*Astérisque*
**312**, 2007, p. 87–98

# 9. CANONICAL AND QUASI-CANONICAL LIFTINGS IN THE SPLIT CASE

*by*

Volker Meusers

***Abstract.*** — Following Gross we sketch a theory of quasi-canonical liftings when the formal $\mathcal{O}_K$-module of height two and dimension one is replaced by a divisible $\mathcal{O}_K$-module of height one and dimension one in the sense of Drinfel'd.

***Résumé* (Relèvements canoniques et quasi-canoniques dans le cas déployé).** — Suivant Gross, on donne une théorie de relèvements quasi-canoniques dans le cas où le $\mathcal{O}_K$-module de hauteur deux et de dimension un est remplacé par un $\mathcal{O}_K$-module divisible de hauteur un et de dimension un au sens de Drinfel'd.

In this paper, we follow up on a remark by Gross [**G**] and discuss a theory of quasi-canonical liftings when the formal $\mathcal{O}_K$-module of height two and dimension one considered in [**Ww1**] is replaced by a divisible $\mathcal{O}_K$-module of height one and dimension one in the sense of Drinfel'd [**D**]. In this situation the statements analogous to those in [**G**], [**Ww1**] are easy consequences of Lubin-Tate theory and of a slight modification of the Serre-Tate theorem for ordinary elliptic curves, as discussed in the appendix to [**Mes**].

## 1. Formal moduli of divisible $\mathcal{O}_K$-modules

Let $K$ be a field complete with respect to some discrete valuation. Let $\mathcal{O}_K$ be its ring of integers, $\mathfrak{p} = (\pi)$ its maximal ideal. We assume the residue field $\mathcal{O}_K/\mathfrak{p}$ to be finite and let $q$ denote the number of its elements. For any non-zero ideal $\mathfrak{a} \subset \mathcal{O}_K$ we set $N(\mathfrak{a}) := |\mathcal{O}_K/\mathfrak{a}|$, *i.e.*, $N(\mathfrak{p}^s) = q^s$. Let $k$ be an algebraic closure of $\mathcal{O}_K/\mathfrak{p}$. Let $M$ be the completion of the maximal unramified extension of $K$ in some fixed separable closure $K^{\mathrm{sep}}$. Denote the completion of $K^{\mathrm{sep}}$ by $C$. Let $\mathcal{O}_M$ and $\mathcal{O}_C$ be the rings of integers in $M$ and $C$ respectively.

Following [**D**, §4] a formal group is a group object in the category of formal schemes. For example any group scheme or any discrete group is a formal group in this sense.

**2000** ***Mathematics Subject Classification.*** — 11G15, 14K07, 14K22, 14L05.
***Key words and phrases.*** — Quasi-canonical liftings, complex multiplication, Lubin-Tate formal groups, Serre-Tate theorem.

For a formal group $F$ let us denote by $F^\circ$ its connected component. Let $\widehat{\mathcal{C}}$ be the category of complete local noetherian $\mathcal{O}_M$-algebras with residue field $k$.

***Definition 1.1***. — Let $R \in \widehat{\mathcal{C}}$. A divisible $\mathcal{O}_K$-module over $R$ is a pair $F$, where $F$ is a formal group over $R$ and $\gamma_F : \mathcal{O}_K \to \mathrm{End}_R(F)$ is a homomorphism such that $F^\circ$ is a formal $\mathcal{O}_K$-module of height $h < \infty$ in the sense of [**VZ**], and such that

$$F/F^\circ \cong (K/\mathcal{O}_K)^j_{\mathrm{Spf}(R)}$$

for some $j < \infty$. The pair $(h, j)$ will be called type of $F$.

To ease the notation, we will suppress the structure map $\gamma_F$ of an $\mathcal{O}_K$-module $F$ and simply write $F$.

Drinfel'd shows that a divisible $\mathcal{O}_K$-module over $k$ is up to isomorphism given by its type $(h, j)$ (see [**D**, §4]).

***Example 1.2***. — For $K = \mathbb{Q}_p$, $\mathcal{O}_K = \mathbb{Z}_p$ the product group $G = \widehat{\mathbb{G}}_{m,R} \times (\mathbb{Q}_p/\mathbb{Z}_p)_R$ is an example of a divisible module of type $(h, j) = (1, 1)$ over $R$.

