.2 first allow us to construct certain formal groups over \mathfrak{o} .

THEOREM 2. Assume K satisfies (F). Let P be an invertible matrix in $M_n(\mathfrak{o})$ and let u be a special element of \mathfrak{A}_n . If $f \in K[[x]]_{\mathfrak{p}}^{\#}$ is of type $(P; u)$, $F(x, y) = f^{-1}(f(x) + f(y))$ is a formal group over \mathfrak{o} . Let $g \in K[[x]]_{\mathfrak{p}}^{\#}$ be of type $(Q; u)$ for an invertible matrix Q and put $G(x, y) = g^{-1}(g(x) + g(y))$. Then we have $G \sim F$ over \mathfrak{o} . If $P = Q$ in particular, we have $G \approx F$ over \mathfrak{o} .

PROOF. Form $h = (u^{-1}\pi) * i$ and $H(x, y) = h^{-1}(h(x) + h(y))$. It is clear that

$$H(x, y) \equiv x + y \pmod{\deg 2}.$$

Assume that the coefficients of H , of terms of degree $\leq r-1$, are integers for some $r \geq 2$. By Lemma 2.3 we have

$$\begin{aligned} \pi H(x, y) &= ((u * h) \circ H)(x, y) \\ &\equiv (u * (h \circ H))(x, y) \pmod{\deg(r+1), \text{ mod } \mathfrak{p}} \\ &= (u * h)(x) + (u * h)(y) \\ &= \pi x + \pi y \equiv 0 \pmod{\mathfrak{p}}. \end{aligned}$$

This implies that the r -th degree coefficients of H are also integers. This proves $H(x, y) \in \mathfrak{o}[[x, y]]$ by induction. All the assertions of our theorem follow from this and from Lemma 2.4, because $F = \varphi^{-1} \circ H \circ \varphi$ if $f = h \circ \varphi$.

As for examples, see § 5.

PROPOSITION 2.5. *Let P be an invertible matrix in $M_n(\mathfrak{o})$ and let u be a special element of \mathfrak{A}_n . Then $f \in K[[x]]^n$ is of type $(P; u)$, if and only if f is of the form $((u^{-1}\pi) * i) \circ \varphi$ with $\varphi \in \mathfrak{o}[[x]]^n$ such that $\varphi(x) \equiv Px \pmod{\deg 2}$.*

PROOF. "Only if" part is Lemma 2.4. Conversely, if $\varphi \in \mathfrak{o}[[x]]^n$ and $\varphi(x) \equiv Px \pmod{\deg 2}$, we have, writing $h = (u^{-1}\pi) * i$,

$$(h \circ \varphi)(x) \equiv Px \pmod{\deg 2}$$

and by Lemma 2.3

$$u * (h \circ \varphi) \equiv (u * h) \circ \varphi = \pi \varphi \equiv 0 \pmod{\mathfrak{p}}.$$

This completes our proof.

Dually to Proposition 2.5 we have

PROPOSITION 2.6. *Let $f \in K[[x]]^n$ be of type $(P; u)$ for an invertible matrix P of $M_n(\mathfrak{o})$ and a special element u of \mathfrak{A}_n ; Let v be a matrix in $\mathfrak{A}_{m,n}$. Then*

$$v * f \equiv 0 \pmod{\mathfrak{p}},$$

if and only if there exists $t \in \mathfrak{A}_{m,n}$ such that $v = tu$.

PROOF. If $v = tu$ with $t \in \mathfrak{A}_{m,n}$, then

$$v * f = t * (u * f) \equiv 0 \pmod{\mathfrak{p}}.$$

Conversely, assume $v * f \equiv 0 \pmod{\mathfrak{p}}$ for $v \in \mathfrak{A}_{m,n}$. Put $h = (u^{-1}\pi) * i$ and $\varphi = h^{-1} \circ f$. Since φ is an invertible element of $\mathfrak{o}[[x]]^n$ by Lemma 2.4, we have

$$(v * h) \circ \varphi \equiv v * (h \circ \varphi) = v * f \equiv 0 \pmod{\mathfrak{p}}$$

by Lemma 2.3, so that

$$(2.5) \quad v * h = ((v * h) \circ \varphi) \circ \varphi^{-1} \equiv 0 \pmod{\mathfrak{p}}.$$

Put $vu^{-1}\pi = \sum_{\nu=0}^{\infty} A_{\nu} T^{\nu}$. Since

$$v * h = v * ((u^{-1}\pi) * i) = (vu^{-1}\pi) * i,$$

we have from (2.5)

$$\sum_{\nu=0}^{\infty} A_{\nu} x^{q^{\nu}} \equiv 0 \pmod{\mathfrak{p}},$$

which implies $vu^{-1} = (vu^{-1}\pi)\pi^{-1} \in \mathfrak{A}_{m,n}$. This completes our proof.

2.4. We now study homomorphisms of formal groups constructed in Theorem 2. $M_{m,n}(\mathfrak{o})$ denotes the module of all the $m \times n$ matrices with elements in \mathfrak{o} .

THEOREM 3. Assume K satisfies (F). Let $u \in \mathfrak{A}_n$ and $v \in \mathfrak{A}_m$ be special and let $f \in K[[x]]_{\mathfrak{o}}^n$ (resp. $g \in K[[x]]_{\mathfrak{o}}^m$) be of type u (resp. of type v). Form $F(x, y) = f^{-1}(f(x) + f(y))$ and $G(x, y) = g^{-1}(g(x) + g(y))$. Then $g^{-1} \circ (Cf) \in \text{Hom}_{\mathfrak{o}}(F, G)$ for $C \in M_{m,n}(\mathfrak{o})$, if and only if there exists $t \in \mathfrak{A}_{m,n}$ such that $vC = tu$.

PROOF. Put $\varphi = g^{-1} \circ (Cf)$. By Proposition 1.6 $\varphi \in \text{Hom}_{\mathfrak{o}}(F, G)$ if and only if $\varphi \in \mathfrak{o}[[x]]_{\mathfrak{o}}^m$. In view of Lemma 2.4 we may assume $f = (u^{-1}\pi) * i$ and $g = (v^{-1}\pi) * i$. If $\varphi \in \mathfrak{o}[[x]]_{\mathfrak{o}}^m$, we have by Lemma 2.3

$$\begin{aligned} (vC) * f &= v * (Cf) = v * (g \circ \varphi) \\ &\equiv (v * g) \circ \varphi = \pi \varphi \equiv 0 \pmod{\mathfrak{p}}. \end{aligned}$$

Hence, by Proposition 2.6, there exists $t \in \mathfrak{A}_{m,n}$ such that $vC = tu$. Conversely, suppose that there is $t \in \mathfrak{A}_{m,n}$ such that $vC = tu$. As $\varphi(x) \equiv Cx \pmod{\text{deg } 2}$, the first-degree coefficients of φ are integral. Assume that i -th degree coefficients of φ are integral for $i \leq r-1$ ($r \geq 2$). By Lemma 2.3 we have then

$$\begin{aligned} \pi \varphi &= (v * g) \circ \varphi \\ &\equiv v * (g \circ \varphi) \pmod{\text{deg } (r+1), \pmod{\mathfrak{p}}} \\ &= v * (Cf) = (vC) * f \\ &= (tu) * f = t * (u * f) \\ &\equiv 0 \pmod{\mathfrak{p}}. \end{aligned}$$

This shows that the r -th degree coefficients of φ are integral. Hence we get $\varphi \in \mathfrak{o}[[x]]_{\mathfrak{o}}^m$ by induction.

COROLLARY. Let F, G be as in Theorem 3. The module $\text{Hom}_{\mathfrak{o}}(F, G)$ is canonically isomorphic to $M_{m,n}(\mathfrak{o}) \cap v^{-1}\mathfrak{A}_{m,n}u$.

By Theorem 3 $g^{-1} \circ (Cf) \in \text{Hom}_{\mathfrak{o}}(F, G)$ for $C \in M_{m,n}(\mathfrak{o})$, if and only if $C \in v^{-1}\mathfrak{A}_{m,n}u$. Our assertion follows from this and from Proposition 1.6.

§ 3. The non-ramified case.

Let $K, \mathfrak{o}, \mathfrak{p}$ and k be as in § 2. In § 3 we assume moreover that:

(F₁) The valuation of K is unramified and (F) is satisfied with $q = p$.

The ring $W(k')$ of Witt vectors over a perfect field k' of characteristic

$p > 0$ satisfies (F_1) (cf. [22]). Under (F_1) we can take p as the fixed prime element of \mathfrak{o} .

3.1. Let x be the set of n variables as usual. Let N be the set of all the non-negative rational integers. For $\alpha = (\alpha_1, \dots, \alpha_n) \in N^n$ we write x^α for $x_1^{\alpha_1} \dots x_n^{\alpha_n}$. Then $|\alpha| = \alpha_1 + \dots + \alpha_n$ is the degree of x^α . For $1 \leq i \leq n$, let ε_i denote the vector of N^n whose j -th component is δ_{ij} ($1 \leq j \leq n$). Then $x^{r\varepsilon_i} = x_i^r$ for $r \in N$. Every element of $K[[x]]$ is written in the form $\sum_{\alpha \in N^n} a_\alpha x^\alpha$ ($a_\alpha \in K$).

LEMMA 3.1. For $r \geq 2$ define the form $A_r(X, Y)$ in $\mathbb{Z}[X, Y]$ as follows: If r is not a power of a prime number, we put $A_r(X, Y) = (X+Y)^r - X^r - Y^r$. If r is a power of a prime number l , we put $A_r(X, Y) = l^{-1}((X+Y)^r - X^r - Y^r)$. Then A_r is a primitive polynomial in $\mathbb{Z}[X, Y]$.

PROOF. Easy. See also [11], III.

For any commutative ring R , A_r is considered a polynomial in $R[X, Y]$.

LEMMA 3.2. Let $\lambda(x) = \sum_{|\alpha|=r} a_\alpha x^\alpha$ ($a_\alpha \in K$) be a form of degree r satisfying

$$(3.1) \quad \lambda(x+y) \equiv \lambda(x) + \lambda(y) \pmod{\mathfrak{p}}.$$

Then, if r is not a power of p , $a_\alpha \in \mathfrak{p}$ for all α . If r is a power of p , $a_\alpha \in \mathfrak{o}$ for all α and $a_\alpha \in \mathfrak{p}$ for $\alpha \neq r\varepsilon_i$ ($1 \leq i \leq n$).

PROOF. Take $\alpha \in N^n$ such that $|\alpha| = r$. If two of $\alpha_1, \dots, \alpha_n$, say α_1 and α_2 , are not equal to 0, the coefficient of $x_1^{\alpha_1} y_2^{\alpha_2} \dots y_n^{\alpha_n}$ on the left side of (3.1) is a_α and no term of this form appears on the right. Hence we have $a_\alpha \in \mathfrak{p}$ for such α . If $\alpha = r\varepsilon_i$, we have

$$a_\alpha \{ (x_i + y_i)^r - x_i^r - y_i^r \} \equiv 0 \pmod{\mathfrak{p}}$$

from (3.1). Then our assertion is a direct consequence of Lemma 3.1.

