COMPOSITIO MATHEMATICA

KEVIN KEATING

Lifting endomorphisms of formal *A*-modules

Compositio Mathematica, tome 67, n° 2 (1988), p. 211-239

<http://www.numdam.org/item?id=CM_1988__67_2_211_0>

Compositio Mathematica 67: 211–239 (1988)

Lifting endomorphisms of formal A-modules

KEVIN KEATING
Department of Mathematics, University of Michigan, Ann Arbor, MI 48109, USA

Received 25 August 1987; accepted in revised form 3 February 1988

Abstract. Let k be a field of characteristic p and let F_n be a 1-parameter formal group law over $k[t]/(t^{n+1})$. Assume that the reduction of F_n (mod (t)) has height $h < \infty$ and that F_n has height $h - 1$. In this paper we compute the endomorphism ring of F_n. The result can be used to compute the endomorphism ring of an ordinary elliptic curve E over $k[t]/(t^{n+1})$ whose reduction (mod (t)) is supersingular.

Introduction

Let F_0 be a formal A-module (or formal group law) of height $h < \infty$ over a field k of characteristic p, and let F be a formal A-module of height $h - 1$ over $R = k[[t]]$ whose special fiber if F_0. The endomorphism ring of F_0 can be quite large – if k is separably closed then $\mathrm{End}_k(F_0)$ is the maximal order in a division algebra. The ring of R-endomorphisms of F is just A. Intermediate between these two are the rings $\mathrm{End}_{R/(t^{n+1})}(F)$, which are A-subalgebras of $\mathrm{End}_k(F_0)$. In this paper we compute $\mathrm{End}_{R/(t^{n+1})}(F)$ using the formal cohomology theory of Lubin-Tate [10] and Drinfeld [1]. The Serre–Tate lifting allows us to apply these results to the endomorphism-lifting problem for ordinary elliptic curves E over $R/(t^{n+1})$ with supersingular special fiber. In another paper [6] we use these results to get information about the Galois character χ_F attached to F.

The work presented here is part of the author's 1987 Harvard Ph.D. thesis, written under the direction of Professor Benedict Gross. His guidance in this research was indispensable.

1. Statement of the theorem

Let K be a complete discretely valued field with finite residue field $\mathbf{F}_q$, and let A be the ring of integers in K. Then either $A \cong \mathbf{F}_q[[x]]$ and $K \cong \mathbf{F}_q((x))$, or K is a finite extension of $\mathbf{Q}_p$. Let R be an A-algebra with structure map γ: $A \to R$. A *one-parameter formal A-module* F over R is a one-parameter formal group law $\tilde{F}$ over R, together with a homomorphism

$$\phi\colon A \to \mathrm{End}_R(\tilde{F})$$

such that the induced map

$$\phi_*\colon A \to \mathrm{End}_R(\mathrm{Lie}\ \tilde{F}) \cong R$$

is equal to γ. If F and G are formal A-modules over R then $\mathrm{Hom}_R(F, G)$ consists of those $f \in \mathrm{Hom}_R(\tilde{F}, \tilde{G})$ such that f intertwines the image of ϕ_F with the image of ϕ_G. That is,

$$f \circ \phi_F(a) = \phi_G(a) \circ f$$

for all $a \in A$. If $A = \mathbf{Z}_p$ then a formal A-module is the same thing as a formal group law.

Let $\pi = \pi_A$ be a uniformizer for A and recall that $A/\pi A \cong \mathbf{F}_q$ is the residue field of A. Let F be a formal A-module over the $\mathbf{F}_q$-algebra R, and for $a \in A$ set

$$[a]_F(x) = \phi(a)(x) \in \mathrm{End}_R(F).$$

Then the power series $[\pi]_F(x)$ is either zero, in which case we say that F has infinite height, or has the form

$$[\pi]_F(x) = s(x^{q^h})$$

with $s'(0) \neq 0$. In the second case we say that F has (finite) height h.

Let F_0 be a formal A-module over the field k of characteristic $p > 0$, and let R be a local A-algebra with maximal ideal $\mathscr{M}_R$ and residue field $k' \supset k$. Then the structure maps $\gamma_k\colon A \to k$ and $\gamma_R\colon A \to R$ make the diagram

$$\begin{array}{ccc} A & \xrightarrow{\gamma_R} & R \\ {\scriptstyle\gamma_k}\downarrow & & \downarrow \\ k & \hookrightarrow & k' \end{array}$$

commute. A *deformation* of F_0 over R is a formal A-module F/R such that

$$F \equiv F_0 \pmod{\mathscr{M}_R}.$$

Let F/R and F'/R be deformations of F_0/k. An isomorphism $\phi\colon F \to F'$ is called a $*$-*isomorphism* if the reduction of ϕ (mod(t)) is the identity of F_0.

Let F/R and F'/R be deformations of F_0/k. An isomorphism $\phi: F \to F'$ is called a $*$-*isomorphism* if the reduction of ϕ (mod(t)) is the identity of F_0.

Let $1 < h < \infty$ and choose a formal A-module F_0 of height h over k. Let R be the discretely valued ring $k[[t]]$. The ring R has a canonical A-algebra structure, given by the composite map

$$A \xrightarrow{\gamma_k} k \overset{i}{\hookrightarrow} R.$$

Let F be a deformation of F_0 over R of height $h-1$. We write

$$[\pi]_F(x) = a_0 x^{q^{h-1}} + \dots$$

with $a_0 \in R \setminus \{0\}$. Set $e = v_t(a_0)$, so that $0 < e < \infty$. Let $R_n = R/(t^{n+1})$ and $F_n = F \otimes_R R_n$; then F_n is the reduction of F (mod (t^{n+1})). Our goal is to compute

$$\mathrm{End}_{R_n}(F_n) = \mathrm{End}_{R_n}(F)$$

for every n. Let $D_{1/h}$ be the division algebra of degree h^2 over K with invariant $1/h$, and let B be the maximal order in $D_{1/h}$. By [1, Prop. 1.7] the ring

$$H = \mathrm{End}_k(F_0)$$

is isomorphic to B when k is separably closed. The reduction maps $R_{n+1} \to R_n$ induce maps

$$\mathrm{End}_{R_{n+1}}(F) \to \mathrm{End}_{R_n}(F).$$

By [1, Prop. 4.1] these maps are injective, and the rings $\mathrm{End}_{R_n}(F)$ can be identified with A-subalgebras H_n of B. In the general case, H is isomorphic to an A-subalgebra of B and $\mathrm{End}_{R_n}(F)$ is identified with an A-subalgebra $H_n \subset H$. The non-commutative ring B has a discrete valuation v_B such that $v_B(a) = h \cdot v_A(a)$. Choose $\pi_B \in B$ such that $v_B(\pi_B) = 1$. We say that π_B is a uniformizer for B. Since the formal A-module F_0 has height h, any uniformizer π_B has the form

$$[\pi_B]_{F_0}(x) = bx^q + \dots$$

for some $b \in k^\times$.

We begin by computing $\mathrm{End}_{R_n}(F)$ in the case where $e = 1$ and k is separably closed. The general case will be handled in Theorem 3.3. Let

$g = h - 1$ and for $m \geqslant 0$ define

$$a(gm) = \frac{(q^h - 1)(q^{gm} - 1)}{(q^g - 1)(q - 1)},$$

so that $a(0) = 0$. The non-negative integers $a(gm)$ are the upper ramification breaks of the Galois character χ_F associated to F (see [4, p. 86]).

THEOREM 1.1. *Let F be a deformation of F_0/k of height $g = h - 1$ with $e = 1$ and k separably closed. Let $f_0 \in \mathrm{End}_k(F_0) \cong B$ be such that*

$$f_0 \in (A + \pi_B^l B) \setminus (A + \pi_B^{l+1} B) \quad (l \geqslant 0).$$

Write $l = hm + b$ with $0 \leqslant b < h$ and set

$$n = a(gm) + q^{gm} . \frac{q^b - 1}{q - 1} + 1.$$

Then $f_0 \in H_{n-1} \setminus H_n$.

REMARK. Some special cases of this theorem were proved independently by Fujiwara (see [2, Prop. 3 and Prop. 4] and [11, Lemma 2]).

