J. Math. Kyoto Univ.
5-1 (1965) 45-59

On formal rings

By

Masayoshi MIYANISHI

(Received August 30, 1965)

Part I

1. In the following, we shall fix a ground field K of positive characteristic p.

Let R be an algebraic system composed by a system of sets of n-indeterminates, $x=(x_1, \cdots, x_n)$, $y=(y_1, \cdots, y_n)$, $\cdots$ (we call them generic points) and two sets of non-zero formal power series with coefficients in K

$$\varphi_i(x_1, \cdots, x_n;\ y_1, \cdots, y_n),\quad \psi_i(x_1, \cdots, x_n;\ y_1, \cdots, y_n),\quad 1 \leqq i \leqq n,$$

with respect to $2n$-indeterminates $x_1, \cdots, x_n;\ y_1, \cdots, y_n$, satisfying the following conditions;

(F1) *R is an abelian formal group with respect to* $(\varphi_1, \cdots, \varphi_n)$, *(see* [1]*),*

(F2) $\psi_i(\psi(x, y), z) = \psi_i(x, \psi(y, z))$, *we call* $(\psi_1, \cdots, \psi_n)$ *the multiplication of x and y in R,*

(F3) $\varphi_i(\psi(x, y), \psi(x, z)) = \psi_i(x, \varphi(y, z))$,

$\qquad \varphi_i(\psi(x, z), \psi(y, z)) = \psi_i(\varphi(x, y), z)$, $1 \leqq i \leqq n$.

We call R a *formal ring* of dimension n defined over K, and write

$$x \cdot y = (\psi_1(x, y), \cdots, \psi_n(x, y)),\quad x \dot{+} y = (\varphi_1(x, y), \cdots, \varphi_n(x, y)).$$

We shall follow the notation and the terminology of [1].

2. Let $\mathcal{O}$ be the ring of all formal power series with respect to $x_1, \cdots, x_n$ which have coefficients in K. For $f \in \mathcal{O}$, and two generic points x, y,

put
$$f(y \cdot x) = \sum_{\alpha} y^{\alpha}(X_{\alpha} f),\quad X_{\alpha} f \in \mathcal{O}, \tag{1}$$

$$f(x \cdot y) = \sum_{\alpha} y^{\alpha}(Y_{\alpha} f),\quad Y_{\alpha} f \in \mathcal{O}, \tag{2}$$

$$f(x \dot{+} y) = \sum_{\beta} y^{\beta}(Z_{\beta} f),\quad Z_{\beta} f \in \mathcal{O}. \tag{3}$$

From the theory of formal groups, it is known that $Z_0 = I$ (identity) and that Z_β is a special semi-derivation of height $h(\beta)+1$. X_α, Y_α, Z_α, $\alpha \in N^n$ are K-linear endomorphisms of K-vector space $\mathcal{O}$.

Put
$$(x \cdot y)^{\gamma} = \sum_{\alpha,\beta} c_{\beta\alpha\gamma} x^{\alpha} y^{\beta},\quad c_{\beta\alpha\gamma} \in K \tag{4}$$

$$(x \dot{+} y)^{\gamma} = \sum_{\alpha,\beta} d_{\beta\alpha\gamma} x^{\alpha} y^{\beta},\quad d_{\beta\alpha\gamma} \in K. \tag{5}$$

Note that $d_{\alpha\beta\gamma} = 0$ if $|\gamma| > |\alpha| + |\beta|$, $c_{\alpha\beta\gamma} = 0$ if $|\gamma| > |\alpha|, |\beta|$,

and that
$$c_{\alpha 0\gamma} = c_{0\alpha\gamma} = 0, \text{ (except } c_{000} = 1), \tag{6}$$
$$d_{\alpha 0\gamma} = d_{0\alpha\gamma} = \delta_{\alpha\gamma},\quad d_{\alpha\beta\gamma}, = d_{\beta\alpha\gamma}.$$

Then applying the argument analogous to the one used in [**1**, $n°11$], we obtain the following relations,

$$X_\beta X_\alpha = \sum_{\gamma} c_{\beta\alpha\gamma} X_\gamma,\qquad Y_\beta Y_\alpha = \sum_{\gamma} c_{\alpha\beta\gamma} X_\gamma,$$
$$Z_\beta Z_\alpha = \sum_{\gamma} d_{\beta\alpha\gamma} Z_\gamma,\qquad X_\alpha Y_\beta = Y_\beta X_\alpha,$$
$$Z_\beta X_\alpha = \sum_{\substack{0 \leq \gamma \leq \alpha \\ \delta}} c_{\beta\gamma\delta} X_{\alpha-\gamma} Z_\delta,\quad Z_\beta Y_\alpha = \sum_{\substack{0 \leq \gamma \leq \alpha \\ \delta}} c_{\gamma\beta\delta} Y_{\alpha-\gamma} Z_\delta. \tag{7}$$

Moreover we have "the generalized Leibnitz formula",

$$T_\alpha(fg) = \sum_{0 \leq \beta \leq \alpha} (T_\beta f)(T_{\alpha-\beta} g),\quad T = X,\ Y,\ Z, \text{ for } f, g \in \mathcal{O}. \tag{8}$$

The next result is easily obtained.

Proposition 1. *The following conditions are equivalent.*

(1) *The multiplication of R is commutative.*

(2) $X_\alpha = Y_\alpha$, *for all* $\alpha \in \boldsymbol{N}^n$.

(3) $c_{\alpha\beta\gamma} = c_{\beta\alpha\gamma}$, *for all* $\alpha, \beta, \gamma \in \boldsymbol{N}^n$.

Then $X_\beta X_\alpha = X_\alpha X_\beta$ *for all* $\alpha, \beta \in \boldsymbol{N}^n$.