If $R \in \widehat{\mathcal{C}}$ is artinian then the category of fppf-abelian sheaves on $R$ with $\mathcal{O}_K$-structure is an abelian category, the category of $\mathcal{O}_K$-modules over $R$. It is useful to view the category of divisible $\mathcal{O}_K$-modules over $R$ as a full sub-category of this category.

***Definition 1.3***. — Fix a divisible $\mathcal{O}_K$-module $G$ over $k$. A deformation of $G$ to $R \in \widehat{\mathcal{C}}$ is a pair $(F, \psi)$ consisting of a divisible $\mathcal{O}_K$-module $F$ over $R$ together with an isomorphism $\psi : F \otimes_R k \xrightarrow{\cong} G$ of $\mathcal{O}_K$-modules.

The deformations of $G$ to $R \in \widehat{\mathcal{C}}$ form a category in a natural way. One checks that it is a groupoid and moreover that no object of this groupoid has non-trivial automorphisms. The last point is due to the fact that for a deformation $F$ the isomorphism $\psi$ is part of the data. Nevertheless we often omit $\psi$ from the notation.

***Definition 1.4***. — For any $R \in \widehat{\mathcal{C}}$ let us denote by $\mathcal{D}_G(R)$ the set of isomorphism classes of the groupoid of deformations of $G$ to $R$. Then $\mathcal{D}_G$ becomes a set-valued functor on $\widehat{\mathcal{C}}$.

Fix a formal $\mathcal{O}_K$-module $H_0$ of height $h = 1$ over $k$. It has a trivial deformation space, *i.e.*, $\mathcal{D}_{H_0}(R) = \{\text{point}\}$ for any $R \in \widehat{\mathcal{C}}$. More precisely $\mathcal{D}_{H_0}$ is representable by $\mathcal{O}_M$. This follows easily from the uniqueness of Lubin-Tate modules (see [**Me1**]; see also Remark 1.11(ii) for a far more general result of Drinfel'd). Let us denote by $H$ the unique lift of $H_0$ to $\mathcal{O}_M$. We assume, as we may, that $H$ is given as the base change

$$H = H_f \otimes_{\mathcal{O}_K} \mathcal{O}_M,$$

where $H_f$ is the Lubin-Tate module over $\mathcal{O}_K$ corresponding to some fixed prime element $\pi \in \mathcal{O}_K$ and some fixed Lubin-Tate series $f \in \mathcal{F}_\pi$. Recall from [**Me1**, Lemma 1.7] that the isomorphism class of $H$ does not depend on these choices. Recall further that for any $R \in \widehat{\mathcal{C}}$ we have $H(R) = \mathfrak{m}_R$ as a set. The $\mathcal{O}_K$-module structure is given as follows: For $q, q' \in H(R)$ and $z \in \mathcal{O}_K$ we have $q +_H q' = H(q, q')$ and $z \cdot_H q = [z]_f(q)$. We often omit the subscript $H$ from the notation.

Now fix some divisible $\mathcal{O}_K$-module $G$ over $k$ of height $h = 1$ such that there is an isomorphism $G/G^\circ \cong (K/\mathcal{O}_K)_k$. Fix an isomorphism of divisible $\mathcal{O}$-modules

$$r \colon G \xrightarrow{\cong} H_0 \times (K/\mathcal{O}_K)_k$$

where $H$ is the unique lift of $G^\circ$ to $\mathcal{O}_M$ as above. Two such isomorphisms differ by an element of the automorphism group of the right hand side. This group is described by the following easy but important lemma.