Using Theorem 1.1 we can calculate $H_n = \mathrm{End}_{R_n}(F)$.

THEOREM 1.2. *Let F be a deformation of F_0 as above. Then*

$$H_n = A + \pi_B^{j(n)} B$$

where $j(n) = hm + b$ whenever

$$a(gm) - q^{gm} + 1 \leqslant n < a(gm) + 1 \qquad (b = 0)$$

$$a(gm) + q^{gm} \cdot \frac{q^{b-1} - 1}{q - 1} + 1 \leqslant n < a(gm) + q^{gm} \cdot \frac{q^b - 1}{q - 1} + 1 \qquad (0 < b < h).$$

REMARKS:

1. The presence of the upper ramification breaks $a(gm)$ in our formulas for $\mathrm{End}_{R_n}(F)$ is not a coincidence. The relation between χ_F and the rings $\mathrm{End}_{R_n}(F)$ is exploited in [2] and [6].

2. The most important special case of this theorem is $A = \mathbf{Z}_p$, $h = 2$, $g = 1$. This occurs when F is the formal group of a universal deformation of a supersingular elliptic curve over $k[[t]]$ (see Section 4). In this case,

$$
\begin{aligned}
j(0) &= 0 \\
j(1) &= 1 \\
j(n) &= 2 && \text{if } 2 \leqslant n < 2 + p \\
j(n) &= 3 && \text{if } 2 + p \leqslant n < 2(1 + p) \\
j(n) &= 4 && \text{if } 2(1 + p) \leqslant n < 2(1 + p) + p^2 \\
&\vdots && \qquad\vdots \qquad \vdots \qquad \vdots \\
j(n) &= 2k && \text{if } 2(1 + p + \cdots + p^{k-1}) \leqslant n \\
& && \quad < 2(1 + p + \cdots + p^{k-1}) + p^k \\
j(n) &= 2k + 1 && \text{if } 2(1 + p + \cdots + p^{k-1}) + p^k \leqslant n \\
& && \quad < 2(1 + p + \cdots + p^k).
\end{aligned}
$$

The proof of Theorem 1.1 has two steps, which we state as propositions.

PROPOSITION 1.3. *Let* $0 \leqslant l \leqslant h$, *and assume that*

$$f_0 \in (A + \pi_B^l B) \setminus (A + \pi_B^{l+1} B).$$

Then $f_0 \in H_{n-1} \setminus H_n$ *with*

$$n = \frac{q^l - 1}{q - 1} + 1.$$

PROPOSITION 1.4. *Choose* $f_0 \in A + \pi_B B$ *and let* $n > 1$ *be such that* $f_0 \in H_{n-1} \setminus H_n$. *Then* $[\pi]_{F_0} \circ f_0 \in H_{n'-1} \setminus H_{n'}$ *where*

$$n' = q^g n + \frac{q^g - 1}{q - 1} + 1.$$

The first proposition says that the Theorem 1.1 holds if l is small enough. The second proposition gives us a way to calculate the maximal lifting of πf_0 given the maximal lifting of f_0. Since the elements of A lift to all levels, an easy inductive argument shows that these two propositions together imply Theorem 1.1.

2. Formal cohomology

To prove Theorem 1.1 we will use the formal cohomology theory developed by Lubin-Tate [10] and Drinfeld [1]. Let k be a field of characteristic $p > 0$ which is also an A-algebra, with structure map $\gamma: A \to k$. Let F_0 be a formal A-module of height $h < \infty$ over k, and let M be a finite dimensional k-vector space. A *symmetric 2-cocycle* of F_0 with coefficients in M is a collection of power series $\Delta(x, y) \in M[[x, y]]$ and $\{\delta_a(x) \in M[[x]]\}_{\alpha \in A}$ satisfying

$$\Delta(x, y) = \Delta(y, x)$$

$$\Delta(x, y) + \Delta(F_0(x, y), z) = \Delta(y, z) + \Delta(x, F_0(y, z))$$

$$\delta_a(x) + \delta_a(y) + \Delta([a]_{F_0}(x), [a]_{F_0}(y)) = \gamma(a) \cdot \Delta(x, y) + \delta_a(F_0(x, y))$$

$$\delta_a(x) + \delta_b(x) + \Delta([a]_{F_0}(x), [b]_{F_0}(x)) = \delta_{a+b}(x)$$

$$\gamma(a) \cdot \delta_b(x) + \delta_a([b]_{F_0}(x)) = \delta_{ab}(x).$$

If $\psi \in M[[x]]$ then the *coboundary* of ψ is the 2-cocycle

$$\Delta^{\psi}(x, y) = \psi(F_0(x, y)) - \psi(x) - \psi(y)$$

$$\delta_a^{\psi}(x) = \psi([a]_{F_0}(x)) - \gamma(a) \cdot \psi(x).$$

The coboundaries form a k-vector subspace of the space of symmetric 2-cocycles. The quotient of the symmetric 2-cocycles by the coboundaries is a k-vector space denoted $\mathrm{H}^2(F_0, M)$. By [10, Prop. 2.6], $\mathrm{H}^2(F_0, k)$ has k-dimension $h - 1$.

The following lemma will simplify many of our calculations by allowing us to work with the single power series $\delta_\pi(x)$ rather than with the whole cocycle $(\Delta(x, y), \{\delta_a(x)\})$. We say that the coccyle $(\Delta, \{\delta_a\})$ is zero if all its component power series are zero.

LEMMA 2.1. *The cocycle* $(\Delta(x, y), \{\delta_a(x)\})$ *is zero if and only if* $\delta_\pi(x) = 0$.

Proof. If the cocycle is zero than clearly $\delta_\pi(x) = 0$. Assume conversely that $\delta_\pi(x) = 0$. The formula

$$\delta_a(x) + \delta_a(y) + \Delta([a]_{F_0}(x), [a]_{F_0}(y)) = \gamma(a) \cdot \Delta(x, y) + \delta_a(F_0(x, y))$$

with $a = \pi$ reduces to

$$\Delta([\pi]_{F_0}(x), [\pi]_{F_0}(y)) = 0,$$

since $\delta_\pi(x) = 0$ and $\gamma(\pi) = 0$. Then since $[\pi]_{F_0}(x) \neq 0$, this implies $\Delta(x, y) = 0$. The formula

$$\gamma(a) \cdot \delta_b(x) + \delta_a([b]_{F_0}(x)) = \delta_{ab}(x)$$

with $\alpha = \pi$ reduces to $\delta_{\pi b}(x) = 0$. The same formula with $b = \pi$ and α arbitrary gives

$$\delta_a([\pi]_{F_0}(x)) = 0,$$

because $\delta_\pi(x) = 0$ and $\delta_{a\pi}(x) = 0$. Again this implies that $\delta_a(x) = 0$, so the cocycle is zero. □

Let F_0/k be a formal A-module of finite height h, and let F/R be a deformation of F_0, where R is a noetherian local A-algebra with residue field k. Denote the maximal ideal of R by $\mathscr{M}_R$ and let

$$R_n = R/\mathscr{M}_R^{n+1}$$

$$F_n = F \otimes_R R_n.$$

To apply the cohomology theory to the problem of lifting endomorphisms we need to define a cocycle which tells us whether a given endomorphism of F_n lifts to an endomorphism of F_{n+1}. For $f_0(x) \in H = \mathrm{End}_k(F_0)$ we define

$$u(x, y) = \frac{\partial}{\partial x} F_0(x, y)$$

$$\alpha_{f_0}(x, y) = \frac{1}{u(0, F_0(f_0(x), f_0(y)))}$$

$$\beta_{f_0}(x) = \frac{1}{u(0, f_0(x))}.$$

Let $f_{n-1}(x) \in \mathrm{End}_{R_{n-1}}(F)$ be an endomorphism which lifts f_0, and let $f_n(x)$ be a lifting of $f_{n-1}(x)$ to a power series in $R_n[[x]]$. By [3, Eqn. 3.4] we get a symmetric 2-cocyle

$$\Delta(x, y) = \alpha_{f_0}(x, y) \cdot [f_n(F_n(x, y)) - F_n(f_n(x), f_n(y))]$$

$$\delta_a(x) = \beta_{af_0}(x) \cdot [f_n \circ [a]_{F_n}(x) - [a]_{F_n} \circ f_n(x)] \quad (a \in A)$$

with coefficients in the k-vector space $M_n = \mathscr{M}_R^n / \mathscr{M}_R^{n+1}$. (The second formula above is a slight correction of that given in [3].) It is clear from the definition that this cocyle is zero if and only if $f_n \in \mathrm{End}_{R_n}(F)$.