PROPOSITION 3.3. Let F be an n -dimensional formal group over \mathfrak{o} and let f be its transformer. Then there exists a special element u of \mathfrak{A}_n such that f is of type u .

PROOF. As $f(x) \equiv x \pmod{\text{deg } 2}$, we have $pf(x) \equiv 0 \pmod{\text{deg } 2, \text{ mod } \mathfrak{p}}$. Suppose that for $\mu \geq 0$ there are matrices C_1, \dots, C_μ in $M_n(\mathfrak{o})$ satisfying

$$(3.2) \quad pf(x) + \sum_{\nu=1}^{\mu} C_\nu f^{\circ \nu}(x^{p^\nu}) \equiv 0 \pmod{\text{deg}(p^\mu + 1), \text{ mod } \mathfrak{p}}.$$

Write $f_i(x) = \sum_{\alpha} a_{\alpha,i} x^\alpha$ for $1 \leq i \leq n$. Since $df_i(x) \in \mathfrak{D}^*(F; \mathfrak{o})$ by the results of §1, the $(\partial/\partial x_j) f_i(x)$ have integral coefficients. In particular we have $\alpha_j a_{\alpha,i} \in \mathfrak{o}$ for $1 \leq j \leq n$. Hence by Lemma 2.1 we get

$$\begin{aligned} a_{\alpha,i}(x+py)^\alpha &= \alpha_1 a_{\alpha,i} \alpha_1^{-1} (x_1 + py_1)^{\alpha_1} \prod_{j=2}^n (x_j + py_j)^{\alpha_j} \\ &\equiv \alpha_1 a_{\alpha,i} \alpha_1^{-1} x_1^{\alpha_1} \prod_{j=2}^n (x_j + py_j)^{\alpha_j} \pmod{\mathfrak{p}} \end{aligned}$$

$$= x_1^{\alpha_1} a_{\alpha,i} \prod_{j=2}^n (x_j + py_j)^{\alpha_j}.$$

By repeating the same argument we have

$$(3.3) \quad a_{\alpha,i}(x+py)^\alpha \equiv a_{\alpha,i}x^\alpha \pmod{\mathfrak{p}}.$$

Put now

$$(3.4) \quad pf(x) + \sum_{\nu=1}^{\mu} f^{\sigma\nu}(x^{p^\nu}) \equiv \sum_{|\beta| \geq p^{\mu+1}} b_\beta x^\beta \pmod{\mathfrak{p}} \quad (b_\beta \in K^n).$$

Substituting x by $F(x, y)$ in (3.4) we get

$$(3.5) \quad pf(F(x, y)) + \sum_{\nu=1}^{\mu} f^{\sigma\nu}(F(x, y)^{p^\nu}) \equiv \sum_{|\beta| \geq p^{\mu+1}} b_\beta F(x, y)^\beta \pmod{\mathfrak{p}}.$$

By (3.3) the left side of (3.5) is congruent mod \mathfrak{p} to

$$\begin{aligned} & pf(F(x, y)) + \sum_{\nu=1}^{\mu} C_\nu f^{\sigma\nu}(F^{\sigma\nu}(x^{p^\nu}, y^{p^\nu})) \\ &= pf(x) + \sum_{\nu=1}^{\mu} C_\nu f^{\sigma\nu}(x^{p^\nu}) + pf(y) + \sum_{\nu=1}^{\mu} C_\nu f^{\sigma\nu}(y^{p^\nu}) \\ &\equiv \sum_{|\beta| \geq p^{\mu+1}} b_\beta (x^\beta + y^\beta). \end{aligned}$$

Thus, denoting by $b_{\beta,i}$ the i -th component of b_β , we get

$$(3.6) \quad \sum_{|\beta| \geq p^{\mu+1}} b_{\beta,i} \{F(x, y)^\beta - x^\beta - y^\beta\} \equiv 0 \pmod{\mathfrak{p}}$$

for $1 \leq i \leq n$. Let r be the minimum value of $|\beta|$ such that $b_{\beta,i} \notin \mathfrak{p}$ for some i . Then (3.6) implies

$$\sum_{|\beta|=r} b_{\beta,i} \{(x+y)^\beta - x^\beta - y^\beta\} \equiv 0 \pmod{\mathfrak{p}}.$$

Applying Lemma 3.2 to this we see $r \geq p^{\mu+1}$. At any rate we have

$$\sum_{|\beta|=p^{\mu+1}} b_{\beta,i} \{(x+y)^\beta - x^\beta - y^\beta\} \equiv 0 \pmod{\mathfrak{p}}.$$

Hence, by Lemma 3.2, $b_{\beta,i} \in \mathfrak{o}$ for $\beta = p^{\mu+1}\epsilon_j$ ($1 \leq j \leq n$) and $b_{\beta,i} \in \mathfrak{p}$ for other β such that $|\beta| = p^{\mu+1}$. Therefore we can find a matrix $C_{\mu+1}$ in $M_n(\mathfrak{o})$ satisfying

$$pf(x) + \sum_{\nu=1}^{\mu} C_\nu f^{\sigma\nu}(x^{p^\nu}) \equiv -C_{\mu+1} x^{p^{\mu+1}} \pmod{\deg(p^{\mu+1}+1), \mathfrak{p}},$$

from which follows

$$(3.7) \quad pf(x) + \sum_{\nu=1}^{\mu+1} C_\nu f^{\sigma\nu}(x^{p^\nu}) \equiv 0 \pmod{\deg(p^{\mu+1}+1), \mathfrak{p}}.$$

Thus we have been able to replace μ by $\mu+1$ in (3.2). This implies the existence of $C_1, C_2, \dots, C_\nu, \dots \in M_n(\mathfrak{o})$ satisfying

$$(3.8) \quad pf(x) + \sum_{\nu=1}^{\infty} C_\nu f^{\sigma^\nu}(x^{\nu^\nu}) \equiv 0 \pmod{\mathfrak{p}}.$$

This means that f is of type u , where $u = pI_n + \sum_{\nu=1}^{\infty} C_\nu T^\nu$.

3.2. By Theorem 2 and Proposition 3.3 every n -dimensional formal group over \mathfrak{o} is obtained from a special element of \mathfrak{A}_n . Let F and G be n -dimensional formal groups over \mathfrak{o} , with the transformers f and g . By Proposition 3.3 there exist special elements u, v of \mathfrak{A}_n such that f (resp. g) is of type u (resp. of type v). By the uniqueness of transformer $F \approx G$ over \mathfrak{o} if and only if $g^{-1} \circ f \in \mathfrak{o}[[x]]_{\mathfrak{o}}^{\#}$. By Theorem 3 this happens if and only if there is $t \in \mathfrak{A}_n$ such that $v = tu$. It is clear that such t is a unit in \mathfrak{A}_n . Let u' and v' be elements of \mathfrak{A}_n . We shall say that v' is left associate with u' , if there is a unit t' in \mathfrak{A}_n such that $v' = t'u'$. We have proved the following theorem:

THEOREM 4. *Assume K satisfies (F_1) . Then every n -dimensional formal group over \mathfrak{o} is obtained from a special element of \mathfrak{A}_n by the method of Theorem 2. The strong isomorphism classes of n -dimensional groups over \mathfrak{o} correspond bijectively to the left associate classes of special elements of \mathfrak{A}_n .*

COROLLARY. *Let M be a complete system of representatives of $\mathfrak{o} \pmod{\mathfrak{p}}$. Then the strong isomorphism classes of n -dimensional formal groups over \mathfrak{o} correspond bijectively to the special elements of \mathfrak{A}_n whose coefficient matrices have elements in M .*

PROOF. Let $u = pI_n + \sum_{\nu=1}^{\infty} C_\nu T^\nu$ be a fixed special element of \mathfrak{A}_n and let $t = I_n + \sum_{\nu=1}^{\infty} A_\nu T^\nu$ be a unit in \mathfrak{A}_n . Then we have

$$tu = pI_n + \sum_{\nu=1}^{\infty} \left(pA_\nu + \sum_{\mu < \nu} A_\mu C_{\nu-\mu}^{\sigma^\mu} \right) T^\nu.$$

Therefore we can choose A_1, A_2, \dots successively and uniquely so that the coefficients of the T^ν in tu have all their elements in M . Our assertion follows from this and from Theorem 4.

3.3. As for the classification of (strong) isomorphism classes of n -dimensional groups over \mathfrak{o} , it is preferable to construct a module space over \mathfrak{o} . In the following we will perform it in case $n=1$ and \mathfrak{o} is complete.

The following lemma is a slight modification of Lemma 2.1 of [16].

LEMMA 3.4. *In addition to the condition (F_1) , suppose that \mathfrak{o} is complete. Let $u = p + \sum_{\nu=1}^{\infty} c_\nu T^\nu$ ($c_\nu \in \mathfrak{o}$) be a special element of $\mathfrak{o}_\sigma[[T]]$. If all the c_ν are in \mathfrak{p} , there is a unit t in $\mathfrak{o}_\sigma[[T]]$ such that $tu = p$. If $c_1, \dots, c_{h-1} \in \mathfrak{p}$ but $c_h \notin \mathfrak{p}$, then there is a unit t in $\mathfrak{o}_\sigma[[T]]$ such that tu is of the form $p + \sum_{\nu=1}^h b_\nu T^\nu$ where*

$b_1, \dots, b_{h-1} \in \mathfrak{p}$ and $b_h \in \mathfrak{p}$.

