Astérisque
312, 2007, p. 67–86

8. CANONICAL AND QUASI-CANONICAL LIFTINGS

by

Stefan Wewers

Abstract. — The present note gives a detailed account of the paper of Gross on canonical and quasi-canonical liftings. These are liftings of formal $\mathcal{O}$-modules with extra endomorphisms, and thus correspond to CM-points in the universal deformation space.

Résumé **(Relèvements canoniques et quasi-canoniques).** — Nous donnons un exposé détaillé des travaux de Gross sur les relèvements canoniques et quasi-canoniques des $\mathcal{O}$-modules formels, qui correspondent aux points CM dans l'espace de déformations universel.

The present note gives a detailed account of Gross' paper [**G**] on canonical and quasi-canonical liftings. We make heavy use of results of Lubin and Tate [**LT2**] and Drinfeld [**D**] which are reviewed in [**VZ**]. All the results presented here have been generalized to the case of arbitrary finite height by J. K. Yu [**Yu**].

I thank Eva Viehmann, Inken Vollaard and Michael Rapoport for careful proof-reading and helpful discussions.

1. Canonical lifts

In this section we study canonical lifts of a formal $\mathcal{O}_K$-module of height two with respect to a quadratic extension L/K. In particular, we prove the first main result of [**G**] which computes the endomorphism ring of the reduction of a canonical lift modulo some power of the prime ideal of $\mathcal{O}_K$.

2000 ***Mathematics Subject Classification.*** — 14L05, 14K22.
Key words and phrases. — Formal $\mathcal{O}$-modules, canonical liftings, Lubin-Tate theory.

1.1. Throughout this note, K denotes a field which is complete with respect to a discrete valuation v, and whose residue class field is finite, with $q = p^f$ elements. We denote by $\mathcal{O}_K$ the ring of integers of K. We fix a prime element π of K, and we assume that $v(\pi) = 1$.

Let $i : \mathcal{O}_K \to R$ be an $\mathcal{O}_K$-algebra. Recall that a *formal $\mathcal{O}_K$-module over R* is given by a commutative formal group law $F(X, Y) = X + Y + \cdots \in R[[X, Y]]$ together with a ring homomorphism $\gamma : \mathcal{O}_K \to \mathrm{End}_R(F)$ such that the induced map $\mathcal{O}_K \to \mathrm{End}_R(\mathrm{Lie}F) \cong R$ is equal to the structure map i. Whenever this is not likely to be confusing, we will omit the maps i and γ from the notation. Given an element $a \in \mathcal{O}_K$, we write $[a]_F(X) = i(a)X + \cdots \in R[[X]]$ for the corresponding endomorphism of F.

If F_1, F_2 are two formal $\mathcal{O}_K$-modules over R, we write $\mathrm{Hom}_R(F_1, F_2)$ for the group of homomorphisms $\alpha : F_1 \to F_2$ of formal $\mathcal{O}_K$-modules, *i.e.*, $\mathcal{O}_K$-linear homomorphisms of formal groups. Similarly, $\mathrm{End}_R(F)$ denotes the (in general non-commutative) ring of $\mathcal{O}_K$-linear endomorphisms of F. Note that $\mathrm{End}_R(F)$ is an $\mathcal{O}_K$-algebra.

1.2. Let k be an algebraic closure of the residue class field of $\mathcal{O}_K$. We regard k as an $\mathcal{O}_K$-algebra, and write $\bar{a} \in k$ for the image of an element $a \in \mathcal{O}_K$.

Let G be a formal $\mathcal{O}_K$-module over k and let $\alpha \in k[[X]]$ be an endomorphism of G, with $\alpha \neq 0$. By [**VZ**, Lemma 2.1], there exists an integer $h = \mathrm{ht}(\alpha) \geq 0$, called the *height* of α, such that $\alpha(X) = \beta(X^{q^h})$, with $\beta'(0) \neq 0$. It is easy to check that the function $\mathrm{ht} : \mathrm{End}_k(G) \to \mathbb{Z}_{\geq 0} \cup \{\infty\}$ (we set $\mathrm{ht}(0) := \infty$) is a valuation on the $\mathcal{O}_K$-algebra $\mathrm{End}_k(G)$. We say that the formal $\mathcal{O}_K$-module G has *height* h, if the endomorphism $[\pi]_G$ has height h. In other words, the restriction of the valuation ht *via* the structure map $\mathcal{O}_K \to \mathrm{End}_k(G)$ is equal to $h^{-1} \cdot v$.

We recall the following fundamental result.

Theorem 1.1. — *For each natural number h, there exists a formal $\mathcal{O}_K$-module G over k of height h. It is unique up to isomorphism. The ring $\mathrm{End}_k(G)$ is isomorphic to the maximal order $\mathcal{O}_D$ of a division algebra D of dimension h^2 over K, with invariant $\mathrm{inv}(D) = 1/h$.*

Proof. — (Compare with [**D**], Proposition 1.7.) The existence of G follows from Lubin-Tate theory, as follows. Let L/K be the unramified extension of degree h. Extend the algebra map $\mathcal{O}_K \to k$ to $\mathcal{O}_L$, which gives k the structure of an $\mathcal{O}_L$-algebra. Let F be the Lubin-Tate module of $\mathcal{O}_L$ with respect to the prime element π, *i.e.*, the (unique) formal $\mathcal{O}_L$-module over $\mathcal{O}_L$ such that $[\pi]_F = \pi X + X^{q^h}$, see [**LT1**]. By restriction, we may regard F as a formal $\mathcal{O}_K$-module. Then $G := F \otimes k$ is a formal $\mathcal{O}_K$-module of height h over k.

The uniqueness of G is more difficult. See *e.g.* [**H**, Theorem 21.9.1].

Let us sketch a proof of the last statement of Theorem 1.1. Set $H := \mathrm{End}_k(G)$. We may assume that G is the reduction to k of the Lubin–Tate module for $\mathcal{O}_L$, where L/K is unramified of degree h. Since the natural map $\mathcal{O}_L = \mathrm{End}(F) \to H$ is injective (see [**VZ**, Lemma 2.6]), we have $\mathcal{O}_L \subset H$. By construction, the group law $G(X,Y) = X + Y + \dots$ and the endomorphisms $[a]_G(X) = \bar{a}X + \dots$, for $a \in \mathcal{O}_K$, are power series with coefficients in $\mathbb{F}_q$. Moreover, we have $[\pi]_G(X) = X^{q^h}$. Hence the polynomial $\Pi(X) := X^q$ defines an element $\Pi \in H$ with $\Pi^h = \pi$. One checks that

$$\Pi([a]_G(X)) = [a^\sigma]_G(\Pi(X)),$$

where $\sigma \in \mathrm{Gal}(L/K)$ is the Frobenius. From there, it is easy to see that the subalgebra $\mathcal{O}_D := \mathcal{O}_L[\Pi]$ of H is the maximal order of a division algebra D of dimension h^2 over K, with invariant $1/h$. It remains to be shown that $\mathcal{O}_D = H$.

Let $\alpha(X) = \bar{a}X + \dots$ be an element of H. Since α commutes with $[\pi]_G(X) = X^{q^h}$, the coefficients of α lie in $\mathbb{F}_{q^h} = \mathcal{O}_L/\pi\mathcal{O}_L$. Let $a \in \mathcal{O}_L$ be a lift of $\bar{a}$. Then $\alpha - [a]_G$ is an endomorphism of G with positive height, and therefore lies in the left ideal $H \cdot \Pi \subset H$. We have shown that the natural map

$$\mathcal{O}_D \longrightarrow H/(H \cdot \Pi)$$

is surjective. Now the desired equality $\mathcal{O}_D = H$ follows from the fact (which is easy to prove) that H is complete with respect to the Π-adic topology. $\square$

1.3. For the rest of this note, we fix a formal $\mathcal{O}_K$-module G of height two over k. By Theorem 1.1, G is uniquely determined, up to isomorphism, and $\mathcal{O}_D := \mathrm{End}_k(G)$ is the maximal order in a quaternion division algebra D over K with invariant $1/2$.

Let L/K be a quadratic extension. Let π_L denote a prime element of L. By [**S**, §XIII.3, Corollaire 3], there exists a K-linear embedding $\kappa : L \hookrightarrow D$. It is unique up to conjugation by elements of $D^\times$. We choose one such embedding and consider L, from now on, as a subfield of D. Note that $\mathcal{O}_L \subset \mathcal{O}_D$. *Via* this last embedding, we may regard G as a formal $\mathcal{O}_L$-module over k. In particular, we obtain a map $\mathcal{O}_L \to \mathrm{End}(\mathrm{Lie}\, G) = k$, which extends the canonical morphism $\mathcal{O}_K \to k$.