PROPOSITION 2.2. *Let $f_n(x) \in R_n[[x]]$ be a power series which lifts $f_0(x) \in \mathrm{End}_k(F_0)$. Then f_n is an endomorphism of F_n if and only if it commutes with $[\pi]_{F_n}$.*

Proof. This follows easily by induction from the construction above and Lemma 2.1. □

We now let $R = k[[t]]$, with canonical A-algebra structure as in Section 1. Let F/R be a deformation of F_0/k of height $g = h - 1$. Choose $f_{n-1} \in \mathrm{End}_{R_{n-1}}(F)$ of the form

$$f_{n-1}(x) = b_0 x^{q^r} + \cdots$$

with $b_0 \in R_{n-1} \setminus \{0\}$. Then $f_{n-1}(x) \in R_{n-1}[[x^{q^r}]]$. We lift f_{n-1} to $f_n \in R_n[[x^{q^r}]]$ and form the cocycle $(\Delta, \{\delta_a\})$ as before. Since

$$f_n(x) \in R_n[[x^{q^r}]]$$

$$[\pi]_{F_n}(x) \in R_n[[x^{q^g}]],$$

the leading term of δ_π has degree at least q^{r+g}.

LEMMA 2.3. *a) If $r > 0$ and the degree of the leading term of δ_π is greater than q^{r+g} then f_{n-1} lifts to $f_n' \in \mathrm{End}_{R_n}(F)$ with leading term of degree q^r.*
b) If $r > 0$ and the degree of the leading term of δ_π is equal to q^{r+g} then f_{n-1} lifts to $f_n' \in \mathrm{End}_{R_n}(F)$ with leading term of degree q^{r-1}.

Proof. If $r > 0$ it follows from the definitions that $\delta_\pi(x)$ is a power series in x^{q^h}. We write

$$\delta_\pi(x) = d(x^{q^h}).$$

Since $[\pi]_{F_0}(x) = s(x^{q^h})$ with s an invertible power series we may set $\psi = d \circ s^{-1}$. Then $f_n' = f_n - (\psi/\beta_{f_0})$ is a power series which lifts f_{n-1}. We observe that

$$
\begin{aligned}
f_n' \circ [\pi]_{F_n} &= f_n \circ [\pi]_{F_n} - \frac{d \circ s^{-1} \circ [\pi]_{F_0}}{\beta_{f_0} \circ [\pi]_{F_0}} \\
&= f_n \circ [\pi]_{F_n} - \frac{\delta_\pi}{\beta_{\pi f_0}} \\
&= [\pi]_{F_n} \circ f_n \\
&= [\pi]_{F_n} \circ f_n'.
\end{aligned}
$$

Then Proposition 2.2 implies that $f_n' \in \mathrm{End}_{R_n}(F)$. If the leading term of δ_π has degree q^{r+g} then the leading term of f_n' has degree q^{r-1}. If the leading term of δ_π has degree greater than q^{r+g} then the degree of the leading term of f_n' is greater than q^{r-1} but no more than q^r. Since this degree must be a power of q, it is equal to q^r. □

3. Proof of the theorem

In this section we assume k is separably closed, $R = k[[t]]$, $g = h - 1$, and $e = 1$. We begin with a technical lemma which will allow us to prove Proposition 1.4. Let $f_0 \in \mathrm{End}_k(F_0) = \mathrm{End}(F_0)$ and let $f_{n-1} \in \mathrm{End}_{R_{n-1}}(F)$ be a lifting of f_0. Then f_{n-1} can be written

$$f_{n-1}(x) = b_0 x^{q^r} + \ldots$$

with $b_0 \in R_{n-1} \setminus \{0\}$. Let $m = v_t(b_0) < n$.

LEMMA 3.1. *Assume that* $m + q^r < q^g m + 1$. *Then*
a) $m + q^r \geqslant n$
b) If $m + q^r > n$ *then* f_{n-1} *lifts to* $f_n' \in \mathrm{End}_{R_n}(F)$ *of the form*

$$f_n'(x) = b_0' x^{q^r} + \ldots$$

with $v_t(b_0') = m$.

c) If $m + q^r = n$ *and* $r > 0$ *then* f_{n-1} *lifts to* $f_n' \in \mathrm{End}_{R_n}(F)$ *of the form*

$$f_n'(x) = b_0' x^{q^{r-1}} + \ldots$$

with $v_t(b_0') = n = m + q^r$.

d) if $m + q^r = n$ *and* $r = 0$ *then* f_{n-1} *does not lift to an endomorphism of* F_n.

Remark. The liftings f_n' supplied by b) and c) satisfy the hypothesis of the lemma.

Proof. By our assumption

$$v_t(b_0 a_0^{q^r} - a_0 b_0^{q^g}) = v_t(b_0 a_0^{q^r})$$

$$= m + q^r.$$

Since $b_0 a_0^{q^r} - a_0 b_0^{q^g} \in (t^n)$ we must have $m + q^r \geqslant n$, which proves a).

Since $f_{n-1}(x) \in \mathrm{End}_{R_{n-1}}(F)$ has leading term of degree q^r, f_{n-1} is a power series in x^{q^r}. Choose a lifting $f_n(x) \in R_n[[x^{q^r}]]$ of f_{n-1}. Abusing our notation slightly, we write

$$f_n(x) = b_0 x^{q^r} + \cdots.$$

The lifting f_n of f_{n-1} gives us a cocycle $(\Delta, \{\delta_a\})$ as described above, with

$$\delta_\pi(x) = \beta_{\pi f}(x) \cdot [f_n \circ [\pi]_{F_n}(x) - [\pi]_{F_n} \circ f_n(x)]$$

$$= (b_0 a_0^{q^r} - a_0 b_0^{q^g}) x^{q^{r+g}} + \cdots.$$

If $m + q^r > n$ then

$$b_0 a_0^{q^r} - a_0 b_0^{q^g} \equiv 0 \pmod{(t^{n+1})},$$

so the leading term of δ_π has degree greater than q^{r+g}. Part b) now follows from Lemma 2.3a). If $m + q^r = n$ then the leading term of δ_π has degree q^{r+g}, so c) follows from Lemma 2.3b). Finally, d) follows from a) and the above remark. □

We now use this lemma to prove Proposition 1.4. We write $f_0 = a + f_0'$ with $a \in A$ and $f_0' \in \pi_B B$. Since endomorphisms in A lift to all levels, it suffices to prove Proposition 1.4 with $f_0 \in \pi_B B$. We are given that f_0 lifts to

$$f_{n-1}(x) = b_0 x^{q^r} + \cdots \quad (b_0 \in R_{n-1} \setminus \{0\})$$

in $\mathrm{End}_{R_{n-1}}(F)$. Since f_{n-1} doesn't lift to an endomorphism of F_n, by Lemma 2.3 we see that $r = 0$. Since $f_0 \in \pi_B B$ we have $m = v_t(b_0) > 0$. Therefore the hypothesis of Lemma 3.1 is satisfied. The lemma implies that

$$v_t(b_0) = n - 1.$$

Now lift $f_{n-1}(x)$ arbitrarily to $f(x) \in R[[x]]$. Since f is well-defined (mod (t^n)), $[\pi]_F \circ f$ is well-defined (mod $(t^{q^g n+1})$). In fact the power series

$$\phi_{q^g n} = ([\pi]_F \circ f) \otimes_R R_{q^g n}$$

is an element of $\mathrm{End}_{R_{q^g n}}(F)$. To show this it suffices by Proposition 2.2 to prove that

$$[\pi]_F \circ ([\pi]_F \circ f) \equiv ([\pi]_F \circ f) \circ [\pi] \quad (\mathrm{mod}\ (t^{q^g n+1})).$$

