KEVIN KEATING

Lifting endomorphisms of formal $A$-modules


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

© Foundation Compositio Mathematica, 1988, tous droits réservés.


NUMDAM

*Article numérisé dans le cadre du programme Numérisation de documents anciens mathématiques*

http://www.numdam.org/
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 is $F_0$. The endomorphism ring of $F_0$ can be quite large – if $k$ is separably closed then $\text{End}_k(F_0)$ 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 $\text{End}_R/F_{\mathfrak{p}}(F)$, which are $A$-subalgebras of $\text{End}_k(F_0)$. In this paper we compute $\text{End}_R/F_{\mathfrak{p}}(F)$ 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 $\chi_E$ 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 $F_q$, and let $A$ be the ring of integers in $K$. Then either $A \cong F_q[[x]]$ and $K \cong F_q((x))$, or $K$ is a finite extension of $Q_p$. Let $R$ be an $A$-algebra with structure map $\gamma: A \to R$. A one-parameter formal $A$-module $F$ over $R$ is a one-parameter
formal group law $\tilde{F}$ over $R$, together with a homomorphism

$$\phi: A \to \text{End}_R(\tilde{F})$$

such that the induced map

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

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

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

for all $a \in A$. If $A = \mathbb{Z}_p$ 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 $A/\pi A \cong \mathbb{F}_q$ is the residue field of $A$. Let $F$ be a formal $A$-module over the $\mathbb{F}_q$-algebra $R$, and for $a \in A$ set

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

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 $\mathfrak{m}_R$ and residue field $k' \supset k$. Then the structure maps $\gamma_k: A \to k$ and $\gamma_R: A \to R$ make the diagram

$$A \xrightarrow{\gamma_R} R$$

$$\gamma_k \downarrow \quad \downarrow$$

$$k \hookrightarrow k'$$

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

$$F \equiv F_0 \pmod{\mathfrak{m}_R}.$$ 

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 $\phi \pmod{(t)}$ is the identity of $F_0$. 

---

**Note:** The original document does not contain a page number indicating the page it forms part of. The page number mentioned at the beginning of the text is likely an error or mislabeling. The text provided corresponds to the content that follows immediately after this page number, assuming it is part of the same document.
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 $\phi \pmod{t}$ 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

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

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

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

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 $F \pmod{(t^{n+1})}$. Our goal is to compute

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

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

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

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

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

By [1, Prop. 4.1] these maps are injective, and the rings $\text{End}_{R_n}(F)$ can be identified with $A$-subalgebras $H_n$ of $B$. In the general case, $H$ is isomorphic to an $A$-subalgebra of $B$ and $\text{End}_{R_n}(F)$ is identified with an $A$-subalgebra $H_n \subseteq H$. 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 $\pi_B$ is a uniformizer for $B$. Since the formal $A$-module $F_0$ has height $h$, any uniformizer $\pi_B$ has the form

$$[\pi_B]_F(x) = bx^d + \ldots$$

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

We begin by computing $\text{End}_{R_n}(F)$ 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 \( m \geq 0 \) define
\[ a(gm) = \frac{(q^h - 1)(q^{em} - 1)}{(q^g - 1)(q - 1)}, \]
so that \( a(0) = 0 \). The non-negative integers \( a(gm) \) are the upper ramification breaks of the Galois character \( \chi_F \) 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 \( f_0 \in \text{End}_k(F_0) \cong B \) be such that
\[ f_0 \in (A + \pi^I_B B) \setminus (A + \pi^{I+1}_B B) \ (l \geq 0). \]
Write \( l = hm + b \) with \( 0 \leq b < h \) and set
\[ n = a(gm) + q^{em} \cdot \frac{q^b - 1}{q - 1} + 1. \]
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 \( H_n = \text{End}_{R_n}(F) \).