PROOF. If all the c_ν are in \mathfrak{p} , it suffices to put $t = pu^{-1}$. Assume $c_1, \dots, c_{h-1} \in \mathfrak{p}$ but $c_h \notin \mathfrak{p}$. We will show that for every $i \geq 1$ we can choose $b_1^{(i)}, \dots, b_h^{(i)} \in \mathfrak{o}$ and a unit t_i of $\mathfrak{o}_\sigma[[T]]$ satisfying

$$(3.9) \quad \begin{cases} b_\nu^{(i+1)} \equiv b_\nu^{(i)} \pmod{\mathfrak{p}^i}, & b_\nu^{(i)} \equiv c_\nu \pmod{\mathfrak{p}} \quad (1 \leq \nu \leq h), \\ t_i \equiv 1 \pmod{\deg 1}, & t_{i+1} \equiv t_i \pmod{\mathfrak{p}^i} \\ t_i u \equiv p + \sum_{\nu=1}^h b_\nu^{(i)} T^\nu \pmod{\mathfrak{p}^i}. \end{cases}$$

First put $b_1^{(1)} = \dots = b_{h-1}^{(1)} = 0$, $b_h^{(1)} = c_h$ and $t_1 = c_h \left(\sum_{\nu=h}^{\infty} c_\nu T^{\nu-h} \right)^{-1}$. As c_h is a unit, $t_1 \in \mathfrak{o}_\sigma[[T]]$. Since

$$t_1 u \equiv c_h T^h \pmod{\mathfrak{p}},$$

(3.9) is satisfied by $\{b_\nu^{(1)}; t_1\}$ with $i=1$. Suppose that we have already found $\{b_\nu^{(j)}; t_j\}$ for $1 \leq j \leq i$ satisfying (3.9). We try to determine $b_\nu^{(i+1)} = b_\nu^{(i)} + p^i d_\nu^{(i)}$ ($1 \leq \nu \leq h$) and $t_{i+1} = t_i + p^i v_i$ so that

$$(3.10) \quad (t_i + p^i v_i) u \equiv p + \sum_{\nu=1}^h (b_\nu^{(i)} + p^i d_\nu^{(i)}) T^\nu \pmod{\mathfrak{p}^{i+1}}.$$

Put $w_i = p^{-i} \left\{ t_i u - \left(p + \sum_{\nu=1}^h b_\nu^{(i)} T^\nu \right) \right\} (\in \mathfrak{o}_\sigma[[T]])$. Since $p^i u \equiv p^i \left(\sum_{\nu=h}^{\infty} c_\nu T^\nu \right) \pmod{\mathfrak{p}^{i+1}}$, (3.10) is reduced to

$$(3.11) \quad v_i \sum_{\nu=h}^{\infty} c_\nu T^\nu \equiv \sum_{\nu=1}^h d_\nu^{(i)} T^\nu - w_i \pmod{\mathfrak{p}}.$$

As w_i has no constant term, we can choose $d_1^{(i)}, \dots, d_h^{(i)} \in \mathfrak{o}$ so that the right hand side of (3.11) has no term of degree $\leq h$. Hence we can find a series $v_i \in \mathfrak{o}_\sigma[[T]]$, without constant term and satisfying (3.11). By induction this proves the existence of $\{b_\nu^{(i)}; t_i\}$ for all i . Put $t = \lim_{i \rightarrow \infty} t_i$ and $b_\nu = \lim_{i \rightarrow \infty} b_\nu^{(i)}$ for $1 \leq \nu \leq h$. Then $\{b_\nu; t\}$ satisfy the requirement of our lemma.

Let F be a 1-dimensional formal group over \mathfrak{o} . We shall say that F is of height h if the reduction of F modulo \mathfrak{p} is of height h (cf. [11]).

PROPOSITION 3.5. Let K be a complete discrete valuation field satisfying (F_1) . The strong isomorphism classes of 1-dimensional formal groups over \mathfrak{o} , of height h ($1 \leq h < \infty$), correspond bijectively to the special elements of the form $u = p + \sum_{\nu=1}^h b_\nu T^\nu$ where $b_1, \dots, b_{h-1} \in \mathfrak{p}$ but b_h is a unit of \mathfrak{o} . Let $v = p + \sum_{\nu=1}^h c_\nu T^\nu$ be another special element of this form. Then the formal group obtained from u is weakly isomorphic to the one obtained from v , if and only if there exists a unit c of \mathfrak{o} such that $c_\nu = c^{1-\sigma^\nu} b_\nu$ for $1 \leq \nu \leq h$.

PROOF. Let F be a 1-dimensional formal group over \mathfrak{o} . Then its transformer f is of type u' for a special element u' . If all the coefficients of u'

are in \mathfrak{p} , then $F(x, y) \approx x + y$ by Lemma 3.4 and Theorem 2. If not, f is also of type u , where u is a special element of the form $p + \sum_{\nu=1}^h b_\nu T^\nu$ ($b_1, \dots, b_{h-1} \in \mathfrak{p}$, $b_h \notin \mathfrak{p}$). We will prove that F is of height h . Since

$$\left(1 + p^{-1} \sum_{\nu=1}^{h-1} b_\nu T^\nu\right)^{-1} u = p + b_h T^h + \dots,$$

it suffices to prove that a formal group obtained from a special element u'' of the form $p + b_h T^h + \dots$ ($b_h \notin \mathfrak{p}$) is of height h . Put $(pu''^{-1}) * i = h$. Then

$$h(x) = x - p^{-1} b_h x^{p^h} + \dots$$

and so

$$\begin{aligned} h^{-1}(ph(x)) &= px - b_h x^{p^h} + \dots + p^{-1} b_h (px - \dots)^{p^h} + \dots \\ &\equiv -b_h x^{p^h} + \dots \pmod{\mathfrak{p}}, \end{aligned}$$

which prove that $h^{-1}(h(x) + h(y))$ is of height h .

Now suppose that there exist a unit c in \mathfrak{o} and a unit $t = \sum_{\nu=0}^{\infty} a_\nu T^\nu$ in $\mathfrak{o}_\sigma[[T]]$ such that $vc = tu$. Comparing the $(\nu + h)$ -th degree coefficients of both members of

$$\left(\sum_{\nu=0}^{\infty} a_\nu T^\nu\right) \left(p + \sum_{\nu=1}^h b_\nu T^\nu\right) = \left(p + \sum_{\nu=1}^h c_\nu T^\nu\right) c$$

for $\nu > 0$, we get

$$(3.12) \quad a_\nu b_h^{\sigma^\nu} + \sum_{\mu=1}^{h-1} a_{\nu+\mu} b_h^{\sigma^{\nu+\mu}} + p a_{\nu+h} = 0.$$

Since b_h is a unit, it follows from (3.12) that $a_\nu \in \mathfrak{p}$ for $\nu \geq 1$. Hence we get $a_\nu \in \mathfrak{p}^2$ for $\nu \geq 1$ again by (3.12). Repeating the same argument we see $a_\nu \in \mathfrak{p}^i$ for every $\nu \geq 1$ and for every $i \geq 1$. This implies $a_\nu = 0$ for $\nu \geq 1$, and $t = a_0 = c$. Our proposition follows from this, from Theorem 3 and from Theorem 4.

In the above proof we proved that $vc = tu$ implied $t = c$. Thereby we did not use the fact that c (resp. t) is a unit. Therefore we get by Theorem 3;

PROPOSITION 3.6. *Let u, v be as in Proposition 3.5 and let F, G be formal groups attached to them. Then the module $\text{Hom}_\sigma(F, G)$ is canonically isomorphic to $\{c \in \mathfrak{o} \mid vc = cu\}$.*

§ 4. Formal groups over a field of characteristic $p > 0$.

Let K be a discrete valuation field satisfying (F) of § 2. For a power series $f \in \mathfrak{o}[[x]]^m$, f^* denotes the power series in $k[[x]]^m$ obtained by reducing the coefficients of f modulo \mathfrak{p} . In § 4 we will study the reductions of formal groups over \mathfrak{o} and their homomorphisms.

4.1. Our first task is to prove two lemmas.

LEMMA 4.1. Let $f \in K[[x]]_0^n$ be of type $(P; u)$ and let $\phi(x') \in \mathfrak{o}[[x']]_0^n$ where x' is a finite set of variables. Then we have

$$f^{-1}(\pi\phi(x')) \equiv 0 \pmod{\mathfrak{p}}.$$

PROOF. Put $h = (u^{-1}\pi)*i$. By Lemma 2.4 it suffices to prove

$$h^{-1}(\pi x) \equiv 0 \pmod{\mathfrak{p}}.$$

Write $h(x) = \sum_{\nu} B_{\nu} x^{q^{\nu}}$ and $h^{-1}(\pi x) = l(x)$. Since $l(x) \equiv \pi x \pmod{\deg 2}$, the first-degree coefficients of l are in \mathfrak{p} . Assume for $r \geq 2$ that the i -th degree coefficients of l are in \mathfrak{p} for all $i \leq r-1$. Write $l(x) = \pi l^{(r)}(x) + \Delta^{(r)}(x)$ where $l^{(r)}(x) \in \mathfrak{o}[[x]]_0^n$ and $\Delta^{(r)}(x) \equiv 0 \pmod{\deg r}$. Then it follows from $h(l(x)) = \pi x$

$$(4.1) \quad l(x) + \sum_{\nu=1}^{r-1} \pi^{q^{\nu}} B_{\nu} l^{(r)}(x)^{q^{\nu}} \equiv \pi x \pmod{\deg(r+1)}.$$

Since $\pi^{q^{\nu}} B_{\nu} \in \pi M_n(\mathfrak{o})$ for $\nu \geq 1$ by Lemma 2.2, it follows from (4.1)

$$l(x) \equiv 0 \pmod{\deg(r+1), \mathfrak{p}}.$$

Hence the r -th degree coefficients of l are also in \mathfrak{p} . Thus we get $l \equiv 0 \pmod{\mathfrak{p}}$ by induction.

LEMMA 4.2. Let $u \in \mathfrak{X}_n$ be special and let $f \in K[[x]]_0^n$ be of type u . Let $\phi_1 \in K[[x']]_0^n$ and $\phi_2 \in \mathfrak{o}[[x']]_0^n$. Then $f \circ \phi_1 \equiv f \circ \phi_2 \pmod{\mathfrak{p}}$, if and only if $\phi_1 \equiv \phi_2 \pmod{\mathfrak{p}}$.

PROOF. Suppose $\phi_1 \equiv \phi_2 \pmod{\mathfrak{p}}$. Then we have clearly $\phi_1 \in \mathfrak{o}[[x]]_0^n$. Put $h = (u^{-1}\pi)*i$ and $h^{-1} \circ f = \varphi$. Since $\varphi \in \mathfrak{o}[[x]]_0^n$ by Lemma 2.4 and $\varphi \circ \phi_1 \equiv \varphi \circ \phi_2 \pmod{\mathfrak{p}}$, we obtain by Lemma 2.1 and 2.2

$$h \circ (\varphi \circ \phi_1) \equiv h \circ (\varphi \circ \phi_2) \pmod{\mathfrak{p}}$$

i. e. $f \circ \phi_1 \equiv f \circ \phi_2 \pmod{\mathfrak{p}}$. Conversely assume $f \circ \phi_1 \equiv f \circ \phi_2 \pmod{\mathfrak{p}}$ and put $\pi\lambda = f^{-1}(f \circ \phi_1 - f \circ \phi_2)$. Then $\lambda \in \mathfrak{o}[[x]]_0^n$ by Lemma 4.1. Since $F(x, y) = f^{-1}(f(x) + f(y))$ has coefficients in \mathfrak{o} , it follows from

$$f \circ \phi_1 = f \circ \phi_2 + f \circ (\pi\lambda)$$

i. e. $\phi_1 = F(\phi_2, \pi\lambda)$ that $\phi_1 \equiv \phi_2 \pmod{\mathfrak{p}}$.

4.2. We now study a certain type of homomorphisms of F^* to G^* for formal groups F, G over \mathfrak{o} .

THEOREM 5. Suppose K satisfies (F). Let F and G be formal groups over \mathfrak{o} , of dimension n and m and with transformers f and g , respectively. Suppose that f (resp. g) is of type u (resp. of type v) for special elements $u \in \mathfrak{X}_n$ and $v \in \mathfrak{X}_m$.