If we put $\varepsilon_i = (0, \cdots, 0, \overset{\overset{i}{\vee}}{1}, 0, \cdots, 0)$, $1 \leqq i \leqq n$, we have

$$\psi_i(x, y) = (x \cdot y)^{\varepsilon_i} = \sum_{\alpha, \beta} c_{\beta\alpha\varepsilon_i} x^\alpha y^\beta, \tag{9}$$

$$\varphi_i(x, y) = (x \dot{+} y)^{\varepsilon_i} = \sum_{\alpha, \beta} d_{\beta\alpha\varepsilon_i} x^\alpha y^\beta. \tag{10}$$

3. Conversely:

Proposition 2. *For each* $\alpha \in \boldsymbol{N}^n$, *let* X_α, Y_α, Z_α *be K-linear endomorphisms of* $\mathcal{O}$ *such that*

(i) $Z_0 = I$ *(identity)*,

(ii) Z_α *is a special semi-derivation of height* $h(\alpha) + 1$,

(iii) *these operators verify the conditions* (6), (7), (8) *for the sets of operators* $\{c_{\alpha\beta\gamma}, d_{\alpha\beta\gamma}\}$, $(\alpha, \beta, \gamma) \in \boldsymbol{N}^n \times \boldsymbol{N}^n \times \boldsymbol{N}^n$,

(iv) *these operators operate on* $\mathcal{O}$ *with the next formulae,* $X_\beta x^\alpha = \sum_\gamma c_{\gamma\beta\alpha} x^\gamma$, $Y_\beta x^\alpha = \sum_\gamma c_{\beta\gamma\alpha} x^\gamma$, $Z_\beta x^\alpha = \sum_\gamma d_{\gamma\beta\alpha} x^\gamma$.

Then formulae (9), (10) *define a formal ring, for which* (1), (2), (3) *are Taylor formulae.*

This result can be proved by an argument analogous to the one used in [2].

4. We shall consider a one-dimensional formal ring.

Let $\psi(x, y) = a_{11} xy + \sum_{k \geqq 3} \sum_{i+j=k} a_{ij} x^i y^j$, where $a_{ij} \in K$, $a_{i0} = a_{0j} = 0$, $i, j \geqq 2$.

We use the following Lemmas.

Lemma 1. If $a_{11} = 0$, *then* $\psi(x, y) = 0$.

Proof. Let α be the smallest integer such that $a_{\alpha j} \neq 0$ for some j and let β be the smallest integer such that $a_{\alpha\beta} \neq 0$. Then $\alpha \geqq 1$ (when $\alpha = 1$, $\beta \geqq 2$). We shall order lexicographically monomials with respect to x, y, z by putting $cx^iy^jz^k < c'x^{i'}y^{j'}z^{k'}$, c, $c' \in K$, c, $c' \neq 0$, if the first non-zero difference of $i'-i$, $j'-j$, $k'-k$ is positive. In $(x \cdot y) \cdot z$ the minimal monomial is $a_{\alpha\beta}^{\alpha+1} x^{\alpha 2} y^{\alpha\beta} z^{\beta}$ and in $x \cdot (y \cdot z)$, the minimal monomial is $a_{\alpha\beta}^{\beta+1} x^{\alpha} y^{\alpha\beta} z^{\beta 2}$. As $(x \cdot y) \cdot z = x \cdot (y \cdot z)$, we have $\alpha = \beta = 1$, which contradicts the assumption. q.e.d.

Lemma 2. (*Theorem of J. Dieudonné* [2] *concerning the classification of one-dimensional formal groups.*) *In the following, we write* $\overline{Z}_k$ *instead of* Z_{p^k}, $k \geqq 0$, *and suppose that the ground field* K *is algebraically closed. Any formal group* G *of dimension* 1 *over* K *is isomorphic to one of the following three types.*
(1) *If* $\overline{Z}_0^p = \lambda \overline{Z}_0$, $\lambda \neq 0$, *G is isomorphic to the multiplicative group (with the group law* $(x, y) \to x + y + xy$).
(2) *If* $\overline{Z}_0^p = 0$ *and if there exists the smallest integer* $r > 0$ *such that* $\overline{Z}_r^p \neq 0$, *then G is isomorphic to the group with the associated hyperalgebra such that* $\overline{Z}_k^p = 0$, *for* $k < r$, *and* $\overline{Z}_k^p = \overline{Z}_{k-r}$, *for* $k \geqq r$.
(3) *If* $\overline{Z}_k^p = 0$, *for all* $k \geqq 0$, *then G is isomorphic to the additive group (with the group law* $(x, y) \to x + y$).

Lemma 3. (1) $c_{p^k, 0, \delta} = 0$ *for any* δ *and* $k \geqq 0$.
(2) $\overline{Z}_k X_0 = 0$, *for* $k \geqq 0$.

Proof. (1) is trivial.
(2) If $f(x) = \sum_{\alpha} a_\alpha x^\alpha$, then $X_0 f = a_0$, that is, X_0 is a function which takes as a value a constant term of $f(x)$. Therefore $\overline{Z}_k X_0 = 0$, $k \geqq 0$ is trivial.

Lemma 4. *As the addition of one-dimensional formal ring, we cannot take the group law of type* (1) *and* (2) *of Lemma* 2.

Proof. Type (1). We have $Z_1^p X_1 = \lambda Z_1 X_1$. However, $Z_1 X_1 = \sum_{\delta} (c_{11\delta} X_0 Z_\delta + c_{10\delta} X_1 Z_\delta) = \sum_{\delta} c_{11\delta} X_0 Z_\delta$. Therefore $Z_1^p X_1 = 0$ from Lemma 3. Hence $Z_1 X_1 = 0$. But when we take x for $f(x)$, we have $Z_1 X_1 f = Z_1 (a_{11} x + \sum_{j \geq 2} a_{1j} x^j)$, and $(Z_1 X_1 f)(e) = a_{11} \neq 0$. This gives a contradiction.

Type (2). It follows that $\overline{Z}_k X_1 = \sum_\delta (c_{p^k,1,\delta} X_0 Z_\delta + c_{p^k,0,\delta} X_1 Z_\delta) = \sum_\delta (c_{p^k,1,\delta} X_0 Z_\delta)$. Hence $\overline{Z}_k^p X_1 = 0$. If we take r for k and x for $f(x)$, we have $\overline{Z}_r^p X_1 = Z_1 X_1 = 0$ and $Z_1 X_1 f \neq 0$. This gives a contradiction.

q.e.d.