**Theorem 1.2.** Let \( F \) be a deformation of \( F_0 \) as above. Then
\[ H_n = A + \pi^{j(n)}_B B \]
where \( j(n) = hm + b \) whenever
\[ a(gm) - q^{em} + 1 \leq n < a(gm) + 1 \quad (b = 0) \]
\[ a(gm) + q^{em} \cdot \frac{q^{b-1} - 1}{q - 1} + 1 \leq n < a(gm) + q^{em} \cdot \frac{q^b - 1}{q - 1} + 1 \quad (0 < b < h). \]

**Remarks:**
1. The presence of the upper ramification breaks \( a(gm) \) in our formulas for \( \text{End}_{R_n}(F) \) is not a coincidence. The relation between \( \chi_F \) and the rings \( \text{End}_{R_n}(F) \) is exploited in [2] and [6].
2. The most important special case of this theorem is $A = \mathbb{Z}_p$, $h = 2$, $g = 1$. 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,

\[ j(0) = 0 \]
\[ j(1) = 1 \]
\[ j(n) = 2 \quad \text{if} \ 2 \leq n < 2 + p \]
\[ j(n) = 3 \quad \text{if} \ 2 + p \leq n < 2(1 + p) \]
\[ j(n) = 4 \quad \text{if} \ 2(1 + p) \leq n < 2(1 + p) + p^2 \]
\[ \vdots \]
\[ j(n) = 2k \quad \text{if} \ 2(1 + p + \cdots + p^{k-1}) \leq n < 2(1 + p + \cdots + p^{k-1}) + p^k \]
\[ j(n) = 2k + 1 \quad \text{if} \ 2(1 + p + \cdots + p^{k-1}) + p^k \leq n < 2(1 + p + \cdots + p^k). \]

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

**Proposition 1.3.** Let $0 \leq l \leq h$, and assume that

\[ f_0 \in (A + \pi_B) \setminus (A + \pi_B^l B). \]

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

\[ n' = q^n + \frac{q^l - 1}{q - 1} + 1. \]

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 $\pi f_0$ 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 $\{\delta_a(x) \in M[[x]]\}_{a \in A}$ 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 $\psi$ is the 2-cocycle

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

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

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 $H^2(F_0, M)$. By [10, Prop. 2.6], $H^2(F_0, k)$ has $k$-dimension $h - 1$.

The following lemma will simplify many of our calculations by allowing us to work with the single power series $\delta_a(x)$ rather than with the whole cocycle $(\Delta(x, y), \{\delta_a(x)\})$. We say that the cocycle $(\Delta, \{\delta_a\})$ 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 $\delta_a(x) = 0$. 
Proof. If the cocycle is zero than clearly \( \delta_n(x) = 0 \). Assume conversely that \( \delta_n(x) = 0 \). 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
\[
\Delta([\pi]_{F_1}(x), [\pi]_{F_1}(y)) = 0,
\]
since \( \delta_n(x) = 0 \) 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 \( a = \pi \) reduces to \( \delta_{ab}(x) = 0 \). The same formula with \( b = \pi \) and \( a \) arbitrary gives
\[
\delta_a([\pi]_{F_0}(x)) = 0,
\]
because \( \delta_n(x) = 0 \) and \( \delta_{an}(x) = 0 \). Again this implies that \( \delta_n(x) = 0 \), so the cocycle is zero. \( \square \)

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 \( \mathcal{M}_R \) and let
\[
R_n = R/\mathcal{M}_R^{n+1}
\]
\[
F_n = F \otimes_R R_n.
\]

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 \( f_0(x) \in H = \text{End}_k(F_0) \) 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 $f_{n-1}(x) \in \text{End}_{k_{n-1}}(F)$ be an endomorphism which lifts $f_n$, 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

$$\Delta(x, y) = \alpha_0(x, y) \cdot [f_n(F_n(x, y)) - F_n(f_n(x), f_n(y))]$$

$$\delta_a(x) = \beta_0(a) \cdot [f_n \circ [a]_{f_n}(x) - [a]_{f_n} \circ f_n(x)] \quad (a \in A)$$

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

**Proposition 2.2.** Let $f_n(x) \in R_n[[x]]$ be a power series which lifts $f_n(x) \in \text{End}_k(F_0)$. 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. $\square$

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 $f_{n-1} \in \text{End}_{k_{n-1}}(F)$ of the form

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

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

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

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

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

**Lemma 2.3.** a) If $r > 0$ and the degree of the leading term of $\delta_n$ is greater than $q^{r+g}$ then $f_{n-1}$ lifts to $f'_n \in \text{End}_{k_n}(F)$ with leading term of degree $q^r$.

b) If $r > 0$ and the degree of the leading term of $\delta_n$ is equal to $q^{r+g}$ then $f_{n-1}$ lifts to $f'_n \in \text{End}_{k_n}(F)$ with leading term of degree $q^{r-1}$.