(i) Put $\varphi = \varphi_w = g^{-1} \circ (w * f)$ for $w \in \mathfrak{X}_{m,n}$. Then $\varphi(x) \in \mathfrak{o}[[x]]_0^m$ if and only if there exists $t \in \mathfrak{X}_{m,n}$ such that $wv = tu$.

(ii) If $\varphi_w \in \mathfrak{o}[[x]]_0^m$, then $\varphi_w^* \in \text{Hom}_k(F^*, G^*)$.

(iii) Let h be of type v' for a special element $v' \in \mathfrak{X}_i$. If $\varphi_w = h^{-1} \circ (w' * g)$ has integral coefficients for $w' \in \mathfrak{X}_{i,m}$, then $\varphi_w^* \circ \varphi_w^* = \varphi_{w'w}^*$.

PROOF. In order to prove (i) we may assume $g = (v^{-1}\pi) * i$. Suppose there is $t \in \mathfrak{X}_{m,n}$ such that $vw = tu$. Clearly the first-degree coefficients of φ are integers. Assume for $r \geq 2$ that the i -th degree coefficients of φ are integers for $i \leq r-1$. By Lemma 2.3 we have

$$\begin{aligned} \pi\varphi &= (v * g) \circ \varphi \equiv v * (g \circ \varphi) \pmod{\deg(r+1), \text{ mod } \mathfrak{p}} \\ &= v * (w * f) = (vw) * f = (tu) * f \\ &= t * (u * f) \equiv 0 \pmod{\mathfrak{p}}. \end{aligned}$$

This implies that the r -th degree coefficients of φ are also integers. This shows $\varphi(x) \in \mathfrak{o}[[x]]_{\mathfrak{p}}^m$ by induction. Conversely, suppose $\varphi = \varphi_w \in \mathfrak{o}[[x]]_{\mathfrak{p}}^m$. By Lemma 2.3 we get

$$\begin{aligned} (vw) * f &= v * (w * f) = v * (g \circ \varphi) \\ &\equiv (v * g) \circ \varphi = \pi\varphi \equiv 0 \pmod{\mathfrak{p}}. \end{aligned}$$

Hence, by Proposition 2.6 we can find $t \in \mathfrak{X}_{m,n}$ such that $vw = tu$. This proves (i). Now we have

$$g \circ (\varphi \circ F) = (g \circ \varphi) \circ F = (w * f) \circ F$$

and by Lemma 2.3

$$\begin{aligned} ((w * f) \circ F)(x, y) &\equiv (w * (f \circ F))(x, y) \pmod{\mathfrak{p}} \\ &= (w * f)(x) + (w * f)(y) \\ &= (g \circ \varphi)(x) + (g \circ \varphi)(y) \\ &= g(G(\varphi(x), \varphi(y))). \end{aligned}$$

Thus we get $g \circ (\varphi \circ F) \equiv g \circ (G \circ \varphi) \pmod{\mathfrak{p}}$. By Lemma 4.2 it follows from this that $\varphi \circ F \equiv G \circ \varphi \pmod{\mathfrak{p}}$. This implies $\varphi^* \in \text{Hom}_k(F^*, G^*)$. Let us prove (iii). By Lemma 2.3 we have

$$\begin{aligned} h \circ (\varphi_{w'} \circ \varphi_w) &= (h \circ \varphi_{w'}) \circ \varphi_w = (w' * g) \circ \varphi_w \\ &\equiv w' * (g \circ \varphi_w) \pmod{\mathfrak{p}} \\ &= w' * (w * f) = (w'w) * f. \end{aligned}$$

By (i) there is $t' \in \mathfrak{X}_{i,m}$ such that $v'w' = t'v$. Since $v'w'w = t'vw = t'tu$, $\varphi_{w'w} = h^{-1} \circ ((w'w) * f)$ has integral coefficients by (i). Since

$$h \circ (\varphi_{w'} \circ \varphi_w) \equiv h \circ \varphi_{w'w} \pmod{\mathfrak{p}}$$

as we have shown, it follows from Lemma 4.2 that

$$\varphi_{w'} \circ \varphi_w \equiv \varphi_{w'w} \pmod{\mathfrak{p}}.$$

This proves (iii).

COROLLARY. Put $E = \mathfrak{o}_\sigma[[T]]$. The submodule of $\text{Hom}_k(F^*, G^*)$, consisting of homomorphisms of the form φ_w^* ($w \in \mathfrak{A}_{m,n}$), is canonically isomorphic to the module of all right E -homomorphisms of E^n/uE^n into E^m/vE^m . In particular the subring of $\text{End}_k F^*$, consisting of homomorphisms of the form $(f^{-1} \circ (w * f))^*$ ($w \in \mathfrak{A}_n$), is canonically isomorphic to the right E -endomorphism ring of E^n/uE^n .

PROOF. If $tu = vw$, then

$$t(uE^n) = vwE^n \subset vE^m.$$

Thus t induces a right E -homomorphism Φ_t of E^n/uE^n into E^m/vE^m . Conversely, as is easily verified, every right E -homomorphism of E^n/uE^n into E^m/vE^m is of the form Φ_t with $t \in \mathfrak{A}_{m,n}$ such that $tu \in v\mathfrak{A}_{m,n}$. We will show that $\varphi_w^* = 0$ if and only if $\Phi_t = 0$: $\varphi_w^* = 0 \Leftrightarrow g^{-1} \circ (w * f) \equiv 0 \pmod{\mathfrak{p}} \Leftrightarrow w * f \equiv 0 \pmod{\mathfrak{p}}$ (by Lemma 4.2) $\Leftrightarrow w \in \mathfrak{A}_{m,n}u$ (by Proposition 2.6) $\Leftrightarrow tu \in v\mathfrak{A}_{m,n}u \Leftrightarrow t \in v\mathfrak{A}_{m,n} \Leftrightarrow tE^n \subset vE^m \Leftrightarrow \Phi_t = 0$. This implies that φ_w^* and Φ_t correspond bijectively. The second assertion follows from this and from Theorem 5, (iii).

4.3. If K satisfies (F_1) , every element of $\text{Hom}_k(F^*, G^*)$ is of the form φ_w^* with $w \in \mathfrak{A}_{m,n}$. To prove it we need the following lemma.

LEMMA 4.3. Suppose K satisfies (F_1) . Let F be an n -dimensional formal group over \mathfrak{o} and let f be its transformer. Put $M = \{\phi \in K[[x]] \mid (\phi \circ F)(x, y) \equiv \phi(x) + \phi(y) \pmod{\mathfrak{p}}\}$. Then M is topologically generated by $\mathfrak{p}[[x]]$ and by $\{f_i^{\sigma^\nu}(x^{p^\nu}) \mid 1 \leq i \leq n, \nu \geq 0\}$ as \mathfrak{o} -module. (We define the topology of $K[[x]]$ by taking $I_\nu = \{f \in K[[x]] \mid f \equiv 0 \pmod{\deg(\nu+1)} (\nu \geq 1)\}$ as a base of neighborhoods of 0.)

PROOF. It is clear that $\mathfrak{p}[[x]] \subset M$. By Lemma 2.3 and by Proposition 3.3 we have

$$\begin{aligned} f^{\sigma^\nu}(F(x, y)^{p^\nu}) &= ((T^\nu * f) \circ F)(x, y) \\ &= (T^\nu * (f \circ F))(x, y) \pmod{\mathfrak{p}} \\ &= (T^\nu * f)(x) + (T^\nu * f)(y) \\ &= f^{\sigma^\nu}(x^{p^\nu}) + f^{\sigma^\nu}(y^{p^\nu}). \end{aligned}$$

This implies $f_i^{\sigma^\nu}(x^{p^\nu}) \in M$ for $1 \leq i \leq n, \nu \geq 0$. Let ϕ be any element of M and let r be the lowest degree such that $\phi \not\equiv 0 \pmod{\deg(r+1), \pmod{\mathfrak{p}}}$. Then $\phi \in M$ implies that the r -th degree homogeneous part $\phi^{(r)}$ of ϕ satisfies

$$(4.2) \quad \phi^{(r)}(x+y) \equiv \phi^{(r)}(x) + \phi^{(r)}(y) \pmod{\deg(r+1), \pmod{\mathfrak{p}}}.$$

By Lemma 3.2 (4.2) implies that r is a power of p , say p^h (if $r < \infty$) and that there exist $c_1, \dots, c_n \in \mathfrak{o}$ satisfying

$$\phi(x) - \sum_{i=1}^n c_i x_i^{p^h} \equiv 0 \pmod{\deg(r+1), \pmod{\mathfrak{p}}}.$$

Hence we get

$$(4.3) \quad \phi(x) - \sum_{i=1}^n c_i f_i^{g^h}(x^{p^h}) \equiv 0 \pmod{\deg(r+1), \text{ mod } \mathfrak{p}}.$$

Applying the same argument to the left side of (4.3) in place of ϕ and repeating this procedure we see in fact that $\mathfrak{p}[[x]]$ and the $f_i^{g^\nu}(x^{p^\nu})$ ($1 \leq i \leq n, \nu \geq 0$) generate a dense \mathfrak{o} -submodule of M .

THEOREM 6. *Suppose K satisfies (F_1) . The map: $\Phi_t \mapsto \varphi_w^*$, defined in Theorem 5, is a bijection of $\text{Hom}_{\mathbb{E}}(E^n/uE^n, E^m/vE^m)$ onto $\text{Hom}_k(F^*, G^*)$. In particular $\text{End}_k F^*$ is canonically isomorphic to $\text{End}_{\mathbb{E}}(E^n/uE^n)$.*

PROOF. It suffices to prove the surjectivity. We may assume $f = (u^{-1}\pi)*i$ and $g = (v^{-1}\pi)*i$. For $\varphi_* \in \text{Hom}_k(F^*, G^*)$, take $\varphi \in \mathfrak{o}[[x]]_{\mathfrak{p}}^m$ such that $\varphi^* = \varphi_*$. Since $\varphi \circ F \equiv G \circ \varphi \pmod{\mathfrak{p}}$, we get by Lemma 4.2

$$(4.4) \quad g \circ \varphi \circ F \equiv g \circ G \circ \varphi \pmod{\mathfrak{p}}.$$

Put $\psi = g \circ \varphi$. Then (4.4) implies

$$(4.5) \quad \psi(F(x, y)) \equiv \psi(x) + \psi(y) \pmod{\mathfrak{p}}.$$

By Lemma 4.3 it follows from (4.5) that there exists $w \in \mathfrak{A}_{m,n}$ satisfying

$$\psi \equiv w * f \pmod{\mathfrak{p}},$$

or

$$g \circ \varphi \equiv w * f \pmod{\mathfrak{p}}.$$

By Lemma 4.2 this implies that $g^{-1} \circ (w * f) \in \mathfrak{o}[[x]]_{\mathfrak{p}}^m$ and $\varphi \equiv g^{-1} \circ (w * f) \pmod{\mathfrak{p}}$. Thus we have $\varphi_w^* = \varphi^* = \varphi_*$, which was to be proved.