Let A be the strict completion of $\mathcal{O}_L$ with respect to k. In other words, A is the completion of the maximal unramified extension of $\mathcal{O}_L$, together with a morphism $A \to k$ extending the morphism $\mathcal{O}_L \to k$.

Definition 1.2. — A *canonical lift* of G with respect to the embedding $\kappa : L \hookrightarrow D$ is a lift F of G over A in the category of $\mathcal{O}_L$-modules.

In more detail, a canonical lift is a formal $\mathcal{O}_K$-module F over A, together with an isomorphism of $\mathcal{O}_K$-modules $\lambda : F \otimes k \xrightarrow{\sim} G$ and an isomorphism of $\mathcal{O}_K$-algebras $\gamma : \mathcal{O}_L \xrightarrow{\sim} \mathrm{End}(F)$, such that the following holds. First, the composition of γ with the regular representation $\mathrm{End}(F) \to \mathrm{End}(\mathrm{Lie}\, F) = A$ is the canonical inclusion $\mathcal{O}_L \subset A$. Second, the composition of γ with the inclusion $\mathrm{End}(F) \hookrightarrow \mathrm{End}(G) = \mathcal{O}_D$ induced by λ is equal to κ. Note that γ is uniquely determined by the lift F and the first condition. We will omit it from our notation and simply write $[a]_F : F \to F$ for the endomorphism $\gamma(a)$. Also, the fixed embedding κ will mostly be understood, and we write $[a]_G : G \to G$ for the endomorphism $\kappa(a)$.

Since G has height one as an $\mathcal{O}_L$-module, it follows from [**VZ**, Theorem 3.8], that a canonical lift F is uniquely determined, up to $*$-isomorphism, by the embedding κ. On the other hand, using Lubin-Tate theory and the uniqueness statement of Theorem 1.1, we also conclude that a canonical lift F exists, for any choice of κ. So it is justified to speak about *the* canonical lift F of G, with respect to κ. By choosing a suitable parameter X for F, we may always assume that

$$[\pi_L]_F(X) = \pi_L X + X^{q^{2/e}},$$

where e is the ramification index of the extension L/K.

1.4. Let F be the canonical lift of G over A, with respect to a fixed embedding $\kappa : L \hookrightarrow D$. For any positive integer n, we set

$$A_n := A/\pi_L^{n+1}A, \qquad F_n := F \otimes_A A_n, \qquad H_n := \mathrm{End}_{A_n}(F_n).$$

Since $\mathcal{O}_L \subset H_n$ for all n, we may consider the rings H_n as left $\mathcal{O}_L$-modules. We have a sequence of $\mathcal{O}_L$-linear maps, which are injective by [**VZ**, Lemma 2.6]:

$$H_n \hookrightarrow H_{n-1} \hookrightarrow \cdots \hookrightarrow H_0 = \mathcal{O}_D.$$

We shall consider H_n as an $\mathcal{O}_L$-submodules of $\mathcal{O}_D$. Since A is complete, we have

$$\cap_{n\geq 0} H_n = \mathcal{O}_L.$$

By [**VZ**, Proposition 3.2], we have an injective map

$$H_{n-1}/H_n \hookrightarrow H^2(G, M_n),$$

where $M_n := (\pi_L^n)/(\pi_L^{n+1})$.

Lemma 1.3. — *Fix $n \geq 1$ and let α be an element of $H_{n-1} - H_n$. Then $[\pi_L]_G \circ \alpha \in H_n - H_{n+1}$. In other words, multiplication with π_L induces an* injective *homomorphism of $\mathcal{O}_L$-modules*

$$H_{n-1}/H_n \hookrightarrow H_n/H_{n+1}.$$

Proof. — We may represent α by a power series $\alpha(X) \in A[[X]]$, without constant coefficient, whose reduction modulo π_L^n is an endomorphism of F_{n-1}. We write α_n for the reduction of α modulo π_L^{n+1}. Set

$$\epsilon := \alpha \circ [\pi]_F -_F [\pi]_F \circ \alpha.$$

Since α_{n-1} is an endomorphism of F_{n-1}, we have $\epsilon \equiv 0 \pmod{\pi_L^n}$. Moreover, if $(\Delta, \{\delta_a\}) \in Z^2(G, M_n)$ denotes the cocycle associated to α_n by [**VZ**, Proposition 3.2], then we have

$$\epsilon \equiv \delta_\pi \pmod{\pi_L^{n+1}}.$$

By assumption, the endomorphism α_{n-1} of F_{n-1} cannot be lifted to an endomorphism of F_n. Therefore, Corollary 3.4 of [**VZ**] shows that $\epsilon(X) = cX^q + \dots$, with $c \in (\pi_L^n) - (\pi_L^{n+1})$.

Set

$$\epsilon' := [\pi_L]_F \circ \alpha \circ [\pi]_F -_F [\pi]_F \circ [\pi_L]_F \circ \alpha.$$

Since $[\pi_L]_F$ is an endomorphism of F, we actually have $\epsilon' = [\pi_L]_F \circ \epsilon$. Using our assumption $[\pi_L]_F(X) = \pi_L X + X^{q^{2/e}}$ and the congruence $\epsilon \equiv 0 \pmod{\pi_L^n}$, we see that

$$\epsilon' = \pi_L c X^q + \cdots \equiv 0 \pmod{\pi_L^{n+1}}.$$

By [**VZ**, Corollary 3.4], this implies that $[\pi_L]_F \circ \alpha_n$ is an endomorphism of F_n, *i.e.*, $[\pi_L] \circ \alpha \in H_n$. Moreover, if $(\Delta', \{\delta'_a\}) \in Z^2(G, M_{n+1})$ denotes the cocycle associated to $[\pi_L] \circ \alpha_{n+1}$, then we have

$$\epsilon' \equiv \delta'_\pi \pmod{\pi_L^{n+2}}.$$

Since $\pi_L c \in (\pi_L^{n+1}) - (\pi_L^{n+2})$, Corollary 3.4 of [**VZ**] shows that $[\pi_L]_F \circ \alpha_n$ cannot be lifted to an endomorphism of F_n. This means that $[\pi_L] \circ \alpha \notin H_{n+1}$. □

We can now prove the main result of this section (Proposition 3.3 in [**G**]).

Theorem 1.4. — *For $n \geq 1$ we have $H_n = \mathcal{O}_L + \pi_L^n \mathcal{O}_D$.*

Proof. — Each group H_n is a submodule of the free rank-two $\mathcal{O}_L$-module $\mathcal{O}_D$ and contains the direct factor $\mathcal{O}_L \subset \mathcal{O}_D$. Therefore, the quotients H_{n-1}/H_n are cyclic $\mathcal{O}_L$-modules. By Lemma 1.3, these quotients are killed by π_L. Hence H_{n-1}/H_n is either 0 or isomorphic to $\mathcal{O}_L/\pi_L\mathcal{O}_L$. We claim that only the second case occurs. The case $n = 1$ is dealt with in the following lemma.

Lemma 1.5. — *We have $H_1 \neq H_0 = \mathcal{O}_D$.*

We will prove this lemma in the next subsection. Lemma 1.3 says that left multiplication with π_L induces an *injective* map $H_{n-1}/H_n \hookrightarrow H_n/H_{n+1}$. So by induction on n, Lemma 1.5 and the arguments preceding it show that $H_n/H_{n+1} \cong \mathcal{O}_L/\pi_L\mathcal{O}_L$ for all n and that $\mathcal{O}_D/H_n$ is an $\mathcal{O}_L$-module of length n, killed by π_L^n. The theorem follows immediately. □

1.5. We are now going to prove Lemma 1.5. We distinguish two cases.

Case 1: L/K is unramified. In this case, we may assume that $\pi_L = \pi$ and hence $[\pi]_F = \pi X + X^{q^2}$. Then

$$\mathcal{O}_D = \mathcal{O}_L \oplus \mathcal{O}_L \cdot \Pi,$$

where $\Pi = X^q$, see the proof of Theorem 1.1. Let $\alpha = \sum_{i \geq q} a_i X^i \in A_1[[X]]$ be a lift of Π with leading term X^q. Let $(\Delta, \{\delta_a\}) \in Z^2(G, M_1)$ be the cocycle associated to α. Using Taylor expansion, we see that

$$\begin{aligned}\delta_\pi(X) &= \alpha([\pi]_{F_1}(X)) -_{F_1} [\pi]_{F_1}(\alpha(X)) \\ &= \big(\alpha(X^{q^2}) + \pi\cdot\alpha'(X^{q^2})X\big) -_{F_1} \big(\pi\alpha(X) + \alpha(X)^{q^2}\big) \\ &= -\pi X^q + \cdots \neq 0.\end{aligned}$$

(Here we use the notation $\alpha' := \partial\alpha/\partial X$.) Therefore, by [**VZ**, Corollary 3.4], we have $\Pi \notin H_1$.