Lemma 5. *If the addition is given by* $\varphi(x, y) = x + y$, *then with some change of variables of type* $x \to x + \sum_{i=1} a_i x^{p^i}$, *we can transfer the multiplication to* $\psi(x, y) = xy$.

Proof $\psi(x, y)$ is given in the next form $\psi(x, y) = b_{00} xy + \sum_{i,j} b_{ij} x^{p^i} y^{p^j}$, $b_{00} \neq 0$. If we change variables by $v_0^{-1}(x) = (1/b_{00}) x$, we have $\psi_0(x, y) = xy + \sum_{i,j} b_{ij}^{(0)} x^{p^i} y^{p^j}$. If some coefficients $b_{i0}^{(0)}$, $b_{0j}^{(0)}$ are not zero, then take α the smallest positive integer such that $b_{\alpha 0}^{(0)} \neq 0$. We can easily show that $b_{0\alpha}^{(0)} \neq 0$, $b_{\alpha 0}^{(0)} = b_{0\alpha}^{(0)}$, and $b_{0i}^{(0)} = 0$ for $0 < i < \alpha$. By a change of variables $v_{(\alpha)}^{-1}(x) = x - b_{0\alpha}^{(0)} x^{p^\alpha}$, we have a new formal series for the multiplication $\psi_{(\alpha)}(x, y) = xy + \sum_{i,j} b_{ij}^{(\alpha)} x^{p^i} y^{p^j}$, where $b_{i0}^{(\alpha)} = b_{0i}^{(\alpha)} = 0$, for $0 < i \leqq \alpha$. Let β be the smallest positive integer such that $b_{\beta 0}^{(\alpha)} \neq 0$, if there exists some coefficient $b_{i0}^{(\alpha)} \neq 0$. Then $\beta > \alpha$. By the analogous process, a change of variables $v_{(\beta)}^{-1}(x) = x - b_{0\beta}^{(\alpha)} x^{p^\beta}$ transfers $\psi_{(\alpha)}(x, y)$ to $\psi_{(\beta)}(x, y) = xy + \sum_{i,j} b_{ij}^{(\beta)} x^{p^i} y^{p^j}$, where $b_{i0}^{(\beta)} = b_{0i}^{(\beta)} = 0$, if $0 < i \leqq \beta$.

Thus continuing this process, we have the following. By the change of variables $v = v_0 v_\alpha v_\beta \cdots$, we have $\bar{\psi}(x, y) = xy + \sum_{(i,j) \geqq (1,1)} \bar{a}_{ij} x^{p^i} y^{p^j}$. But from the associative law for the multiplication, we have $\bar{\psi}(x, y) = xy$.

q.e.d.

Summarizing the preceding Lemmas, we get:

Theorem. *If the ground field* K *of characteristic* $p > 0$ *is algebraically closed, any one-dimensional formal ring is isomorphic to the formal ring of type* $(x + y, xy)$.

Corollary. *Any one-dimensional formal ring is commutative.*

Remark. We can prove Corollary by the method of M. Lazard [7]. In his argument, we have only to replace $h(x, y)$ by $x\cdot y \dot{-} y\cdot x$.

5. Let R be a formal ring of dimension n. Define $\theta_{ij}(x)\in\mathcal{O}$, $1\leqq i, j\leqq n$, as follows;

$$\psi_i(y, x)=\sum_{j=1}^{n}\theta_{ij}(x)y_j+\text{(terms of total degree }\geqq 2\text{ with respect to }y=(y_1, \cdots, y_n)).$$

Then from the distributive law $\psi_i(z, \varphi(x, y))=\varphi_i(\psi(z, x), \psi(z, y))$, we get $\theta_{ij}(\varphi(x, y))=\theta_{ij}(x)+\theta_{ij}(y)$, $1\leqq i, j\leqq n$. Also from the associative law, $\psi_i(z, \psi(x, y))=\psi_i(\psi(z, x), y)$, we get $\theta_{ij}(\psi(x, y))=\sum_{k=1}^{n}\theta_{ik}(x)\theta_{kj}(y)$, $1\leqq i, j\leqq n$.

If we associate to R a $n\times n$-matrix $\theta(x)=(\theta_{ij}(x))$, we have a representation of R, $\theta(\varphi(x, y))=\theta(x)+\theta(y)$, $\theta(\psi(x, y))=\theta(x)\cdot\theta(y)$.

Lemma 6. *If all $\theta_{ij}(x)$, $1\leqq i, j\leqq n$ are zero, then all $\psi_i(x, y)$ $1\leqq i\leqq n$, are zero.*

Proof. Assume that $\psi_i(y, x)$ is not zero. Let s be the smallest integer such that in $\psi_i(y, x)$, there exists a term $ax^\gamma y^\delta$ where $|\delta|=s$, and $a\neq 0$. Then $s\geqq 2$. Let $z=(z_1, \cdots, z_n)$ be another generic point. We have $\psi_i(z, \psi(y, x))=\psi_i(\psi(z, y), x)$. In the left hand side, the minimal value of total degree with respect to z is s, but in the right hand side, the minimal value of total degree with respect to z is $>s$. This gives a contradiction. q. e. d.

Part 2

In Part 2 and Part 3, the ground field K is assumed to be algebraically closed. Moreover we add the next condition to the definition of formal ring:

$(F4)$ *$\psi_1, \cdots, \psi_n$ are analytically independent over K.*

We shall prove that the underlying additive group of a formal ring is unipotent.

