Elliptic curves and canonical subgroups of formal groups

By *Noriko Yui* at København

Abstract

We shall discuss the liftability of the Frobenius morphism of an elliptic curve and a formal group to characteristic 0, by employing the method developed by Jonathan Lubin. A sufficient condition for the liftability of the Frobenius morphism is given.

§ 0. Introduction

All formal groups discussed in this paper are commutative and 1-dimensional.

Let R be a ring with quotient field L, which is a finite extension of the field $\mathbb{Q}_p$ of p-adic numbers, $\mathfrak{M}$ the maximal ideal of R and $k = R/\mathfrak{M}$ the residue field of characteristic $p \neq 0$. Let E be an elliptic curve over L given by a Weierstrass minimal model and $\Gamma(u, v)$ the formal group associated to E (which we shall describe explicitly in § 1). Both are defined over R.

We suppose that E has good reduction modulo $\mathfrak{M}$. Then $E^* = E \pmod{\mathfrak{M}}$ and $\Gamma^*(u, v) = \Gamma(u, v) \pmod{\mathfrak{M}}$ are meaningful objects defined over k. They are studied in § 2 with a view toward seeing how much property of E^* can be recovered from its formal group $\Gamma^*(u, v)$. Finally in § 3, we discuss the liftability of the Frobenius morphism F of E^* and $\Gamma^*(u, v)$ induced by the p-th power map of k to characteristic 0, i.e. to $R[\![x]\!]$. If E^* is ordinary, a lifting always exists, because of the presence of p-torsion points on E^*. However, if E^* is supersingular, there is no p-torsion point on E^*. This phenomenon leads us to a natural question: When can the Frobenius morphism F be lifted to characteristic 0, in supersingular case? An answer is given in Theorem (3. 4): Let $b(p)$ denote the coefficient of u^p in $[p]_\Gamma(u)$. Then a sufficient condition for the liftability of F is $0 < v(b(p)) < \dfrac{p}{p+1}$ (where v is the unique extension of the p-adic valuation v_p of $\mathbb{Q}_p$ to L normalized so that $v(p) = 1$).

Notations. As usual, $\mathbb{N}$, $\mathbb{Z}$ and $\mathbb{Q}$ denote the set of natural numbers, the ring of rational integers and the field of rational numbers, respectively. For any rational prime p, $\mathbb{F}_p$, $\mathbb{Z}_p$ and $\mathbb{Q}_p$ denote the field of p elements, the ring of p-adic integers and the field of

0075-4102/78/0303-0020$02.00

p-adic rationals, respectively. v_p denotes the additively written p-adic valuation of $\mathbb{Q}_p$, normalized so that $v_p(p)=1$.

If R is a commutative ring with the identity element 1, $R[x_1, x_2, \ldots, x_n]$ (resp. $R[\![x_1, x_2, \ldots, x_n]\!]$) denotes the ring of polynomials (resp. the ring of formal power series) over R in the variables $x_1, x_2, \ldots, x_n$. If f and g are elements of $R[\![x_1, x_2, \ldots, x_n]\!]$, $f \equiv g \pmod{\deg r}$ means that $f-g$ contains no monomials of total degree less that r.

§ 1. Formal groups of elliptic curves

Let E be an elliptic curve defined over a field L by the equation

$$y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6 \tag{1. 1}$$

where $a_i \in L$ for all i and x, y are coordinates in the affine plane.

Denote by $E(L)$ the set of all L-rational points on E and the point at infinity $(0,1,0)$. It is well known that $E(L)$ has the additive group structure with the point at infinity as its zero element.

Now choosing a local parameter $u=-\dfrac{x}{y}$ near zero and putting $w=-\dfrac{1}{y}$ $\left(\text{so } x=\dfrac{u}{w},\ y=-\dfrac{1}{w}\right)$ in (1. 1), E is written in (u, w) coordinate system as

$$w=u^3+a_1uw+a_2u^2w+a_3w^2+a_4uw^2+a_6w^3. \tag{1. 2}$$

Substituting w recursively in the right hand side of (1. 2), we get the formal power series expansion for E in u:

$$\begin{aligned} w=u^3 &+a_1u^4+(a_1^2+a_2)\,u^5+(a_1^3+2\,a_1a_2+a_3)\,u^6 \\ &+(a_1^4+3\,a_1^2a_2+3\,a_1a_3+a_2^2+a_4)\,u^7 \\ &+(a_1^5+4\,a_1^3a_2+5\,a_1^2a_3+3\,a_1a_2^2+3\,a_1a_4+3\,a_2a_3)\,u^8 \\ &+\cdots. \end{aligned} \tag{1. 3}$$

We can derive easily from (1. 3) the formal power series expansions of x and y.

$$x=\frac{u}{w}=u^{-2}P(u), \quad y=-\frac{x}{u}=-u^{-3}P(u)$$

where

$$\begin{aligned} P(u)&=1-a_1u-a_2u^2-a_3u^3-(a_1a_3+a_4)\,u^4-(a_2a_3+a_1a_4)\,u^5+\cdots \\ &\in \mathbb{Z}[a_1, a_2, a_3, a_4, a_6]\,[\![u]\!]. \end{aligned} \tag{1. 4}$$

The group law of E can also be expanded into a formal power series in u. Let $P_i=(u_i, w_i)$, $i=1, 2, 3$ be L-rational points on E such that $P_3=P_1 \underset{E}{+} P_2$. Then we have

$$\begin{aligned} u_3=\Gamma(u_1, u_2)&=u_1+u_2-a_1u_1u_2-a_2(u_1^2u_2+u_1u_2^2) \\ &\quad -2\,a_3(u_1^3u_2+u_1u_2^3)+(a_1a_2-3\,a_3)\,u_1^2u_2^2+\cdots \\ &\in \mathbb{Z}[a_1, a_2, a_3, a_4, a_6]\,[\![u_1, u_2]\!]. \end{aligned} \tag{1. 5}$$

The $\Gamma(u, v)$ is *the formal group (law on one parameter) associated to the elliptic curve E.* We simply say that $\Gamma(u, v)$ is *the formal group of E.* (See Tate [7], [8].)