**Proof.** If $r > 0$ it follows from the definitions that $\delta_n(x)$ is a power series in $x^q$. We write

$$\delta_n(x) = d(x^q).$$
Since \([\pi]_{F_0}(x) = s(x^{d'})\) 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

\[
f'_n \circ [\pi]_{F_n} = f_n \circ [\pi]_{F_n} - \frac{d \circ s^{-1} \circ [\pi]_{F_0}}{\beta_{f_0} \circ [\pi]_{F_0}}
\]

\[
= f_n \circ [\pi]_{F_n} - \frac{\delta_n}{\beta_{f_0}}
\]

\[
= [\pi]_{F_n} \circ f_n
\]

Then Proposition 2.2 implies that \(f'_n \in \text{End}_{R_n}(F)\). If the leading term of \(\delta_n\) has degree \(q^{r+g}\) then the leading term of \(f'_n\) has degree \(q^{r-1}\). If the leading term of \(\delta_n\) 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 \(q^r\). \qed

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 \(f_0 \in \text{End}_k(F_0) = \text{End}(F_0)\) and let \(f_{n-1} \in \text{End}_{R_{n-1}}(F)\) be a lifting of \(f_0\). Then \(f_{n-1}\) can be written

\[
f_{n-1}(x) = b_0 x^{d'} + \ldots
\]

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

**Lemma 3.1.** Assume that \(m + q^r < q^g m + 1\). Then

a) \(m + q^r \geq n\)

b) If \(m + q^r > n\) then \(f_{n-1}\) lifts to \(f'_n \in \text{End}_{R_n}(F)\) of the form

\[
f'_n(x) = b_0 x^{d'} + \ldots
\]

with \(v_e(b_0) = m\).
c) If \( m + q' = n \) and \( r > 0 \) then \( f_{n-1} \) lifts to \( f'_n \in \text{End}_{\mathfrak{a}}(F) \) of the form

\[
f'_n(x) = b'_0x^{r-1} + \ldots
\]

with \( v'_i(b'_0) = n = m + q' \).

d) If \( m + q' = n \) 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

\[
v'_i(b'_0a'_0 - a'_0b'_0) = v'_i(b'_0a'_0)
\]

\[
= m + q'.
\]

Since \( b'_0a'_0 - a'_0b'_0 \in (t^n) \) we must have \( m + q' \geq n \), which proves a).

Since \( f_{n-1}(x) \in \text{End}_{\mathfrak{a}}(F) \) has leading term of degree \( q' \), \( f_{n-1} \) is a power series in \( x^{q'} \). Choose a lifting \( f_n(x) \in \mathbb{R}_n[[x^{q'}]] \) of \( f_{n-1} \). Abusing our notation slightly, we write

\[
f_n(x) = b_0x^{q'} + \ldots
\]

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

\[
\delta_n(x) = \beta_{q'}(x) \cdot [f_n \circ [\pi]_{\mathfrak{a}}(x) - [\pi]_{\mathfrak{a}} \circ f_n(x)]
\]

\[
= (b'_0a'_0 - a'_0b'_0)x^{q'-\varepsilon} + \ldots
\]

If \( m + q' > n \) then

\[
b'_0a'_0 - a'_0b'_0 \equiv 0 \pmod{(t^{n+1})},
\]

so the leading term of \( \delta_n \) has degree greater than \( q'-\varepsilon \). Part b) now follows from Lemma 2.3a). If \( m + q' = n \) then the leading term of \( \delta_n \) has degree \( q'-\varepsilon \), 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

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

in \( \text{End}_{R_{n-1}}(F) \). 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 \( m = v_1(b_0) > 0 \). Therefore the hypothesis of Lemma 3.1 is satisfied. The lemma implies that

\[
v_1(b_0) = n - 1.
\]

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

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

is an element of \( \text{End}_{R_{q^n}}(F) \). 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 \text{(mod \( (r^{q^n+1}) \))}.
\]

We have

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

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

\[
[\pi]_F \circ ([\pi]_F \circ f) = [\pi]_F \circ (f \circ [\pi]_F + \varepsilon)
\]

\[
\equiv [\pi]_F \circ (f \circ [\pi]_F) \quad \text{(mod \( (r^{q^n+1}) \))}
\]

\[
\equiv ([\pi]_F \circ f) \circ [\pi]_F \quad \text{(mod \( (r^{q^n+1}) \))}.
\]

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

\[
\phi_{q^n}(x) \equiv [\pi]_F \circ f(x) \quad \text{(mod \( (r^{q^n+1}) \))}
\]

\[
\equiv a_0 b_0^{q^n} x^{q^n} + \cdots \quad \text{(mod \( (r^{q^n+1}) \))}
\]

with

\[
v_1(a_0 b_0^{q^n}) = 1 + q^n(n - 1).
\]
When applied to $\phi_{q^n}$ the hypothesis of Lemma 3.1 translates to

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

The hypothesis is satisfied because $n > 1$.