1. First we quote some results of J. Dieudonné from [1], [4], [5].

Lemma 1. (Homomorphism theorem, [1])

Let G and $\overline{G}$ be formal groups of dimension m and n defined over K and u be a homomorphism from G to $\overline{G}$ defined over K. By appropriate changes of variables in G and $\overline{G}$, we can suppose that we have,

$$
\begin{aligned}
&u_i(x)=x_i\,, && \text{for}\quad 1\leqq i\leqq r_0\,,\\
&u_i(x)=x_i^p\,, && \text{for}\quad r_0+1\leqq i\leqq r_0+r_1\,,\\
&\qquad\cdots\cdots\cdots\cdots\cdots\cdots && \\
&u_i(x)=x_i^{p^t}, && \text{for}\quad r_0+\cdots+r_{t-1}+1\leqq i\leqq r_0+\cdots+r_t\,,\\
&u_i(x)=0\,, && \text{for}\quad i>r_0+\cdots+r_t\,.
\end{aligned}
$$

We shall denote $\rho=r_0+\cdots+r_t$ and call ρ the *rank* of u and t (the greatest integer such that $r_t\neq 0$) the *height* of u. We say that u is *injective* if $\rho=\dim G$, *surjective* if $\rho=\dim \overline{G}$, and *isogeny* if u is both injective and surjective.

Corollary. *Let (G, u) be a subgroup of a formal group G'. Then there exist an isomorphism $G'\rightarrow G_1'$ and an isogeny $G\rightarrow H_1$ of G onto a typical subgroup of G_1' such that the diagram*

$$
\begin{array}{ccc}
G & \xrightarrow{\quad u \quad} & G' \\
\downarrow & & \downarrow \\
H_1 & \xrightarrow[j]{\quad} & G_1'
\end{array}
$$

is commutative.

The proof is given in [1], [5].

Lemma 2. *Any abelian formal group over K is isogenous to a direct product of additive Witt groups, multiplicative groups and simple groups.* (See [4], [8])

Lemma 3. *Any abelian simple group of dimension n over K is isogenous to a group $G_{n,1,m}$ where m is a positive integer prime to n. $G_{n,1,m}$ has a hyperalgebra characterized by the following multiplication law,*

$$\begin{aligned} &\bar{Z}^p_{h,i} = \bar{Z}_{h,i+1}, && h=0,1,\cdots;\ 1\leqq i\leqq n-1,\\ &\bar{Z}^p_{h,n} = 0, && 0\leqq h\leqq m,\\ &\bar{Z}^p_{m+h,n} = \bar{Z}_{h,1}, && h=0,1,\cdots. \quad \textit{Here}\quad \bar{Z}_{h,i} = Z_{p^h\varepsilon_i}. \end{aligned}$$

2. Any abelian formal group G of dimension n is isogenous to a group $G' = \prod_i W_{n_i} \times \prod_j G_{n_j,1,m_j} \times (G_m)^l$, $(n_j, m_j) = 1$, $\sum_i n_i + \sum_j n_j + l = n$. Let u be an isogeny from G' to G. Then there exists a unipotent subgroup $u(\prod_i W_{n_i}) = \boldsymbol{U}$ in G. By Corollary, there exist an isomorphism $G \to G_1$ and an isogeny $\boldsymbol{U} \to \boldsymbol{U}_1$ of $\boldsymbol{U}$ onto a typical subgroup $\boldsymbol{U}_1$ of G_1 such that:

(1) $G_1/\boldsymbol{U}_1$ has no unipotent subgroup,

(2) the diagram $\begin{array}{ccc} G & \longrightarrow & G_1 \\ \uparrow & & \uparrow \\ \boldsymbol{U} & \longrightarrow & \boldsymbol{U}_1 \end{array}$ is commutative.

We have the next result of J. Dieudonné [5].

Lemma 4. *Let G be a commutative formal group of dimension n and let (J, L) be an arbitrary partition of* $[1, n]$. *There exist two uniquely determined systems of power series without constant terms $u(x) = (u_i(x))_{1\leq i\leq n}$ and $v(x) = (v_i(x))_{1\leq i\leq n}$ such that $u_k(x) = 0$ for $k\in L$, $v_j(x) = 0$ for $j\in J$ and $u(x) \dot{+} v(x) = x$.*

3. Let R be a formal ring of dimension n. For our purpose, we can assume that R contains a typical unipotent subgroup $\boldsymbol{U}$ such that $R/\boldsymbol{U}$ has no unipotent subgroup. Let J be a subset of $[1, n]$ corresponding to $\boldsymbol{U}$. Then J satisfies the following conditions;

(1) Card $(J) = \dim \boldsymbol{U}$,

(2) for any system $(y_j)_{j\in J} = y$ of indeterminates, define $j(y) = (j_i(y))$ as the system of power series $j_i(y) = y_i$, for $i\in J$, $j_i(y) = 0$ otherwise; then we have $\varphi_i(j(y), j(z)) = 0$, for all $i\notin J$.

By Lemma 4, there exist two uniquely determined systems of power series $r(x) = (r_j(x))_{j\in J}$ and $h(x) = (h_i(x))_{1\leq i\leq n}$ such that $h_i(x) = 0$ for $i\in J$, and $x = j(r(x)) \dot{+} h(x)$. Then we have $h(x \dot{+} y) = h(h(x) \dot{+} h(y))$, $h(x\cdot y) = h(h(x)\cdot h(y))$.

For the proof of the latter equality, we need the next Lemma.

Lemma 5. *Let G, G' be abelian formal groups with their typical unipotent subgroups $(\boldsymbol{U}, j)$, $(\boldsymbol{U}', j')$ such that $G/\boldsymbol{U}$, $G'/\boldsymbol{U}'$ have no unipotent subgroup, and u be a homomorphism from G to G'. Then there exists a homomorphism $u': \boldsymbol{U}\to\boldsymbol{U}'$ such that $u\cdot j=j'\cdot u'$,*

$$\begin{tikzcd} \boldsymbol{U} \arrow[r, "j"] \arrow[d, "u'"'] & G \arrow[d, "u"] \\ \boldsymbol{U}' \arrow[r, "j'"'] & G' \end{tikzcd} .$$

Proof. Let $x=j(r(x)\dot{+}h(x)$, $x'=j'(r'(x'))\dot{+}h'(x')$ be partitions corresponding to $(G, \boldsymbol{U})$ and $(G', \boldsymbol{U}')$ respectively. Since $\boldsymbol{U}$ is unipotent and $G'/\boldsymbol{U}'$ has no unipotent subgroup, a composition of homomorphisms $\boldsymbol{U}\to G\to G'\to G'/\boldsymbol{U}'$ is trivial. Hence, for a generic point x of $\boldsymbol{U}$, $h'(u(j(x)))=0$ and $u(j(x))=j'(r'(u(j(x))))$. We can prove easily that $r'\cdot u\cdot j$ is a homomorphism. Therefore we have only to take $r'\cdot u\cdot j$ as u'. q.e.d.