Likewise, we can expand the canonical invariant differential form

$$\omega_0 = \frac{dx}{2y + a_1 x + a_3}$$

on E into a formal power series in u. By (1. 4), we get

$$\begin{aligned} \omega_0 &= du\{1 + a_1 u + (a_1^2 + a_2) u^2 + (a_1^3 + 2 a_1 a_2 + 2 a_3) u^3\} \\ &\quad + (a_1^4 + 3 a_1^2 a_2 + 6 a_1 a_3 + a_2^2 + 2 a_4) u^4 + \cdots \\ &= \sum_{n=1}^{\infty} a(n) u^{n-1} du \end{aligned} \tag{1. 6}$$

where $a(n) \in \mathbb{Z}[a_1, a_2, a_3, a_4, a_6]$ for all n and $a(1) = 1$.

From here on, we confine ourselves to the case that L is a field complete with respect to a rank-one valuation v, which is the extension of the p-adic valuation v_p of $\mathbb{Q}_p$. Let R denote the ring of integers in L, $\mathfrak{M}$ the maximal ideal of R and $k = R/\mathfrak{M}$ the residue field of characteristic $p > 0$.

Let E be an elliptic curve defined over L. Then there exists the equation of the form (1. 1) for E with $a_i \in R$ for all i and with the discriminant of minimal order. Such an equation for E is called *a Weierstrass minimal model for E.*

The formal group $\Gamma(u, v)$ associated to E is, thus, defined over R.

Hence the reductions of E and $\Gamma(u, v)$ modulo $\mathfrak{M}$ are defined over k. We put $E^* = E \pmod{\mathfrak{M}}$ and $\Gamma^*(u, v) = \Gamma(u, v) \pmod{\mathfrak{M}}$.

Now we define, for any $n \in \mathbb{N}$, the endomorphism $[n]_\Gamma$: "multiplication by n" on $\Gamma(u, v)$ by

$$[n]_\Gamma(u) = \Gamma(u, [n-1]_\Gamma(u)), \quad [1]_\Gamma(u) = u.$$

Then we obtain by using (1. 5) that for $n = 2, 3, \ldots$

$$\begin{aligned} &[2]_\Gamma(u) = 2u - a_1 u^2 - 2 a_2 u^3 + (a_1 a_2 - 7 a_3) u^4 + \cdots, \\ &[3]_\Gamma(u) = 3u - 3 a_1 u^2 + (a_1^2 - 8 a_2) u^3 + 3(4 a_1 a_2 - 13 a_3) u^4 + \cdots, \\ &\quad \cdots\cdots\cdot \end{aligned} \tag{1. 7}$$

In particular, we have for $n = p = \mathrm{char}(k)$,

$$[p]_\Gamma(u) = pu \cdot g_0(u) + g(u^{p^h})$$

where $g_0(u) = 1 + \cdots \in R[\![u]\!]$, $g(u) \in R[\![u]\!]$ and $h \in \mathbb{N}$. In characteristic $p > 0$, we have either

$$[p]_\Gamma(u) \equiv c_1 u^{p^h} + c_2 u^{p^{2h}} + \cdots \pmod{\mathfrak{M}} \tag{1. 8}$$

with $c_1 \neq 0$ in k, or

$$[p]_\Gamma(u) \equiv 0 \pmod{\mathfrak{M}}.$$

The *height* of $\Gamma^*(u, v)$ is defined to be the integer h in this expression and denoted by $\mathrm{ht}(\Gamma^*)$. When the latter case occurs, we say that $\Gamma^*(u, v)$ has *infinite height*.

(1. 1) Proposition. *Suppose that E has good reduction modulo $\mathfrak{M}$, i.e., $E^* = E \pmod{\mathfrak{M}}$ also defines an elliptic curve over k. Then the formal group $\Gamma^*(u, v)$ of E^* has height* 1 *or* 2.

Proof. The "multiplication by p" on E^* is an isogeny of degree p^2, and p^h in the expansion (1. 8) is the inseparable degree of that isogeny. So p^h must divide p^2, whence $h=1, 2$. qed.

(1. 2) Remark. We consider the case that E has bad reduction modulo $\mathfrak{M}$. So $E^* = E \pmod{\mathfrak{M}}$ has a singularity. The singularity is either a cusp or a node. If the singularity is a cusp, the group law of E^* is given by usual addition of point coordinates. Hence $\Gamma^*(u, v)$ is of type $G_a(u, v) = u + v$ and hence $h = \mathrm{ht}(\Gamma^*) = \infty$. If the singularity is a node, the group law of E^* is given by multiplication of point coordinates. Hence $\Gamma^*(u, v)$ is of type $G_m(u, v) = u + v \pm uv$ and hence $h = \mathrm{ht}(\Gamma^*) = 1$. This is because

$$[p]_{G_m}(u) = (1 \pm u)^p - 1 \equiv (\pm u)^p \pmod{\mathfrak{M}}.$$

We say that E has *additive reduction* in the first case and *multiplicative reduction* in the latter case.