Case 2: L/K is ramified. Then π_L satisfies an Eisenstein equation over $\mathcal{O}_K$, which we may normalize to

$$\pi_L^2 + a\pi_L + \pi = 0,$$

with $a \in \pi\mathcal{O}_K$. Assuming, as usual, that $[\pi_L]_F = \pi_L X + X^q$, a short computation yields the congruence

$$[\pi]_F(X) \equiv -\pi_L X^q - X^{q^2} + \dots \pmod{\pi}. \tag{1.1}$$

Let $j \in \mathcal{O}_D$ be an element which generates an unramified quadratic extension of K. We may assume that $j(X) = \bar{u}X + \dots$, where $\bar{u} \in k$ generates the quadratic extension of the residue class field of $\mathcal{O}_K$. Lift j to a power series $\alpha(X) = uX + \cdots \in A_1[[X]]$ modulo π, and let $(\Delta, \{\delta_a\}) \in Z^2(G, M_1)$ be the associated cocycle. Then $u^q \not\equiv u \pmod{\pi_L}$. Using the congruence (1.1), we compute

$$\begin{aligned}\delta_\pi(X) &= \alpha([\pi]_{F_1}(X)) -_{F_1} [\pi]_{F_1}(\alpha(X)) \\ &= \big(u(-\pi_L X^q - X^{q^2}) + \dots\big) -_{F_1} \big(-\pi_L\alpha(X)^q - \alpha(X)^{q^2}\big) \\ &= \pi_L(u^q - u)X^q + \dots\end{aligned}$$

As in Case 1, we use [**VZ**, Corollary 3.4], to conclude that $j \notin H_1$.

2. Isogenies and Tate modules

In this section we review the connection between the endomorphism ring and the isogeny classes of a formal $\mathcal{O}_K$-module on the one hand, and lattices inside the Tate module on the other hand. These results will be used in the following section on quasi-canonical lifts.

2.1. As in the previous sections, K denotes a field which is complete with respect to a discrete valuation and has a finite residue field of order $q = p^f$. We let k denote an algebraic closure of the residue field of K. Furthermore, A is a flat local $\mathcal{O}_K$-algebra which is a complete discrete valuation ring with residue field k, and M is the fraction field of A. We fix an algebraic closure $\bar{M}$ of M.

Let F be a formal $\mathcal{O}_K$-module of finite height h over A (not necessarily a canonical lift). We write

$$\Lambda(F) := F(\bar{M})_{\mathrm{tor}} = \cup_n F[\pi^n]$$

for the torsion subgroup of F and

$$T(F) := \varprojlim_n F[\pi^n]$$

for the Tate module of F. These are $\mathcal{O}_K$-modules with a continuous, $\mathcal{O}_K$-linear action of $\mathrm{Gal}(\bar{M}/M)$. As $\mathcal{O}_K$-modules, we have non-canonical isomorphisms

$$\Lambda(F) \cong (K/\mathcal{O}_K)^h, \qquad T(F) \cong \mathcal{O}_K^h.$$

Set $V(F) := T(F) \otimes_{\mathcal{O}_K} K$; then we have a canonical short exact sequence of $\mathrm{Gal}(\bar{M}/M)$-$\mathcal{O}_K$-modules

$$0 \to T(F) \longrightarrow V(F) \longrightarrow \Lambda(F) \to 0. \tag{2.1}$$

Let A' be a finite extension of A, and let F' be a formal $\mathcal{O}_K$-module over A'. An *isogeny* between F and F' defined over A' is a nonzero homomorphism $\alpha : F \otimes_A A' \to F'$ of formal $\mathcal{O}_K$-modules. If such an isogeny exists, then we say that F' is *isogenous* to F (over A'). For simplicity, we shall write $\alpha : F \to F'$, and consider α as a power series in $\mathcal{O}_{\bar{M}}[[X]]$ whose coefficients generate a finite extension of A. We say that α is defined over A' if $\alpha \in A'[[X]]$.

Given an isogeny $\alpha : F \to F'$, we obtain a diagram

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & N \arrow[d] & \\
0 \arrow[r] & T(F) \arrow[r] \arrow[d, "T(\alpha)"] & V(F) \arrow[r] \arrow[d, "V(\alpha)", "\cong"'] & \Lambda(F) \arrow[r] \arrow[d, "\Lambda(\alpha)"] & 0 \\
0 \arrow[r] & T(F') \arrow[r] \arrow[d] & V(F') \arrow[r] \arrow[d] & \Lambda(F') \arrow[r] \arrow[d] & 0 \\
 & \operatorname{Coker} T(\alpha) & 0 & 0 &
\end{tikzcd} \tag{2.2}$$

with exact rows and columns. Note that N is equal to the kernel of α; it is a finite $\mathcal{O}_K$-submodule. A trivial version of the snake lemma shows that we have a canonical isomorphism $N \cong \operatorname{Coker} T(\alpha)$.

The following theorem states that every finite $\mathcal{O}_K$-submodule of $\Lambda(F)$ arises as the kernel of an isogeny. More precisely:

Theorem 2.1. — *Let $N \subset \Lambda(F)$ be a finite $\mathcal{O}_K$-submodule, $\Gamma' \subset \Gamma$ the stabilizer of N, $M' \subset \bar{M}$ the fixed field of Γ' and A' the valuation ring of M'. Then the formula*

$$\alpha(X) := \prod_{z \in N} (X -_F z) \in A'[[X]]$$

defines an isogeny $\alpha : F \to F'$ over A'. It has the following properties.

1. *$\mathrm{Ker}(\alpha) = N$.*

2. *Let $\beta : F \to F''$ be an isogeny with $N \subset \mathrm{Ker}(\beta)$. Then there exists a unique isogeny $\gamma : F' \to F''$ with $\beta = \gamma \circ \alpha$.*

Proof. — See [**H**, §35.2]. □

2.2. It will be more convenient for us to reformulate Theorem 2.1 in terms of lattices $T' \subset V(F)$ (instead of finite subgroups $N \subset \Lambda(F)$). Let F be a formal $\mathcal{O}_K$-module of finite height over A. Set $T := T(F)$ and $V := V(F)$.

Corollary 2.2. — 1. *Let $T' \subset V$ be an $\mathcal{O}_K$-lattice containing the lattice T (a* superlattice*). Then there exists an isogeny $\alpha : F \to F'$ such that $T' = V(\alpha)^{-1}(T(F'))$. If T'' is a superlattice of T' and $\beta : F \to F''$ an isogeny with $T'' = V(\beta)^{-1}(T(F''))$, then there exists a unique isogeny $\gamma : F' \to F''$ such that $\beta = \gamma \circ \alpha$.*

2. *Let $T' \subset T$ be an $\mathcal{O}_K$-sublattice. Then there exists an isogeny $\alpha : F' \to F$ such that $T' = \mathrm{Im}(T(\alpha))$. If $T'' \subset T'$ is another sublattice, and $\beta : F'' \to F$ is an isogeny such that $T'' = \mathrm{Im}(T(\beta))$, then there exists a unique isogeny $\gamma : F'' \to F'$ with $\beta = \alpha \circ \gamma$.*

Proof. — Given T' as in Part 1, we set $N := T'/T$. *Via* the short exact sequence (2.1), we consider N as a (finite) $\mathcal{O}_K$-submodule of V. Let $\alpha : F \to F'$ be the isogeny with kernel N, which exists by Theorem 2.1.1. Then the diagram (2.2) shows that $T' = V(\alpha)^{-1}(T(F'))$. This proves the first assertion in Part 1. The second assertion follows from Theorem 2.1.2.

We are now going to prove Part 2 of the corollary. Let $T' \subset T$ be a sublattice. Choose an integer n such that $\pi^n T \subset T'$. By Part 1 of the corollary, there exists an isogeny $\beta : F \to F'$ such that $V(\beta)^{-1}(T(F')) = \pi^{-n}T'$. The kernel of β is isomorphic to $\pi^{-n}T'/T$, which is an $\mathcal{O}_K$-module killed by π^n. Therefore, Theorem 2.1.2 shows that there exists an isogeny $\alpha : F' \to F$ with $\alpha \circ \beta = [\pi^n]_F$. By construction, we have

$$\mathrm{Im}(T(\alpha)) = \pi^n \cdot V(\beta)^{-1}(T(F')) = T'.$$

This proves the first assertion of Part 2. The proof of the second assertion is left to the reader. □

2.3. Let F, T and V be as before. The faithful representation of $\mathrm{End}(F)$ on V extends to a faithful representation

$$\mathrm{End}^0(F) := \mathrm{End}(F) \otimes_{\mathcal{O}_K} K \hookrightarrow \mathrm{End}_K(V).$$

We will from now on consider elements of $\mathrm{End}^0(F)$ as elements of $\mathrm{End}_K(V)$.