***Lemma 1.5***

*(1) We have*

$$\mathrm{Hom}_{\mathcal{O}_K,k}((K/\mathcal{O}_K)_k, H_0) = \{0\} = \mathrm{Hom}_{\mathcal{O}_K,k}(H_0, (K/\mathcal{O}_K)_k)$$

*and*

$$\mathrm{End}_{\mathcal{O}_K,k}(H_0) = \mathcal{O}_K = \mathrm{End}_{\mathcal{O}_K,k}((K/\mathcal{O}_K)_k).$$

*(2) In particular there is a canonical isomorphism*

$$\mathcal{O}_K \times \mathcal{O}_K \longrightarrow \mathrm{End}_{\mathcal{O}_K,k}(H_0 \times (K/\mathcal{O}_K)_k).$$

*It induces an isomorphism*

$$\mathcal{O}_K^\times \times \mathcal{O}_K^\times \longrightarrow \mathrm{Aut}_{\mathcal{O}_K,k}(H_0 \times (K/\mathcal{O}_K)_k).$$

*Proof.* — It clearly suffices to prove the first point. We have

$$\mathrm{Hom}_{\mathcal{O}_K,k}((K/\mathcal{O}_K)_k, H_0) = \mathrm{Hom}_{\mathcal{O}_K}(K/\mathcal{O}_K, H_0(k)) = \{0\}$$

by adjunction and because $H_0(k) = \{0\}$. We have

$$\mathrm{Hom}_{\mathcal{O}_K,k}(H_0, (K/\mathcal{O}_K)_k) = \mathrm{Hom}_{\mathcal{O}_K,k}(H_0, (K/\mathcal{O}_K)_k^\circ) = \{0\}$$

because $H_0$ is connected and $(K/\mathcal{O}_K)^\circ = \{0\}$ . We have

$$\mathrm{End}_{\mathcal{O}_K,k}(H_0) = \mathcal{O}_K$$

because by Lubin-Tate theory every endomorphism of $H_0$ is uniquely given by its differential at zero. We have

$$\mathrm{End}_{\mathcal{O}_K,k}((K/\mathcal{O}_K)_k) = \mathrm{End}_{\mathcal{O}_K}(K/\mathcal{O}_K)$$

by adjunction. Since the natural map

$$\mathcal{O}_K \longrightarrow \mathrm{End}_{\mathcal{O}_K}(K/\mathcal{O}_K)$$

is well known to be an isomorphism we are done. □

We want to sketch a proof of the following theorem (compare the analogous statement in [**VZ**, Theorem 3.8]):

***Theorem 1.6* (Universal deformation).** — *For any $R \in \widehat{\mathcal{C}}$ and fixed isomorphism $r$ there is a natural isomorphism*

$$\eta_R \colon \mathcal{D}_G(R) \xrightarrow{\cong} H(R).$$

In particular $\mathcal{D}_G$ can be given the structure of an $\mathcal{O}_K$-module (depending on $r$ of course). Since we assume $H = H_f \otimes_{\mathcal{O}_K} \mathcal{O}_M$, the $\mathcal{O}_K$-module structure is given by Lubin-Tate theory as recalled above.

The proof will take up the rest of this section. One proceeds as in [**Mes**, appendix]: In the course of the proof we will identify both, $\mathcal{D}_G(R)$ and $H(R)$ for $R \in \widehat{\mathcal{C}}$ artinian, with a certain Ext-group. So let us briefly recall the definition and some basic properties of these groups. A careful discussion can be found in [**Mt**, chapter VII].

For objects $M''$ and $M'$ of an abelian category $\mathcal{A}$ let

$$\mathcal{E}xt_{\mathcal{A}}(M'', M')$$

denote the groupoid of extensions $(M, p, i) \colon M' \overset{i}{\hookrightarrow} M \overset{p}{\twoheadrightarrow} M''$. It is well known that the map

$$\begin{array}{ccc} \mathrm{Hom}_{\mathcal{A}}(M'', M') & \longrightarrow & \mathrm{Aut}_{\mathcal{E}xt_{\mathcal{A}}(M'', M')}((M, p, i)) \\ \varphi & \longmapsto & \mathrm{id}_M + i \circ \varphi \circ p \end{array}$$

is an isomorphism of groups. In particular the automorphism group of $(M, p, i)$ is trivial if and only if $\mathrm{Hom}_{\mathcal{A}}(M'', M')$ is. Let

$$\mathrm{Ext}_{\mathcal{A}}(M'', M')$$

be the class of isomorphism classes of $\mathcal{E}xt_{\mathcal{A}}(M'', M')$. Assume it to be a set. Sometimes we will not distinguish an extension from its isomorphism class. Using Baer-addition $\mathrm{Ext}_{\mathcal{A}}(M'', M')$ becomes an abelian group in the usual way. For $N' \in \mathcal{A}$ let

$$\delta_{(M,p,i),N'} \colon \mathrm{Hom}_{\mathcal{A}}(M', N') \longrightarrow \mathrm{Ext}_{\mathcal{A}}(M'', N'). \tag{1.1}$$

be the boundary homomorphism.