(1. 3) Proposition. *Let $\omega_0 = \dfrac{dx}{2y + a_1 x + a_3}$ be the canonical invariant differential on E and let $\omega_0 = \sum_{n=1}^{\infty} a(n)\, u^{n-1} du$, $a(n) \in R$ and $a(1) = 1$ be the formal power series expansion in u given by* (1. 6). *Suppose that E has good reduction modulo $\mathfrak{M}$. Then we have*

(a) $a(p) \not\equiv 0 \pmod{\mathfrak{M}} \Leftrightarrow h = \mathrm{ht}(\Gamma^*) = 1 \overset{\text{defn}}{\Leftrightarrow} E^*$ *is ordinary.*

(b) $a(p) \equiv 0 \pmod{\mathfrak{M}} \Leftrightarrow h = \mathrm{ht}(\Gamma^*) = 2 \overset{\text{defn}}{\Leftrightarrow} E^*$ *is supersingular.*

Proof. Put

$$f(u) = \sum_{n=1}^{\infty} \frac{a(n)}{n} u^n.$$

Then we have

$$\Gamma(u, v) = f^{-1}(f(u) + f(v))$$

and

$$[p]_\Gamma(u) = f^{-1}(p f(u)).$$

Writing $[p]_\Gamma(u)$ in the following form

$$[p]_\Gamma(u) = pu + \sum_{m=2}^{\infty} b(m)\, u^m,$$

we get

$$f^{-1}\left(p\left(u + \sum_{n=2}^{\infty} \frac{a(n)}{n} u^n\right)\right) = pu + \sum_{m=2}^{\infty} b(m)\, u^m. \tag{1. 9}$$

Taking modulo $\mathfrak{M}$ of (1. 9), we can derive immediately that

$$b(m) \equiv 0 \pmod{\mathfrak{M}} \quad \text{for} \quad (m, p) = 1,$$

and

$$b(p) \equiv a(p) \pmod{\mathfrak{M}}.$$

So in characteristic $p>0$, $[p]_\Gamma(u)$ takes the form

$$[p]_\Gamma(u) \equiv a(p)\, u^p + \sum_{i=2}^{\infty} b(p^i)\, u^{p^i} \pmod{\mathfrak{M}}.$$

Therefore the assertions (a) and (b) follow immediately from Proposition (1. 1). qed.

§ 2. Formal groups and p-torsion points on elliptic curves

The notations L, R, $\mathfrak{M}$ and k being the same as in § 1, let $\bar{k}$ denote the algebraic closure of k.

Let E be an elliptic curve over L given by a Weierstrass minimal model and $\Gamma(u, v) \in R[\![u, v]\!]$ the formal group of E. Suppose that E has good reduction modulo $\mathfrak{M}$. Then we have

(2. 1) Theorem (cf. Hasse [3]).

(a) $h = \mathrm{ht}(\Gamma^*) = 1 \Leftrightarrow E^*$ *has* p *points of order* p *in* $\bar{k}$.

(b) $h = \mathrm{ht}(\Gamma^*) = 2 \Leftrightarrow E$ *has no point of order* p *in* $\bar{k}$.

Proof. Let ${}_pE^*(\bar{k})$ denote the group of points of order p on E^* defined over $\bar{k}$. We know that the order of the group ${}_pE^*(\bar{k})$ is equal to the separable degree of the isogeny "multiplication by p" on E^* of degree p^2 (cf. [6]). While p^h in the expansion (1. 8) provides us the inseparable degree of that isogeny. Thus the order of ${}_pE^*(\bar{k})$ is equal to p^{2-h} and the assertions follow immediately. qed.

Now we shall investigate the relationship between p-torsion points on E^* and the invariant differentials on E and E^*. E^* is given by the equation

$$y^2 + a_1^* xy + a_3^* y = x^3 + a_2^* x^2 + a_4^* x + a_6^*$$

where $a_i^* = a_i \pmod{\mathfrak{M}}$.

(2. 2) Theorem. *Let* ω *be an invariant differential of* E *and* ω^* *denote the reduction of* ω *modulo* $\mathfrak{M}$, *which is an invariant differential on* E^*. *Then we have*

(a) E^* *has* p *points of order* p *in* $\bar{k} \Leftrightarrow \omega^*$ *is logarithmic.*

(b) E^* *has no point of order* p *in* $\bar{k} \Leftrightarrow \omega^*$ *is exact.*

Before giving a proof to Theorem (2. 2), we consider the differentials on the elliptic curve E^*. Let $K = k(x, y)$ denote the function field of E^* over k and $\mathrm{Diff}_k(K)$ the space of differentials of K over k. Then every element of $\mathrm{Diff}_k(K)$ can be expressed uniquely in the form

(2. 1) $$\omega^* = d\theta + \eta^p x^{p-1} dx$$

with some $\theta, \eta \in K$ (once the p-variable x of K is fixed).

The Cartier operator $\mathscr{C}: \mathrm{Diff}_k(K) \to \mathrm{Diff}_k(K)$ is defined, for ω^* given by (2. 1), by letting

$$\mathscr{C}(\omega^*) = \eta \, dx.$$

A differential ω^* of K is called *logarithmic* (resp. *exact*) if it is of the form dz/z (resp. dz) for some $z(\neq 0) \in K$. This definition is equivalent to say that ω^* is logarithmic (resp. exact) if and only if $\mathscr{C}(\omega^*) = \omega^*$ (resp. $\mathscr{C}(\omega^*) = 0$).