4.4. Now we will show that, if K satisfies (F_1) , any formal group over k is obtained by reducing a formal group over \mathfrak{o} .

The following lemma is due to [12].

LEMMA 4.4. *Let R be a commutative ring and let $X = (X_1, \dots, X_n)$ and $Y = (Y_1, \dots, Y_n)$ be systems of n variables. Suppose that a form $\Delta(X, Y)$ of degree r in $R[X, Y]$ is a commutative 2-cocycle, i. e.*

$$(4.6) \quad \begin{aligned} \Delta(X, Y) &= \Delta(Y, X), \\ \Delta(Y, Z) - \Delta(X+Y, Z) + \Delta(X, Y+Z) - \Delta(X, Y) &= 0. \end{aligned}$$

Then, if r is not a power of a prime number, Δ is a 2-coboundary, i. e. there is a form $\Gamma(X)$ of degree r such that

$$\Delta(X, Y) = \Gamma(X) - \Gamma(X+Y) + \Gamma(Y).$$

If r is a power of a prime, Δ is cohomologous to a linear combination of $A_r(X_i, Y_i)$ ($1 \leq i \leq n$) with coefficients in R .

PROOF. In case $n=1$ this is Lemma 3 of [11]. (For the proof of this case see also [7], p. 62.) In general we can reduce the case $n=m$ to the case $n=m-1$ by making use of the result of Lyndon [15] on normal co-

homology groups. (See also [12]). For the convenience of the reader we will perform this reduction in the following. We first note $\Delta(X, 0) = 0 = \Delta(0, X)$. (Put $Y = Z = 0$ in (4.6)). Let us write $X' = (X_1, \dots, X_{m-1})$, $Y' = (Y_1, \dots, Y_{m-1})$, i. e. $X = (X', X_m)$, $Y = (Y', Y_m)$ and $\Delta(X, Y) = \Delta(X', X_m, Y', Y_m)$. Define Δ_1 by

$$(4.7) \quad \Delta_1(X, Y) = \Delta(X, Y) - \{ \Delta(0, X_m, X', 0) - \Delta(0, X_m + Y_m, X' + Y', 0) + \Delta(0, Y_m, Y', 0) \}.$$

Then Δ_1 is also a commutative 2-cocycle cohomologous to Δ . Putting $X' = 0$, $Y_m = 0$ in (4.7) we get

$$(4.8) \quad \Delta_1(0, X_m, Y', 0) = 0$$

and by commutativity

$$(4.8') \quad \Delta_1(X', 0, 0, Y_m) = 0.$$

Now putting $X' = 0$, $Y_m = Z_m = 0$ in (4.6) for $\Delta = \Delta_1$ we get

$$\Delta_1(Y', 0, Z', 0) - \Delta_1(Y', X_m, Z', 0) + \Delta_1(0, X_m, Y' + Z', 0) - \Delta_1(0, X_m, Y', 0) = 0.$$

By (4.8) this implies

$$(4.9) \quad \Delta_1(Y', X_m, Z', 0) = \Delta_1(Y', 0, Z', 0).$$

In the same way we obtain

$$(4.10) \quad \Delta_1(X', Y_m, 0, Z_m) = \Delta_1(0, Y_m, 0, Z_m).$$

Putting $Y' = Z_m = 0$ in (4.6) for $\Delta_1 = \Delta$ we get

$$\begin{aligned} \Delta_1(0, Y_m, Z', 0) - \Delta_1(X', X_m + Y_m, Z', 0) \\ + \Delta_1(X', X_m, Z', Y_m) - \Delta_1(X', X_m, 0, Y_m) = 0. \end{aligned}$$

By (4.8), (4.9) and (4.10) this implies

$$\Delta_1(X', X_m, Z', Y_m) = \Delta_1(X', 0, Z', 0) + \Delta_1(0, X_m, 0, Y_m),$$

which completes the reduction: the case $n = m \Rightarrow$ the case $n = m - 1$.

THEOREM 7. *Suppose K satisfies (F_1) of § 3. For any formal group F_* over k there exists a formal group F over \mathfrak{o} such that $F^* = F_*$.*

PROOF. Let n be the dimension of F_* . Take $\varphi(x) \in \mathfrak{o}[[x]]^{\mathfrak{g}}$ such that $\varphi(x) \equiv x \pmod{\text{deg } 2}$ and $u(T) = pI_n + \sum_{\nu=1}^{\infty} C_{\nu} T^{\nu} \in \mathfrak{A}_n$ and form $f = ((pu^{-1}) * i) \circ \varphi$. Then $F(x, y) = f^{-1}(f(x) + f(y))$ is a formal group over \mathfrak{o} . We will prove that we can choose the coefficients of φ and C_1, C_2, \dots successively so that $F^* = F_*$. Suppose that we have already chosen the i -th degree coefficients of φ for $i \leq r - 1$ and the C_{ν} for $p^{\nu} < r$ so that

$$(4.11) \quad F^* \equiv F_* \pmod{\text{deg } r}.$$

Letting the other coefficients of φ be equal to 0 and the C_ν for $\nu \geq r$ be equal to 0-matrix for example, form $g = ((pu^{-1}) * i) \circ \varphi$ and $G(x, y) = g^{-1}(g(x) + g(y))$. Then G is a formal group over \mathfrak{o} and we have

$$(4.12) \quad G^* \equiv F_* \pmod{\deg r}.$$

It follows from (4.12) and from the associative law of formal group that the r -th degree homogeneous part Δ of $G^* - F_*$ is a commutative 2-cocycle in $k[[x]]^n$ (cf. [11], [12]). If r is not a power of p , we can find by Lemma 4.4 $\phi \in \mathfrak{o}[[x]]^n$ whose components are forms of degree r and satisfy

$$(4.13) \quad G^*(x, y) - F_*(x, y) \equiv \phi^*(x) - \phi^*(x+y) + \phi^*(y) \pmod{\deg(r+1)}.$$

Let h be the element of $\mathfrak{o}[[x]]_0^n$, obtained by replacing φ by $\varphi - \phi$ in the definition of g and put $H(x, y) = h^{-1}(h(x) + h(y))$. Since $h \equiv g - \phi \pmod{\deg(r+1)}$, we get

$$\begin{aligned} H(x, y) &= h^{-1}(h(x) + h(y)) \\ &\equiv g^{-1}(g(x) + g(y)) - \{\phi(x) + \phi(y) - \phi(x+y)\} \pmod{\deg(r+1)}. \end{aligned}$$

This implies

$$\begin{aligned} H^*(x, y) &\equiv G^*(x, y) - \{\phi^*(x) + \phi^*(y) - \phi^*(x+y)\} \pmod{\deg(r+1)} \\ &\equiv F_*(x, y) \pmod{\deg(r+1)}. \end{aligned}$$

Thus we have been able to replace r by $r+1$ in (4.11). If r is a power of p , say $r = p^h$, we can find by Lemma 4.4 $\phi \in \mathfrak{o}[[x]]^n$ whose components are forms of degree r and $D \in M_n(\mathfrak{o})$ such that

$$(4.14) \quad G^*(x, y) - F_*(x, y) \equiv \phi^*(x) - \phi^*(x+y) + \phi^*(y) - D^* A_r(x, y) \pmod{\deg(r+1)},$$

where we have written $A_r(x, y) = (A_r(x_1, y_1), \dots, A_r(x_n, y_n))$. Replacing φ by $\varphi - \phi$ and u by $u + DT^h$ in the definition of g , we get an element h of $\mathfrak{o}[[x]]_0^n$. Since

$$p \left(pI_n + \sum_{\nu=1}^{h-1} C_\nu T^\nu + DT^h \right)^{-1} \equiv p \left(pI_n + \sum_{\nu=1}^{h-1} C_\nu T^\nu \right)^{-1} - p^{-1} DT^h \pmod{\deg(h+1)},$$

we have

$$(4.15) \quad h(x) \equiv g(x) - \phi(x) - p^{-1} D x^r \pmod{\deg(r+1)}.$$

Put $H(x, y) = h^{-1}(h(x) + h(y))$. Then we get from (4.15)

$$(4.16) \quad H(x, y) \equiv G(x, y) - \{\phi(x) + \phi(y) - \phi(x+y)\} + D A_r(x, y) \pmod{\deg(r+1)}.$$

It follows from (4.14) and (4.16) that

$$\begin{aligned} H^*(x, y) &\equiv G^*(x, y) - \{\phi^*(x) + \phi^*(y) - \phi^*(x+y)\} + D^* A_r(x, y) \\ &\equiv F_*(x, y) \pmod{\deg(r+1)}. \end{aligned}$$

Thus we have been able to replace r by $r+1$ in (4.11) in this case too. This proves the existence of u and φ satisfying $F^* = F_*$.

When K satisfies (F_1) , all the formal groups over k are obtained from special elements by Theorem 7 and homomorphisms of these groups are described in Theorem 6 and its corollary. In case where \mathfrak{o} is the ring of Witt vectors over a perfect field k' of characteristic $p > 0$, these results are nothing other than the main results of Dieudonné [4]. Using these results Dieudonné [5] gave a complete classification of isogeny classes of formal groups over k' when k' is algebraically closed. For this see also [2], [8] and [16].

§ 5. Examples and applications.

5.1. The group of Witt vectors of length n .

Let k be a perfect field of characteristic $p > 0$ and let $\mathfrak{o} = W(k)$ be the ring of Witt vectors over k . Put $u = pI_n - C_1T$ where $C_1 = \begin{pmatrix} 0 & 1 & & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \dots & \dots & 1 \\ 0 & \dots & \dots & 0 \end{pmatrix} \in M_n(\mathfrak{o})$. Then

it is easily verified that the reduction of the formal group with the transformer $(pu^{-1}) * i$ is the group of Witt vectors of length n (cf. [5], p. 120).

5.2. The group $G_{n,m}$ for $n \geq 2, m \geq 1$.

Let k, \mathfrak{o} and C_1 be as in 5.1. Put $u = pI_n - C_1T - C_{m+1}T^{m+1}$ with $C_{m+1} = \begin{pmatrix} 0 & \dots & \dots & 0 \\ \vdots & & & \vdots \\ 0 & \dots & \dots & 0 \\ 1 & 0 & \dots & 0 \end{pmatrix}$ and form $h = (pu^{-1}) * i$ and $H(x, y) = h^{-1}(h(x) + h(y))$.