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

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

with

$$\phi_{n' - 1}(x) = b'_0 x + \cdots$$

and

$$n' - 1 = v_i(b'_0) = (1 + q^e (n-1) + q^e + q^{e-1} + \cdots + q) = q^e n + \frac{q^e - 1}{q - 1}.$$ 

Therefore

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

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

To prove Proposition 1.3 we need another lemma.

**Lemma 3.2.** Let $f_{n-1} \in \text{End}_{R_{n-1}}(F)$ as before and assume that $m + q' > q^e m + 1 = n$. Then $f_{n-1}$ lifts to $f'_n \in \text{End}_{R_n}(F)$ of the form

$$f'_n(x) = b'_0 x^{q^e - 1} + \cdots$$

with $v_i(b'_0) = q^e m + 1 = n$. 

Proof. Just as in the proof of Lemma 3.1 we lift \( f_{n-1}(x) \) to \( f_n(x) \in \mathbb{R}_n[[x^q]] \) with
\[
 f_n(x) = b_0 x^q + \cdots.
\]
As before \( f_n \) gives us a cocycle \((\Delta, \{\delta_a\})\) with coefficients in \( M_n \) in which
\[
 \delta_a(x) = \beta_{\sigma_0}(x) \cdot [f_n \circ [\pi]_{\mathbb{F}_q}(x) - [\pi]_{\mathbb{F}_q} \circ f_n(x)]
 = (b_0 a_0^q - a_0 b_0^q) x^{q^2} + \cdots.
\]
The valuation of the leading term of \( \delta_a \) is given by
\[
 v_1(b_0 a_0^q - a_0 b_0^q) = v_1(a_0 b_0^q) = q^m + 1 = n.
\]
Therefore the first nonzero term of \( \delta_a \) has degree \( q^m \); by Lemma 2.3 b), \( f_{n-1} \) lifts to \( f_n' \in \text{End}_{\mathbb{K}_n}(F) \) with leading term of degree \( q^{r-1} \).

Using this lemma we prove Proposition 1.3 in the cases where \( h \not\parallel l \). If \( l \geq 0 \) then
\[
 (A + \pi_{B}^l B) \setminus (A + \pi_{B}^{l+1} B) \subseteq A + (\pi_{B}^l B \setminus \pi_{B}^{l+1} B),
\]
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
\[
 f_0(x) = b_0 x^q + \cdots
\]
with \( b_0 \in k^\times \). By Lemma 3.2, \( f_0 \) lifts to \( f'_1(x) \in \text{End}_{\mathbb{K}_1}(F) \) of the form
\[
 f'_1(x) = b_0^l x^{q^l-1} + \cdots
\]
with \( v_1(b_0^l) = 1 \). The endomorphism \( f'_1 \) satisfies the hypothesis of Lemma 3.1; parts b) and c) of the lemma imply that \( f'_1 \) lifts to
\[
 f_{n-1}(x) = b_0^l x + \cdots \in \text{End}_{\mathbb{K}_{n-1}}(F)
\]
with
\[ n - 1 = \nu_i(b_0^n) \]
\[ = 1 + q^{l-1} + q^{l-2} + \cdots + q \]
\[ = \frac{q^l - 1}{q - 1}. \]

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
\[ f_0 \in B \setminus (A + \pi B) \]
and \( f_0 \) has the form
\[ f_0(x) = b_0x + \cdots \]
with \( b_0 \in F_{q^l} \setminus F_q \). We need to show that no lifting
\[ f_1(x) = b_0x + \cdots \]
of \( f_0 \) to \( R_1[[x]] \) is an \( R_1 \)-endomorphism of \( F \). From \( f_1 \) we get a cocycle \((\Delta, \{\delta_x\})\) with coefficients in \( M_1 \) such that
\[ \delta_x(x) = (b_0a_0 - a_0b_0^q)x^q + \cdots. \]

Since \( b_0 \in F_{q^l} \setminus F_q \) we have \( \nu_i(b_0 - b_0^q) = 0 \); hence \( b_0a_0 - a_0b_0^q \) is nonzero in \( R_1 \), and \( \delta_x(x) \neq 0 \). Thus \( f_1 \notin \text{End}_{R_1}(F) \), which proves the proposition when \( l = 0 \).