The invariant differentials on E^* form a 1-dimensional k-vector space $\mathfrak{D}_1$, which is closed under the Cartier operator. Hence, once we choose a basis for $\mathfrak{D}_1$, the Cartier operator $\mathscr{C}$ can be represented by an element of k. Let $\omega_0^* = \dfrac{dx}{2y + a_1^* x + a_3^*}$ be the canonical invariant differential on E^*. We take ω_0^* as the basis for $\mathfrak{D}_1$ once and for all. Then we have

(2. 3) Theorem. *The image of ω_0^* under the Cartier operator $\mathscr{C}$ is given by*

$$\mathscr{C}(\omega_0^*) = A^{1/p} \omega_0^*$$

where the Cartier operator $\mathscr{C}$ is represented by the element $A^{1/p}$ and A is given by the value

$$\begin{array}{ll} a_1^* & \text{if } p=2, \\ a_1^{*2} + a_2^* & \text{if } p=3, \end{array}$$

and if $p \geqq 5$,

$$\sum_{2i+3j=\frac{p-1}{2}} \frac{\left(\frac{p-1}{2}\right)!}{i!\,j!\left(\frac{p-1}{2} - i - j\right)!} a^i b^j 4^{\frac{p-1}{2}-i-j},$$

with

$$(2.2) \qquad \begin{aligned} a &= -\frac{(a_1^{*2} + 4a_2^*)^2}{12} + 4a_4^* + 2a_1^* a_3^*, \\ b &= \frac{(a_1^{*2} + 4a_2^*)^3}{216} - \frac{(a_1^{*2} + 4a_2^*)(a_1^* a_3^* + 2a_4^*)}{6} + a_3^{*2} + 4a_6^*. \end{aligned}$$

Proof. Write ω_0^* in the following form

$$\omega_0^* = (2y + a_1^* x + a_3^*)^{-p} Q(x, y) \, dx$$

with

$$Q(x, y) = (2y + a_1^* x + a_3^*)^{p-1}.$$

To get the image of ω_0^* under the Cartier operator $\mathscr{C}$, it suffices to compute the coefficient A of x^{p-1} in $Q(x, y)$, because all other terms give exact differentials. If $p=2$, $A = a_1^*$ and if $p=3$, $A = a_1^{*2} + a_2^*$. Assume now that $p \geqq 5$. Then we get the classical Weierstrass equation for E^* by replacing x and y by

$$X = x + \frac{a_1^{*2} + 4a_2^*}{12}, \quad Y = 2y + a_1^* x + a_3^*.$$

The classical Weierstrass equation for E^* is the following equation:

$$Y^2 = 4X^3 + aX + b$$

where a and b are prescribed in (2. 2).

Hence the coefficient A of x^{p-1} in

$$Q(X, Y) = (4X^3 + aX + b)^{\frac{p-1}{2}}$$

is given by

$$A = \sum_{2i+3j=\frac{p-1}{2}} \frac{\left(\frac{p-1}{2}\right)!}{i!\,j!\left(\frac{p-1}{2} - i - j\right)!} a^i b^j 4^{\frac{p-1}{2}-i-j}.$$

This is the Deuring formula for *the Hasse invariant of* E^* ([1]).

(2. 4) Remark. We can express the invariant differential $\omega^* \in \mathrm{Diff}_k(K)$ also in the form

$$\omega^* = d\theta + \varphi^p \frac{dx}{x} \qquad \text{with} \quad \theta, \varphi \in K.$$

We define the modified Cartier operator $\mathscr{C}' : \mathrm{Diff}_k(K) \to \mathrm{Diff}_k(K^p)$ by letting, for ω^* given in the above form,

$$\mathscr{C}'(\omega^*) = \varphi^p \frac{d^p x^p}{x^p}.$$

Then the image of the canonical invariant differential ω_0^* under $\mathscr{C}'$ is given by

$$\mathscr{C}'(\omega_0^*) = A\,\omega_0^{*p}.$$

(2. 5) Theorem. *Let A be the Hasse invariant on E^* given as in Theorem* (2. 3). *Put*

$$H = \{\alpha \in k \mid A\alpha^p = 0\}$$

and

$$G = \{\alpha \in k \mid A\alpha^p = \alpha\}.$$

Then H is a k-vector space and G generates a k-vector space $\langle G \rangle$. Moreover we have

(a) $\mathfrak{D}_1$ *is equal to* $H\omega_0^* \Leftrightarrow A = 0 \Leftrightarrow$ *every* $\omega^* \in \mathfrak{D}_1$ *is exact.*

(b) $\mathfrak{D}_1$ *is equal to* $\langle G \rangle \omega_0^* \Leftrightarrow A \neq 0 \Leftrightarrow$ *every* $\omega^* \in \mathfrak{D}_1$ *is logarithmic.*

Proof. We can see easily that H becomes a k-vector space and that G itself is not a k-vector space, but it generates a k-vector space $\langle G \rangle$. Since $\mathfrak{D}_1$ is an 1-dimensional k-vector space with the basis ω_0^*, any element $\omega^* \in \mathfrak{D}_1$ can be expressed in the form

$$\omega^* = \alpha\omega_0^* \qquad \text{with some} \qquad \alpha(\neq 0) \in k.$$

Now $H\omega_0^*$ is contained in $\mathfrak{D}_1$, so it follows that $H\omega_0^* = \{0\}$ or $H\omega_0^* = \mathfrak{D}_1$. Similarly, we have either $\langle G \rangle \omega_0^* = \{0\}$ or $\langle G \rangle \omega_0^* = \mathfrak{D}_1$.

(a) $H\omega_0^* = \mathfrak{D}_1 \Leftrightarrow A = 0 \Leftrightarrow \mathscr{C}(\omega^*) = 0$ for every $\omega^* \in \mathfrak{D}_1 \Leftrightarrow$ every $\omega^* \in \mathfrak{D}_1$ is exact.

(b) $\langle G \rangle \omega_0^* = \mathfrak{D}_1 \Leftrightarrow A \neq 0 \Leftrightarrow \mathscr{C}(\omega^*) = \omega^*$ for every $\omega^* \in \mathfrak{D}_1 \Leftrightarrow$ every $\omega^* \in \mathfrak{D}_1$ is logarithmic. qed.

