87. On Formal Groups over Complete Discrete Valuation Rings. III

Applications to Elliptic Curves

By Keiichi OSHIKAWA
Department of Mathematics, Musashi Institute of Technology

(Communicated by Shokichi IYANAGA, M. J. A., Sept. 13, 1982)

1. Let E_A be an elliptic curve defined over $\boldsymbol{Q}(A_1, A_2, A_3, A_4, A_6)$ by the equation:

$$y^2+A_1xy+A_3y=x^3+A_2x^2+A_4x+A_6 \tag{1}$$

in (x, y)-plane. Let $u=-x/y$, $w=-1/y$. (1) is then represented by the equation:

$$w=u^3+A_1uw+A_2u^2w+A_3w^2+A_4uw^2+A_6w^3$$

in (u, w)-plane. Then we get the formal expansion

$$w=u^3+A_1u^4+(A_1^2+A_2)u^5+(A_1^3+2A_1A_2+A_3)u^6+\cdots. \tag{2}$$

Denote by $h_A(u)$ the right hand side of (2). Then $h_A(u)$ has coefficients in $\boldsymbol{Z}[A_1, A_2, A_3, A_4, A_6]$.

Now we regard E_A as a plane cubic model of an abelian variety of dimension 1. $(0, 0)\in E_A$ in (u, w)-plane is denoted by O, which is zero for the group law additively expressed in the abelian variety E_A. O is the point at infinity of E_A in (x, y)-plane.

Let $P_i=(u_i, w_i)\in E_A$ in (u, w)-plane $(i=1, 2, 3)$ and $P_3=P_1+P_2$, the addition being performed in the abelian variety E_A.

Then we have

$$\begin{aligned} u_3=F_A(u_1, u_2)&=u_1+u_2-A_1u_1u_2-A_2(u_1^2u_2+u_1u_2^2) \\ &\quad -2A_3(u_1^3u_2+u_1u_2^3)+(A_1A_2-3A_3)u_1^2u_2^2+\cdots. \end{aligned} \tag{3}$$

$F_A(u_1, u_2)$ is a generic formal group.

Let $a_i\in R$, $i=1, 2, 3, 4$ or 6. If we substitute a_i to A_i in (1), we get an elliptic curve defined over K, which we shall denote E from now on. The formal group $F(u_1, u_2)$ over R associated with this E is obtained from (3) by the above substitutions. (Cf. [2]–[4], [6], [11], [13].)

Denote by $E(K)$ the set of K-rational points and the point at infinity of E in (x, y)-plane.

If $P=(x, y)\in E(K)$ in (x, y)-plane satisfies $\nu(x)<0$ or $\nu(y)<0$, we have $\nu(x)=-2m$, $\nu(y)=-3m$ and $x=x'/\pi^{2m}$, $y=y'/\pi^{3m}$ where x', y' are units in R, and m is an integer. In this case, we write $N(P)=m$ and we put $N(O)=\infty$. We define now $E(\pi^n)=\{P\mid N(P)\geqq n\}$. If $E(\pi^n)$ is represented in (u, w)-plane, it consists of the origin and the point

$(\pi^m u', \pi^{3m} w')$ $(m \geqq n)$, where u', w' are units in R.

2. It is well-known that $E(\pi^n)$ is a subgroup of the abelian variety E. Now we have

Proposition 3. *The map* $(u, w) \to u$ *is an isomorphism* $E(\pi^n) \to (\mathfrak{p}^n, \dot{+})$, *where we define* $(\mathfrak{p}^n, \dot{+})$ *by the formal group* F *associated with* E. (Cf. Tate [11] Theorem 3, p. 189.)

Let α be defined as in I ([9]) for the formal group $F(u_1, u_2)$. Since $(\mathfrak{p}^n, \dot{+})$ with $n > \alpha$ is an R-module as shown in I ([9]), we can define in $E(\pi^n)$ a structure of R-module by the isomorphism of Proposition 3.

From Proposition 3 and I, we obtain the following

Theorem 4. *In the same notations as above,* $E(\pi^n)$ *is isomorphic as* R*-module to* $\mathfrak{p}^n$, *when* $n > \alpha$.

Corollary. *When* k *is a finite field with cardinal* p^f, $E(\pi)$ *is a product of a free* Z_p*-module of rank* $e \cdot f$ *and a finite abelian group of a* p*-power order.*

As the formal group F associated with E can be regarded as a specialization of the generic formal group F_A, the results of II ([10]) can be applied to obtain more explicit issues. For example we have

Theorem 5. *Let a torsion point* $P \in E(\pi^n)$ *of a finite order* p^n *be represented by* (u, w) *in* (u, w)*-plane. Then*

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

where μ, h' *have the same meanings as in Theorem* 2.

