60. On Formal Groups over Complete Discrete Valuation Rings. I

By Keiichi OSHIKAWA
Department of Mathematics, Musashi Institute of Technology

(Communicated by Shokichi IYANAGA, M. J. A., May 12, 1982)

1. Introduction. Let R be a complete discrete valuation ring, K the quotient field of R, $\mathfrak{p}$ the maximal ideal of R, π a generator of $\mathfrak{p}$. Put $R/\mathfrak{p}=k$. We assume that the characteristic $\mathrm{ch}(K)$ of K is 0, and $\mathrm{ch}(k)=p$. We denote with ν the additively written valuation of K with $\nu(\pi)=1$. We put $\nu(p)=e$.

Let $F(X, Y)$ be a commutative formal group over R. Let n be any natural number $\geqq 1$. If $u, v\in \mathfrak{p}^n$, then $F(u, v)\in\mathfrak{p}^n$. We shall write $u\dotplus v$ for $F(u, v)$. Thus $\mathfrak{p}^n$ forms a commutative group with this operation $\dotplus$, which will be denoted with $(\mathfrak{p}^n, \dotplus)$. It is well-known that there exists a formal power series $l_F(X)\in K[[X]]$ of the form

$$l_F(X)=\sum_{n=1}^{\infty} c_n X^n, \quad c_1=1, \quad nc_n\in R$$

such that

$$F(X, Y)=l_F^{-1}(l_F(X)+l_F(Y)). \qquad \text{(Cf. Fröhlich [1].)}$$

It is also known that for sufficiently large n, $(\mathfrak{p}^n, \dotplus)$ is mapped isomorphically onto $\mathfrak{p}^n$ (a commutative group with ordinary addition as operation) by l_F, the inverse map being given by l_F^{-1} (cf. [1]).

In this note, we shall give a "precise" value of α, such that this takes place for $n>\alpha$.

This result implies that, if $(\mathfrak{p}^n, \dotplus)$ has a torsion element u, $\nu(u)$ should be bounded by a value depending on F.

In a subsequent note we shall estimate the above value α under the hypothesis that $F(X, Y)$ is a "specialization of a generic formal group" in the sense which will be explained later.

Our results will be then applied to elliptic curves to improve the classical "Theorem of Lutz".

In the sequel $\boldsymbol{Z}, \boldsymbol{Q}, \boldsymbol{Z}_p, \boldsymbol{F}_p$ will mean as usual the ring of rational integers, the rational number field, the ring of p-adic integers and the finite field with p elements, respectively.

The detailed proofs will appear elsewhere.

I would like to thank Prof. S. Iyanaga who has encouraged me to complete this study. I also thank Prof. M. Hazewinkel for giving me precious advice.

2. The properties of $(\mathfrak{p}, \dotplus)$. For natural number $m\geqq 2$, let us define inductively $[2](X)=F(X,X)$, $[m](X)=F(X,[m-1](X))$. $[m](X)$ is clearly represented by a formal power series in X with coefficients in R beginning with mX.

Put

$$[p](X)=pX+d_2X^2+\cdots+d_nX^n+\cdots.$$

We have $d_i \in R$. We define now

$$\alpha=-\operatorname*{Min}_{i\geqq 2}\frac{1}{i-1}\nu\left(\frac{d_i}{p}\right)$$

(obviously $-\alpha$ is the slope of the first segment of the Newton polygon of $[p](X)/pX$ as defined in [3], p. 90).

Proposition 1. *If $\nu(x)>\alpha$, $x\in K$, then for any natural number n, we have*

$$[p^n](x)=p^nx(1+x_n) \quad \textit{with} \quad x_n\in\mathfrak{p}.$$

This is easily shown by induction on n.

It is known that l_F converges on $\mathfrak{p}^n$ for any natural number n, and we have a homomorphism $l_F:(\mathfrak{p}^n, \dot{+})\to\mathfrak{p}^n$. (Cf. Fröhlich [1] Theorem 3, p. 109.) We have also

$$l_F(X)=\lim_{n\to\infty}p^{-n}[p^n](X)$$

by Hazewinkel [2] (Proposition (5.4.5), p. 31). Hence follows by Proposition 1 $\nu(l_F(x))=\nu(x)$.

Then we have the following

Theorem 1. *If $n>\alpha$, l_F^{-1} converges on $\mathfrak{p}^n$, and $l_F:(\mathfrak{p}^n, \dot{+})\to\mathfrak{p}^n$ is an isomorphism.*

Remark 1. As $-\alpha$ is the slope of a segment of the Newton polygon of $[p](x)/pX$, there exists $\xi\in\bar{K}$ such that $[p](\xi)=0$, and $\bar{\nu}(\xi)=\alpha$ ([3], Theorem 14 Cor. p. 98), where $\bar{K}$ is the algebraic closure of K, and $\bar{\nu}$ is the extension of ν to $\bar{K}$.

Our value of α is "precise" in the following sense.

Suppose $K\ni\xi$ for ξ with $[p](\xi)=0$, $\nu(\xi)=\alpha$. In this case, "$(\mathfrak{p}^n, \dot{+})\simeq\mathfrak{p}^n$ for $n>\alpha$" can not hold for any smaller value of α than ours.

Remark 2. In case $ch(k)=0$, it is easily seen that l_F^{-1} converges on $\mathfrak{p}^n$ for any $n>0$.

Now we can define in $(\mathfrak{p}^n, \dot{+})$, if $n>\alpha$, a structure of R-module by defining $[r](X)=l_F^{-1}(rl_F(X))$ for $r\in R$, and l_F gives an R-module isomorphism of $(\mathfrak{p}^n, \dot{+})$ into $\mathfrak{p}^n$.

In $(\mathfrak{p}^n, \dot{+})$ we can define a structure of $\boldsymbol{Z}_p$-module. In fact we have, $R\supset\boldsymbol{Z}_p$. Let $r\in\boldsymbol{Z}_p$ and $r=m+r'$, $m\in\boldsymbol{Z}$, $r'\in\boldsymbol{Z}_p$ with $p^n|r'$, where $n>\alpha$.

For $x\in\mathfrak{p}$, we can define

$$[r](x)=[m](x)+l_F^{-1}(r'l_F(x)).$$

We see easily that $(\mathfrak{p}, \dot{+})$ is a $\boldsymbol{Z}_p$-module by this operation $[r](x)$.

Corollary 1. *When k is a finite field with cardinal p^f. $(\mathfrak{p}^n, \dot{+})$ is* *a $\boldsymbol{Z}_p$-module of rank ef, for $n>\alpha$.*

Corollary 2. (a) *A torsion element u of* ($\mathfrak{p}$, $\dot{+}$) *has a p-power order.*

(b) *Let k be a finite field with cardinal p^f.* ($\mathfrak{p}$, $\dot{+}$) *is the direct product of a free $\boldsymbol{Z}_p$-module of rank ef and a finite abelian group with p-power order.*

References

[1] A. Fröhlich: Formal groups. Lect. Notes in Math., vol. 74, Springer-Verlag, Berlin (1968).
[2] M. Hazewinkel: Formal Groups and Applications. Academic Press, New York (1978).
[3] N. Koblitz: p-adic numbers, p-adic analysis, and zeta-functions. Graduate texts in mathematics 58, Springer-Verlag, Berlin (1977).
[4] E. Lutz: Sur l'équation $y^2=x^3-Ax-B$ dans les corps $\mathfrak{p}$-adiques. J. reine angew. Math., **177**, 238–247 (1937).