We have

$$[\pi]_F \circ f = f \circ [\pi]_F + \varepsilon$$

with $\varepsilon \equiv 0$ (mod (t^n)). Therefore

$$\begin{aligned} [\pi]_F \circ ([\pi]_F \circ f) &= [\pi]_F \circ (f \circ [\pi]_F + \varepsilon) \\ &\equiv [\pi]_F \circ (f \circ [\pi]_F) \quad (\mathrm{mod}\ (t^{q^g n+1})) \\ &\equiv ([\pi]_F \circ f) \circ [\pi]_F \quad (\mathrm{mod}\ (t^{q^g n+1})). \end{aligned}$$

We wish to determine the maximal lifting of $\phi_{q^g n} \in \mathrm{End}_{R_{q^g n}}(F)$. We have

$$\begin{aligned} \phi_{q^g n}(x) &\equiv [\pi]_F \circ f(x) \qquad (\mathrm{mod}\ (t^{q^g n+1})) \\ &\equiv a_0 b_0^{q^g} x^{q^g} + \cdots \quad (\mathrm{mod}\ (t^{q^g n+1})) \end{aligned}$$

with

$$v_t(a_0 b_0^{q^g}) = 1 + q^g(n-1).$$

When applied to $\phi_{q^g n}$ the hypothesis of Lemma 3.1 translates to

$$[1 + q^g(n - 1)] + q^g < q^g[1 + q^g(n - 1)] + 1.$$

The hypothesis is satisfied because $n > 1$.

We now apply Lemma 3.1 repeatedly to find the largest n' such that $\phi_{q^g n}$ lifts to $\mathrm{End}_{R_{n'-1}}(F)$. By b) and c) of the lemma we lift $\phi_{q^g n}$ to

$$\phi_{n'-1} \in \mathrm{End}_{R_{n'-1}}(F)$$

with

$$\phi_{n'-1}(x) = b_0' x + \cdots$$

and

$$\begin{aligned} n' - 1 &= v_t(b_0') \\ &= (1 + q^g(n - 1) + q^g + q^{g-1} + \cdots + q) \\ &= q^g n + \frac{q^g - 1}{q - 1}. \end{aligned}$$

Therefore

$$n' = q^g n + \frac{q^g - 1}{q - 1} + 1.$$

By d) of Lemma 3.1, $\phi_{n'-1}$ does not lift to $\mathrm{End}_{R_{n'}}(F)$. This completes the proof of Proposition 1.4. □

To prove Proposition 1.3 we need another lemma.

LEMMA 3.2. *Let* $f_{n-1} \in \mathrm{End}_{R_{n-1}}(F)$ *as before and assume that* $m + q^r > q^g m + 1 = n$. *Then* f_{n-1} *lifts to* $f_n' \in \mathrm{End}_{R_n}(F)$ *of the form*

$$f_n'(x) = b_0' x^{q^{r-1}} + \cdots$$

with $v_t(b_0') = q^g m + 1 = n$.

Proof. Just as in the proof of Lemma 3.1 we lift $f_{n-1}(x)$ to $f_n(x) \in R_n[[x^{q^r}]]$ with

$$f_n(x) = b_0 x^{q^r} + \cdots .$$

As before f_n gives us a cocycle $(\Delta, \{\delta_a\})$ with coefficients in M_n in which

$$\begin{aligned} \delta_\pi(x) &= \beta_{\pi f_0}(x) \cdot [f_n \circ [\pi]_{F_n}(x) - [\pi]_{F_n} \circ f_n(x)] \\ &= (b_0 a_0^{q^r} - a_0 b_0^{q^g}) x^{q^{r+g}} + \cdots . \end{aligned}$$

The valuation of the leading term of δ_π is given by

$$\begin{aligned} v_t(b_0 a_0^{q^r} - a_0 b_0^{q^g}) &= v_t(a_0 b_0^{q^g}) \\ &= q^g m + 1 \\ &= n. \end{aligned}$$

Therefore the first nonzero term of δ_π has degree q^{r+g}; by Lemma 2.3 b), f_{n-1} lifts to $f_n' \in \mathrm{End}_{R_n}(F)$ with leading term of degree q^{r-1}. □

Using this lemma we prove Proposition 1.3 in the cases where $h \nmid l$. If $l \geqslant 0$ then

$$(A + \pi_B^l B) \setminus (A + \pi_B^{l+1} B) \subset A + (\pi_B^l B \setminus \pi_B^{l+1} B),$$

so it suffices to consider only those f_0 with

$$f_0 \in \pi_B^l B \setminus \pi_B^{l+1} B.$$

In that case f_0 has the form

$$f_0(x) = b_0 x^{q^l} + \cdots$$

with $b_0 \in k^\times$. By Lemma 3.2, f_0 lifts to $f_1'(x) \in \mathrm{End}_{R_1}(F)$ of the form

$$f_1'(x) = b_0' x^{q^{l-1}} + \cdots$$

with $v_t(b_0') = 1$. The endomorphism f_1' satisfies the hypothesis of Lemma 3.1; parts b) and c) of the lemma imply that f_1' lifts to

$$f_{n-1}''(x) = b_0'' x + \cdots \in \mathrm{End}_{R_{n-1}}(F)$$

with

$$n - 1 = v_t(b_0'') = 1 + q^{l-1} + q^{l-2} + \cdots + q = \frac{q^l - 1}{q - 1}.$$

By d) of the same lemma we know that f_{n-1} does not lift to an endomorphism of F_n, which proves Proposition 1.3 for $0 < l < h$.

If $l = 0$ then

$$f_0 \in B \setminus (A + \pi_B B)$$

and f_0 has the form

$$f_0(x) = b_0 x + \cdots$$

with $b_0 \in \mathbf{F}_{q^h} \setminus \mathbf{F}_q$. We need to show that no lifting

$$f_1(x) = b_0 x + \cdots$$

of f_0 to $R_1[[x]]$ is an R_1-endomorphism of F. From f_1 we get a cocycle $(\Delta, \{\delta_a\})$ with coefficients in M_1 such that

$$\delta_\pi(x) = (b_0 a_0 - a_0 b_0^{q^g}) x^{q^g} + \cdots.$$

Since $b_0 \in \mathbf{F}_{q^h} \setminus \mathbf{F}_q$ we have $v_t(b_0 - b_0^{q^g}) = 0$; hence $b_0 a_0 - a_0 b_0^{q^g}$ is nonzero in R_1, and $\delta_\pi(x) \neq 0$. Thus $f_1 \notin \operatorname{End}_{R_1}(F)$, which proves the proposition when $l = 0$.

If $l = h$ then

$$f_0 \in (A + \pi_B^h B) \setminus (A + \pi_B^{h+1} B)$$

and we write $f_0 = a + \pi g_0$ for some $a \in A$ and

$$g_0(x) \in B \setminus \pi_B B$$

$$g_0(x) = b_0 x + \ldots,$$

with $b_0 \in \mathbf{F}_{q^h} \setminus \mathbf{F}_q$. We can assume $a = 0$ and $f_0 = \pi g_0$. As in the proof of Proposition 1.4 we lift g_0 arbitrarily to $g \in R[[x]]$. Since

$$[\pi]_F \circ g \equiv g \circ [\pi]_F \pmod{(t)}$$

we have

$$[\pi]_F \circ ([\pi]_F \circ g) \equiv ([\pi]_F \circ g) \circ [\pi]_F \pmod{(t^{q^g+1})}.$$

By Proposition 2.2 we conclude that

$$\begin{aligned} f_{q^g}(x) &\equiv [\pi]_F \circ g(x) \pmod{(t^{q^g+1})} \\ &\equiv a_0 b_0^{q^g} x^{q^g} + \cdots \pmod{(t^{q^g+1})} \end{aligned}$$

is an element of $\mathrm{End}_{R_{q^g}}(F)$.