Let T', T'' be $\mathcal{O}_K$-superlattices of T inside V. Let $\alpha : F \to F'$ and $\beta : F \to F''$ be the corresponding isogenies, as in Corollary 2.2.1. We identify $V(F')$ and $V(F'')$ with V, *via* the isomorphisms $V(\alpha)$ and $V(\beta)$. Then $T' = T(F')$ and $T'' = T(F'')$.

Corollary 2.3. — *The map which sends a homomorphism $\psi : F' \to F''$ to the induced endomorphism $\tilde{\psi} : V \cong V(F') \to V(F'') \cong V$ is a bijection*

$$\mathrm{Hom}(F', F'') \xrightarrow{\sim} \{\, \tilde{\psi} \in \mathrm{End}^0(F) \mid \tilde{\psi}(T') \subset T'' \,\}.$$

Proof. — Let $\psi : F' \to F''$ be a homomorphism and $\tilde{\psi} \in \mathrm{End}_K(V)$ the induced endomorphism of V. By definition, we have $\tilde{\psi}(T') \subset T''$. We have to show that $\tilde{\psi} \in \mathrm{End}^0(F)$. Set $\gamma := \psi \circ \alpha : F \to F''$. The isogeny γ corresponds, *via* Corollary 2.2.2, to the sublattice $\tilde{\psi}(T) \subset T''$. From the same point of view, the isogeny $\beta : F \to F''$ corresponds to the sublattice $T \subset T''$. Choose an integer n such that $\pi^n \tilde{\psi}(T) \subset T$. Then by Corollary 2.2.2, there exists an endomorphism $\phi : F \to F$ such that $\beta \circ \phi = \gamma \circ [\pi^n]_F$. One checks that $\phi = \pi^n \tilde{\psi}$, as elements of $\mathrm{End}_K(V)$, which shows that $\tilde{\psi} \in \mathrm{End}^0(F)$.

Conversely, let $\tilde{\psi}$ be an element of $\mathrm{End}^0(F) \subset \mathrm{End}_K(V)$ with $\tilde{\psi}(T') \subset T''$. By definition, we can write $\tilde{\psi} = \pi^{-n}\phi$ for some endomorphism $\phi : F \to F$. The isogeny $\alpha \circ [\pi^n]_F : F \to F'$ (resp. the isogeny $\beta \circ \phi : F \to F''$) corresponds, *via* Corollary 2.2.1, to the superlattice $\pi^{-n}T' \supset T$ (resp. the superlattice $\phi^{-1}(T'') \supset T$). The assumption $\tilde{\psi}(T') \subset T''$ together with $\tilde{\psi} = \pi^{-n}\phi$ implies $\pi^{-n}T' \subset \phi^{-1}(T'')$. Therefore, by Corollary 2.2.1, there exists an isogeny $\psi : F' \to F''$ with $\psi \circ \alpha \circ [\pi^n]_F = \beta \circ \phi$. By construction, $\tilde{\psi}$ is the image of ψ under the embedding $\mathrm{Hom}(F', F'') \hookrightarrow \mathrm{End}_K(V)$. This concludes the proof of the corollary. □

3. Quasi-canonical lifts

A quasi-canonical lift is a lift whose endomorphism ring is an order in a quadratic extension L/K. In this section we show that every quasi-canonical lift is isogenous to a canonical lift, and we determine the set of isomorphism classes of all quasi-canonical lifts together with its natural Galois action.

3.1. We now come back to the situation of Section 1. In particular, G is the (unique) formal $\mathcal{O}_K$-module of height two over k. We fix a quadratic extension L/K, an $\mathcal{O}_K$-linear embedding $\kappa : \mathcal{O}_L \hookrightarrow \mathcal{O}_D := \mathrm{End}_k(G)$. We denote by F the canonical lift of G with respect to κ. Recall that F is defined over A, the strict completion of $\mathcal{O}_L$ with respect to the map $\mathcal{O}_K \to k$ induced by the $\mathcal{O}_L$-action on $\mathrm{Lie}(G)$.

Let M denote the fraction field of A, $\bar{M}$ an algebraic closure of M and $\Gamma := \mathrm{Gal}(\bar{M}/M)$. We let $T := T(F)$ denote the Tate-module of F and $V := T \otimes_{\mathcal{O}_K} K$. Note that T has the structure of a free $\mathcal{O}_L$-module of rank one, and that the Γ-action on T is continuous and $\mathcal{O}_L$-linear. By Lubin–Tate theory, the resulting homomorphism

$$\rho : \Gamma = \mathrm{Gal}(\bar{M}/M) \longrightarrow \mathcal{O}_L^\times \tag{3.1}$$

yields an isomorphism $\Gamma^{\mathrm{ab}} \xrightarrow{\sim} \mathcal{O}_L^\times$. Identifying Γ with the inertia subgroup of $\mathrm{Gal}(\bar{L}/L)$, the homomorphism (3.1) is the inverse of the reciprocity map $L^\times \to \mathrm{Gal}(\bar{L}/L)^{\mathrm{ab}}$ of local class field theory, restricted to $\mathcal{O}_L^\times$. See [**LT1**].

Fix an integer $s \geq 0$. Let

$$\mathcal{O}_s := \mathcal{O}_K + \mathcal{O}_L \cdot \pi^s$$

denote the order of $\mathcal{O}_L$ generated by $\mathcal{O}_K$ and the ideal $\mathcal{O}_L \cdot \pi^s$. It is easy to see that every order of $\mathcal{O}_L$ containing $\mathcal{O}_K$ is equal to $\mathcal{O}_s$, for some s. Let M_s/M be the ring class field of $\mathcal{O}_s^\times$, *i.e.*, the fixed field of the subgroup $\Gamma_s \subset \Gamma$, where Γ_s is the inverse image of $\mathcal{O}_s^\times \subset \mathcal{O}_L^\times$ under the inverse reciprocity homomorphism (3.1). In other words, we have

$$\mathrm{Gal}(M_s/M) \cong \mathcal{O}_L^\times/\mathcal{O}_s^\times.$$

An easy computation shows that, for $s \geq 1$,

$$[M_s : M] = |\mathcal{O}_L^\times/\mathcal{O}_s^\times| = \begin{cases} q^{s-1}(q+1), & \text{if } L/K \text{ is unramified,} \\ q^s, & \text{if } L/K \text{ is ramified.} \end{cases}$$

Definition 3.1. — A *quasi-canonical lift of G of level s* (with respect to the embedding $\kappa : \mathcal{O}_L \hookrightarrow \mathcal{O}_D$) is a lift F of G, defined over some finite extension A'/A, together with an $\mathcal{O}_K$-algebra isomorphism $\gamma : \mathcal{O}_s \xrightarrow{\sim} \mathrm{End}(F')$, such that the following holds.

1. The composition of γ with the representation $\mathrm{End}(F') \hookrightarrow \mathrm{End}(\mathrm{Lie}\, F') = A'$ is the canonical embedding $\mathcal{O}_s \hookrightarrow A'$.
2. The composition of γ with the embedding $\mathrm{End}(F') \hookrightarrow \mathcal{O}_D$ is equal to the restriction of κ to $\mathcal{O}_s \subset \mathcal{O}_L$.

To ease the notation, we will usually omit the isomorphism γ and the embedding κ from our notation. Note that a quasi-canonical lift of level 0 is the same thing as a canonical lift (which exists and is unique). For general s, we have the following result.

Theorem 3.2. — *Let $\mathcal{O}_{M_s}$ denote the ring of integers of M_s.*

1. *Let F' be a quasi-canonical lift of level s. Then there exists an isogeny*

$$\alpha : F \longrightarrow F'$$

of degree q^s, defined over $\mathcal{O}_{M_s}$. It is unique up to composing α with an element of $\mathrm{Aut}(F) = \mathcal{O}_L^\times$. In particular, F' can be defined over $\mathcal{O}_{M_s}$.

