74. *On Formal Groups over Complete Discrete Valuation Rings. II*

Generic Formal Group and Specializations

By Keiichi OSHIKAWA
Department of Mathematics, Musashi Institute of Technology

(Communicated by Shokichi IYANAGA, M. J. A., June 15, 1982)

1. Let $Z[A_1, A_2, \cdots, A_t, \cdots]$ be the ring of polynomials in countably infinite variables over Z. Let

$$F_A(X, Y)=X+Y+\sum_{i+j\geqq 2} c_{ij}X^iY^j$$

be a commutative formal group over $Z[A_1, A_2, \cdots, A_t, \cdots]$.

Let $a_i \in R(i=1, 2, \cdots)$, R being as in [5], and let

$$\varphi: Z[A_1, A_2, \cdots, A_t, \cdots]\longrightarrow R$$

be a ring homomorphism defined by $\varphi(A_i)=a_i$ and $\varphi(d)=d$ if d is in Z. Let

$$\varphi_*F_A(X, Y)=X+Y+\sum_{i+j\geqq 2} \varphi(c_{ij})X^iY^j.$$

Then $\varphi_*F_A(X, Y)$ is a formal group over R. We shall call $\varphi_*F_A(X, Y)$ *a specialization of the generic formal group* $F_A(X, Y)$.

In general, let A, B be commutative rings. Let $\lambda: A\to B$ be a ring homomorphism, $G(X, Y)$ formal power series with coefficients in A. We denote the formal power series obtained from $G(X, Y)$ applying the homomorphism λ to the coefficients of $G(X, Y)$ by $\lambda_*G(X, Y)$ (cf. [1]).

We shall consider $F_A(X, Y)$ and $a_i \in R$, consequently also $\varphi_*F_A(X, Y)$, as fixed, and denote this $\varphi_*F_A(X, Y)$ simply by $F(X, Y)$. If we reduce the coefficients of $F(X, Y)$ mod $\mathfrak{p}$, we obtain a formal group over k which we denote with $\bar{F}(X, Y)$.

On the other hand, let g be a polynomial in $Z[A_1, A_2, \cdots, A_t, \cdots]$. We define $\psi(g)$ to be the polynomial which is obtained from g by reducing its coefficients mod p. Then

$$\psi: Z[A_1, A_2, \cdots, A_t, \cdots]\longrightarrow F_p[A_1, A_2, \cdots, A_t, \cdots]$$

is a ring homomorphism, $\psi_*F_A(X, Y)$ is a commutative formal group over $F_p[A_1, A_2, \cdots, A_t, \cdots]$. Denote this $\psi_*F_A(X, Y)$ by $\bar{F}_A(X, Y)$. If we denote with $\bar{\varphi}$ the ring homomorphism $F_p[A_1, A_2, \cdots, A_t, \cdots]\to k$ defined by $\bar{\varphi}(A_i)=a_i$ mod $\mathfrak{p}$ and $\bar{\varphi}(\bar{d})=\bar{d}$ if $\bar{d}$ is in F_p, we have clearly $\bar{\varphi}_*\bar{F}_A(X, Y)=\bar{F}(X, Y)$.

Let us define $[m]_A(X)=F_A([m-1]_A(X), X)$, $\overline{[m]}_A(X)=\bar{F}_A(\overline{[m-1]}_A(X), X)$, and $\overline{[m]}(X)=\bar{F}(\overline{[m-1]}(X), X)$, inductively like $[m](X)$ in [5].

Then the following diagram (D) is commutative.

$$\text{(D)}\qquad \begin{array}{ccc} [m]_A(X) & \xrightarrow{\varphi_*} & [m](X) \\ \downarrow \psi_* & & \downarrow \text{reduction mod } \mathfrak{p} \\ [\overline{m}]_A(X) & \xrightarrow{\overline{\varphi}_*} & [\overline{m}](X) \end{array}$$

The following result is well-known (cf. [3] Lemma 5, p. 266).