Then, as is seen from [5], H^* is the group $G_{n,m}$ ($= G_{n,0,m}$ by the notation of [5]). Suppose that \mathfrak{o} contains a primitive $(p^{m+n} - 1)$ -th root w of unity. Put $W = \begin{pmatrix} w^{p^{n-1}} & & 0 \\ \vdots & \ddots & \vdots \\ 0 & & w^p \\ & & & w \end{pmatrix}$. Then as $w^\sigma = w^p$, we have $WC_1 = C_1W^\sigma$ and $WC_{m+1} =$

$C_{m+1}W^{\sigma^{m+1}}$, so that $Wu = uW$. By Theorem 3 this implies $h^{-1}(Wh(x)) \in \text{End}_{\mathfrak{o}} H$. On the other hand $(T * i)(x) = x^p \in \text{End}_k H^*$, since H is defined over \mathbf{Z}_p . Let E be the \mathbf{Z}_p -subalgebra of $\text{End}_k H^*$ generated by $(h^{-1} \circ (Wh))^*$ and $T * i$. The coefficients of components of $h^{-1} \circ (Wh)$ are polynomials in $\mathbf{Q}_p[w]$. Since $h^{-1} \circ (Wh) \in \mathfrak{o}[[x]]_0^{\mathfrak{g}}$, these polynomials belong to $\mathbf{Z}_p[w]$, the ring of integers in $\mathbf{Q}_p(w)$. Therefore we have

$$(5.1) \quad (T * i) \circ (h^{-1} \circ (Wh))^* = (h^{-1} \circ (W^\sigma h))^* \circ (T * i).$$

If $(m, n) = 1$ and k is algebraically closed, $\text{End}_k H^*$ is isomorphic to the (unique) maximal order in the central division algebra of rank $(m+n)^2$ over \mathbf{Q}_p , and

invariant $n/(m+n)$ ([5], p. 129-130). Since $\mathbf{Q}_p(w)$ is the unramified extension of degree $m+n$ of \mathbf{Q}_p and $T*i$ is clearly a prime element in $\text{End}_k H^*$, (5.1) implies $E = \text{End}_k H^*$ when $(m, n) = 1$.

5.3. The Lubin-Tate group ($n=1$).

Suppose K satisfies (F) of §2. For $\alpha \in \mathfrak{o}$, $\alpha \neq 0$, $u_\alpha = \pi - \alpha^{\sigma-1}T$ is a special element. Put $f_\alpha = ((u_\alpha^{-1}\pi)*i)$. An easy computation shows

$$(5.2) \quad f_\alpha(x) = \sum_{\nu=0}^{\infty} \pi^{-(1+\sigma+\dots+\sigma^{\nu-1})} \alpha^{\sigma^\nu-1} x^{\sigma^\nu}.$$

By Theorem 2, $F_\alpha(x, y) = f_\alpha^{-1}(f_\alpha(x)+f_\alpha(y))$ is a formal group over \mathfrak{o} . Since $\alpha u_\alpha = u_1 \alpha$, $f_1^{-1}(\alpha f_\alpha(x))$ has integral coefficients by Theorem 3. When $\pi^\sigma = \pi$ and $\alpha = 1$, F_α coincides with the group constructed in [10], Theorem 2. (Theorem 2 of [10] can be reduced to the case $a=1$ by replacing K by its unramified extension of degree a .)

5.4. Interpretation of the Artin-Hasse function.

Suppose K satisfies (F₁) of §3. Put $g(x) = -\log(1-x) = \sum_{m=1}^{\infty} m^{-1}x^m$. It is easily verified that g is of type $p-T$. Put now

$$L(\alpha, x) = \sum_{\nu=0}^{\infty} p^{-\nu} \alpha^{\sigma^\nu} x^{p^\nu} \quad \text{for } \alpha \in \mathfrak{o}.$$

Then $g^{-1}(L(\alpha, x))$ has integral coefficients by the result of 5.3. This is a homomorphism of F_α to $g^{-1}(g(x)+g(y)) = x+y-xy$. Since $g^{-1}(x) = 1 - \exp(-x)$, $\exp(-L(\alpha, x))$ has coefficients in \mathfrak{o} . This is nothing other than the Artin-Hasse exponential function ([1]).

5.5. The characteristic equation for the Frobenius endomorphism.

Suppose K satisfies (F). Assume $\pi^\sigma = \pi$ and let u be a special element of \mathfrak{A}_n such that $uT = Tu$. This implies that all coefficients of u are σ -invariant. Since the elements of u and T generate a commutative subring of $\mathfrak{o}_s[[T]]$, we can consider the cofactor matrix w of u :

$$(5.3) \quad uw = wu = (\det u)I_n.$$

Form $f = (u^{-1}\pi)*i$ and $F(x, y) = f^{-1}(f(x)+f(y))$. By (5.3) and by Theorem 5, (i) $(f^{-1} \circ (w*f))* \in \text{End}_k F^*$. Then by Theorem 5, (iii) and by Lemma 4.1,

$$(5.4) \quad f^{-1} \circ ((\det u)*f) \equiv (f^{-1} \circ (u*f)) \circ (f^{-1} \circ (w*f)) \pmod{\mathfrak{p}} \\ \equiv 0.$$

Write $\det u = \pi^n + \sum_{\nu=1}^{\infty} c_\nu T^\nu$, $c_\nu \in \mathfrak{o}$. Since $c_\nu^\sigma = c_\nu$, $f^{-1} \circ (c_\nu f) \in \text{End}_\mathfrak{o} F$ for $\nu \geq 1$ by Theorem 3. Put $[c_\nu]^* = (f^{-1} \circ (c_\nu f))^*$ and $\xi(x) = x^q$. Since $f^\sigma = f$, (5.4) implies that ξ satisfies the equation

$$[\pi^n]^* + \sum_{\nu=1}^{\infty} [c_\nu]^* \xi^\nu = 0$$

in $\text{End}_k F^*$.

§ 6. Formal groups over \mathbf{Z} . Applications to zeta functions.

6.1. Suppose that for every prime number p and for every $\nu \geq 1$ there is given a matrix $C_{p\nu}$ in $M_n(\mathbf{Z})$ and that $C_{p\nu}$ commutes with $C_{l\mu}$ if p and l are distinct primes. Let s be a complex variable and consider the (formal) Dirichlet series

$$(I_n + C_p p^{-s} + \dots + C_{p\nu} p^{\nu-1-\nu s} + \dots)^{-1} = \sum_{\nu=0}^{\infty} A_{p\nu} p^{-\nu s}.$$

Since $A_{p\nu}$ is expressed by $C_p, \dots, C_{p\nu}$ with coefficients in \mathbf{Z} , $A_{p\nu}$ commutes with $A_{l\mu}$ if $p \neq l$. Hence we can consider the global Dirichlet series

$$(6.1) \quad \prod_p (I_n + C_p p^{-s} + \dots + C_{p\nu} p^{\nu-1-\nu s} + \dots)^{-1} = \sum_{m=1}^{\infty} A_m m^{-s},$$

where $A_{mm'} = A_m A_{m'} = A_{m'} A_m$ if $(m, m') = 1$.

THEOREM 8. Let $\{C_{p\nu}\}$ and $\{A_m\}$ be as above and form $f(x) = \sum_{m=1}^{\infty} m^{-1} A_m x^m \in \mathbf{Q}[[x]]_0^*$. Then

$$(6.2) \quad pf(x) + \sum_{\nu=1}^{\infty} C_{p\nu} f(x^{p^\nu}) \equiv 0 \pmod{p\mathbf{Z}_p}$$

for every p and $F(x, y) = f^{-1}(f(x) + f(y))$ is a formal group over \mathbf{Z} .

PROOF. Put

$$(6.3) \quad p \left(pI_n + \sum_{\nu=1}^{\infty} C_{p\nu} T^\nu \right)^{-1} = \sum_{\nu=0}^{\infty} B_{p\nu} T^\nu.$$

Replacing T by pT in (6.3) we get $B_{p\nu} = p^{-\nu} A_{p\nu}$. Now

$$(6.4) \quad pf(x) + \sum_{\nu=1}^{\infty} C_{p\nu} f(x^{p^\nu}) = p \sum_{m=1}^{\infty} m^{-1} A_m x^m + \sum_{\nu=1}^{\infty} C_{p\nu} \sum_{m=1}^{\infty} m^{-1} A_m x^{mp^\nu}.$$

For $p \nmid k$ let $D_{kp\nu}$ be the coefficient of x^{kp^ν} on the right side of (6.4). If $\nu = 0$, then

$$D_{kp\nu} = pk^{-1} A_k \equiv 0 \pmod{p\mathbf{Z}_p}.$$

If $\nu \geq 1$, then

$$\begin{aligned} D_{kp\nu} &= pk^{-1} p^{-\nu} A_{kp^\nu} + \sum_{\mu=1}^{\nu} C_{p\mu} (kp^{\nu-\mu})^{-1} A_{kp^{\nu-\mu}} \\ &= k^{-1} A_k \left(p^{-(\nu-1)} A_{p\nu} + \sum_{\mu=1}^{\nu} C_{p\mu} p^{-(\nu-\mu)} A_{p^{\nu-\mu}} \right) \\ &= k^{-1} A_k \left(pB_{p\nu} + \sum_{\mu=1}^{\nu} C_{p\mu} B_{p^{\nu-\mu}} \right) \\ &= 0. \end{aligned}$$

Thus (6.2) is proved. Moreover, by Theorem 2 the coefficients of F are p -integral for every p . Hence $F(x, y) \in \mathbf{Z}[[x, y]]$. This completes our proof.

COROLLARY 1. Any 1-dimensional formal group over \mathbf{Z} is strongly iso-

morphic to one obtained in Theorem 8. The strong isomorphism classes correspond bijectively to Dirichlet series of the form (6.1) with $n=1$ such that $0 \leq C_{p^\nu} < p$.

PROOF. Let F be a 1-dimensional formal group over \mathbf{Z} and let f be its transformer. By Theorem 4 we can find $C_p, C_{p^2}, \dots \in \mathbf{Z}$ for every p satisfying

$$pf(x) + \sum_{\nu=1}^{\infty} C_\nu f(x^{p^\nu}) \equiv 0 \pmod{p\mathbf{Z}_p}.$$

Let G be the formal group over \mathbf{Z} obtained from the Dirichlet series $\prod_p \left(1 + \sum_{\nu=1}^{\infty} C_{p^\nu} p^{\nu-1-\nu s}\right)^{-1}$. By Theorem 8 and Theorem 2 $F \approx G$ over \mathbf{Z}_p for every p . Since the strong isomorphism of F to G is unique, this implies $F \approx G$ over \mathbf{Z} . The second assertion is a consequence of the Corollary of Theorem 4.

COROLLARY 2. Notations and assumptions being as in Theorem 8, assume moreover that the C_{p^ν} commute with each other for a fixed prime p . Put $[C_{p^\nu}] = f^{-1} \circ (C_{p^\nu} f)$ and $\xi(x) = x^p$. Then $[C_{p^\nu}] \in \text{End}_{\mathbf{Z}} F$ for $\nu \geq 1$ and ξ satisfies the equation

$$(6.5) \quad [pI_n]^* + \sum_{\nu=1}^{\infty} [C_{p^\nu}]^* \xi^\nu = 0$$

in $\text{End}_k F^*$, where $k = \mathbf{Z}/p\mathbf{Z}$.