2. *The set of $*$-isomorphism classes of all quasi-canonical lifts of level s is a principal homogeneous space under the action of $\mathrm{Gal}(M_s/M)$.*

Remark 3.3. — The proof of this theorem will show that the action of $\mathrm{Gal}(M_s/M)$ on the set of $*$-isomorphism classes can be described as follows. Let (F', λ) be a quasi-canonical lift of level s (with $\lambda : F' \otimes k \xrightarrow{\sim} G$), and $\sigma \in \Gamma$. Then the lift $(F', \lambda)^\sigma$ is $*$-isomorphic to the lift $(F', [\rho(\sigma)^{-1}]_G \circ \lambda)$. Therefore, by Theorem 3.2.2, two quasi-canonical lifts of the same level are always isomorphic as formal $\mathcal{O}_K$-modules.

3.2. Let $\alpha : F \to F'$ and $\beta : F \to F''$ be two isogenies with source F. We say that α and β are *isomorphic* if there exists an isomorphism of formal $\mathcal{O}_K$-modules $\gamma : F' \xrightarrow{\sim} F''$ with $\beta = \gamma \circ \alpha$.

Fix an isogeny $\alpha : F \to F'$. To simplify the notation, we will identify $V(F')$ with V *via* the isomorphism $V(\alpha)$. Then, by Corollary 2.2.1, α corresponds, up to isomorphism, to an $\mathcal{O}_K$-superlattice $T' \supset T$ in V. Moreover, by Corollary 2.3, α induces an isomorphism of $\mathcal{O}_K$-algebras

$$\mathrm{End}(F') \xrightarrow{\sim} \{ \phi \in L = \mathrm{End}^0(F) \mid \phi(T') \subset T' \}. \tag{3.2}$$

This exhibits $\mathrm{End}(F')$ as an order of $\mathcal{O}_L$.

Lemma 3.4. — *Let T be a free $\mathcal{O}_L$-module of rank one, $V := T \otimes_{\mathcal{O}_K} K$. Let $T' \supset T$ be an $\mathcal{O}_K$-superlattice in V. Then there exists a generator t of T (*i.e., *$T = \mathcal{O}_L \cdot t$) and integers $n, s \geq 0$ such that*

$$\pi_L^n \cdot T' = (\mathcal{O}_K \cdot \pi^{-s} + \mathcal{O}_L) \cdot t.$$

Moreover, the multiplicator $\mathcal{O}_{T'}$ of T' is equal to the order $\mathcal{O}_s \subset \mathcal{O}_L$.

Proof. — For $T' \supset T$ as in Part 1, define

$$n := \max\{ n' \mid \pi_L^{n'} T' \supset T \}, \qquad s := \min\{ s' \mid \pi^{s'} \pi_L^n T' \subset T \}.$$

Then $\pi_L^n T'/T$ is a cyclic $\mathcal{O}_K$-module, generated by an element of the form $\pi^{-s} t$. Moreover, any t with this property is a generator of T. It follows that $\pi_L^n T' = (\mathcal{O}_K \cdot \pi^{-s} + \mathcal{O}_L) \cdot t$. The proof of the fact that $\mathcal{O}_s$ is the multiplicator of T' is standard and left to the reader. □

A superlattice $T' \supset T$ is called *minimal of level s* if $T' = (\mathcal{O}_K \cdot \pi^{-s} + \mathcal{O}_L) \cdot t$, for some generator t of T. The corresponding isogenies $\alpha : F \to F'$ are also called *minimal of level s*. We let X_s denote the set of isomorphism classes of minimal isogenies of level s. The Galois group Γ acts on X_s, in a natural way. There is also an action of $\mathcal{O}_L^\times$ on X_s, given by composing $\alpha : F \to F'$ with the automorphism $[a]_F : F \xrightarrow{\sim} F$, for $a \in \mathcal{O}_L^\times$.

Proposition 3.5. — *The actions of Γ and $\mathcal{O}_L^\times$ on X_s are anti-compatible* via *the reciprocity homomorphism $\rho : \Gamma \to \mathcal{O}_L^\times$,* i.e., *for $\sigma \in \Gamma$ there exists an isomorphism $\gamma_\sigma : (F')^\sigma \xrightarrow{\sim} F'$ such that the diagram*

$$\begin{tikzcd} F \arrow[r, "\alpha^\sigma"] \arrow[d, "{[\rho(\sigma)^{-1}]_F}"'] & (F')^\sigma \arrow[d, "\gamma_\sigma"] \\ F \arrow[r, "\alpha"] & F' \end{tikzcd}$$

commutes. Furthermore, X_s is a principal homogeneous space under the induced action of $\mathrm{Gal}(M_s/M) \cong \mathcal{O}_L^\times/\mathcal{O}_s^\times$.

Proof. — If the isogeny $\alpha : F \to F'$ corresponds to the lattice T', then $\alpha \circ [a]_F : F \to F'$, for $a \in \mathcal{O}_L$, corresponds to the lattice $a^{-1} \cdot T'$. Therefore, it follows immediately from Lemma 3.4 that the action of $\mathcal{O}_L^\times$ on X_s is transitive, and the stabilizer of each element is equal to $\mathcal{O}_s^\times$. To see that this action is compatible with the Galois action, fix an element $\sigma \in \Gamma$. Clearly, the kernel of α^σ can be identified with $(T'/T)^\sigma = \rho(\sigma)\cdot T'/T$. Since this is also the kernel of $\alpha\circ[\rho(\sigma)^{-1}]_F$, the existence of γ_σ follows from Theorem 2.1. The proposition is proved. □

Proof of Theorem 3.2. — We first prove Part 1 of the theorem. Let F' be a quasi-canonical lift of level s. Set $T' := T(F')$ and $V' := T'\otimes_{\mathcal{O}_K} K$. The isomorphism $\mathcal{O}_s \xrightarrow{\sim} \mathrm{End}(F')$ extends to an isomorphism $L \xrightarrow{\sim} \mathrm{End}^0(F')$, which gives V' the structure of an L-vector space of dimension one and identifies $\mathcal{O}_s$ with the multiplicator of the lattice $T' \subset V'$.

Let $T'' \subset T'$ be a maximal $\mathcal{O}_L$-submodule of rank one. Then $T' = (\mathcal{O}_K\cdot\pi^{-s}+\mathcal{O}_L)\cdot t$ for some generator t of T'', by Lemma 3.4. Let $\alpha : F'' \to F'$ be an isogeny with $\mathrm{Im}(T(\alpha)) = T''$, see Corollary 2.2.2. By Corollary 2.3, α induces an isomorphism

$$\mathrm{End}(F'') \cong \{\, \phi \in \mathrm{End}^0(F') = L \mid \phi(T'') = T'' \,\} \cong \mathcal{O}_L.$$

Therefore, $F'' \cong F$ as formal $\mathcal{O}_K$-modules. Choosing an arbitrary isomorphism $F'' \cong F$, we can regard $\alpha : F \cong F'' \to F'$ as an element of X_s. Since $\mathcal{O}_L^\times$ acts transitively on X_s, by Proposition 3.5, we have proved Part 1 of Theorem 3.2.

Now we prove Part 2 of the theorem. In view of Part 1 and Proposition 3.5, we only need to show the following. For every minimal isogeny $\alpha : F \to F'$ of level s, there exists an isomorphism $\lambda : F' \otimes k \xrightarrow{\sim} G$ which makes F' a quasi-canonical lift. For this, we may assume that the isogeny α is given, as a power series with coefficients in $\mathcal{O}_{M_s}$, by the formula of Theorem 2.1:

$$\alpha(X) := \prod_{\gamma\in\mathrm{Ker}(\alpha)} (X -_F \gamma).$$

Here $\mathrm{Ker}(\alpha)$ is simply considered as a subset of the maximal ideal of the ring of integers of $\bar{M}$. Therefore, the reduction of α to k is $\bar{\alpha}(X) = X^{q^s}$. By the proof of Theorem 1.1, we may assume that $\Pi(X) := X^q$ is an endomorphism of G and lies in the normalizer of $\mathcal{O}_L = \mathrm{End}(F) \subset \mathcal{O}_D$. In particular, $\bar{\alpha} = \Pi^s$ is an endomorphism of G. Therefore, $F' \otimes k$ is actually *equal* to G. We define the isomorphism $\lambda : F' \otimes k \xrightarrow{\sim} G$ as the identity and claim that (F', λ) is a quasi-canonical lift.

By construction, we have an isomorphism

$$\mathrm{End}(F') \cong \{\, \phi \in L = \mathrm{End}^0(F) \mid \phi(T') = T' \,\} \cong \mathcal{O}_s. \tag{3.3}$$

Hence the image of the natural injection $\mathrm{End}(F') \hookrightarrow \mathrm{End}(\mathrm{Lie}\, F') = \mathcal{O}_{M_s}$ is an $\mathcal{O}_K$-algebra isomorphic to $\mathcal{O}_s$. It must therefore be equal to $\mathcal{O}_s$. Let $\gamma : \mathcal{O}_s \xrightarrow{\sim} \mathrm{End}(F')$ be the resulting isomorphism. Then Condition 1 of Definition 3.1 holds by construction.