Let $[\overline{p}](X)\neq 0$ (resp. $[\overline{p}]_A(X)\neq 0$). The exponent of X in the first non-vanishing term of $[\overline{p}](X)$ (resp. $[\overline{p}]_A(X)$) is a p-power p^h (resp. $p^{h'}$). Moreover $[\overline{p}](X)$ (resp. $[\overline{p}]_A(X)$) is a formal power series in X^{p^h} (resp. $X^{p^{h'}}$). If $[\overline{p}](X)=0$ (resp. $[\overline{p}]_A(X)=0$), we shall write $h=\infty$ (resp. $h'=\infty$).

Then h (resp. h') is called the height of $\overline{F}(X, Y)$ (resp. $\overline{F}_A(X, Y)$). We call h also the height of $F(X, Y)$ following [1].

For $a\in \boldsymbol{Z}$, we define $\infty+a=\infty\cdot\infty=\infty$, $a/\infty=0$, $a<\infty$, and if $a>0$, $\infty\cdot a=a^\infty=\infty$.

2. By the above result and the commutative diagram (D) we obtain the following

Lemma. (a) *If* $c_m \notin p\boldsymbol{Z}[A_1, A_2, \cdots, A_t, \cdots]$ *in* $[p]_A(X)=pX+\sum_{i=2}^{\infty} c_i X^i$, *then m is a multiple of* $p^{h'}$.

(b) *Let* $[p](X)=pX+\sum_{i=2}^{\infty} d_i X^i$ *where* $d_i=\varphi(c_i)$, *and* $d_s \notin pR$ *whereas* $d_1=p, d_2, \cdots, d_{s-1}\in pR$. *Then* $s=\mu p^{h'}$, *where μ is an integer* $\geqq 1$. *If all* $d_i\in pR$, *we shall write* $\mu=\infty$.

(c) *We have* $p^{h'}\leqq \mu p^{h'}\leqq p^h$, *also when* $h'=\infty$ *or* $\mu=\infty$ *or* $h=\infty$.

Now let $h'<h<\infty$. From Lemma, we get the following formula.

$$(1)\qquad [p](X)=pXg_0(X)+\sum_{t=1}^{r-1} X^{tp^{h'}}g_t(X)+X^{p^h}g_h(X)$$

where $g_0(X)$, $g_t(X)$, $g_h(X)\in R[[X]]$ and $r=p^{h-h'}$. The first term d_{p^h} of $g_h(X)$ is a unit in R. Moreover the coefficients of $g_t(X)$ belong to $\mathfrak{p}$, $g_\mu(X)$ has a non zero constant term $d_{\mu p^{h'}}$, which is not in pR, and $g_t(X)$, $g_h(X)\in R[[X^{p^h}]]$ (cf. [4], [7]).

From now on, we shall use the notation h', μ, h always in the above sense.

Now we put

$$\beta=\mathrm{Min}\left(\mathrm{Max}\left(\frac{e-1}{p^{h'}-1}, \frac{e}{p^h-1}\right), \frac{e}{\mu p^{h'}-1}\right).$$

Then we get following Proposition 2, by the definition of α and Lemma.

Proposition 2. *We have* $\beta\geqq\alpha$, *where α is defined as in* [5].

Remark 1. (a) If $n>e/(p-1)$, we have $(\mathfrak{p}^n, \dotplus)\cong\mathfrak{p}^n$ as R-module. In fact, we have $e/(p-1)\geqq\beta\geqq\alpha$.

(b) Let $F(X, Y)=X+Y+XY$. Then

$$l_F(X)=\log(1+X)=X-\frac{1}{2}X^2+\cdots+\frac{(-1)^{n-1}}{n}X^n+\cdots.$$

Put $U^n=\{1+x\,|\,x\in\mathfrak{p}^n\}$. Then an isomorphism $\rho: U^n\to(\mathfrak{p}^n, \dotplus)$ is defined by $\rho(1+x)=x$. Thus, for $n>e/(p-1)$ $U^n \cong \mathfrak{p}^n$ as R-module by log. This is a classical result (cf. Serre [6] p. 220).