As usual, we lift f_{q^g} to $f_{q^g+1} \in R_{q^g+1}[[x^{q^g}]]$ with

$$f_{q^g+1}(x) = c_0 x^{q^g} + \cdots$$

$$c_0 \equiv a_0 b_0^{q^g} \pmod{(t^{q^g+1})}.$$

We get a cocycle $(\Delta, \{\delta_a\})$ with coefficients in M_{q^g+1} such that

$$\delta_\pi(x) = (c_0 a_0^{q^g} - a_0 c_0^{q^g}) x^{q^{2g}} + \cdots .$$

The first coefficient of δ_π satisfies

$$c_0 a_0^{q^g} - a_0 c_0^{q^g} \equiv a_0^{q^g+1}(b_0^{q^g} - b_0^{q^{2g}}) \pmod{(t^{q^g+2})}.$$

Since $b_0 \in \mathbf{F}_{q^h} \setminus \mathbf{F}_q$ we have $b_0^{q^g} \neq b_0^{q^{2g}}$ in $\mathbf{F}_{q^h}$. Therefore

$$a_0^{q^g+1}(b_0^{q^g} - b_0^{q^{2g}})$$

is non-zero in M_{q^g+1}. Hence δ_π has leading term of degree $q^{2g} = q^{r+g}$, so by Lemma 2.3 b) f_{q^g} lifts to

$$f_{q^g+1} \in \mathrm{End}\,(F_{q^g+1})$$

with leading term of degree q^{2g-1}.

The lifting f_{q^g+1} satisfies the hypothesis of Lemma 3.1. We apply parts b) and c) of that lemma to show that f_{q^g+1} lifts to $f_{n-1} \in \mathrm{End}_{R_{n-1}}(F)$ of the form

$$f_{n-1}(x) = c_0' x + \cdots$$

with

$$n - 1 = v_t(c_0') = q^g + 1 + q^{g-1} + \cdots + q^2 + q = \frac{q^h - 1}{q - 1}.$$

By Lemma 3.1d), f_{n-1} does not lift to $\mathrm{End}_{R_n}(F)$. This completes the proof of Proposition 1.3. □

We now prove a more general version of Theorem 1.1 which makes no assumptions about e or k.

THEOREM 3.3. *Let F/R be a deformation of height $g = h - 1$ of the formal A-module F_0/k of height h. We write*

$$[\pi]_F(x) = a_0 x^{q^g} + \cdots$$

and set $e = v_t(a_0) > 0$. Choose $f_0 \in \mathrm{End}_k(F_0) \subset B$ which satisfies

$$f_0 \in (A + \pi_B^l B) \setminus (A + \pi_B^{l+1} B)$$

for some $l > 0$. Write $l = hm + b$ with $0 \leqslant b < h$. Then f_0 lifts to $\mathrm{End}_{R_{n-1}}(F)$ but not to $\mathrm{End}_{R_n}(F)$, where

$$n = e \cdot \left[a(gm) + q^{gm} \cdot \frac{q^b - 1}{q - 1} + 1 \right].$$

Proof. Assume for the present that k is separably closed. By [1, Prop. 4.2] there exists an A-subalgebra $R' = k[[u]]$ of R and a formal A-module F' defined over R' which satisfies

a) $[\pi]_{F'}(x) = ux^{q^g} + \cdots$, and

b) there exists a $*$-isomorphism $\phi: F \to F' \otimes_{R'} R$ defined over R.

Let $R_n' = R'/(u^{n+1})$. Theorem 1.1 says that $f_0' = \phi \circ f_0 \circ \phi^{-1}$ lifts to $f_{n-1}' \in \mathrm{End}_{R_{n-1}'}(F')$ but that f_{n-1}' doesn't lift to $\mathrm{End}_{R_n'}(F')$, where

$$l = hm + b$$

$$n = a(gm) + q^{gm} \cdot \frac{q^b - 1}{q - 1} + 1.$$

Let

$$f_{ne-1} = \phi^{-1} \circ f'_{n-1} \circ \phi$$
$$\in \operatorname{End}_{R_{ne-1}}(F).$$

Then f_{ne-1} is a lifting of f_0 which doesn't lift to $\operatorname{End}_{R_{ne}}(F)$. For if f_{ne} lifts f_{ne-1} then $f'_{ne} = \phi \circ f_{ne} \circ \phi^{-1}$ is an endomorphism of the reduction of F' (mod (tu^n)) which lifts f'_0. The endomorphism f'_{ne} lifts uniquely to a power series f'_n over $R'_n = R'/(u^{n+1})$. We have

$$[\pi]_{F'_n} \circ f'_n - f'_n \circ [\pi]_{F'_n} \in R'_n[[x]]$$

$$[\pi]_{F'_n} \circ f'_n - f'_n \circ [\pi]_{F'_n} \equiv 0 \pmod{(tu^n)}.$$

Therefore

$$[\pi]_{F'_n} \circ f'_n - f'_n \circ [\pi]_{F'_n} \equiv 0 \pmod{(u^{n+1})}.$$

Proposition 2.2 implies that $f'_n \in \operatorname{End}_{R'_n}(F')$, which is a contradiction. Therefore f_{ne-1} does not lift to $\operatorname{End}_{R_{ne}}(F)$.

We now consider the case where k is not separably closed. Let $F^s_0 = F_0 \otimes_k k_s$ and $F^s = F \otimes_R R^s$, with $R^s = k_s[[t]]$. We have proved the theorem for F^s/R^s. We need to show that if $f_0 \in \operatorname{End}_{k_s}(F^s_0)$ is invariant under $G = \operatorname{Gal}(k_s/k)$ then any lifting $f_n \in \operatorname{End}_{R^s_n}(F^s)$ of f_0 is also invariant under G. If $\sigma \in G$ the endomorphism $f_n - \sigma f_n$ of F^s_n induces the zero endomorphism on F^s_0. By [1, Prop. 4.1] this implies that $f_n - \sigma f_n = 0$. □

We can now compute $\operatorname{End}_{R_n}(F)$ without assuming $e = 1$ or $k = k_s$.

THEOREM 3.4. *Let F be a deformation of F_0 as above. Then*

$$\operatorname{End}_{R_n}(F) = \operatorname{End}_k(F_0) \cap (A + \pi_B^{j(n)} B)$$

where $j(n) = hm + b$ whenever

$$a(gm) - q^{gm} + 1 \leqslant \frac{n}{e} < a(gm) + 1 \quad (b = 0)$$

$$a(gm) + q^{gm} \cdot \frac{q^{b-1} - 1}{q - 1} + 1 \leqslant \frac{n}{e} < a(gm) + q^{gm} \cdot \frac{q^b - 1}{q - 1} + 1$$

$$(0 < b < h).$$

4. Application to elliptic curves

The main motivation for the study of one-parameter formal Lie groups is their relation to elliptic curves. We would like to derive an analogue of Theorem 3.3 for elliptic curves E over $R = k[[t]]$ whose reduction (mod (t)) is supersingular. Associated to an elliptic curve E/R is a formal Lie group F/R whose special fiber F_0 is the formal group of the special fiber E_0 of E. If E is an ordinary elliptic curve with supersingular reduction then F is a formal group of the type considered in Sections 1 and 3, with $A = \mathbf{Z}_p$, $h = 2$, and $g = 1$. Theorem 3.3 can be applied to F to determine when $f_0 \in \mathrm{End}_k(F_0)$ lifts to $\mathrm{End}_{R_n}(F)$. To apply this data to elliptic curves we need a special case of the Serre-Tate lifting [8, pp. 5–6].

THEOREM 4.1. *Let S be an Artin local ring with residue field k. Consider the category $\mathscr{C}_1$ of elliptic curves E/S with supersingular reduction E_0/k, and let F_E/S be the formal group of such a curve. Let $\mathscr{C}_2$ be the category of pairs $(\mathscr{E}, G)$, with $\mathscr{E}/k$ a supersingular elliptic curve and G/S a lifting of the formal group of $\mathscr{E}$. Then the functor*

$$\mathscr{C}_1 \to \mathscr{C}_2$$

$$E \mapsto (E_0, F_E)$$

is an equivalence of categories.