Apply this in the case that $\mathcal{A}$ is the category of $\mathcal{O}_K$-modules on some fixed artinian $R \in \widehat{\mathcal{C}}$. In this case the Ext-groups are in fact $\mathcal{O}_K$-modules.

***Definition 1.7.*** — Let $R \in \widehat{\mathcal{C}}$ be artinian. For any two $\mathcal{O}_K$-modules $M'$ and $M''$ over $R$ let

$$\mathrm{Ext}_{\mathcal{O}_K, R}(M'', M')$$

denote the $\mathcal{O}_K$-module of extension classes of $M''$ by $M'$ constructed above.

Recall that we view the category of divisible $\mathcal{O}_K$-modules on artinian $R$ as a full sub-category of the category of all $\mathcal{O}_K$-modules.

***Lemma 1.8*** (compare [**Mes**, I.2.4.3]). — *Let $R \in \widehat{\mathcal{C}}$ be artinian. Given an extension of the form*

$$H_R \overset{i}{\hookrightarrow} F \overset{p}{\twoheadrightarrow} (K/\mathcal{O}_K)_R$$

*of $\mathcal{O}_K$-modules over $R$, then $F$ is a divisible $\mathcal{O}_K$-module such that $F^\circ \cong H_R$ and $F/F^\circ \cong (K/\mathcal{O}_K)_R$. If one uses the isomorphism $r\colon G \xrightarrow{\cong} H_0 \times (K/\mathcal{O}_K)_k$ then $F$ becomes a deformation of $G$ to $R$. This association yields a functor between the groupoid of extensions of $(K/\mathcal{O}_K)_R$ by $H_R$ and the groupoid of deformations of $G$ to $R$.*

*Proof.* — Since $(K/\mathcal{O}_K)_R$ is totally disconnected and $H_R$ is connected it follows that $i\colon H_R \xrightarrow{\cong} F^\circ$. The snake lemma implies that $p$ induces an isomorphism $p'\colon F/F^\circ \xrightarrow{\cong} (K/\mathcal{O}_K)_R$. It follows that $F$ is divisible. Since $H_R(k) = \{0\}$ the extension $H_R \hookrightarrow F \twoheadrightarrow (K/\mathcal{O}_K)_R$ yields an injective map $F(k) \hookrightarrow (K/\mathcal{O}_K)_R(k) = K/\mathcal{O}_K$. Since $k$ is algebraically closed it is an isomorphism. This isomorphism gives us a canonical splitting map $(K/\mathcal{O}_K)_k \hookrightarrow F \otimes k$. Thus the extension is canonically split over $k$. Together with the identification $r\colon G \xrightarrow{\cong} H_0 \times (K/\mathcal{O}_K)_k$ we get an isomorphism $\psi\colon F \otimes k \xrightarrow{\cong} G$ such that the pair $(F, \psi)$ is a deformation of $G$. One checks that it is functorial. □

***Proposition 1.9*** (compare [**Mes**, appendix Prop.2.1]). — *Assume $R \in \widehat{\mathcal{C}}$ to be artinian. Then the functor of the preceding lemma is an equivalence of groupoids and there is a natural isomorphism*

$$\epsilon_R\colon \mathcal{D}_G(R) \xrightarrow{\cong} \mathrm{Ext}_{\mathcal{O}_K,R}((K/\mathcal{O}_K)_R, H_R).$$

*Proof.* — fully faithful: It is enough to see that every object in either groupoid has a trivial automorphism group. For deformations, this was noted above. For extensions, recall that the automorphism group is isomorphic to $\mathrm{Hom}_{\mathcal{O}_K,R}((K/\mathcal{O}_K)_R, H_R) = \{0\}$.