PROOF. Since C_{p^ν} commutes with $lI_n + \sum_{\mu=1}^{\infty} C_{l^\mu} T^\mu$ for any l , $[C_{p^\nu}]$ is l -integral by Theorem 3. Hence $[C_{p^\nu}] \in \text{End}_{\mathbf{Z}} F$ by Proposition 1.6. The equation (6.5) is a direct consequence of (6.2) and of Lemma 4.1.

6.2. The results of 6.1 can be applied to zeta functions of the following types:

- (a) Dirichlet L -functions.
- (b) Zeta functions of elliptic curves over \mathbf{Q} .
- (c) Dirichlet series obtained from a rational representation of Hecke operators in the space of cusp forms of dimension -2 with respect to a congruence unit group of an indefinite quaternion algebra over \mathbf{Q} (cf. [19]).

We have already studied (a) and (b) in [10]. We note that we can remove the assumption on S in [10], Theorem 5:

THEOREM 9. Let C be a 1-dimensional abelian variety over \mathbf{Q} and let F be a formal minimal model for C over \mathbf{Z} (cf. [10]). Let $L_p(s)$ be the p -factor of the L function of C and put $L_S(s) = \prod_{p \in S} L_p(s)$ for any set S of prime numbers. Then the formal group obtained from $L_S(s)$ is strongly isomorphic to F over $\bigcap_{p \in S} (\mathbf{Z}_p \cap \mathbf{Q})$.

PROOF. Let G be the formal group obtained from $L_S(s)$. Since $L_p(s) = 1, (1 \pm p^{-s})^{-1}$ or of the form $(1 - a_p p^{-s} + p^{1-2s})^{-1}$, G is a formal group over \mathbf{Z} by Theorem 8. As a strong isomorphism of G to F is unique if it exists, it

suffices to prove $F \approx G$ over \mathbf{Z}_p for every $p \in S$. Let C_p be the reduction of C modulo p . The cases where C_p has a singular point were treated in [10]. Suppose that C_p is an abelian variety with $L_p(s) = (1 - a_p p^{-s} + p^{1-2s})^{-1}$. Since the Frobenius ξ of C_p satisfies

$$\xi^2 - a_p \xi + p = 0,$$

the transformer f of F satisfies

$$(6.6) \quad f^{-1}(pf(x) - a_p f(x^p) + f(x^{p^2})) \equiv 0 \pmod{p\mathbf{Z}_p}.$$

By Lemma 4.2 it follows from (6.6)

$$(6.7) \quad pf(x) - a_p f(x^p) + f(x^{p^2}) \equiv 0 \pmod{p\mathbf{Z}_p}.$$

The fact $F \approx G$ over \mathbf{Z}_p follows from (6.7), Theorem 8 and Theorem 2. This completes the proof of our theorem.

Notations being as above, put $L_C(s) = \prod_p L_p(s)$ and let G be the formal group attached to it. Then there is $\varphi(x) \in \mathbf{Z}[[x]]$ such that $\varphi(x) \equiv x \pmod{\text{deg } 2}$ and $F \circ \varphi = \varphi \circ G$. If the conjecture of Weil [21] on $L_C(s)$ is true, the power series φ would be the “ q -expansion” of a suitable automorphic function with respect to $\Gamma_0(N)$ where N is the conductor of C .

It would be interesting to see that our results yield a simple proof of a special case of the main result of Eichler [6] and Shimura [18]. Let $j(z)$ be the elliptic modular function and put $L = \mathbf{Q}(j(z), j(Nz))$ for $N \geq 2$. Then L is a field of algebraic function over \mathbf{Q} and LC is the field of automorphic functions with respect to the subgroup $\Gamma_0(N)$ of $\text{SL}(2, \mathbf{Z})$. We shall consider the case where the genus of L is equal to 1. Let C be a complete non-singular model for L over \mathbf{Q} . Since $j(z)$ has q -expansion

$$(6.8) \quad j(z) = q^{-1} + 744 + \dots$$

with coefficients in \mathbf{Z} where $q = \exp(2\pi\sqrt{-1}z)$, the infinite point $z = i\infty$ corresponds to a rational point \mathfrak{P} on C and C can be considered an abelian variety over \mathbf{Q} , with the origin \mathfrak{P} . Expanding the group law of C by means of the local parameter $j(z)^{-1}$ at \mathfrak{P} , we get a formal group F over \mathbf{Q} . By the theory of reduction there exists a finite set S' of prime numbers such that for $p \in S'$ the reduction C_p of $C \pmod{p}$ is non-singular and $j(z)^{-1}$ is a local parameter at the origin of C_p . Then, for $p \in S'$ F has p -integral coefficients and the p -th power endomorphism of the reduction F_p of $F \pmod{p}$ satisfies the same characteristic equation as that of C_p . Let f be the transformer of F . Then $df(x)$ is the canonical invariant differential on F , i.e. the $j(z)^{-1}$ -expansion of a differential of the first kind on C . Let $\varphi(q)$ be the q -expansion of $j(z)^{-1}$. Then $\varphi(x) \in \mathbf{Z}[[x]]$ and $\varphi(x) \equiv x \pmod{\text{deg } 2}$ by (6.8). Put

$$df(\varphi(x)) = \sum_{m=1}^{\infty} a_m x^{m-1} dx \quad (a_1 = 1).$$

Then, as is well-known, $\sum_{m=1}^{\infty} a_m q^m$ is the q -expansion of a cusp form of dimension -2 with respect to $\Gamma_0(N)$ and by Hecke [9] the Dirichlet series $\sum_{m=1}^{\infty} a_m m^{-s}$ has an Euler product of the form

$$\prod_{p \nmid N} (1 - a_p p^{-s})^{-1} \prod_{p \mid N} (1 - a_p p^{-s} + p^{1-2s})^{-1}, \quad a_p \in \mathbf{Z}.$$

Form $G(x, y) = g^{-1}(g(x) + g(y))$ with $g = f \circ \varphi$. By Theorem 8 G is a formal group over \mathbf{Z} , so that F is also a formal group over \mathbf{Z} . Let p be a prime number such that $p \in S'$ and $p \nmid N$. Then, by Corollary 2 of Theorem 8 the Frobenius of G_p is a root of the equation

$$(6.9) \quad p - a_p X + X^2 = 0.$$

Since $F \approx G$ over \mathbf{Z} , (6.9) is also the characteristic equation for the Frobenius of F_p , and then of C_p . Therefore $(1 - a_p p^{-s} + p^{1-2s})^{-1}$ coincides with the L function of C_p . This proves the principal theorem of [18] in this case.

REMARK. By considering Néron's minimal model for L , we can prove that the p -factor of the Hecke Dirichlet series coincides with that of the zeta function of L , assuming only that $j(z)^{-1}$ is a local parameter at the origin of C_p . See [10] as for the case C_p is singular. In view of the conjecture of Weil it is plausible that F is a formal minimal model for C .

6.3. We now deal with (c). We use the terminology, notations and results of Shimura [19]. Let Φ be an indefinite quaternion algebra over \mathbf{Q} and let \mathfrak{o} be a maximal order in Φ . For a natural number N prime to the discriminant of Φ , Γ_N denotes the group consisting of units γ in \mathfrak{o} such that $N(\gamma) = 1$ and $\gamma \equiv 1 \pmod{N\mathfrak{o}}$. Γ_N is a discontinuous group operating on the upper half plane. Let \mathfrak{R}_N be the field of automorphic functions relative to Γ_N and let n be its genus. Take $\mathfrak{X}_N, \mathfrak{C}_N$ and J_N as in [19]. \mathfrak{X}_N is a function field over \mathbf{Q} such that $\mathfrak{X}_N \mathbf{C} = \mathfrak{R}_N, \mathfrak{C}_N$ is its complete non-singular model and J_N is a Jacobian of \mathfrak{C}_N , each defined over \mathbf{Q} . Let $\mathfrak{D}_0(\mathfrak{C}_N)$ and $\mathfrak{D}_0(J_N)$ be the spaces of differentials of the first kind on \mathfrak{C}_N and J_N , respectively. For $f, g \in \mathfrak{X}_N, gdf \in \mathfrak{D}_0(\mathfrak{C}_N)$ if and only if $gf' \in S_2(\Gamma_N)$. Let $\omega = \{\omega_1, \dots, \omega_n\}$ be a base of $\mathfrak{D}_0(\mathfrak{C}_N)$, defined over \mathbf{Q} . Fixing a canonical map $\mathfrak{C}_N \rightarrow J_N$ (which may not be defined over \mathbf{Q}), let w and η be the corresponding bases of $S_2(\Gamma_N)$ and $\mathfrak{D}_0(J_N)$, respectively. For $\alpha \in \mathfrak{o}$ such that $N\alpha > 0, (N, \alpha) = 1, \Gamma_N \alpha \Gamma_N$ operates on $S_2(\Gamma_N)$ on the one hand. Let $\mathfrak{X}_2(\Gamma_N \alpha \Gamma_N)$ denote its representation matrix relative to w . On the other hand $\Gamma_N \alpha \Gamma_N$ yields a correspondence X_q of \mathfrak{C}_N over \mathbf{Q} where $q = \alpha\mathfrak{o}$ and then induces an endomorphism ξ of J_N . This ξ is defined over \mathbf{Q} ([19], p. 325). Denoting by $M^a(\xi)$ the representation matrix of ξ with respect to η ,

we have

$$(6.10) \quad M^d(\xi) = \mathfrak{X}_2(\Gamma_N \alpha \Gamma_N)$$

([19], p. 327), where $M^d(\xi) \in M_n(\mathbf{Q})$. By [19] the $\mathfrak{X}_2(\Gamma_N \alpha \Gamma_N)$ are semi-simple and commute with each other, and their eigenvalues are algebraic integers. Hence there is a regular matrix P in $M_n(\mathbf{Q})$ such that the $P^{-1}\mathfrak{X}_2(\Gamma_N \alpha \Gamma_N)P$ are all in $M_n(\mathbf{Z})$. By changing the bases if necessary, we may assume that the $\mathfrak{X}_2(\Gamma_N \alpha \Gamma_N)$ are already in $M_n(\mathbf{Z})$.

Let S_1 be the set of prime numbers which fail to satisfy at least one of P. 1)~10) in [19]. Then S_1 is a finite set. Let S_2 be the set of prime divisors of $d(\Phi)$. By Theorem 4 of [19] we have for $p \in S_1 \cup S_2$

$$(6.11) \quad \tilde{X}_q = \Pi + \Pi' \circ \tilde{Y}_p,$$

where q is an integral left \mathfrak{o} -ideal such that $N(q) = p$, Π is the Frobenius of $\tilde{\mathcal{C}}_N$ and Y_p is defined on p. 315 of [19]. Correspondingly we have

$$(6.12) \quad \tilde{\xi}_p = \pi + \pi' \circ \tilde{\eta}_p.$$

Now let $t = \{t_1, \dots, t_n\}$ be a system of local parameters ($\in \mathbf{Q}(J_N)$) at the origin of J_N . Expanding the group law of J_N into power series relative to t , we get an n -dimensional formal group F over \mathbf{Q} . We shall call this formal group a *formal model* for J_N . (A formal model is also obtained from the t -expansion of a base of $\mathfrak{D}_0(J_N)$, defined over \mathbf{Q}). By the theory of reduction ([20], Chapter III) there is a finite set S_3 of prime numbers such that for $p \in S_3$:

- (i) t is a system of local parameters at the origin of $\tilde{J}_N =$ the reduction of $J_N \pmod p$.
- (ii) The differentials η_1, \dots, η_n have good reductions $\pmod p$ and yield a base of $\mathfrak{D}_0(\tilde{J}_N)$.