To apply this result we let $E_n = E \otimes_R R_n$ so that F_n/R_n is the formal group of E_n. Theorem 4.1 implies that

$$\mathrm{End}_{R_n}(E) = \mathrm{End}_k(E_0) \cap \mathrm{End}_{R_n}(F).$$

To compute $\mathrm{End}_{R_n}(F)$ we need to know the valuation e of the leading term of $[p]_F(x)$. This can be found for instance in [5, Th. 12.4.3], which says that

$$\begin{aligned} e &= v_t(j - j_0) \quad (j_0 \neq 0{,}1728) \\ &= \tfrac{1}{2} v_t(j - j_0) \quad (j_0 = 1728, p > 3) \\ &= \tfrac{1}{3} v_t(j - j_0) \quad (j_0 = 0, p > 3) \\ &= \tfrac{1}{6} v_t(j - j_0) \quad (j_0 = 0, p = 3) \\ &= \tfrac{1}{12} v_t(j - j_0) \quad (j_0 = 0, p = 2). \end{aligned}$$

Here $j_0 \in k$ denotes the reduction of j (mod (t)).

Using Theorem 3.3 and Theorem 4.1 we can now determine the maximal lifting of $\phi \in \mathrm{End}_k(E_0)$. The result can be conveniently formulated in terms of the characteristic polynomial of ϕ. Recall that $\mathrm{End}_k(F_0)$ is a $\mathbf{Z}_p$-subalgebra of the maximal order B in the quaternionic division algebra over $\mathbf{Q}_p$. For $\phi \in \mathrm{End}_k(E_0)$ we let $\tilde{\phi} \in \mathrm{End}_k(F_0)$ be the induced map on the formal group of E_0. We wish to find l such that

$$\tilde{\phi} \in (\mathbf{Z}_p + \pi_B^l B) \setminus (\mathbf{Z}_p + \pi_B^{l+1} B).$$

Therefore we want to calculate

$$\begin{aligned} l &= \sup_{a \in \mathbf{Z}_p} v_B(\tilde{\phi} - a) \\ &= \sup_{a \in \mathbf{Z}} v_B(\tilde{\phi} - a). \end{aligned}$$

If $a \in \mathbf{Z}$ then $\tilde{\phi} - a \in \mathrm{End}_k(F_0)$ is induced by $\phi - a \in \mathrm{End}_k(E_0)$. Hence we have

$$v_B(\tilde{\phi} - a) = v_p(\deg(\phi - a)).$$

Therefore we want to find

$$l = \sup_{a \in \mathbf{Z}} v_p(\deg(\phi - a)),$$

which can be computed in terms of the discriminant $(\mathrm{Tr}\,\phi)^2 - 4 \deg \phi$ of ϕ.

Recall that we have defined the nonnegative integers

$$a(gm) = \frac{(q^h - 1)(q^{gm} - 1)}{(q^g - 1)(q - 1)} \quad (m \geqslant 0).$$

In the elliptic curve case we have $g = 1$, $h = 2$, and $q = p$, so the formula above reduces to

$$a(m) = \frac{(p + 1)(p^m - 1)}{p - 1}.$$

THEOREM 4.2. *Assume $p > 2$ and let $\phi \in \mathrm{End}_k(E_0) \setminus \mathbf{Z}$. Then*

$$\sup_{a \in \mathbf{Z}} v_p(\deg(\phi - a)) = v_p((\mathrm{Tr}\,\phi)^2 - 4 \deg \phi).$$

Therefore ϕ *lifts to* $\mathrm{End}_{R_{n-1}}(E)$ *but does not lift to* $\mathrm{End}_{R_n}(E)$, *where*

$$n = (a(m) + 1)e \qquad \text{if } v_p((\mathrm{Tr}\ \phi)^2 - 4 \deg \phi) = 2m, \quad \text{and}$$

$$n = (a(m) + p^m + 1)e \quad \text{if } v_p((\mathrm{Tr}\ \phi)^2 - 4 \deg \phi) = 2m + 1.$$

Proof. Let $u = v_p((\mathrm{Tr}\ \phi)^2 - 4 \deg \phi)$. In view of Theorem 3.3 and the arguments above, it suffices to verify that

$$\sup_{a \in \mathbf{Z}} v_p(\deg(\phi - a)) = u.$$

We have

$$\begin{aligned} \deg (\phi - a) &= a^2 - (\mathrm{Tr}\ \phi)a + \deg \phi \\ &= (a - \tfrac{1}{2} \mathrm{Tr}\ \phi)^2 - \tfrac{1}{4}[(\mathrm{Tr}\ \phi)^2 - 4 \deg \phi], \end{aligned}$$

and since $p > 2$ it follows that

$$\sup_{a \in \mathbf{Z}} v_p(\deg (\phi - a)) \geqslant u,$$

with equality if u is odd. If u is even we observe that since $\phi \notin \mathbf{Z}$, the characteristic polynomial of ϕ is irreducible over $\mathbf{Q}_p$. Therefore

$$(\mathrm{Tr}\ \phi)^2 - 4 \deg \phi = p^u \cdot \alpha$$

with $a \in \mathbf{Z}$ not a square (mod p). It follows that

$$v_p(\deg (\phi - a)) \leqslant u$$

$$\sup_{a \in \mathbf{Z}} v_p(\deg(\phi - a)) = u,$$

which completes the proof. □

The case $p = 2$ is a bit more complicated.

THEOREM 4.3. *Assume* $p = 2$ *and let* $\phi \in \mathrm{End}_k(E_0) \setminus \mathbf{Z}$. *Then* ϕ *lifts to* $\mathrm{End}_{R_{n-1}}(E)$ *but does not lift to* $\mathrm{End}_{R_n}(E)$, where

$$n = (a(m) + 1)e \qquad \text{if } (\mathrm{Tr}\ \phi)^2 - 4 \deg \phi = 2^{2m}\alpha$$
$$\text{with } \alpha \equiv -3 \pmod 8;$$

$$n = (a(m-1) + 2^{m-1} + 1)e \quad \textit{if } (\mathrm{Tr}\,\phi)^2 - 4 \deg \phi = 2^{2m}\alpha$$
$$\textit{with } \alpha \equiv -1, 3 \pmod 8;$$

$$n = (a(m-1) + 2^{m-1} + 1)e \quad \textit{if } v_2((\mathrm{Tr}\,\phi)^2 - 4 \deg \phi) = 2m + 1.$$

Proof: If $u = v_2((\mathrm{Tr}\,\phi)^2 - 4 \deg \phi)$ is odd then $\mathrm{Tr}\,\phi$ is even and $u \geqslant 3$. We again have

$$\deg(\phi - a) = (a - \tfrac{1}{2}\mathrm{Tr}\,\phi)^2 - \tfrac{1}{4}[(\mathrm{Tr}\,\phi)^2 - 4 \deg \phi]$$

and we conclude that

$$\sup_{a \in \mathbf{Z}} \deg(\phi - a) = u - 2.$$

This formula combined with Theorem 3.3 proves the theorem for u odd.

If u is even then

$$(\mathrm{Tr}\,\phi)^2 - 4 \deg \phi = 2^u\alpha$$

with

$$\alpha \equiv -1, \pm 3 \pmod 8,$$

because the characteristic polynomial of ϕ is irreducible over $\mathbf{Q}_2$. If $u = 0$ this implies that both $\mathrm{Tr}\,\phi$ and $\deg \phi$ are odd and hence that

$$(\mathrm{Tr}\,\phi)^2 - 4 \deg \phi \equiv -3 \pmod 8$$

$$\sup_{a \in \mathbf{Z}} v_2(a^2 - (\mathrm{Tr}\,\phi)a + \deg \phi) = 0.$$

If $u > 0$ then $\mathrm{Tr}\,\phi$ is even and we write

$$\deg(\phi - a) = (a - \tfrac{1}{2}\mathrm{Tr}\,\phi)^2 - \tfrac{1}{4}[(\mathrm{Tr}\,\phi)^2 - 4 \deg \phi]$$
$$= (a - \tfrac{1}{2}\mathrm{Tr}\,\phi)^2 - 2^{u-2}\alpha.$$