Remark. Corollary of Theorem 4 and Theorem 5 cover the results of Cassels [1] and Oort [8].

3. Now, we have the following known results for the height of formal groups associated with elliptic curves E. When E has a good reduction $\tilde{E}$ mod $\mathfrak{p}$, $\tilde{E}$ is defined over k. Let $\bar{F}$ be the reduction of F mod $\mathfrak{p}$. $\bar{F}$ is also defined over k and the height h of $\bar{F}$ is 1 or 2. (Cf. [6], [11], [13].) When E has bad reduction mod $\mathfrak{p}$, we have $h = \infty$ if $\tilde{E}$ has a cusp, and $h = 1$ if $\tilde{E}$ has a node. (Cf. [13].)

As this holds also clearly for h', *the only possible values of* h *(resp.* h'*) are* 1, 2, ∞.

Using this, we get the following theorem improving the classical result proved by Weil and Lutz ([12], [7]).

Theorem 6. *Let* $\mathrm{ch}(k) = p$, *and* $A_1 = A_2 = A_3 = 0$ *in* (1) $E(\pi^n)$ *is isomorphic to* $\mathfrak{p}^n$ *as* R*-module, if any one of the following conditions is satisfied*

(a) $p \geqq 5$ *and* $n > e/(p-1)$

(b) $p = 3$ *and* $n > e/8$

(c) $p = 2$ *and* $n > 0$.

Remark. By a similar reasoning as above, we see for example that $E(\pi^n)$ is isomorphic to $\mathfrak{p}^n$, when

$$\mathrm{ch}\,(k)=2,\ 2\,|\,a_1,\ a_2,\ a_3 \text{ and } n>0.$$

4. Finally, we mention an application to the torsion point of $E_0(K)$ defined as follows*).

$$E_0(K)=\{P\,|\,P\in E(K),\ \tilde{P}\in \tilde{E}_{ns}(k)\}$$

where $\tilde{E}_{ns}$ is the nonsingular part of the reduction $\tilde{E}$ of E mod $\mathfrak{p}$ and $\tilde{E}_{ns}(k)=\tilde{E}_{ns}\cap\tilde{E}(k)$. It is known that the kernel of the reduction map $E_0(K)\to\tilde{E}_{ns}(k)$ is $E(\pi)$. (Cf. [11].)

By Theorem 2 we obtain

Theorem 7. *Let $e/(\mu p^{h'}-1)<1$. The subgroup of $E_0(K)$ consisting of torsion elements, is mapped injectively into $\tilde{E}_{ns}(k)$ by the reduction map* (Katz [5]).

References

[1] J. W. S. Cassels: A note on the division values of $\wp(u)$. Proc. Cambridge Phil. Soc., **45**, 167–172 (1949).

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

[3] W. L. Hill: Formal groups and zeta-functions of elliptic curves. Invent. math., **12**, 321–336 (1971).

[4] T. Honda: Formal groups and zeta-functions. Osaka J. Math., **5**, 199–213 (1968).

[5] N. M. Katz: Galois properties of torsion points on Abelian varieties. Invent. math., **62**, 481–502 (1981).

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

[7] E. Lutz: Sur l'équation $y^2=x^3-Ax-B$ dans les corps $\mathfrak{p}$-adiques. Journ. reine angew. Math., **177**, 238–247 (1937).

[8] F. Oort: Elliptic curves: Diophantine torsion solutions and singular j-invariants. Math. Ann., **207**, 139–162 (1974).

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

[10] ——: Ditto II. ibid., **58A**, 265–268 (1982).

[11] J. Tate: The arithmetic of elliptic curves. Invent. math., **23**, 179–206 (1974).

[12] A. Weil: Sur les fonctions elliptique $\mathfrak{p}$-adiques. Comptes rendus, **203**, 22–24 (1936).

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

*) A point P in projective 2-space $\boldsymbol{P}_2(K)$ over K can be represented by (x_0, x_1, x_2) where $x_i\in R(i=0,1,2)$ and one of x_0, x_1, x_2 is a unit in R. Then we define $\tilde{P}=(\tilde{x}_0, \tilde{x}_1, \tilde{x}_2)$ in $\boldsymbol{P}_2(k)$ where $\tilde{x}_i=x_i$ mod $\mathfrak{p}$.