Assume $p \in S_1 \cup S_2 \cup S_3$. Then F has coefficients in \mathbf{Z}_p and an endomorphism of $\tilde{\xi}$ of J_N , corresponding to some $\Gamma_N \alpha \Gamma_N$, induces an endomorphism of F over \mathbf{Z}_p . Let f be the transformer of F and let $f^{-1} \circ (C(\tilde{\xi})f)$ ($C(\tilde{\xi}) \in M_n(\mathbf{Z}_p)$) denote this endomorphism of F . Since $\tilde{\xi}'$ is also defined over \mathbf{Q} , it induces the endomorphism $f^{-1} \circ (C(\tilde{\xi}')f)$ of F over \mathbf{Z}_p . Now it follows from (6.12) that

$$\tilde{\xi}'_p = \pi' + \tilde{\eta}'_p \circ \pi$$

and then

$$(6.13) \quad p - \tilde{\xi}'_p \circ \pi + \tilde{\eta}'_p \circ \pi^2 = 0.$$

This implies

$$f^{-1}(pf(x) - C(\tilde{\xi}'_p)f(x^p) + C(\tilde{\eta}'_p)f(x^{p^2})) \equiv 0 \pmod{p\mathbf{Z}_p},$$

or by Lemma 4.2

$$(6.14) \quad pf(x) - C(\xi'_p)f(x^p) + C(\eta'_p)f(x^{p^2}) \equiv 0 \pmod{p\mathbf{Z}_p}.$$

Let E be the subring of $\text{End}_{\mathbf{Q}}J_N$ generated by endomorphisms corresponding to $\{F_N \alpha F_N \mid \alpha \in \mathfrak{o}, N(\alpha) > 0, (\alpha, N) = 1\}$. Then, as $E \otimes \mathbf{Q}$ is a commutative semi-simple algebra over \mathbf{Q} , the map $\xi \mapsto \xi'$ yields an isomorphism of E into $\text{End}_{\mathbf{Q}}J_N$. Now J_N is self-dual and $M^d(\xi')$ is the transposed matrix of $M^d(\xi)$, since $M^d(\xi) \in M_n(\mathbf{Q})$. (For example see [20], p. 25). As $M^d(\xi')$ is conjugate with $M^d(\xi)$, $M^d(\xi)$ and $M^d(\xi')$ have the same trace. Therefore there is an invertible matrix $P_1 \in M_n(\mathbf{Q})$ such that

$$(6.15) \quad M^d(\xi') = P_1^{-1}M^d(\xi)P_1 \quad \text{for all } \xi \in E.$$

Now since the t -expansion of η is a base of $\mathfrak{D}^*(F; \mathbf{Q})$ and $C(\xi')$ ($\xi \in E$) is the representation matrix of ξ' relative to the canonical base $df(x)$ of $\mathfrak{D}^*(F; \mathbf{Q})$, we can find an invertible matrix $P_2 \in M_n(\mathbf{Q})$ such that

$$(6.16) \quad C(\xi') = P_2^{-1}M^d(\xi')P_2 \quad \text{for all } \xi \in E.$$

Putting $P_3 = P_1P_2$, we get from (6.15), (6.16)

$$(6.17) \quad C(\xi') = P_3^{-1}M^d(\xi)P_3 \quad \text{for all } \xi \in E.$$

Let S_4 be the set of prime numbers p such that P_3 or P_3^{-1} is not p -integral, and put $S = \bigcup_{i=1}^4 S_i$. S is a finite set. For $p \notin S$ we get from (6.14) and (6.17)

$$(6.18) \quad pP_3f(x) - M^d(\xi_p)P_3f(x^p) + M^d(\eta_p)P_3f(x^{p^2}) \equiv 0 \pmod{p\mathbf{Z}_p}.$$

Now replacing the parameters $t = {}^t(t_1, \dots, t_n)$ by $u = P_3t$, we obtain the formal model $H(x, y) = P_3F(P_3^{-1}x, P_3^{-1}y)$ of J_N , with the transformer $h(x) = P_3f(P_3^{-1}x)$. For $p \notin S$ we have

$$(P_3^{-1}x)^{p^\nu} \equiv P_3^{-1}x^{p^\nu} \pmod{p\mathbf{Z}_p}$$

and then by Lemma 4.2

$$(6.19) \quad f((P_3^{-1}x)^{p^\nu}) \equiv f(P_3^{-1}x^{p^\nu}) \pmod{p\mathbf{Z}_p}.$$

By (6.18) and (6.19) we get finally

$$(6.20) \quad ph(x) - M^d(\xi_p)h(x^p) + M^d(\eta_p)h(x^{p^2}) \equiv 0 \pmod{p\mathbf{Z}_p}$$

for $p \notin S$.

Now we have

$$(6.21) \quad M^d(\xi_p) = \mathfrak{F}_2(p; N_0) \quad \text{and} \quad M^d(\eta_p) = R_2(p; N_0)$$

([19], p. 327). Let M be the product of all primes in S and put $\mathbf{Z}'_S = \bigcap_{p \notin S} (\mathbf{Z}_p \cap \mathbf{Q})$.

The Dirichlet series

$$\prod_{p \nmid MN} [I_n - \mathfrak{F}_2(p; N_0)p^{-s} + R_2(p; N_0)p^{1-2s}]^{-1} = \sum_{(m, MN)=1} \mathfrak{F}_2(m; N_0)m^{-s}$$

is a main part of the one defined in [19]. Let G be the formal group over \mathbf{Z} corresponding to it by Theorem 8. By Theorem 2 it follows from (6.20) and (6.21) that $G \approx H$ over \mathbf{Z}_p for every $p \in S$. Hence $G \approx H$ over \mathbf{Z}'_S by the uniqueness of strong isomorphism. We have proved the following theorem:

THEOREM 10. *Let notations be as in [19] and let \mathfrak{F}_2 be an integral representation as above. Then there is a finite set S of prime numbers such that the formal group obtained from the Dirichlet series $\sum_{(m, MN)=1} \mathfrak{F}_2(m; N_0) m^{-s}$ is strongly isomorphic over \mathbf{Z}'_S to a formal model for J_N .*

Thus the matrix Dirichlet series $\sum \mathfrak{F}_2(m; N_0) m^{-s}$ itself (not only its determinant) has important significance for J_N . What kind of curve over \mathbf{Q} has a Jacobian whose formal completion is isomorphic to a formal group corresponding to a matrix Dirichlet series with Euler product?

6.4. All zeta functions, which we studied in 6.2 and 6.3, are of the form $\prod_p (I_n + C_p p^{-s} + C_{p^2} p^{1-2s})^{-1}$. Do there exist number-theoretic Dirichlet series of the form (6.1) such that not all C_{p^ν} are equal to 0 for $\nu \geq 3$? If such ones exist, formal groups over \mathbf{Z} obtained from them would be non-algebraic. Their transformers would be obtained from analytic functions, perhaps satisfying suitable kinds of differential equations.

Osaka University

References

- [1] E. Artin and H. Hasse, Die beiden Ergänzungssätze zum Reziprozitätsgesetz der l^n -ten Potenzreste im Körper der l^n -ten Einheitswurzeln, Abh. Math. Sem. Univ. Hamburg, **6** (1928), 146-162.
- [2] I. Barsotti, Moduli canonici e gruppi analitici commutativi, Ann. Scuola Norm. Sup. Pisa, **13** (1959), 303-372.
- [3] N. Bourbaki, Algèbre, Chapitre IV., 2^e éd., Hermann, Paris, 1959.
- [4] J. Dieudonné, Lie groups and Lie hyperalgebras over a field of characteristic $p > 0$ (IV), Amer. J. Math., **77** (1955), 429-452.
- [5] J. Dieudonné, Groupes de Lie et hyperalgèbres de Lie sur un corps de caractéristique $p > 0$ (VII), Math. Ann., **134** (1957), 114-133.
- [6] M. Eichler, Quaternäre quadratische Formen und die Riemannsche Vermutung für die Kongruenzzetafunktion, Arch. Math., **5** (1954), 355-366.
- [7] A. Fröhlich, Formal groups, Lecture Notes in Mathematics, Springer, Berlin-Heidelberg-New York, 1968.
- [8] P. Gabriel, Sur les catégories localement noethériennes et leurs applications aux algèbres étudiées par Dieudonné, Séminaire J. P. Serre, (1960).
- [9] E. Hecke, Über Modulfunktionen und die Dirichletscher Reihen mit Eulerscher Produktentwicklung II, Math. Ann., **114** (1937), 316-351; Mathematische Werke, 672-707.
- [10] T. Honda, Formal groups and zeta-functions, Osaka J. Math., **5** (1968), 199-213.
- [11] M. Lazard, Sur les groupes de Lie formels à un paramètre, Bull. Soc. Math.

- France, **83** (1955), 251-274.
- [12] M. Lazard, Lois de groupes et analyseurs, *Ann. Sci. École Norm. Sup.*, (3) **72** (1955), 299-400.
 - [13] J. Lubin, One-parameter formal Lie groups over p -adic integer rings, *Ann. of Math.*, **80** (1964), 464-484.
 - [14] J. Lubin and J. Tate, Formal complex multiplication in local fields, *Ann. of Math.*, **81** (1965), 380-387.
 - [15] R. Lyndon, The cohomology theory of group extensions, *Duke Math. J.*, **15** (1948), 271-292.
 - [16] Y. Manin, The theory of commutative formal groups over fields of finite characteristic, *Russian Math. Surveys*, **18** (1963), 1-81.
 - [17] A. Néron, Modèles minimaux des variétés abéliennes sur les corps locaux et globaux, *Publ. Math. I. H. E. S.*, **21** (1964).
 - [18] G. Shimura, Correspondances modulaires et les fonctions ζ de courbes algébriques, *J. Math. Soc. Japan*, **10** (1958), 1-28.
 - [19] G. Shimura, On the zeta-functions of the algebraic curves uniformized by certain automorphic functions, *J. Math. Soc. Japan*, **13** (1961), 275-331.
 - [20] G. Shimura and Y. Taniyama, Complex multiplication of abelian varieties and its applications to number theory, *Publ. Math. Soc. Japan*, No. 6, 1961.
 - [21] A. Weil, Über die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen, *Math. Ann.*, **168** (1967), 149-156.
 - [22] E. Witt, Zyklische Körper und Algebren der Charakteristik p vom Grad p^n , *J. Reine Angew. Math.*, **176** (1936), 126-140.
-