If $\alpha \equiv -3 \pmod 8$ then

$$\sup_{a \in \mathbf{Z}} v_2(\deg(\phi - a)) = u.$$

If $\alpha \equiv -1,3 \pmod 8$ then

$$\sup_{a \in \mathbf{Z}} v_2(\deg(\phi - a)) = u - 1.$$

These formulas combined with Theorem 3.3 give us our result. □

As an example we let $R = \mathbf{F}_9[[t]]$ and consider the elliptic curve E/R which has Weierstrass equation

$$y^2 = x^3 + tx^2 + x.$$

The reduction of this curve (mod (t)) is a supersingular elliptic curve $E_0/\mathbf{F}_9$. Let $i \in \mathbf{F}_9$ be a square root of -1. The curve E_0 has an automorphism i of order 4 given by

$$i(x, y) = (-x, iy)$$

and an automorphism ω of order 3 given by

$$\omega(x, y) = (x + i, y).$$

Let J be the subalgebra of $\mathrm{End}(E_0)$ generated by i and ω. By computing the discriminant of J we find that J is a maximal order in $J \otimes_{\mathbf{Z}} \mathbf{Q}$. Therefore $J = \mathrm{End}(E_0)$, and we may write an arbitrary endomorphism ϕ of E_0 in the form

$$\phi = a + bi + c\omega + di\omega \quad (a, b, c, d \in \mathbf{Z}).$$

We wish to calculate the largest n such that ϕ lifts to an endomorphism of $E \pmod{(t^n)}$. Since

$$j = \frac{t^6}{t^2 - 1}$$

$$= -t^6 + t^8 - t^{10} + \cdots$$

and $p = 3$ we have

$$j_0 = 0$$

$$e = \tfrac{1}{6} v_t(j - j_0)$$

$$= 1.$$

In order to apply Theorem 4.2 we calculate

$$\begin{aligned} \operatorname{Tr} \phi &= 2a - c \\ \deg \phi &= a^2 + b^2 + c^2 + d^2 - ac - bd \\ (\operatorname{Tr} \phi)^2 - 4 \deg \phi &= -4b^2 - 3c^2 - 4d^2 + 4bd \\ &= -(2b - d)^2 - 3(c^2 + d^2). \end{aligned}$$

Since $v_3(c^2 + d^2) = \min\{2v_3(c), 2v_3(d)\}$ we find that

$$v_3((\operatorname{Tr} \phi)^2 - 4 \deg \phi) = \min\{2v_3(2b - d), 2v_3(c) + 1, 2v_3(d) + 1\}.$$

Denote this integer by l. The theorem implies that ϕ lifts to $\operatorname{End}_{R_{n-1}}(E)$ but not to $\operatorname{End}_{R_n}(E)$, where n is given by

$$n = 2 \cdot 3^{l/2} - 1 \quad (l \text{ even})$$

$$n = 3^{(l+1)/2} - 1 \quad (l \text{ odd}).$$

For example, $a + i$ does not lift (mod (t^2)), while $a + 3i$ lifts (mod (t^5)) but not (mod (t^6)). Also, 3ω lifts (mod (t^8)) but not (mod (t^9)).

5. Endomorphisms of quasi-canonical liftings

In this section we state an analogue of Theorem 1.1 for quasi-canonical liftings [3]. The proof is omitted. Using this result and the Serre-Tate lifting one can calculate the endomorphism rings of certain elliptic curves defined over Artin local rings.

Let K be a complete discretely valued field with finite residue field $\mathbf{F}_q$ and let A be the ring of integers in K, with uniformizer $\pi = \pi_A$. Let $\mathcal{O}$ be the ring of integers in a separable quadratic extension L of K, let M be the completion of the maximal unramified extension of L, and let W be the ring of integers in M. Let k be the residue field of $\mathcal{O}$ and let F_0/k be a formal A-module of height 2. By [1, Prop. 1.7], $B = \operatorname{End}_k(F_0)$ is isomorphic to the maximal order in the division algebra D of degree 4 over K. Therefore the ring $\mathcal{O}$ embeds in $B = \operatorname{End}(F_0)$. We choose an embedding

$$\alpha: \mathcal{O} \to \operatorname{End}_k(F_0)$$

such that the induced map

$$\mathcal{O} \to \mathrm{End}_k(\mathrm{Lie}\ F_0) \cong k$$

is the reduction map. This makes F_0 into a formal $\mathcal{O}$-module. By [9, Th. 1] there is a formal $\mathcal{O}$-module F/W which lifts F_0. By [1, Prop. 4.2], the $\mathcal{O}$-module lifting F of F_0 is unique up to $*$-isomorphism. We call F the canonical lifting of F_0 associated to the pair $(\mathcal{O}, \alpha)$.

The $\mathcal{O}$-module F can also be viewed as an A-module. Let $\bar{W}$ be the ring of integers in an algebraic closure $\bar{M}$ of M and let $\mathcal{M}$ be the maximal ideal of $\bar{W}$. Choose a formal A-module $F'/\bar{W}$ which is isogenous to F by the map

$$\phi: F \to F'.$$

Let $M' \subset \bar{M}$ be the finite extension of M generated by

$$\ker \phi \subset F(\mathcal{M}),$$

with π' a uniformizing element of M'. Both F' and ϕ can be defined over the ring of integers W' of M'. The endomorphism ring of F' is an A-order in

$$\mathrm{End}_W(F) \cong \mathcal{O}$$

which we write as

$$\mathcal{O}_s = A + \pi^s\mathcal{O}.$$

We say that F' is a quasi-canonical lifting of F_0 of level s. In [3, Prop. 5.3] it is shown that quasi-canonical liftings of all levels $s \geqslant 1$ exist, that M'/M is a totally ramified Galois extension of degree

$$q^s + q^{s-1} \quad (\mathcal{O}/A \text{ unramified})$$

$$q^s \qquad\qquad (\mathcal{O}/A \text{ ramified}),$$

and that the coefficient of x^q in $[\pi]_{F'}(x)$ has π'-valuation 1.

In [3, Prop. 3.3] Gross calculated the endomorphism ring of F over $W_n = W/(\pi_W^{n+1})$:

$$\mathrm{End}_{W/(\pi_W^{n+1})}(F) \cong \mathcal{O} + \pi_{\mathcal{O}}^n B.$$

We wish to make the corresponding calculation for the quasi-canonical lifting F'. That is, we want to determine the rings $\mathrm{End}_{W_n'}(F')$, where $W_n' = W'/(\pi')^{n+1}$. In order to do this we define e to be the ramification degree of M' over K. Using the formulas for the ramification degree of M' over M we see that

$$e = q^s + q^{s-1} \quad (\mathcal{O}/A \text{ unramified})$$

$$e = 2q^s \quad (\mathcal{O}/A \text{ ramified}).$$

Also recall that for $g = 1$ we have

$$a(m) = \frac{(q^m - 1)(q + 1)}{q - 1}.$$

THEOREM 5.1. *Let F_0/k be a formal A-module, let F'/W' be a quasi-canonical lifting of F_0 of level $s \geqslant 1$, and choose $f_0 \in \mathrm{End}_k(F_0) \cong B$ with*

$$f_0 \in (\mathcal{O}_s + \pi_B^l B)\setminus(\mathcal{O}_s + \pi_B^{l+1} B)$$

for some $l \geqslant 0$. Then f_0 lifts to $\mathrm{End}_{W_{n-1}'}(F')$ but not to $\mathrm{End}_{W_n'}(F')$, where

$$n = a\left(\frac{l}{2}\right) + 1 \qquad (l < 2s,\ l \text{ even})$$

$$n = a\left(\frac{l-1}{2}\right) + q^{(l-1)/2} + 1 \qquad (l < 2s,\ l \text{ odd})$$

$$n = a(s-1) + q^{s-1} + \left(\frac{l+1}{2} - s\right)e + 1 \qquad (l \geqslant 2s).$$

REMARK. If $\mathcal{O}/A$ is ramified then $e = 2q^s$ is even. If $\mathcal{O}/A$ is unramified and $l \geqslant 2s$ is even then

$$\mathcal{O}_s + \pi_B^l B = \mathcal{O}_s + \pi_B^{l+1} B.$$

Therefore n as defined above is a positive integer.

Theorem 5.1 allows us to compute $\mathrm{End}_{W_n'}(F')$.