Let $\kappa' : \mathcal{O}_s \hookrightarrow \mathcal{O}_D$ be the composition of γ with the embedding $\mathrm{End}(F') \hookrightarrow \mathcal{O}_D$ induced by the identification $F' \otimes k = G$. We have to show that κ' is equal to the restriction of κ to $\mathcal{O}_s$ (see Condition 2 of Definition 3.1). Tracing back the definitions, we see that $\kappa' = (\kappa|_{\mathcal{O}_s})^{\bar{\alpha}}$ is the conjugate of $\kappa|_{\mathcal{O}_s}$ by $\bar{\alpha} = \Pi^s \in \mathcal{O}_D$. Since we assumed Π to lie in the normalizer of the image of κ, we have already proved that κ' and $\kappa|_{\mathcal{O}_s}$ have the same image and are equal up to composition with an element of $\mathrm{Gal}(L/K) \cong \mathbb{Z}/2$. However, if L/K is ramified, then the assumption that Π normalizes $\mathcal{O}_L$ already implies that $\Pi \in \mathcal{O}_L$, and we get $\kappa' = \kappa|_{\mathcal{O}_s}$ as desired. Now assume that L/K is unramified. Then it suffices to show that κ' and $\kappa|_{\mathcal{O}_s}$ agree modulo the maximal ideal $\mathcal{O}_D \cdot \Pi$. But this is a consequence of Condition 1 of Definition 3.1. This concludes the proof of Theorem 3.2. □

4. Canonical subgroups

The main result of this section is Proposition 4.6 which computes the valuation of the formal modulus of a quasi-canonical lift. The heart of the proof of this proposition is the study of *canonical subgroups* and their behavior under isogenies. The relevance of canonical subgroups was first pointed out in [**L**].

4.1. We continue with the notation used in the last section. In particular, A is the completion of the maximal unramified extension of $\mathcal{O}_L$ and M the fraction field of A. We choose an algebraic closure $\bar{M}$ of M and let $v : \bar{M} \to \mathbb{Q} \cup \{\infty\}$ denote the exponential rank-one valuation with $v(\pi) = 1$.

Let M'/M be some finite extension, and let A' denote the valuation ring of M'. Throughout this section, we will implicitly assume that the extension M'/M is 'sufficiently large'. In practice this will mean that sometimes we have to enlarge M' in order to make certain torsion points M'-rational.

For the moment, we fix an arbitrary lift F of the formal $\mathcal{O}_K$-module G, defined over A' (not necessarily the canonical lift). By [**VZ**, Theorem 3.8], F is isomorphic to the pullback of the universal deformation $\tilde{F}$ of G *via* a unique $\widehat{\mathcal{O}}_K^{\mathrm{nr}}$-algebra morphism $R^{\mathrm{univ}} \to A$. Moreover, R^{univ} can be written as a power series algebra $\widehat{\mathcal{O}}_K^{\mathrm{nr}}[[u]]$. (The proof of this result in [**VZ**] does not provide us with a natural choice of the parameter u, but this is irrelevant for us by Remark 4.2 below. See [**HG**] for a more explicit choice of the parameter u.)

Definition 4.1. — The image of the parameter u under the morphism $R^{\mathrm{univ}} \to A'$ corresponding to F is denoted by $u(F)$ and is called the *formal modulus* of the lift F. The rational number $v(F) := \min\{v(u(F)), 1\}$ is called the *valuation* of F.

Remark 4.2. — It is clear that the valuation $v(F)$ is actually independent of the choice of the parameter u. Therefore, $v(F)$ depends only on the isomorphism class of F as a formal $\mathcal{O}_K$-module, and not on the chosen isomorphism $\lambda : F \otimes k \xrightarrow{\sim} G$. Indeed, a unit $\gamma \in \mathcal{O}_D^\times$ induces an automorphism $\tilde{\gamma}$ of the universal deformation space of G (which sends the pair (F,λ) to the pair $(F,\gamma\circ\lambda)$). Applying the automorphism $\tilde{\gamma}$ amounts to replacing the parameter u by $u' := \tilde{\gamma}^* u$.

Definition 4.3. — A sub-$\mathcal{O}_K$-module $H \subset F[\pi]$ of length one is called a *canonical subgroup* if

$$v(x) > v(y)$$

for all $x \in H$ and $y \in F[\pi] - H$.

Note that a canonical subgroup, if it exists, is unique. We may therefore speak about *the* canonical subgroup of F. The two last definitions are related to each other in the following manner.

Proposition 4.4

1. *Write* $[\pi]_F = \sum_{i\geq 1} a_i X^i$, *with* $a_i \in A'$. *Then* $v(F) = \min\{v(a_q), 1\}$.
2. *The lift* F *has a canonical subgroup if and only if*

$$v(F) < \frac{q}{q+1}.$$

Proof. — It follows from the proof of [**VZ**, Theorem 3.8], that we can choose for the parameter u defining the isomorphism $R^{\mathrm{univ}} \cong \widehat{\mathcal{O}}_K^{\mathrm{nr}}[[u]]$ the qth coefficient of $[\pi]_{\tilde{F}}$, where $\tilde{F}$ is the universal deformation of G. Therefore, Part 1 of the proposition is a direct consequence of the definition of $v(F)$. Now Part 2 is easily seen by looking at the Newton polygon of $[\pi]_F$. Indeed, the slope filtration on the set $F[\pi] - \{0\}$ is also a filtration of $\mathcal{O}_K$-modules. But as an $\mathcal{O}_K$-module, $F[\pi]$ has length two, so there can be at most two finite negative slopes. Also, breaks occur only at $i = 1, q^2$ and possibly at $i = q$. Since $v(a_1) = 1$ and $v(a_{q^2}) = 0$, we have a break at $i = q$ if and only if $v(F) < q/(q+1)$. □

4.2. Fix a lift F of G defined over A' and a sub-$\mathcal{O}_K$-module $H \subset F[\pi]$ of length one. Let $\alpha : F \to F'$ be the isogeny with kernel H, defined by Theorem 2.1. Recall that α is given by the power series

$$\alpha(X) := \prod_{x\in H} (X -_F x). \tag{4.1}$$

Let us choose an isomorphism $\lambda' : F' \otimes k \xrightarrow{\sim} G$. We will use λ' as an identification, *i.e.*, we will regard F' as a lift of G. As in Section 3.2, one can choose λ' in such a way that $\alpha \otimes k$ gets identified with the isogeny $\Pi = X^q : G \to G$. However, this choice is not at all canonical. In what follows, we are mainly interested in relating the two valuations $v(F)$ and $v(F')$. By Remark 4.2, the choice that we have made is irrelevant for this problem.

Let $\beta : F \to F'$ be the unique isogeny such that $[\pi]_F = \beta \circ \alpha$. Then $H' := \ker(\beta)$ is equal to the image of $F[\pi]$ under the isogeny α. Clearly, H' is an $\mathcal{O}_K$-module of length one.

Proposition 4.5

1. *Suppose that H is the canonical subgroup of F. There are two cases:*
   (a) *If $v(F) \leq \frac{1}{q}$ then $v(F') = q \cdot v(F)$ and H' is not canonical.*
   (b) *If $\frac{1}{q} < v(F) < \frac{q}{q+1}$ then $v(F') = 1 - v(F)$ and H' is the canonical subgroup of F'.*
2. *Suppose that H is* not *the canonical subgroup of F. Again we have two cases:*
   (a) *If $v(F) \leq \frac{q}{q+1}$ then $v(F') = q^{-1} \cdot v(F)$.*
   (b) *If $v(F) \geq \frac{q}{q+1}$ then $v(F') = 1/(q+1)$.*

   In both cases, H' is the canonical subgroup of F'.

Proof. — Suppose that H is canonical. By Proposition 4.4, we have $v(F) < q/(q+1)$. Moreover, the proof of this proposition shows that the Newton polygon of $[\pi]_F$ has exactly two finite negative slopes, namely

$$s_1 = -\frac{1 - v(F)}{q - 1}, \qquad s_2 = -\frac{v(F)}{q^2 - q}.$$

Here s_1 is the slope above the interval $[1, q]$ and corresponds to the canonical subgroup, whereas s_2 is the slope above $[q, q^2]$.