For generic points x, y of R, we have

$$\begin{aligned} x\cdot y&=j(r(x\cdot y))\dot{+}h(x\cdot y)\\ &=(j(r(x))\dot{+}h(x))\cdot(j(r(y))\dot{+}h(y))\\ &=j(r(x))\cdot\{j(r(y))\dot{+}h(y)\}\dot{+}h(x)\cdot j(r(y))\\ &\qquad\dot{+}j(h(x)\cdot h(y))\dot{+}h(h(x)\cdot h(y)). \end{aligned}$$

Here from Lemma 5, $j(r(x))\cdot\{j(r(y))\dot{+}h(y)\}$, $h(x)\cdot j(r(y))$ are contained in $j(\boldsymbol{U})$ because the multiplication by $j(r(y))\dot{+}h(y)$, $h(x)$ are homomorphisms of the formal group R. Hence we have the equality $h(x\cdot y)=h(h(x)\cdot h(y))$.

Put $L=[1, n]-J$. For a system $\bar{x}=(\bar{x}_k)_{k\in L}$ of indeterminates, let $\sigma(\bar{x})$ be the system $(\sigma_i(\bar{x}))_{1\le i\le n}$ of power series such that $\sigma_i(\bar{x})=0$ for $i\in J$, $\sigma_i(\bar{x})=\bar{x}_i$ for $i\in L$.

Put $\quad \sigma\Phi(\bar{x}, \bar{y})=h(\sigma(\bar{x})\dot{+}\sigma(\bar{y}))$, $\sigma\Psi(\bar{x}, \bar{y})=h(\sigma(\bar{x})\cdot\sigma(\bar{y}))$.

Then we can show that Φ, Ψ define a ring law on the quotient group $R/\boldsymbol{U}$, and that the system $\overline{h}(x)=(h_i(x))_{i\in L}$ is a homomorphism from R to $R/\boldsymbol{U}$.

Now we consider the next assertion:

Theorem 1. *There is no formal ring of which underlying formal group is isogenous to* $(G_m)^t\times\prod_{(n,m)=1}G_{n,1,m}$, *where* G_m *is the multiplicative group.*

If we can prove Theorem 1, we know that there exists only trivial ring law on $R/\boldsymbol{U}$, that is, all $(\Psi_i)_{i\in L}$ are zero.

Therefore
$$\begin{aligned} x\cdot y &= j(r(x\cdot y))\dot{+}h(x\cdot y)=j(r(x\cdot y))\dot{+}h(h(x)\cdot h(y))\\ &=j(r(x\cdot y))\dot{+}h(\sigma\overline{h}(x)\cdot\sigma\overline{h}(y))\\ &=j(r(x\cdot y))\dot{+}\sigma\Psi(\overline{h}(x),\overline{h}(y))\\ &=j(r(x\cdot y)).\end{aligned}$$

This contradicts to our hypothesis that $\psi_1,\cdots,\psi_n$ are analytically independent over K, if $R/\boldsymbol{U}\neq 0$. Hence we have:

Theorem 2. *The underlying abelian formal group of a formal ring is unipotent.*

Part 3

1. We denote by $\mathcal{O}_r$ the ring $\mathcal{O}^{p^r}$, $r\in\boldsymbol{Z}$ and put $\mathcal{O}'=\bigcup_r\mathcal{O}_r$.

From now on, when we denote an index by $\alpha=(\alpha_1,\cdots,\alpha_n)$, it always means the index of which components are of the following type,

$$a_{-t}p^{-t}+a_{-t+1}p^{-t+1}+\cdots+a_{-1}p^{-1}+a_0+a_1p+\cdots+a_rp^r \qquad (*)$$

where $a_{-t},\cdots,a_r$ are integers such that $0\leqq a_{-t},\cdots,a_r\leqq p-1$.

For such α, we define $h(\alpha)$ the smallest integer r for which $\alpha_i<p^{r+1}$, $1\leqq i\leqq n$ and $\alpha!=\prod_{h=-\infty}^{r}\prod_{i=1}^{n}(\lambda_{hi})!$ where $\alpha_i=\sum_{h=-\infty}^{r}\lambda_{hi}p^h$, $1\leqq i\leqq n$, are expressions of α_i in the form $(*)$.

Let G be a commutative formal group of dimension n. In the following, we shall extend the notion in [1, $n°4$, 5, 6, 7, 12], following verbatim the argument in [1]. We call a K-endomorphism Δ of $\mathcal{O}'$ a *semi-derivation of height* r if Δ satisfies $\Delta(\mathcal{O}_r)\subset\mathcal{O}_r$, $\Delta(fg)=f\Delta(g)+g\Delta(f)$, for $f\in\mathcal{O}_r$, $g\in\mathcal{O}'$, and a *special semi-derivation* if Δ is semi-derivation and satisfies $\Delta(f)=0$, for $f\in\mathcal{O}_r$. Denote by $D_{r,i}$ a semi-derivation of height r such that if $\alpha_i=ap^r+b+c$, $0\leqq a<p$, $a\in\boldsymbol{Z}$; $0\leqq b<p^r$, $p^{-r-1}c\in\boldsymbol{N}$, we have $D_{r,i}(x_1^{\alpha_1}\cdots x_n^{\alpha_n})=ax_1^{\alpha_1}\cdots x_{i-1}^{\alpha_{i-1}}\cdot x_i^{\alpha_i-p^r}\cdot x_{i+1}^{\alpha_{i+1}}\cdots x_n^{\alpha_n}$. Put $D_\alpha=\prod_{h=-\infty}^{r}\prod_{i=1}^{n}D_{h,i}^{\lambda_{hi}}$ for $\alpha=(\alpha_1,\cdots,\alpha_n)$, $\alpha_i=\sum_{h=-\infty}^{r}\lambda_{hi}p^h$, $1\leqq i\leqq n$.