(2. 6) Theorem. *Let* $u=-\frac{x}{y}$ *be a local parameter of E at zero,* $\omega_0=\sum_{n=1}^{\infty} a(n)\, u^{n-1} du$ *the canonical invariant differential on E given by* (1. 6) *and* $[p]_\Gamma(u)=pu+\sum_{m=2}^{\infty} b(m)\, u^m$ *the "multiplication by p" on* $\Gamma(u,v)$. *Let A be the Hasse invariant of* E^* *obtained in Theorem* (2. 3). *Then*

$$A\equiv a(p)\equiv b(p) \pmod{\mathfrak{M}}.$$

Proof. We have only to show the first congruence, since the latter congruence is already shown in the proof of Proposition (1. 3). By definition of the Cartier operator, we have

$$\mathscr{C}(\omega_0^*)=A^{1/p}\frac{x}{2y+a_1^*x+a_3^*}\frac{dx}{x}=A^{1/p}\left(\sum_{n=1}^{\infty} a(n)^*\, u^{n-1} du\right)=A^{1/p}du+\cdots$$

where $a(n)^*=a(n) \pmod{\mathfrak{M}}$.

On the other hand, we also have

$$\mathscr{C}(\omega_0^*)=\mathscr{C}\left(\sum_{n=1}^{\infty} a(n)^*\, u^{n-1} du\right)=a(p)^{*1/p}\, du+\cdots.$$

Hence we obtain the congruence

$$A\equiv a(p) \pmod{\mathfrak{M}}. \qquad \text{qed.}$$

(2. 7) *Proof of Theorem* (2. 2). We have the following equivalent statements:

(a) every $\omega^*\in\mathfrak{D}_1$ is exact $\Leftrightarrow \mathscr{C}(\omega^*)=0 \overset{\text{Thm. (2. 5)}}{\Leftrightarrow} A=0 \overset{\text{Thm. (2. 6)}}{\Leftrightarrow} a(p)\equiv 0 \pmod{\mathfrak{M}}$ $\overset{\text{Prop. (1. 3)}}{\Leftrightarrow} h=2 \overset{\text{Thm. (2. 1)}}{\Leftrightarrow} E^*$ has no point of order p in k.

(b) every $\omega^*\in\mathfrak{D}_1$ is logarithmic $\Leftrightarrow \mathscr{C}(\omega^*)=\omega^* \overset{\text{Thm. (2. 5)}}{\Leftrightarrow} A\not\equiv 0 \overset{\text{Thm. (2. 6)}}{\Leftrightarrow} a(p)\not\equiv 0 \pmod{\mathfrak{M}}$ $\overset{\text{Prop. (1. 3)}}{\Leftrightarrow} h=1 \overset{\text{Thm. (2. 1)}}{\Leftrightarrow} E^*$ has p points of order p in k. qed.

§ 3. Canonical subgroups of formal groups

The notations L, R, $\mathfrak{M}$, k and $\bar{k}$ being the same as before, let $\bar{L}$ be the algebraic closure of L, $\bar{R}$ the integral closure of R in $\bar{L}$, $\bar{\mathfrak{M}}$ the maximal ideal of $\bar{R}$ and v the unique prolongation of the p-adic valuation v_p of $\mathbb{Q}_p$ to L, additively written and normalized so that $v(p)=1$. The unique extension to $\bar{L}$ of v will also be denoted by v.

Let $\Phi(x,y)$ be a formal group over R and let $\Phi^*(x,y)=\Phi(x,y) \pmod{\mathfrak{M}}$. The elements of $\bar{\mathfrak{M}}$ form an abelian group $\Phi(\bar{R})$ under $\Phi(x,y)$ by the operation $\alpha * \beta=\Phi(\alpha,\beta)$. The elements of $\Phi(\bar{R})$ of finite order form a torsion subgroup of $\Phi(\bar{R})$. In particular, $\operatorname{Ker}[p]_\Phi$ is a torsion p-subgroup of $\Phi(\bar{R})$, since $[p]_\Phi(\alpha*\beta)=\Phi([p]_\Phi(\alpha),[p]_\Phi(\beta))=0$ for any $\alpha,\beta\in\operatorname{Ker}[p]_\Phi$. (For detail, see [2].) For any positive real number λ, we put

$$\Phi(\bar{R})_\lambda=\{\alpha\in\Phi(\bar{R})\,|\,v(\alpha)\geqq\lambda\}.$$

Then it is easy to see that $\Phi(\bar{R})_\lambda$ is a subgroup of $\Phi(\bar{R})$. A subgroup S of $\Phi(\bar{R})$ is called a congruence torsion subgroup of $\Phi(x,y)$ if there is a positive real number λ for which

$$S=\{\alpha\in\Phi(\bar{R})_\lambda;\ \text{there is an } n\in\mathbb{N} \text{ such that } \alpha\in\operatorname{Ker}[p^n]_\Phi\}.$$

(3. 1) Definition. The canonical subgroup $\operatorname{can}(\Phi)$ of $\Phi(x, y)$ is a congruence torsion subgroup of order p in $\operatorname{Ker}[p]_\Phi$.