Pick an element $y \in F[\pi] - H$; then $v(y) = -s_2 = v(F)/(q^2 - q)$. It follows from (4.1) that the element $z := \alpha(y) \in H'$ has valuation

$$v(z) = \sum_{x \in H} v(y -_F x) = q \cdot v(y) = \frac{v(F)}{q - 1}.$$

Now if $v(F) \leq 1/q$ then $v(z) \leq 1/(q^2 - q)$. This means that $-v(z)$ is equal to the slope of the Newton polygon of $[\pi]_{F'}$ above the interval $[q, q^2]$. We conclude that

$$v(F') = (q^2 - q) \cdot v(z) = q \cdot v(F)$$

and that H' is not the canonical subgroup of F'. On the other hand, if $v(F) > 1/q$ then $v(z) > 1/(q^2 - q)$. Therefore, $v(z)$ is equal to the slope above the interval $[1, q]$. We conclude that

$$v(F') = 1 - (q - 1) \cdot v(F) = 1 - v(F)$$

and that H' is the canonical subgroup of F'. This finishes the proof of Case 1. The proof of Case 2 is similar and left to the reader. □

4.3. Let us now assume that the lift F is the canonical lift of G with respect to some fixed embedding $\kappa : L \hookrightarrow D$. Note that we have $v(F) = 1$ if L/K is unramified and $v(F) = 1/2$ if L/K is ramified. In the former case, F has no canonical subgroup, whereas in the latter case the canonical subgroup of F is the kernel of $[\pi_L]_F$.

For $s = 1, 2, \ldots$, we define isogenies $\alpha_s : F \to F_s$ inductively, as follows. First, choose a non-canonical $\mathcal{O}_K$-submodule $H \subset F[\pi]$ of height one. Set $F_1 := F/H$ and let $\alpha_1 : F \to F_1$ be the natural projection. For $s \geq 1$, choose a non-canonical $\mathcal{O}_K$-submodule $H_s \subset F_s[\pi]$ of height one, set $F_{s+1} := F_s/H_s$ and let $\alpha_{s+1} : F \to F_{s+1}$ be the composition of α_s with the natural projection $F_s \to F_{s+1}$. As we have seen in the last section, we can see F_s as a lift of G in such a way that the isogeny α_s reduces to the endomorphism $\Pi^s : G \to G$ modulo the maximal ideal of A'. This choice is by no means canonical; however, for the statement of the next proposition, the choice that we have made is irrelevant, see Remark 3.3 and Remark 4.2.

Proposition 4.6. — *The lift F_s is quasi-canonical of level s, and we have*

$$v(F_s) = \begin{cases} \dfrac{1}{q^{s-1}(q+1)}, & \text{if } L/K \text{ is unramified and } s \geq 1, \\ \dfrac{1}{2q^s}, & \text{if } L/K \text{ is ramified.} \end{cases}$$

Proof. — We proceed by induction over s. We start the induction at $s = 1$ if L/K is unramified and at $s = 0$ in the ramified case (one has to be careful with the notation: plugging in $s = 0$ into F_s should be understood as F). If L/K is unramified, then $v(F) = 1 > q/(q+1)$, and Proposition 4.5, Case 2(b), shows that $v(F_1) = 1/(q+1)$. This is indeed as in the statement of the proposition. The statement of the proposition is also true for $s = 0$ if L/K is ramified.

Suppose now that $s \geq 1$ or that L/K is ramified. Then $v(F_s) \leq q/(q+1)$, so Proposition 4.5, Case 2(a), shows that

$$v(F_{s+1}) = \frac{v(F_s)}{q}.$$

We see that the formula for $v(F_s)$ follows by induction.

Since F_s is isogenous to F, it is a quasi-canonical lift of some level. By construction, the isogeny $\alpha_s : F \to F_s$ has degree q^s. Let n be the maximal integer such that α_s factors over $[\pi_L^n] : F \to F$. The proof of Theorem 3.2 shows that F_s is quasi-canonical of level $s' := s - 2n/e$.

Suppose $n > 0$. By the induction hypothesis, $F_{s'}$ is quasi-isogenous of level s'. Therefore, by Remark 3.3, $F_{s'}$ and F_s are isomorphic as formal $\mathcal{O}_K$-modules. But then we have $v(F_s) = v(F_{s'})$. This gives a contradiction with the formula for $v(F_s)$ which we have already proved. We conclude that $n = 0$, *i.e.*, that F_s is quasi-canonical of level s. □

Corollary 4.7. — *Let F_s be a quasi-canonical lift of level s and $\mathcal{O}_{M_s}/A$ be the smallest extension over which it can be defined. Then the formal modulus $u(F_s) \in \mathcal{O}_{M_s}$ of F_s is a uniformizer for the valuation ring $\mathcal{O}_{M_s}$.*

Proof. — It follows from Theorem 3.2 that $\mathcal{O}_{M_s}$ is the ring of integers of the extension M_s/M, the ring class field of $\mathcal{O}_s^\times$. Moreover, we may assume that F_s is the lift constructed before Proposition 4.5. Therefore, the formula for $v(F_s)$ in Proposition 4.5 shows that the valuation of $u(F_s)$ is equal to the reciprocal of the degree $[M_s : M]$. This concludes the proof. □

Corollary 4.8. — *Let F_s and F_{s+1} be quasi-canonical lifts of level s and $s+1$, respectively. Let $\beta : F_s \to F_{s+1}$ be an isogeny of height one. Then $H := \ker(\beta)$ is not the canonical subgroup, and*

$$v(\mathrm{Lie}(\beta)) = v(F_{s+1}).$$

Proof. — We note that β identifies F_{s+1} with the quotient F_s/H. It follows from the proof of Proposition 4.6 that H is not the canonical subgroup of F_s and that therefore the nonzero elements $x \in H$ have valuation

$$v(x) = \frac{v(F_s)}{q^2 - q}.$$

Set $b := \mathrm{Lie}(\beta)$. The formula for β in terms of H (see Theorem 2.1) shows that

$$v(b) = \sum_{x \in H - \{0\}} v(x) = \frac{v(F_s)}{q}.$$

By Corollary 4.7, this is equal to $v(F_{s+1})$. □

5. Some complements

We prove some technical results which are needed in [**R**].

5.1. Let K and k be as before. Let G be the formal $\mathcal{O}_K$-module of height two over k, with endomorphism ring $\mathcal{O}_D$. We have seen in [**VZ**] that the formal cohomology group $H^2(G,k)$ has dimension $h-1=1$. Therefore, the universal deformation ring of G is $W[[t]]$ (where $W = \hat{\mathcal{O}}_K^{\mathrm{nr}}$ is the completion of the maximal unramified extension of $\mathcal{O}_K$).

Let A be a complete local $\mathcal{O}_K$-algebra with residue field k and $I \lhd A$ an ideal with $\mathfrak{m}_A \cdot I = 0$. Set $\bar{A} := A/I$. Let F, F' be two deformations of G over A and $\bar{\alpha} : F \otimes \bar{A} \to F' \otimes \bar{A}$ a homomorphism which is defined modulo I. Then the obstruction for lifting $\bar{\alpha}$ to a homomorphism $\alpha : F \to F'$ is an element of the k-vector space

$$H^2(G, I) \cong H^2(G,k) \otimes_k I.$$

Indeed, as in [**VZ**, Section 3], a lift $\alpha(X) \in A[[X]]$ of $\bar{\alpha}$ as a power series defines a cocycle $(\Delta; \delta_a)$,

$$\Delta(X,Y) := \alpha(X +_F Y) -_{F'} \alpha(X) -_{F'} \alpha(Y),$$
$$\delta_a(X) := \alpha([a]_F(X)) -_{F'} [a]_{F'}(\alpha(X)).$$

The cohomology class of this cocycle is independent of the chosen lift α. It vanishes if and only if there exists some lift α which is a homomorphism $F \to F'$. If this is the case, then the lift which is a homomorphism is unique.

Let F be the universal deformation of G over $W[[t]]$, and let F' be another universal deformation over $W[[t']]$. Hence the pair (F, F') is defined over the formal scheme $\mathcal{S} = \mathrm{Spf}\, R$, where $R := W[[t,t']]$.

Proposition 5.1. — *Let $\alpha : G \to G$ be an isogeny,* i.e., $\alpha \neq 0$. *Let J be the minimal ideal of R such that α lifts to an isogeny $F \to F'$ modulo J. Then the closed formal subscheme $\mathcal{T}$ of $\mathcal{S}$ defined by J is a relative divisor over* $\mathrm{Spf}\, W$.