If \( l = h \) then
\[ f_0 \in (A + \pi B) \setminus (A + \pi B) \]
and we write \( f_0 = a + \pi g_0 \) for some \( a \in A \) and
\[ g_0(x) \in B \setminus \pi B \]
\[ g_0(x) = b_0x + \ldots, \]
with \( b_0 \in F_{q^h} \setminus F_q \). 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

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

By Proposition 2.2 we conclude that

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

\[ = \alpha_0 b_0^{q^g} x^{q^g} + \cdots \pmod{(t^{q+1})} \]

is an element of 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

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

\[ c_0 \equiv \alpha_0 b_0^{q^g} \pmod{(t^{q+1})}. \]

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

\[ \delta_{\pi}(x) = (c_0 d_0^{q^g} - \alpha_0 c_0^{q^g}) x^{q^{2g}} + \cdots. \]

The first coefficient of \( \delta_x \) satisfies

\[ c_0 d_0^{q^g} - \alpha_0 c_0^{q^g} \equiv a_0^{q^g+1} (b_0^{q^g} - b_0^{q^{2g}}) \pmod{(t^{q+2})}. \]

Since \( b_0 \in F_q \setminus F_q \) we have \( b_0^{q^g} \neq b_0^{q^{2g}} \) in \( F_q \). Therefore

\[ a_0^{q^g+1} (b_0^{q^g} - b_0^{q^{2g}}) \]

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

\[ f_{q^g+1} \in \text{End}(F_{q^g+1}) \]

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 \( f_{n-1} \in \text{End}_{R_{n-1}}(F) \) of the form

\[ f_{n-1}(x) = c_0' x + \cdots \]
with
\[ n - 1 = v_i(e_0') \]
\[ = q^e + 1 + q^{e-1} + \cdots + q^2 + q \]
\[ = \frac{q^h - 1}{q - 1}. \]

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

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 \( \text{Folk} \) of height \( h \). We write
\[ [\pi]_F(x) = a_0 x^e + \cdots \]
and set \( e = v_i(a_0) > 0 \). Choose \( f_0 \in \text{End}_k(F_0) \subset B \) 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 \( 0 \leq b < h \). Then \( f_0 \) lifts to \( \text{End}_{R_{n-1}}(F) \) but not to \( \text{End}_{R_n}(F) \), where
\[ n = e \cdot \left[ a(gm) + q^{em} \cdot \frac{q^b - 1}{q - 1} + 1 \right]. \]

**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) \( [\pi]_F(x) = ux^e + \cdots \), 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 \( f'_{n-1} \in \text{End}_{R_{n-1}}(F') \) but that \( f'_{n-1} \) doesn’t lift to \( \text{End}_{R_n}(F') \), where
\[ l = hm + b \]
\[ n = a(gm) + q^{em} \cdot \frac{q^b - 1}{q - 1} + 1. \]
Let

\[ f_{ne-1} = \phi^{-1} \circ f'_{ne-1} \circ \phi \]

\[ \in \text{End}_{R_{ne-1}}(F). \]

Then \( f_{ne-1} \) is a lifting of \( f_0 \) which doesn't lift to \( \text{End}_{R_{ne}}(F) \). 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 \( F'(\mod (t_{un})) \) which lifts \( f'_{0} \). The endomorphism \( f'_{ne} \) lifts uniquely to a power series \( f'_n \) over \( R'_n = R'/\langle u'^{n+1} \rangle \). We have

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

\[ [\pi]_{F_n} \circ f'_n - f'_n \circ [\pi]_{F_n} \equiv 0 \pmod {\langle tu'^{n} \rangle}. \]

Therefore

\[ [\pi]_{F_n} \circ f'_n - f'_n \circ [\pi]_{F_n} \equiv 0 \pmod {\langle u'^{n+1} \rangle}. \]

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

We now consider the case where \( k \) is not separably closed. Let \( F^0 = F_0 \otimes_k k_s \) 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 \( f_0 \in \text{End}_{k_s}(F^0) \) is invariant under \( G = \text{Gal}(k_s/k) \) then any lifting \( f_n \in \text{End}_{R_n}(F^0) \) of \( f_0 \) is also invariant under \( G \). If \( \sigma \in G \) the endomorphism \( f_n - \sigma f_n \) of \( F^0_n \) induces the zero endomorphism on \( F^0 \). By [1, Prop. 4.1] this implies that \( f_n - \sigma f_n = 0 \). \( \square \)