essentially surjective: Let $F$ be a deformation of $G$ to $R$. We need to define homomorphisms $i\colon H_R \hookrightarrow F$ and $p\colon F \twoheadrightarrow (K/\mathcal{O}_K)_R$ such that $p \circ i = 0$. For this we let $p$ on $R$-valued points be defined as follows :

$$F(R) \twoheadrightarrow F(k) = F \otimes k(k) \xrightarrow[r\circ\psi]{\cong} H_0(k) \times (K/\mathcal{O}_K)_k(k) \underset{\mathrm{pr}_2}{\twoheadrightarrow} K/\mathcal{O}_K = (K/\mathcal{O}_K)_R(R).$$

Since $K/\mathcal{O}_K$ is discrete the kernel of $p$ equals $F^\circ$. Because $R$ is artinian local it follows that $F^\circ \otimes k = (F \otimes k)^\circ \cong G^\circ \cong H_0$. Since $H_R$ is the unique lift of $H_0$ to $R$ it follows that $F^\circ$ is isomorphic to $H_R$ and we get the map $i\colon H_R \cong F^\circ \hookrightarrow F$. This proves the first assertion. The second follows by passage to isomorphism classes. □

To calculate the Ext-group, we use

***Proposition 1.10***. — *For any artinian $R \in \widehat{\mathcal{C}}$ the connecting homomorphism associated to the sequence $\mathcal{O}_K \hookrightarrow K \twoheadrightarrow K/\mathcal{O}_K$ is an isomorphism*

$$\delta_R\colon H(R) = \mathrm{Hom}_{\mathcal{O}_K,R}(\mathcal{O}_K, H_R) \xrightarrow{\cong} \mathrm{Ext}_{\mathcal{O}_K,R}((K/\mathcal{O}_K)_R, H_R).$$

*Proof.* — Assume $\mathfrak{m}_R^{n+1} = 0$ for some $n >> 0$. Then $H$ is killed by $\mathfrak{p}^n$ (compare [**K**, Lemma 1.1.2]). Associated to the short exact sequence

$$(\mathcal{O}_K)_R \overset{i}{\hookrightarrow} K_R \overset{p}{\twoheadrightarrow} (K/\mathcal{O}_K)_R$$

and $H_R$ we have the boundary map (1.1)

$$\delta_{(K_R,p,i),H_R} \colon \mathrm{Hom}_{\mathcal{O}_K,R}((\mathcal{O}_K)_R, H_R) \longrightarrow \mathrm{Ext}_{\mathcal{O}_K,R}((K/\mathcal{O}_K)_R, H_R).$$

If we identify $H(R)$ with $\mathrm{Hom}_{\mathcal{O}_K,R}((\mathcal{O}_K)_R, H_R)$ this gives us the desired map $\delta_R$. Because the prime element $\pi \in \mathcal{O}_K$ acts invertibly on $K$ and nilpotently on $H$ one sees easily that

$$\mathrm{Hom}_{\mathcal{O}_K,R}(K, H) = \{0\} = \mathrm{Ext}_{\mathcal{O}_K,R}(K, H).$$

By the exactness of the long Ext-sequence, it follows that $\delta_R$ is an isomorphism. □

*Proof of Theorem 1.6.* — Combining Proposition 1.9 and Proposition 1.10 we get the desired isomorphism for artinian $R \in \widehat{\mathcal{C}}$ as

$$\eta_R = \delta_R^{-1} \circ \epsilon_R.$$

For general $R$ we can pass to the limit over its artinian quotients. □

***Remark 1.11***

(i) How does one calculate the inverse of $\delta_R$? For $R = k$ both sides are trivial and so is $\delta_k$. In the general case $\delta_R^{-1}$ can be computed by an approximation process with respect to the "$\mathfrak{p}$-adic topology" on both $\mathrm{Ext}_{\mathcal{O}_K,R}(\mathcal{O}_K, H_R)$ and $H(R)$. For details we refer to [**K**, page 151f], [**Mes**, appendix].