We define a differential operator D as a linear combination $\sum_\alpha u_\alpha D_\alpha$ where $u_\alpha\in\mathcal{O}'$ and $u_\alpha=0$ for α such that $h(\alpha)$ is large enough. For any differential operator D we can define uniquely an *invariant* differential operator Z such that $Z(e)f=D(e)f$, $f\in\mathcal{O}'$. Denote by Z_α the invariant differential operator characterized by the initial condition $Z_\alpha(e)=(1/\alpha)D_\alpha(e)$. Put $X_\alpha=\prod_{h=-\infty}^{r}\prod_{i=1}^{n}\overline{Z}_{h,i}^{\lambda_{hi}}$, for $\alpha=(\alpha_1,\cdots,\alpha_n)$, $\alpha_i=\sum_{h=-\infty}^{r}\lambda_{hi}p^h$, $1\leqq i\leqq n$, where $\overline{Z}_{h,i}=Z_{p^h\varepsilon_i}$.

We denote by $\mathcal{G}$ the algebra formed (over K) by invariant differential operators of $\mathcal{O}'$ and call it the *hyperalgebra* of G. Also we denote by $\mathcal{G}_r$ (resp. $\mathcal{S}_r$) the set of semi-derivations (resp. special semi-derivations) of height r of $\mathcal{G}$. Then $\mathcal{G}=\bigcup_r\mathcal{G}_r$, $\mathcal{G}_r$ is Lie algebra and $\mathcal{S}_r$ is the ideal of $\mathcal{G}_r$. Moreover $\mathcal{S}_r$ is the associative algebra over K. Then Theorem 2 of [1, $n°9$] holds in our case.

Lemma 1. *The associative algebra $\mathcal{S}_r$ has the special semi-derivations X_α, $0\leqq\alpha_i<p^r$ as its base over K; the Lie algebra $\mathcal{G}_r$ is the direct sum of $\mathcal{S}_r$ and the vector space over K which has $\overline{Z}_{r,1},\cdots,\overline{Z}_{r,n}$ as its base.*

Remark. Z_α can be defined from "Taylor series" for $f\in\mathcal{O}'$,

$$f(x\dot{+}y)=\sum_\alpha y^\alpha(Z_\alpha f),\ Z_\alpha f\in\mathcal{O}'.$$

2. Let $\overline{G}$ be another commutative formal group of dimension m and let $u=(u_1, \cdots, u_m)$ be a homomorphism from G to $\overline{G}$, where we admit to take elements of $\mathcal{O}'$ as u_i, $1\leqq i\leqq m$. For $Z\in\mathcal{G}$, $f\in\mathcal{O}'(\overline{G})$, we define an invariant differential operator $u'(Z)\in\overline{\mathcal{G}}$ by $u'(Z)(e)\overline{f}=Z(e)(\overline{f}\cdot u)$. Then u' is a homomorphism from $\mathcal{G}$ to $\overline{\mathcal{G}}$ such that $u'(\mathcal{G}_r)\subset\overline{\mathcal{G}}_{r+t}$, $u'(\mathcal{S}_r)\subset\overline{\mathcal{S}}_{r+t}$, for $r\in Z$, where t is an integer such that $u_i\in\mathcal{O}_{-t}$, $1\leqq i\leqq m$. Moreover if v is a homomorphism of $\overline{G}$ to another commutative formal group $\overline{\overline{G}}$, we have $(v\cdot u)'=v'\cdot u'$. It is trivial that for the identity I of formal group G, $(I)'$ is the identity of Lie hyperalgebra $\mathcal{G}$ of G.

3. Lemma 2. (1) *For $G_{n,1,m}$, $(n, m)=1$, we have the following relations,*

$$\overline{Z}^p_{h,i}=\overline{Z}_{h,i+1},\ 1\leqq i\leqq n-1,\ h=0,\ \pm1,\ \pm2,\ \cdots,$$

$$\overline{Z}^p_{h,n}=\overline{Z}_{h-m,1},\qquad h=0,\ \pm1,\ \pm2,\ \cdots.$$

(2) *For multiplicative group G_m, we have the relations,*

$$\overline{Z}^p_h=\overline{Z}_h,\ h=0,\ \pm1,\ \pm2,\ \cdots.$$

Proof. (1) First we prove that the relations

$$\overline{Z}^p_{h,i}=\overline{Z}_{h,i+1},\ 1\leqq i\leqq n-1,\ h=0,\ 1,\ 2,\ \cdots,$$

$\overline{Z}^p_{h+m,n}=\overline{Z}_{h,1}$, $h=0, 1, \cdots$, described in Lemma 3, Part 2 hold

if they are considered as K-linear endomorphisms of $\mathcal{O}'$. Let f be an element of $\mathcal{O}_{-t}$, t: positive integer. Taking account of the fact that the group laws of $G_{n,1,m}$ are defined over the prime field, it is easy to show that $Z_\alpha f=\{Z_{p^t\alpha}(f\cdot\boldsymbol{p}^t)\}(\boldsymbol{p}^{-t})$, for any $Z_\alpha\in\mathcal{G}$ where $\boldsymbol{p}$ (resp. $\boldsymbol{p}^{-1}$) is a homomorphism $\boldsymbol{p}: x\to x^p$ (resp. $\boldsymbol{p}^{-1}: x\to x^{p^{-1}}$). Taking $\overline{Z}_{h,i}$ (resp. $\overline{Z}_{h+m,n}$), we have $\overline{Z}^p_{h,i}f=\{\overline{Z}^p_{h+t,i}(f\cdot\boldsymbol{p}^t)\}(\boldsymbol{p}^{-t})=\{\overline{Z}_{h+t,i+1}(f\cdot\boldsymbol{p}^t)\}(\boldsymbol{p}^{-t})=\overline{Z}_{h,i+1}f$, (resp. $\overline{Z}^p_{h+m,n}f=\{\overline{Z}^p_{h+m+t,n}(f\cdot\boldsymbol{p}^t)\}(\boldsymbol{p}^{-t})=\{\overline{Z}_{h+t,1}(f\cdot\boldsymbol{p}^t)\}(\boldsymbol{p}^{-t})=\overline{Z}_{h,1}f$.) Hence follows the requirement.