THEOREM 5.2. *Let F' be a quasi-canonical lifting of level $s \geqslant 1$ as above. Then*

$$\mathrm{End}_{W_n'}(F') = \mathcal{O}_s + \pi_B^{j(n)} B$$

where $j(n)$ is given by

a) $j(n) = 2k$ *if* $k < s$ *and*

$$a(k-1) + q^{k-1} + 1 \leqslant n < a(k) + 1.$$

b) $j(n) = 2k + 1$ *if* $k < s$ *and*

$$a(k) + 1 \leqslant n < a(k) + q^k + 1.$$

c) $j(n) = k$ *if* $k \geqslant 2s$ *and*

$$a(s-1) + q^{s-1} + \left(\frac{k}{2} - s\right)e + 1 \leqslant n < a(s-1) + q^{s-1} + \left(\frac{k+1}{2} - s\right)e + 1.$$

The proof of Theorem 5.1 uses induction. The first step is given by the following proposition.

PROPOSITION 5.3. *Let $l \leqslant 2s + 1$ and*

$$f_0 \in (\mathcal{O}_s + \pi_B^l B) \setminus (\mathcal{O}_s + \pi_B^{l+1} B).$$

Then f_0 lifts to $\mathrm{End}_{W_{n-1}'}(F')$ *but not to* $\mathrm{End}_{W_n'}(F')$, *where*

$$\begin{aligned} n &= a\left(\frac{l}{2}\right) + 1 && (l \text{ even}, l < 2s) \\ &= a\left(\frac{l-1}{2}\right) + q^{(l-1)/2} + 1 && (l \text{ odd}, l < 2s) \\ &= a(s-1) + q^{s-1} + \left(\frac{l+1}{2} - s\right)e + 1 && (l = 2s, 2s+1). \end{aligned}$$

If $l \leqslant 2s$ this proposition follows easily from Theorem 1.1. If $l = 2s + 1$ the situation is quite delicate, especially when $\mathcal{O}/A$ is ramified. For a proof of this proposition, see [7, pp. 34–39].

The inductive step in the proof of Theorem 5.1 is given by the following proposition, whose proof can be found in [7, pp. 32–34].

PROPOSITION 5.4. *Let* $f_0 \in \mathrm{End}_k(F_0)$ *be such that* f_0 *lifts to* $\mathrm{End}_{W'_{n-1}}(F')$ *but not to* $\mathrm{End}_{W'_n}(F')$ *for some* $n \geqslant (e-1)/(q-1)$. *Then* $\pi f_0 \in \mathrm{End}_k(F_0)$ *lifts to* $\mathrm{End}_{W'_{n'-1}}(F')$ *but not to* $\mathrm{End}_{W'_{n'}}(F')$, *where* $n' = n + e$.

This proposition is a generalization of [3, Prop. 3.3], and is proved in a similar manner. Theorem 5.1 now follows by induction.

We give an example where F' is the formal group of an elliptic curve. Let W be the ring of integers in the completion of the maximal unramified extension of $\mathbf{Q}_2$, and consider the elliptic curve E/W with Weierstrass equation

$$y^2 + y = x^3.$$

Since E/W has good supersingular reduction $E_0/\bar{\mathbf{F}}_2$ the formal group F of E is a deformation of the formal group F_0 of E_0. Let $\omega \in W$ be a primitive cube root of unity. Then E has complex multiplication by the full ring of integers $\mathbf{Z}[\omega]$ of $\mathbf{Q}(\omega)$, via the map

$$\alpha\colon \mathbf{Z}[\omega] \to \mathrm{End}(E_0)$$

given by

$$\omega(x, y) = (\omega x, y).$$

It follows that the formal group F is a canonical lifting of F_0. Hence by [3, Prop. 3.3],

$$\mathrm{End}_{W_n}(F) \cong \mathcal{O} + 2^n B,$$

where

$$B = \mathrm{End}\,(F_0)$$

$$\mathcal{O} \cong \mathbf{Z}_2[\omega].$$

To get a quasi-canonical lifting of F_0 we need to construct an elliptic curve which is isogenous to E. Let $\pi' \in \bar{\mathbf{Q}}_2$ be a cube root of 2, and set $W' = W[\pi']$. Over W' we define another elliptic curve E, with Weierstrass equation

$$Y^2 + 3\pi' XY + Y = X^3.$$

This curve has good reduction E_0, so the formal group F' of E' is a deformation of F_0. In addition, there is an isogeny ϕ: $E \to E'$ given by

$$X = \frac{x^2 - \pi' x}{1 + (\pi')^2 x}$$

$$Y = \frac{(\pi' x^2 + (\pi')^2 x - 3y - 1)(y + 1)}{(1 + (\pi')^2 x)^2}.$$

The isogeny ϕ has degree 2, with kernel $\{\infty, (-\frac{1}{2}\pi', -\frac{1}{2})\}$. The isogeny $\tilde{\phi}$: $F \to F'$ induced by ϕ also has degree 2. We find that End $(E') \cong \mathbf{Z}[2\omega]$; the Serre-Tate lifting implies then that End $(F') \cong \mathbf{Z}_2[2\omega]$. Therefore F' is a quasi-canonical lifting of F_0 of level $s = 1$.

We now apply Theorem 5.2 and the remark after Theorem 5.1 to show that

$$\mathrm{End}_{W_0'}(F') \cong B$$

$$\mathrm{End}_{W_1'}(F') \cong \mathcal{O}_1 + \pi_B B$$

$$\mathrm{End}_{W_n'}(F') \cong \mathcal{O}_1 + \pi_B^2 B \quad 1 < n \leqslant 5$$

$$\mathrm{End}_{W_n'}(F') \cong \mathcal{O}_1 + \pi_B^4 B \quad 5 < n \leqslant 9$$

$$\vdots \qquad \vdots \qquad \vdots \qquad \vdots$$

$$\mathrm{End}_{W_n'}(F') \cong \mathcal{O}_1 + \pi_B^{2k} B \quad 4k - 3 < n \leqslant 4k + 1,$$

where $W_n' = W'/(\pi')^{n+1}$ and $\mathcal{O}_1 = \mathbf{Z}_2 + 2\omega\mathbf{Z}_2$. For instance, the frobenius endomorphism Fr of F_0 satisfies

$$\mathrm{Fr} \in \mathcal{O}_1 + \pi_B B$$

$$\mathrm{Fr} \notin \mathcal{O}_1 + \pi_B^2 B.$$

Therefore Fr lifts to $\mathrm{End}_{W_1'}(F')$ but not to $\mathrm{End}_{W_2'}(F')$. The endomorphism of F_0 induced by $\alpha(\omega)$ is not an element of $\mathcal{O}_1 + \pi_B B$, so it doesn't lift to $\mathrm{End}_{W_1'}(F')$.

References

1. V.G. Drinfeld: Elliptic modules (Russian). *Math. Sbornik* 94 (136) (1974), 594–627, 656; English translation: *Math. USSR-Sob.* 23 (1976), 561–592.
2. Y. Fujiwara: On Galois actions on p-power torsion points of some one-dimensional formal groups over $\mathbf{F}_p[[t]]$, *J. Algebra* 113 (1988) 491–510.
3. B. Gross: On canonical and quasi-canonical liftings, *Invent. Math.* 84 (1986) 321–326.
4. B. Gross: Ramification in p-adic Lie extensions, *Astérisque* 65 (1979) 81–102.
5. N. Katz and B. Mazur: *Arithmetic Moduli of Elliptic Curves*, Princeton University Press (1985).
6. K. Keating: Galois characters associated to formal A-modules, *Comp. Math.* 67 (1988) 241–269.
7. K. Keating: Lifting endomorphisms of formal groups, Harvard Ph. D. thesis, 1987.
8. J. Lubin, J.-P. Serre and J. Tate: Seminar at Woods Hole Institute on algebraic geometry (1964).
9. J. Lubin and J. Tate: Formal complex multiplication in local fields, *Ann. of Math.* (2) 81 (1965) 380–387.
10. J. Lubin and J. Tate: Formal moduli for one-parameter formal Lie groups, *Bull. Soc. Math. France* 94 (1966) 49–59.
11. Y. Fujiwara: On divisibilities of special values of real analytic Eisenstein series, to appear in *J. Fac. Sci. Univ. Tokyo.*