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

**Theorem 3.4.** Let \( F \) be a deformation of \( F_0 \) as above. Then

\[ \text{End}_{R_n}(F) = \text{End}_k(F_0) \cap (A + \pi^{(n)}_B) \]

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

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

\[ a(gm) + q^{gm} \cdot \frac{q^{b-1} - 1}{q - 1} + 1 \leq \frac{n}{e} < a(gm) + q^{gm} \cdot \frac{q^{b} - 1}{q - 1} + 1 \]

\((0 < b < h)\).
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 \( A = \mathbb{Z}_p \), \( h = 2 \), and \( g = 1 \). Theorem 3.3 can be applied to \( F \) to determine when \( f_0 \in \text{End}_k(F_0) \) lifts to \( \text{End}_{R_n}(F) \). 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 \( \mathcal{C}_1 \) of elliptic curves \( E/S \) with supersingular reduction \( E_0/k \), and let \( F_0/S \) be the formal group of such a curve. Let \( \mathcal{C}_2 \) be the category of pairs \( (\mathcal{E}, G) \), with \( \mathcal{E}/k \) a supersingular elliptic curve and \( \mathcal{E}/S \) a lifting of the formal group of \( \mathcal{E} \). Then the functor

\[ \mathcal{C}_1 \to \mathcal{C}_2 \]

\[ E \mapsto (E_0, F_0) \]

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

\[ \text{End}_{R_n}(E) = \text{End}_k(E_0) \cap \text{End}_{R_n}(F). \]

To compute \( \text{End}_{R_n}(F) \) 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

\[ e = v_t(j - j_0) \quad (j_0 \neq 0, 1728) \]

\[ = \frac{1}{2}v_t(j - j_0) \quad (j_0 = 1728, p > 3) \]

\[ = \frac{1}{3}v_t(j - j_0) \quad (j_0 = 0, p > 3) \]

\[ = \frac{1}{6}v_t(j - j_0) \quad (j_0 = 0, p = 3) \]

\[ = \frac{1}{12}v_t(j - j_0) \quad (j_0 = 0, p = 2). \]

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 $\phi \in \text{End}_k(E_0)$. The result can be conveniently formulated in terms of the characteristic polynomial of $\phi$. Recall that $\text{End}_k(F_0)$ is a $\mathbb{Z}_p$-subalgebra of the maximal order $B$ in the quaternionic division algebra over $\mathbb{Q}_p$. For $\phi \in \text{End}_k(E_0)$ we let $\bar{\phi} \in \text{End}_k(F_0)$ be the induced map on the formal group of $E_0$. We wish to find $l$ such that

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

Therefore we want to calculate

$$l = \sup_{a \in \mathbb{Z}_p} v_p(\bar{\phi} - a) = \sup_{a \in \mathbb{Z}} v_p(\phi - a).$$

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

$$v_p(\phi - a) = v_p(\deg(\phi - a)).$$

Therefore we want to find

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

which can be computed in terms of the discriminant $(\text{Tr} \phi)^2 - 4 \deg \phi$ of $\phi$. Recall that we have defined the nonnegative integers

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

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 $\phi \in \text{End}_k(E_0) \setminus \mathbb{Z}$. Then

$$\sup_{a \in \mathbb{Z}} v_p(\deg(\phi - a)) = v_p((\text{Tr} \phi)^2 - 4 \deg \phi).$$
Therefore \( \phi \) lifts to \( \text{End}_{R_{n-1}}(E) \) but does not lift to \( \text{End}_{R_n}(E) \), where

\[
\begin{align*}
  n &= (a(m) + 1)e & \text{if } & v_p((\text{Tr } \phi)^2 - 4 \deg \phi) = 2m, \\
  n &= (a(m) + p^n + 1)e & \text{if } & v_p((\text{Tr } \phi)^2 - 4 \deg \phi) = 2m + 1.
\end{align*}
\]

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

\[
\sup_{a \in \mathbb{Z}} v_p(\deg(\phi - a)) = u.
\]

We have

\[
\deg (\phi - a) = a^2 - (\text{Tr } \phi)a + \deg \phi = (a - \frac{1}{2} \text{Tr } \phi)^2 - \frac{1}{4}(\text{Tr } \phi)^2 - 4 \deg \phi,
\]

and since \( p > 2 \) it follows that

\[
\sup_{a \in \mathbb{Z}} v_p(\deg (\phi - a)) \geq u,
\]

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

\[
(\text{Tr } \phi)^2 - 4 \deg \phi = p^n \cdot a
\]

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

\[
\begin{align*}
  v_p(\deg (\phi - a)) & \leq u, \\
  \sup_{a \in \mathbb{Z}} v_p(\deg(\phi - a)) & = u,
\end{align*}
\]

which completes the proof.