Next we consider a homomorphism $\boldsymbol{p}^{-1}: x\to x^{p^{-1}}$. Then the derived homomorphism $(\boldsymbol{p}^{-1})'$ of the hyperalgebra of $G_{n,1,m}$ is characterized by

$$(p^{-1})'(\overline{Z}_{h,i})=\overline{Z}_{h+1,i},\ h=0,\ \pm 1,\ \pm 2,\ \cdots,\ 1\leqq i\leqq n.$$

To prove the relations (1), operate $(p^{-1})'$ on $\overline{Z}_{h,i}$, $1\leqq i\leqq n-1$, (resp. $\overline{Z}_{h,n}$) by t-times repeatedly so that $h+t$ (resp. $h+t-m$) is positive. Then putting $q=(p^{-1})'$, we have

$$q^{t}(\overline{Z}^{p}_{h,i})=(q^{t}(\overline{Z}_{h,i}))^{p}=\overline{Z}^{p}_{h+t,i}=\overline{Z}_{h+t,i+1}=q^{t}(\overline{Z}_{h,i+1}),$$

(resp. $q^{t}(\overline{Z}^{p}_{h,n})=\overline{Z}^{p}_{h+t,n}=\overline{Z}_{h+t-m,1}=q^{t}(\overline{Z}_{h-m,1})$.)

Therefore we get the requirement, taking account of the fact that $(p^{-1})'$ is bijective.

(2) The proof is completely analogous to the one of (1), using the fact that $\overline{Z}^{p}_{h}=\overline{Z}_{h}$, $h=0, 1, 2, \cdots$. q.e.d.

From Lemma 1 and Lemma 2, we have:

Corollary. *If a commutative formal group G is isomorphic to a direct product of multiplicative groups and simple groups $G_{n,1,m}$, $(n, m)=1$, the mapping of the hyperalgebra $\mathcal{G}$ of G; $Z\in\mathcal{G}\to Z^{p}\in\mathcal{G}$ is bijective.*

4. We shall define a *quasi-formal ring R* with the same definition as a formal ring, only adding the following requirement:

(1) $\varphi_1, \cdots, \varphi_n$ are formal series which admit no terms but those of the following type, $x_1^{\alpha_1}\cdots x_n^{\alpha_n}y_1^{\beta_1}\cdots y_n^{\beta_n}$, $\alpha_1, \cdots, \alpha_n$; $\beta_1, \cdots, \beta_n$ being non-negative integers,

(2) $\psi_1, \cdots, \psi_n$ admit terms $x_1^{\alpha_1}\cdots x_n^{\alpha_n}y_1^{\beta_1}\cdots y_n^{\beta_n}$, $\alpha_1, \cdots, \alpha_n$; $\beta_1, \cdots, \beta_n$ being non-negative numbers of the type (*).

For $f\in\mathcal{O}'$, write $f(y\cdot x)=\sum_{\alpha}y^{\alpha}(X_{\alpha}f)$, $f(x\cdot y)=\sum_{\alpha}y^{\alpha}(Y_{\alpha}f)$, $f(x\dot{+}y)=\sum_{\alpha}y^{\alpha}(Z_{\alpha}f)$, $X_{\alpha}f$, $Y_{\alpha}f$, $Z_{\alpha}f\in\mathcal{O}'$. Then X_{α}, Y_{α}, Z_{α} are K-linear endomorphisms of $\mathcal{O}'$. Moreover put $(x\cdot y)^{\gamma}=\sum_{\alpha,\beta}c_{\beta\alpha\gamma}x^{\alpha}y^{\beta}$, $(x\dot{+}y)^{\gamma}=\sum_{\alpha,\beta}d_{\beta\alpha\gamma}x^{\alpha}y^{\beta}$, $c_{\alpha\beta\gamma}$, $d_{\alpha\beta\gamma}\in K$. Then we write

$$X_{\beta}X_{\alpha}=\sum_{\gamma}c_{\beta\alpha\gamma}X_{\gamma},\quad Y_{\beta}Y_{\alpha}=\sum_{\gamma}c_{\alpha\beta\gamma}Y_{\gamma},\quad Z_{\beta}Z_{\alpha}=\sum_{\gamma}d_{\beta\alpha\gamma}Z_{\gamma},$$

$$Z_\beta X_\alpha = \sum_{\substack{0\leq\gamma\leq\alpha \\ \delta}} c_{\beta\gamma\delta} X_{\alpha-\gamma} Z_\delta,\ Z_\beta Y_\gamma = \sum_{\substack{0\leq\gamma\leq\alpha \\ \delta}} c_{\gamma\beta\delta} Y_{\alpha-\gamma} Z_\delta.$$

5. Let R be a formal ring of dimension n and assume that there exists an isogeny u from the underlying additive group of R to G, where G is isomorphic to $(G_m)^l \times \prod_{\substack{n_i, m_i \\ (n_i, m_i)=1}} G_{n_i,1,m_i}$, $l+\sum_i n_i = n$.

Let $\bar{\varphi} = (\bar{\varphi}_1, \cdots, \bar{\varphi}_n)$, $\bar{\psi} = (\bar{\psi}_1, \cdots, \bar{\psi}_n)$ be ring laws for R and $\varphi = (\varphi_1, \cdots, \varphi_n)$ be the group law for G. Then by Lemma 1, Part 2, changing variables in R and G, we can suppose that u is a homomorphism of the form written in Lemma 1, and that $\bar{\varphi}$, $\bar{\psi}$, φ are laws defined for the variables which have been changed, $\bar{x}_1, \cdots, \bar{x}_n$ for R and $x_1, \cdots, x_n$ for G. Then

$x_i = u_i(\bar{x}) = \bar{x}_i^{p^h}$, if $r_0+\cdots+r_{h-1}+1 \leqq i \leqq r_0+\cdots+r_h$, $0\leqq h\leqq t$.