Proof. — We have to show that J is generated by one element which is neither a unit nor divisible by p. Suppose, for the moment, that $\alpha \notin \mathcal{O}_K$ and set $L = K(\alpha) \subset D$. Let M be the completion of the maximal unramified extension of L and F_1 the canonical lift of G with respect to $\mathcal{O}_L \subset \mathcal{O}_D$ (which is defined over $\mathcal{O}_M$). There is a unique homomorphism of $\mathcal{O}_K$-algebras $\varphi : W[[t,t']] \to \mathcal{O}_M$ which induces the identity on k, such that the pair (F_1, F_1) is $*$-isomorphic to the pullback of the pair (F, F') *via* φ. By construction, J is contained in the kernel of φ. This shows $J \neq R$, at least if $\alpha \notin K$. The case $\alpha \in K$ is handled in a similar way.

Suppose that $J \subset (\pi)$. This means that α lifts to an isogeny $F \to F'$ over $k[[t,t']]$. Setting $t' = 0$, the isogeny α would then induce an isogeny between $F \otimes_{W[[t]]} k((t))$ and $G \otimes_k k((t))$. But $F \otimes_{W[[t]]} k((t))$ has height $h - 1 = 1$ (see [**VZ**]) and is therefore not isogenous to the height-two module $G \otimes_k k((t))$. This gives a contradiction and shows that $J \not\subset (\pi)$.

Let $\mathfrak{m}$ denote the maximal ideal of R. Set $A := R/\mathfrak{m}J$ and $I := J/\mathfrak{m}J$. Then $\mathfrak{m} \cdot I = 0$, and $\bar{A} = A/I \cong R/J$. Clearly, α lifts to a homomorphism $F \otimes \bar{A} \to F' \otimes \bar{A}$ but *not* to a homomorphism $F \otimes A \to F' \otimes A$. The responsible obstruction is a nonzero element in

$$H^2(G, I) \cong H^2(G, k) \otimes_k I \cong I.$$

Let f be the image of this obstruction in I. The element f depends on the choice of an isomorphism $H^2(G,k) \cong k$, but the ideal $(f) \lhd A$ does not. Clearly, α lifts to a homomorphism $F \otimes A' \to F' \otimes A'$ over the ring $A' = A/(f)$. This implies $I = (f)$. Now Nakayama's Lemma shows that J is generated by one element. The proposition is proved. □

5.2. Let A be the ring of integers of a finite extension of the fraction field of W. Let λ denote a uniformizer of A. For each positive integer n, we set $A_n := A/(\lambda^{n+1})$ and $M_n := (\lambda^n)/(\lambda^{n+1})$.

Let F_1, F_2, F_3 be three lifts of G over A. We define

$$H_n := \mathrm{Hom}(F_1 \otimes A_n, F_2 \otimes A_n), \quad H'_n := \mathrm{Hom}(F_1 \otimes A_n, F_3 \otimes A_n).$$

As for endomorphisms, the natural reduction maps $H_n, H'_n \to \mathrm{End}(G) = \mathcal{O}_D$ are injective. We will consider H_n and H'_n as subsets of $\mathcal{O}_D$. Note that H_n and H'_n are in fact sub-$\mathcal{O}_K$-modules of $\mathcal{O}_D$. The obstruction theory reviewed above gives injective maps

$$\kappa_n : H_{n-1}/H_n \hookrightarrow H^2(G, M_n), \qquad \kappa'_n : H'_{n-1}/H'_n \hookrightarrow H^2(G, M_n).$$

Proposition 5.2. — *Let $\alpha : G \to G$ be an isogeny defined over k which does not lift to a homomorphism $F_1 \to F_2$. Let n be the unique positive integer such that $\alpha \in$*

$H_{n-1} - H_n$. Let $\beta : F_2 \to F_3$ be an isogeny defined over A, and let m denote the valuation of $b := \mathrm{Lie}(\beta) \in A$. We make the following assumptions:

1. *β has height one.*
2. *$m \le (q-1)n$.*

Then $\beta \circ \alpha \in H'_{n+m-1} - H'_{n+m}$.

Proof. — (compare with the proof of Lemma 1.3) We may represent α as a power series with coefficients in A without constant coefficient such that α_{n-1}, the reduction of α modulo λ^n, is a homomorphism $F_1 \otimes A_{n-1} \to F_2 \otimes A_{n-1}$. We define

$$\epsilon := \alpha \circ [\pi]_{F_1} -_{F_2} [\pi]_{F_2} \circ \alpha.$$

Then $\epsilon \equiv 0 \pmod{\lambda^n}$. Moreover, we have $\epsilon \equiv \delta_\pi \pmod{\lambda^{n+1}}$, where $(\Delta, \{\delta_a\})$ denotes the cocycle associated to α_n. The assumption $\alpha \notin H_n$ implies $\epsilon(X) = cX^q + \dots$, with $\mathrm{ord}_\lambda(c) = n$. Similarly, define

$$\epsilon' := \beta \circ \alpha \circ [\pi]_{F_1} -_{F_3} [\pi]_{F_3} \circ \beta \circ \alpha.$$

Then $\epsilon' = \beta \circ \epsilon$. Write $\beta(X) = \sum_i b_i X^i$. It follows from Assumption 1 that the Newton polygon of β has slope $-m/(q-1)$ over $[1, \dots, q]$. This means that

$$\mathrm{ord}_\lambda(b_i) \ge \frac{q-i}{q-1} \cdot m, \quad i = 1, \dots, q$$

(with equality for $i = 1, q$). Now Assumption 2, together with an easy calculation, shows that

$$\epsilon' = \beta \circ \epsilon = b_1 c X^q + \dots \equiv 0 \quad (\lambda^{n+m}).$$

Since $\mathrm{ord}_\lambda(b_1 c) = n + m$, we conclude as in the proof of Lemma 1.3 that $\beta \circ \alpha \in H'_{n+m-1} - H'_{n+m}$. □

Corollary 5.3. — *Suppose that F_1, F_2, F_3 are quasi-canonical liftings of G of level $r, s, s+1$ (with respect to some embedding $\kappa : L \hookrightarrow D$). Suppose that $r \le s$. Suppose, moreover, that A is the minimal $\mathcal{O}_K$-algebra over which the lifts F_1, F_2, F_3 can be defined. (By Theorem 3.2 and Corollary 4.7, A is the ring of integers of the ring class extension of $\mathcal{O}_{s+1}$.)*

Let $\alpha : G \to G$ be an element of $\mathcal{O}_D$ and $\beta : F_2 \to F_3$ an isogeny of height one, defined over A. We assume that α does not lift to a homomorphism $F_1 \to F_2$. Let n be the maximal integer such that α can be lifted to a homomorphism $F_1 \to F_2$ modulo λ^n. Then $\beta \circ \alpha$ can be lifted to a homomorphism $F_1 \to F_3$ modulo λ^{n+1}, but not *modulo λ^{n+2}.*

Proof. — It follows from Corollary 4.8 that $\mathrm{ord}_\lambda(\mathrm{Lie}(\beta)) = 1$. Hence we can apply Proposition 5.2, which proves the corollary. □

References

[D] V. G. Drinfel'd – Elliptic modules, *Math. USSR Sbornik* **23** (1974), no. 4, p. 561–592.

[G] B. H. Gross – On canonical and quasi-canonical liftings, *Invent. math.* **84** (1986), p. 321–326.

[H] M. Hazewinkel – *Formal groups and Applications*, Academic Press, 1978.

[HG] M. J. Hopkins & B. H. Gross – Equivariant vector bundles on the Lubin-Tate moduli space, in *Topology and representation theory (Evanston, IL, 1992)*, Contemp. Math., vol. 158, 1994, p. 23–88.

[L] J. Lubin – *Canonical subgroups of formal groups*, Trans. Amer. Math. Soc., vol. 251, 1979.

[LT1] J. Lubin & J. Tate – Formal complex multiplication in local fields, *Ann. Math.* **81** (1965), p. 380–387.

[LT2] ______, Formal moduli for one-parameter formal Lie groups, *Bull. Soc. Math. France* **94** (1966), p. 49–60.

[R] M. Rapoport – Deformations of isogenies of formal groups, this volume, p. 139–169.

[S] J.-P. Serre – *Corps locaux*, Hermann, 1968.

[VZ] E. Viehmann & K. Ziegler – Formal moduli of formal $\mathcal{O}_K$-modules, this volume, p. 57–66.

[Yu] J. K. Yu – On the moduli of quasi-canonical liftings, *Compositio Math.* **96** (1995), no. 3, p. 293–321.

S. Wewers, IWR, Im Neuenheimer Feld 368, 69120 Heidelberg, Germany
E-mail : stefan.wewers@iwr.uni-heidelberg.de