The case \( p = 2 \) is a bit more complicated.

**Theorem 4.3.** Assume \( p = 2 \) and let \( \phi \in \text{End}_k(E_0) \backslash \mathbb{Z}. \) Then \( \phi \) lifts to \( \text{End}_{R_{n-1}}(E) \) but does not lift to \( \text{End}_{R_n}(E) \), where

\[
\begin{align*}
  n &= (a(m) + 1)e & \text{if } & (\text{Tr } \phi)^2 - 4 \deg \phi = 2^m \cdot a \\
  & & & \text{with } a \equiv -3 \pmod{8};
\end{align*}
\]
Proof: If \( u = \sqrt{2} \left( \text{Tr} \, \phi^2 - 4 \, \text{deg} \, \phi \right) \) is odd then \( \text{Tr} \, \phi \) is even and \( u \geq 3 \).

We again have

\[
\text{deg} \, (\phi - a) = (a - \frac{1}{2} \text{Tr} \, \phi)^2 - \frac{1}{4}[(\text{Tr} \, \phi)^2 - 4 \, \text{deg} \, \phi]
\]

and we conclude that

\[
\sup_{a \in \mathbb{Z}} \text{deg} \, (\phi - a) = u - 2.
\]

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

If \( u \) is even then

\[
(\text{Tr} \, \phi)^2 - 4 \, \text{deg} \, \phi = 2^u \alpha
\]

with

\[
\alpha \equiv -1, \pm 3 \pmod{8},
\]

because the characteristic polynomial of \( \phi \) is irreducible over \( \mathbb{Q}_2 \). If \( u = 0 \) this implies that both \( \text{Tr} \, \phi \) and \( \text{deg} \, \phi \) are odd and hence that

\[
(\text{Tr} \, \phi)^2 - 4 \, \text{deg} \, \phi \equiv -3 \pmod{8}
\]

\[
\sup_{a \in \mathbb{Z}} v_2(a^2 - (\text{Tr} \, \phi)a + \text{deg} \, \phi) = 0.
\]

If \( u > 0 \) then \( \text{Tr} \, \phi \) is even and we write

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

If \( \alpha \equiv -3 \pmod{8} \) then

\[
\sup_{a \in \mathbb{Z}} v_2(\text{deg} \, (\phi - a)) = u.
\]
If $\alpha \equiv -1,3 \pmod{8}$ then

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

These formulas combined with Theorem 3.3 give us our result. \qed

As an example we let $R = \mathbb{F}_9[[t]]$ 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 $E_0/\mathbb{F}_9$. Let $i \in \mathbb{F}_9$ 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 $\omega$ of order 3 given by

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

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

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

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

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

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

and $p = 3$ we have

$$j_0 = 0$$

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

$$= 1.$$
In order to apply Theorem 4.2 we calculate

\[ \text{Tr } \phi = 2a - c \]

\[ \text{deg } \phi = a^2 + b^2 + c^2 + d^2 - ac - bd \]

\[ (\text{Tr } \phi)^2 - 4 \text{ deg } \phi = -4b^2 - 3c^2 - 4d^2 + 4bd \]

\[ = -(2b - d)^2 - 3(c^2 + d^2). \]

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

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

Denote this integer by \( l \). The theorem implies that \( \phi \) lifts to \( \text{End}_{k_{n-1}}(E) \) but not to \( \text{End}_{k_n}(E) \), 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, \( 3\omega \) 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 \( F_q \) 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], \( B = \text{End}_k(F_0) \) is isomorphic to the maximal order in the division algebra \( D \) of degree 4 over \( K \). Therefore the ring \( \mathcal{O} \) embeds in \( B = \text{End}(F_0) \). We choose an embedding

\[ x : \mathcal{O} \rightarrow \text{End}_k(F_0) \]
such that the induced map

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

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

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

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

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

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

$$\text{End}_{W'}(F) \cong \mathcal{O}$$

which we write as

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

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 $s \geq 1$ exist, that $M'/M$ is a totally ramified Galois extension of degree

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

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

and that the coefficient of $x^s$ in $[\pi]_F(x)$ has $\pi'$-valuation 1.