We define ψ_i as follows;

$$\psi_i(x_1, \cdots, x_n; y_1, \cdots, y_n) = \{\bar{\psi}_i(x_1, \cdots, x_{r_0}, x_{r_0+1}^{p^{-1}}, \cdots, x_{r_0+r_1}^{p^{-1}}, \cdots, x_n^{p^{-t}}; y_1, \cdots, y_{r_0}, y_{r_0+1}^{p^{-1}}, \cdots, y_{r_0+r_1}^{p^{-1}}, \cdots y_n^{p^{-t}})\}^{p^h},$$

if $r_0+\cdots+r_{h-1}+1 \leqq i \leqq r_0+\cdots+r_h$, $0\leqq h\leqq t$.

Thus we can define a structure of quasi-formal ring on G with $\varphi = (\varphi_1, \cdots, \varphi_n)$, $\psi = (\psi_1, \cdots, \psi_n)$. Then by Lemma 6, Part 1 and the condition $(F4)$, we can easily see that in some ψ_i, there exists a term of the type $a(x)y_j^{p^h}$ where $a(x)$ is a formal series in $\mathcal{O}'$ and h is an integer. Let h be the smallest integer such that there appear terms of the preceding type in ψ_i, $1\leqq i\leqq n$.

Write $\psi_i(y, x) = \sum_{j=1}^n \theta_{ij}(x) y_j^{p^h} +$ (terms of total degree $>p^h$ with respect to $y=(y_1, \cdots, y_n)$ or terms of the following type $a(x)y_1^{\alpha_1}\cdots y_n^{\alpha_n}$ where some α_i, $\alpha_j \neq 0$, $i\neq j$.)

Then from $\varphi_i(\psi(z, x), \psi(z, y)) = \psi_i(z, \varphi(x, y))$, we have

$$\theta_{ij}(\varphi(x, y)) = \theta_{ij}(x) + \theta_{ij}(y),\ 1\leqq i, j\leqq n. \qquad \cdots(**)$$

From the assumption, there exists some $\theta_{ij}(x) \neq 0$. From $(**)$, we can know easily that in $\theta_{ij}(x)$, the terms of the smallest total degree have the form $ax_k^{p^t}$, $a\in K$, $1\leqq k\leqq n$, t: integer. Therefore we know that in some $\psi_i(x, y)$, $1\leqq i\leqq n$ there exists a term $ax_k^{p^t}y_j^{p^h}$. If we operate $\overline{Z}_{t,k}X_{p^h\varepsilon_j}$ to x_i, we have

$$(\overline{Z}_{t,k}X_{p^h\varepsilon_j}x_i)(e)=\overline{Z}_{t,k}(\theta_{ij}(x))(e)=a\neq 0\,.$$

On the other hand, we have $\overline{Z}_{t,k}=\sum_{\alpha}a_\alpha Z_\alpha^p$, $a_\alpha\in K$, from Corollary of Lemma 2. And by operating the above endomorphism to elements of $\mathcal{O}_r$, where r is large enough, it is easy to see that the sum of right hand side does not contain a constant term.

For $\alpha\neq 0$, we have

$$Z_\alpha X_{p^h\varepsilon_j}^{\boldsymbol{\cdot}}=\sum\{c_{\alpha,0,\delta}X_{p^h\varepsilon_j}+c_{\alpha,p^h\varepsilon_j,\delta}X_0+\sum_{0<\gamma<p}{}_{h\varepsilon_j}c_{\alpha,0,\delta}X_{p^h\varepsilon_j-\gamma}\}Z_\delta\,.$$

If $0<\gamma<p^h\cdot\varepsilon_j$, $X_{p^h\varepsilon_j-\gamma}Z_\delta x_i=0$, for if not $\delta=(\delta_1,\cdots,\delta_n)$, δ_i: non-negative integers, $Z_\delta x_i=0$ by the definition of Z_δ and the assumption of group laws of a quasi-formal ring, and if $\delta=(\delta_1,\cdots,\delta_n)$, δ_i: non-negative integers, $(X_{p^h\varepsilon_j-\gamma}Z_\delta)x_i=0$ by the assumption on h. We know that $c_{\alpha,0,\delta}=0$ and $Z_\alpha X_0=0$. Hence $Z_\alpha^p X_{p^h\varepsilon_j}x_i=0$, and $\overline{Z}_{t,k}X_{p^h\varepsilon_j}x_i=0$. This gives a contradiction. Thus we have completed the proof of Theorem 1.

Bibliography

[1] J. Dieudonné, Groupes de Lie et hyperalgèbres de Lie sur un corps de caractéristique $p>0$, Comm. Math. Helv., 28, 1954, pp. 87-118.
[2] J. Dieudonné, Lie groups and Lie hyperalgebras over a field of characteristic $p>0$, (II), Amer. Jour. Math., 77, 1955, pp. 218-244.
[3] J. Dieudonné, Groupes de Lie et hyperalgèbres de Lie sur un corps de caractéristique $p>0$, (III), Math. Zeit. 62, 1955, pp. 53-75.
[4] J. Dieudonn, Groupes de Lie et hyperalgèbres de Lie sur un corps de caractéristique $p>0$, (VII), Math. Ann., 134, 1957, pp. 114-133.
[5] J. Dieudonné, Lie groups and Lie hyperalgebras over a field of characteristic $p>0$, (VIII), Amer. Jour. Math., 80, 1958, pp. 740-772.
[6] M. J. Greenberg, Algebraic rings, Trans. A. M. S., 3, 1964, pp. 472-481
[7] M. Lazard, La non-existence des groupes de Lie formels non abéliens à un paramètre, Comt. Rend. (Paris), 239, 1954, pp. 942-945.
[8] Ju. I. Manin, Theory of commutative formal groups over a field of positive characteristic, Uspekhi Math. Nauk, 18, 1963, pp. 1-90.