(3. 2) Theorem (cf. Lubin [4]). *Let $\Phi(x, y)$ be a standard generic formal group over R with $h = ht(\Phi^*) < \infty$ and let*

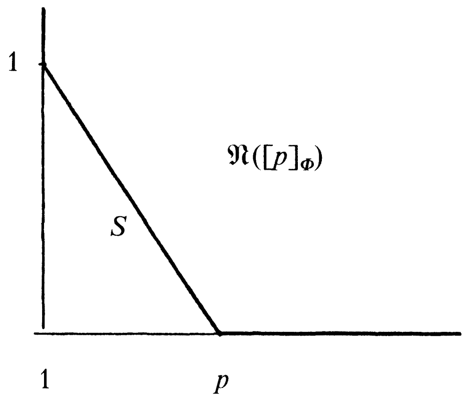
$$[p]_\Phi(x) = pxg_0(x) + \sum_{i=1}^{h-1} \alpha_i x^{p^i} g_i(x) + \alpha_h x^{p^h} g_h(x)$$

where $v(\alpha_i) > 0$ for each $1 \leqq i \leqq h-1$, $v(\alpha_h) = 0$ and $g_0(x)$, $g_i(x)$ for each $1 \leqq i \leqq h-1$ are units in $R[\![x]\!]$ and $g_h(x) \in R[\![x]\!]$, be the "multiplication by p" on $\Phi(x, y)$. Then the following statements are equivalent:

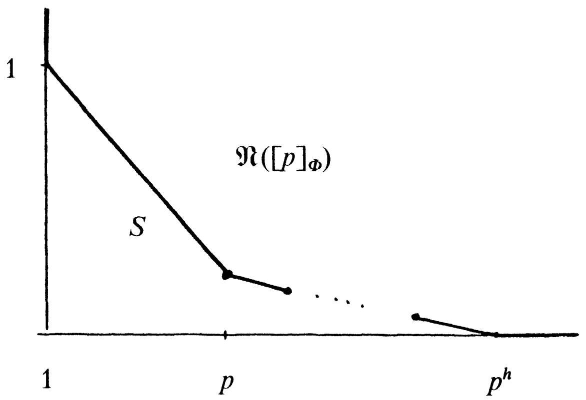
(i) *$\Phi(x, y)$ has the canonical subgroup* $\operatorname{can}(\Phi)$.

$$\text{(ii)} \begin{cases} v(\alpha_1) = 0 & \text{if } h = 1, \\ v(\alpha_1) < \dfrac{p^h - p}{p^h - 1} & \text{if } h \geqq 2. \end{cases}$$

(iii) *The Newton polygon $\mathfrak{N}([p]_\Phi)$ of $[p]_\Phi(x)$ has a vertex at $(p, v(\alpha_1))$ and has the shape as illustrated below*:



if $h = 1$



if $h \geqq 2$.

When one of the above conditions is satisfied, the canonical subgroup $\operatorname{can}(\Phi)$ *of $\Phi(x, y)$ is explicitly given by*

$$\operatorname{can}(\Phi) = \begin{cases} \{0\} \cup \left\{\alpha \in \Phi(\bar{R})_\lambda \mid v(\alpha) = \dfrac{1}{p-1}\right\} & \text{if } h = 1 \\ \{0\} \cup \left\{\alpha \in \Phi(\bar{R})_\lambda \mid v(\alpha) = \dfrac{1 - v(\alpha_1)}{p-1} \text{ with } v(\alpha_1) < \dfrac{p^h - p}{p^h - 1}\right\} & \text{if } h \geqq 2, \end{cases}$$

where $\lambda = -$(slope of the segment S in $\mathfrak{N}([p]_\Phi)$), i.e.

$$\lambda = \begin{cases} \dfrac{1}{p-1} & \text{if } h = 1 \\ \dfrac{1 - v(\alpha_1)}{p-1} & \text{if } h \geqq 2. \end{cases}$$

Proof. A formal group $\Phi(x, y)$ over R with height $h < \infty$ is called *a standard generic* if it has the formal moduli $(\alpha_1, \alpha_2, \ldots, \alpha_{h-1}) \in \mathfrak{M} \times \mathfrak{M} \times \cdots \times \mathfrak{M}$ (see [5]) and $[p]_\Phi(x)$ necessarily has the prescribed form.

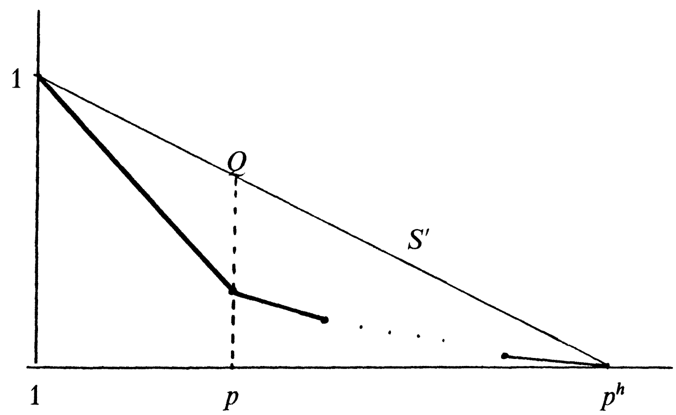
First we shall prove the assertions when $h=1$. We know that $h=1 \Leftrightarrow \alpha_1$ is a unit in R, i.e. $v(\alpha_1)=0 \Leftrightarrow \operatorname{Ker}[p]_\Phi$ has order p. Hence by Definition (3. 1), one can see at once that $\operatorname{can}(\Phi)=\operatorname{Ker}[p]_\Phi$. This implies that $\operatorname{can}(\Phi)$ always exists whenever $h=1$. The equivalences follow immediately. Now the segment S of the Newton polygon $\mathfrak{N}([p]_\Phi)$ gives rise to exactly $p-1$ distinct roots of $[p]_\Phi(x)=0$ with order $\dfrac{1}{p-1} = -(\text{slope of } S)$.

Hence we get the group

$$\operatorname{can}(\Phi)=\operatorname{Ker}[p]_\Phi=\{0\} \cup \left\{\alpha \in \Phi(\bar{R})_{\frac{1}{p-1}} \mid v(\alpha)=\frac{1}{p-1}\right\}.$$

Now we shall consider the case of $h \geqq 2$.

