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 proofreading 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. □

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