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

$$\text{End}_{W/(\pi_n^{s+1})}(F) \cong \mathcal{O} + \pi^s B.$$
We wish to make the corresponding calculation for the quasi-canonical lifting $F'$. That is, we want to determine the rings $\text{End}_{W'}(F')$, 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

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

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

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 $s \geq 1$, and choose $f_0 \in \text{End}_k(F_0) \cong B$ with

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

for some $l \geq 0$. Then $f_0$ lifts to $\text{End}_{W'_{n-1}}(F')$ but not to $\text{End}_{W'_n}(F')$, where

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

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

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

**Remark.** If $\mathcal{O}/A$ is ramified then $e = 2q^r$ is even. If $\mathcal{O}/A$ is unramified and $l \geq 2s$ 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 $\text{End}_{W'_n}(F')$. 

Lifting endomorphisms of formal $A$-modules 235
THEOREM 5.2. Let $F'$ be a quasi-canonical lifting of level $s \geq 1$ as above. Then

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

where $j(n)$ is given by

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

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

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

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

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

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

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

PROPOSITION 5.3. Let $l \leq 2s + 1$ 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 $\text{End}_{W_{n-1}}(F')$ but not to $\text{End}_{W_n}(F')$, where

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

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

$$= a(s - 1) + q^{s-1} + \left(\frac{l + 1}{2} - s\right)e + 1 \quad \text{(l = 2s, 2s + 1).}$$
If \( l \leq 2s \) 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 \( f_0 \in \operatorname{End}_k(F_0) \) be such that \( f_0 \) lifts to \( \operatorname{End}_{W[n]}(F') \) but not to \( \operatorname{End}_{W[q]}(F') \) for some \( n \geq (e - 1)/(q - 1) \). Then \( \pi f_0 \in \operatorname{End}_k(F_0) \) lifts to \( \operatorname{End}_{W[n']}\left( F' \right) \) but not to \( \operatorname{End}_{W[q]}\left( F' \right) \), 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 \( \mathbb{Q}_2 \), and consider the elliptic curve \( E/W \) with Weierstrass equation

\[
y^2 + y = x^3.
\]

Since \( E/W \) has good supersingular reduction \( E_0/\mathbb{F}_2 \) 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 \( \mathbb{Z}[\omega] \) of \( \mathbb{Q}(\omega) \), via the map

\[
\alpha: \mathbb{Z}[\omega] \to \operatorname{End}(E_0)
\]

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],

\[
\operatorname{End}_k(F) \cong \mathcal{O} + 2^a B,
\]

where

\[
B = \operatorname{End}(F_0)
\]

\[\mathcal{O} \cong \mathbb{Z}_2[\omega].\]
To get a quasi-canonical lifting of $F_0$ we need to construct an elliptic curve which is isogenous to $E$. Let $\pi' \in \mathcal{O}_2$ 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 $\phi: E \to E'$ given by

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

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

The isogeny $\phi$ has degree 2, with kernel $\{\infty, (-\frac{1}{2}\pi', -\frac{1}{2})\}$. The isogeny $\tilde{\phi}: F \to F'$ induced by $\phi$ also has degree 2. We find that $\text{End}(E') \cong \mathbb{Z}[2\omega]$; the Serre-Tate lifting implies then that $\text{End}(F') \cong \mathbb{Z}_2[2\omega]$. 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

$$\text{End}_{w_0}(F') \cong B$$

$$\text{End}_{w_1}(F') \cong \mathcal{O}_1 + \pi_B B$$

$$\text{End}_{w_2}(F') \cong \mathcal{O}_1 + \pi_B^2 B \quad 1 < n \leq 5$$

$$\text{End}_{w_3}(F') \cong \mathcal{O}_1 + \pi_B^4 B \quad 5 < n \leq 9$$

$$\vdots$$

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

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

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

$$\text{Fr} \notin \mathcal{O}_1 + \pi_B^2 B.$$
Therefore Fr lifts to End_{W_1}(F') but not to End_{W_2}(F'). The endomorphism of $F_0$ induced by $\alpha(\omega)$ is not an element of $\mathcal{O}_1 + \pi_2 B$, so it doesn't lift to End_{W_1}(F').

References