(i) $\Rightarrow$ (ii). Suppose that $\Phi(x, y)$ has the canonical subgroup $\operatorname{can}(\Phi)$, then $[p]_\Phi(x)$ must have a polynomial factor of degree p. This forces that the Newton polygon of $[p]_\Phi(x)$ has a vertex at p by noting that all the coefficients of x^i for $i<p$ have order $\geqq 1$. The Newton polygon of $[p]_\Phi(x)$ has a vertex at $(p, v(\alpha_1))$, if and only if $v(\alpha_1)$ is smaller than the order of the point Q where Q is defined by



$$S': y = -\frac{1}{p^h-1}x + \frac{p^h}{p^h-1}.$$

The point Q has the coordinate $\left(p, \dfrac{p^h-p}{p^h-1}\right)$. Hence we get the assertion (ii).

(ii) $\Leftrightarrow$ (iii) are clear.

(iii) $\Rightarrow$ (i). If the Newton polygon of $[p]_\Phi(x)$ has the shape as (iii), the segment S yields $p-1$ roots $\beta_1, \beta_2, \ldots, \beta_{p-1} \in \bar{R}$ with $v(\beta_i)=\dfrac{1-v(\alpha_1)}{p-1} = -(\text{slope of } S)$. The roots are distinct, because $\frac{d}{dx}[p]_\Phi(x) \neq 0$ for any $x \in \bar{R}$. Put $f(x) = x \prod_{i=1}^{p-1}(x-\beta_i)$. Then $f(x)$ is a monic polynomial over R such that $f(x) \equiv x^p \pmod{\mathfrak{M}}$ and that $f(x)$ divides $[p]_\Phi(x)$ by Lubin's Local Factorization Principle ([4]). Hence the canonical subgroup $\operatorname{can}(\Phi)$ exists and it is given explicitly by the group

$$\operatorname{can}(\Phi) = \left\{0, \beta_1, \beta_2, \ldots, \beta_{p-1} \mid v(\beta_i) = \frac{1-v(\alpha_1)}{p-1} \text{ with } v(\alpha_1) < \frac{p^h-p}{p^h-1}\right\} \qquad \text{qed.}$$

(3. 3) Theorem (cf. Lubin [4]). *Let $\Phi(x, y)$ be a standard generic formal group over R with $h = \operatorname{ht}(\Phi^*) < \infty$. Suppose that $\Phi(x, y)$ has the canonical subgroup $\operatorname{can}(\Phi)$. Then the Frobenius morphism F of $\Phi(x, y)$ induced by the p-th power map $x \to x^p$ of k can be lifted back to $R[\![x]\!]$.*

Proof. Put

$$f(x) = \prod_{\alpha \in \operatorname{can}(\Phi)} (x-\alpha).$$

Then $f(x)$ is a monic polynomial over R of degree p satisfying $f(x) \equiv x^p \pmod{\mathfrak{M}}$. So $f(x)$ is a good candidate for a lifting of the Frobenius morphism F. In order for $f(x)$ to be indeed a lifting of F, $f(\Phi(x, y))$ must be the ideal $(f(x), f(y))$, which is the set of all formal power series $g(x, y) \in R[\![x, y]\!]$ satisfying $g(\alpha, \alpha') = 0$ for $\alpha, \alpha' \in \operatorname{can}(\Phi)$. But we see that for any $\alpha, \alpha' \in \operatorname{can}(\Phi)$, $\Phi(\alpha, \alpha') \in \operatorname{can}(\Phi)$. This implies that $f(\Phi(x,y)) \subset (f(x), f(y))$. The other inclusion is clear. Hence we get

$$f(\Phi(x, y)) = (f(x), f(y)).$$

We have a commutative diagram

$$\begin{tikzcd} \Phi(x, y) \arrow[r, "f"] \arrow[d, "\bmod \mathfrak{M}"'] & f(\Phi(x, y)) \arrow[d, "\bmod \mathfrak{M}"] \\ \Phi^*(x, y) \arrow[r, "F"] & \Phi^{*(p)}(x^p, y^p) \end{tikzcd}$$

where $\Phi^{*(p)}(x^p, y^p)$ denotes the formal power series in x^p, y^p with the coefficients of the p-th power of those of $\Phi^*(x, y)$. qed.

(3. 4) Theorem. *Let E be an elliptic curve over L given by a Weierstrass minimal model and $\Gamma(u, v)$ be the formal group of E. Suppose that E has good reduction modulo $\mathfrak{M}$. Then we have*

(a) *If $h = \operatorname{ht}(\Gamma^*) = 1$, $\Gamma(u, v)$ always has the canonical subgroup $\operatorname{can}(\Gamma)$; $\operatorname{can}(\Gamma) = \operatorname{Ker}[p]_\Gamma$.*

(b) *If $h = \operatorname{ht}(\Gamma^*) = 2$, $\Gamma(u, v)$ has the canonical subgroup $\operatorname{can}(\Gamma)$, if and only if $b(p) \equiv 0 \pmod{\mathfrak{M}}$ and $v(b(p)) < \frac{p}{p+1}$, where $b(p)$ is the coefficient of u^p in $[p]_\Gamma(u)$. If $\operatorname{can}(\Gamma)$ exists, it is explicitly given by the group*

$$\operatorname{can}(\Gamma) = \{0\} \cup \left\{\alpha \in \Gamma(\bar{R})_\lambda \mid v(\alpha) = \frac{1-v(b(p))}{p-1}\right\}$$

where $\lambda = \frac{1-v(b(p))}{p-1}$.

Proof. Apply the same arguments as in the proof of Theorem (3. 2).