Remark 2. Let $F_V(X, Y)$ be $f_V^{-1}(f_V(X)+f_V(Y))$ over $Z[V_1, V_2, \cdots, V_n, \cdots]$, where

$$f_V(X)=\sum_{n=0}^{\infty} a_n(V)X^{p^n}, \qquad a_0(V)=1,$$

$$a_n(V)=\sum_{i_1+i_2+\cdots+i_k=n} \frac{V_{i_1}V_{i_2}^{p^{i_1}}\cdots V_{i_k}^{p^{i_1+i_2+\cdots+i_{k-1}}}}{p^k}.$$

If we substitute $v_j \in R$ to V_j, we obtain p-typical formal group which we denote $F_v(X, Y)$. It is known that every formal group $F(X, Y)$ over R is strictly isomorphic to a $F_v(X, Y)$ over R (cf. [1] p. 94 (15, 2, 9)) and the height h of F is equal to the height of F_v.

Thus, we have the following result for any formal group $F(X, Y)$ over R from Theorem 1 and Proposition 2, by replacing $F_A(X, Y)$ by $F_V(X, Y)$. *If* $n>\mathrm{Max}\,((e-1)/(p-1),\ e/(p^h-1))$, $(\mathfrak{p}^n, \dot{+})$ *is isomorphic to* $\mathfrak{p}^n$ *as R-module.*

For $u \in (\mathfrak{p}, \dot{+})$ with a finite order, which should be therefore a p-power, we have the next

Theorem 2. (a) *If $u \in (\mathfrak{p}, \dot{+})$ has a finite order, then*

$$\nu(u) \leqq \frac{e}{\mu p^{h'}-1}.$$

(b) *If the order of u is p^n, then*

$$\nu(u) \leqq \frac{e}{(\mu p^{h'})^n-(\mu p^{h'})^{n-1}}$$

(cf. Lang [7] p. 62).

Let $\bar{\mathfrak{p}}=\{x \mid x \in \bar{K}, \bar{\nu}(x)>0\}$. For a real number $\lambda>0$, put $S=\{x \mid x \in \bar{\mathfrak{p}}, \bar{\nu}(x) \geqq \lambda, [p](x)=0\}$. The elements of $\bar{\mathfrak{p}}$ as well as $\mathfrak{p}$ form a commutative group $(\bar{\mathfrak{p}}, \dot{+})$ and S is a subgroup of $(\bar{\mathfrak{p}}, \dot{+})$. If the cardinal of S is p, S is called the canonical subgroup of F ([4], [7]). We obtain following Theorem 3 without using the concept of "the standard generic formal group" in Lubin ([4]).

Theorem 3. *Let $h<\infty$. F has a canonical subgroup S, if and only if one of the following conditions* (a), (b) *is satisfied*

(a) $h=1$

(b) $h \geqq 2$, $h'=1$ *and* $\mu=1$, *and for every t with* $1<t \leqq p^{h-1}$,

$$\nu(d_p)<\frac{(tp-p)e+(p-1)\nu(d_{tp})}{tp-1}$$

where d_{tp} is a constant term of $g_t(X)$ in (1).

Then $S=\{x \mid x \in \bar{\mathfrak{p}}, [p](x)=0, \bar{\nu}(x)=\alpha\} \cup \{0\}$,

where
$$\alpha=\frac{e-\nu(d_p)}{p-1}.$$

We can prove this theorem by using the Newton polygon of $[p](x)$ as in Lubin ([4], Theorem B, p. 110).

References

[1] M. Hazewinkel: Formal Groups and Applications. Academic Press, New York (1978).

[2] S. Lang: Elliptic curves, Diophantine analysis. Grundlehren, **231**, Springer-Verlag, Berlin (1978).

[3] M. Lazard: Sur les groupes de Lie formels à un paramètre. Bull. Soc. math. France, **83**, 251–274 (1955).

[4] J. Lubin: Canonical subgroups of formal groups. Trans. Amer. Math. Soc., **251**, 103–127 (1979).

[5] K. Oshikawa: On formal groups over complete discrete valuation rings. I. Proc. Japan Acad., **58**A, 216–218 (1982).

[6] J.-P. Serre: Corps locaux. Hermann, Paris (1962).

[7] N. Yui: Elliptic curves and canonical subgroups of formal groups. J. reine angew. Math., **303/304**, 319–331 (1978).