(3. 5) Examples. Let L be a finite extension of $\mathbb{Q}_p$ with a uniformizing element π. Let E be an elliptic curve defined over $\mathbb{Z}_p[\pi]$ with the discriminant Δ and $E^* = E \pmod{\pi}$. Let $\Gamma(u, v)$ be the formal group of E.

Case (I). Suppose $p=2$.

(Ia) Let E be given by

$$y^2 + xy = x^3 + a_2 x^2 + a_6 \quad \text{with} \quad v(a_6) = 0.$$

Then E has good reduction at π, because $v(\Delta) = v(a_6) = 0$. Since

$$[2]_\Gamma(u) \equiv -u^2 \pmod{\pi}, \pmod{\deg 3},$$

E^* is ordinary. Hence $\Gamma(u, v)$ possesses the canonical subgroup $\operatorname{can}(\Gamma)$.

(Ib) Let E be given by

$$y^2 + a_3 y = x^3 + a_4 x + a_6 \quad \text{with} \quad v(a_3) = 0.$$

Then $v(\Delta) = v(a_3^4) = 4\, v(a_3) = 0$. So E has good reduction at π. Now we have

$$[2]_\Gamma(u) \equiv -7\, a_3 u^4 \pmod{\pi}, \pmod{\deg 5}.$$

Hence E^* is supersingular. $\Gamma(u, v)$ does not have the canonical subgroup, because $b(2) = 0$.

(Ic) Let E be given by

$$y^2 + a_1 xy + a_3 y = x^3 \quad \text{with} \quad v(a_3) = 0.$$

Then $v(\Delta) = v(-8\, a_1^3 a_3^3 - 27\, a_3^4 + 9\, a_1^3 a_3^3) = 0$. So E has good reduction at π. From (1. 7), we get

$$[2]_\Gamma(u) = 2\,u - a_1 u^2 - 2\, a_3 u^3 - 7\, a_3 u^4 \pmod{\deg 5},$$

so it follows from Theorem (3. 4) that $\Gamma(u, v)$ has the canonical subgroup $\operatorname{can}(\Gamma) \Leftrightarrow v(a_1) = 0$ or $0 < v(a_1) < \frac{2}{3}$.

Case (II). Suppose $p=3$.

(IIa) Let E be given by

$$y^2 = x^3 + a_2 x^2 + a_6 \quad \text{with} \quad v(a_6) = 0.$$

Then E has good reduction at π, because $v(\Delta) = v(-a_2^3 a_6) = 0$. From (1. 7), we get

$$[3]_\Gamma(u) = 3\,u - 8\, a_2 u^3 \pmod{\deg 4}.$$

Hence by Theorem (3. 4), $\Gamma(u, v)$ has the canonical subgroup $\operatorname{can}(\Gamma) \Leftrightarrow v(a_2) = 0$ or $0 < v(a_2) < \frac{3}{4}$.

(IIb) Let E be given by

$$y^2 = x^3 + a_4 x + a_6 \quad \text{with} \quad v(a_4) = 0.$$

Then $\nu(\Delta)=\nu(-a_4^3)=0$. So E has good reduction at π. We have

$$\Gamma(u, v)=u+v-2\,a_4(u^4v+uv^4)-4\,a_4(u^3v^2+u^2v^3)$$
$$-15\,a_6(u^3v^4+u^4v^3)-9\,a_6(u^5v^2+u^2v^5)+\cdots$$

and

$$[3]_\Gamma(u)\equiv 3\,u \pmod{\deg 5}.$$

E^* is supersingular and $\Gamma(u, v)$ does not possess the canonical subgroup $\mathrm{can}(\Gamma)$.

Case (III). Suppose $p=5$.

Let E be an elliptic curve given by the equation

$$y^2=x^3+a_4x+a_6 \quad \text{with} \quad \nu(a_6)=0.$$

Then $\nu(\Delta)=\nu\bigl(-16\,(4\,a_4^3+27\,a_6^2)\bigr)=0$, which implies that E has good reduction at π. We have $\Gamma(u, v)$ given as in case (IIb) and

$$[5]_\Gamma(u)\equiv 5\,u-1248\,a_4u^5 \pmod{\deg 6}.$$

Hence by Theorem (3. 4), $\Gamma(u, v)$ possesses the canonical subgroup $\mathrm{can}(\Gamma)\Leftrightarrow \nu(a_4)=0$ or $0<\nu(a_4)<\dfrac{5}{6}$.

References

[1] *M. Deuring*, Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, Abh. Math. Sem. Hamburg **14** (1941), 197—272.

[2] *A. Fröhlich*, Formal Groups, Lecture Notes in Mathematics, Berlin-Heidelberg-New York 1968.

[3] *H. Hasse*, Existenz separabler zyklischer unverzweigter Erweiterungskörper vom Primzahlgrade p über elliptischen Funktionenkörpern der Charakteristik p, J. reine angew. Math. **172** (1934), 77—85.

[4] *J. Lubin*, Canonical subgroups of formal groups, University of Copenhagen Preprint Series No. **8** (1975).

[5] *J. Lubin* and *J. Tate*, Formal moduli for one-parameter formal Lie groups, Bull. Soc. Math. France **94** (1966), 49—60.

[6] *G. Shimura* and *Y. Taniyama*, Complex Multiplication of Abelian Varieties, Math. Soc. Japan (1961).

[7] *J. Tate*, Rational points on elliptic curves, mimeographed Haverford College Lecture Note (1961).

[8] *J. Tate*, The arithmetic of elliptic curves, Invent. Math. **23** (1974), 179—206.

Matematisk Institut, København Universitet, Universitetsparken 5, DK-2100 København Ø

Current address: Department of Mathematics, University of Ottawa, Ottawa, Ontario, Canada K1N 6N5

Eingegangen 12. Februar 1978