(ii) In particular it follows from this theorem that the formal moduli space of the divisible module $G = H_0 \times (K/\mathcal{O}_K)_k$ is representable by a formal power series ring in one variable over $\mathcal{O}_M$. More generally, Drinfel'd shows that the formal moduli space of a divisible module of type $(h, j)$ over $k$ is representable by a power series ring in $h + j - 1$ variables (compare [**D**, Prop.4.5]).

***Definition 1.12***. — For $R \in \widehat{\mathcal{C}}$ and fixed $r$, let $F$ be a lift of $G$ to $R$. Let us set

$$q(F, r) = \eta_R(\text{ isom. class of } F) \in H(R).$$

We simply write $q(F)$ if $\gamma_F$ and $r$ are understood. As in [**Ww1**], Definition 4.1 we refer to the element $q(F) \in H(R) = \mathfrak{m}_R$ as the formal modulus or coordinate of the lift $F$.

***Example 1.13***. — If $K = \mathbb{Q}_p$, $\mathcal{O}_K = \mathbb{Z}_p$, and $H = \widehat{\mathbb{G}}_m$ we are in the situation of [**Mes**], Appendix. If we let $q_{\mathrm{Tate}}(F) \in 1 + \widehat{\mathbb{G}}_m(R)$ denote the coordinate introduced in [**Mes**], then the relations are simply

$$q_{\mathrm{Tate}}(F) = 1 + q(F) \in 1 + \widehat{\mathbb{G}}_m(R).$$

and

$$q_{\mathrm{Tate}}(F)^z = (1 + q(F))^z = 1 + z \cdot_{\widehat{\mathbb{G}}_m} q(F).$$

## 2. Lifting endomorphisms

Let $F$ and $F'$ be deformations of $G$ to $R$ with coordinates $q = q(F), q' = q(F') \in H(R)$. We want to describe in terms of our chosen coordinates which endomorphisms $\rho_0 \in \mathrm{End}_{\mathcal{O}_K,R}(G)$ lift to homomorphisms $\rho\colon F \to F'$.

***Proposition 2.1*** (compare [**Mes**, Appendix Prop.3.3]). — *Let $\rho_0\colon F_0 \to F_0'$ be given by multiplication by $z_1$ on $(K/\mathcal{O}_K)_R$ and by multiplication by $z_0$ on $H(R)$. Then $\rho_0$ lifts to a (necessarily unique) homomorphism $\rho\colon F \to F'$ if and only if we have the equality*

$$z_1 q - z_0 q' = 0 \in H(R),$$

*where the last expression is more precisely written as $[z_1]_H(q) -_H [z_0]_H(q')$.*

*Sketch of proof.* — This follows from rigidity (see [**VZ**, Lemma 2.6], for formal $\mathcal{O}_K$-modules), the description of lifts in terms of extensions and the following well known and simple lemma applied to $M' = N' = H$, $M'' = N'' = K/\mathcal{O}_K$ and $\varphi = z_1$ and $\psi = z_0$. □

***Lemma 2.2*** (compare [**CE**, chap.XIV, exercise 18]). — *Let*

$$\begin{tikzcd} M' \arrow[r, tail, "i"] \arrow[d, "\varphi"'] & M \arrow[r, two heads, "p"] & M'' \arrow[d, "\psi"] \\ N' \arrow[r, tail, "i'"'] & N \arrow[r, two heads, "p'"'] & N'' \end{tikzcd}$$

*be a commutative diagram in an arbitrary abelian category. Then it can be completed by a homomorphism $\rho\colon M \to N$ if and only if the extension obtained by pushing out the upper sequence along $\varphi$ is isomorphic to the extension obtained by pulling back the lower sequence along $\psi$.*

***Example 2.3***. — For reasons explained above (see [**Me1**, Example 1.3]), the analogous formula of [**Mes**], Appendix reads:

$$(q_{\mathrm{Tate}})^{z_1}(q'_{\mathrm{Tate}})^{-z_0} = (1+q)^{z_1}(1+q')^{-z_0} = 1 + (z_1 q -_{\widehat{\mathbb{G}}_m} z_0 q') = 1.$$

Specialize to $R = \mathcal{O}_C$. As a consequence of proposition (1.9) we can describe the ring of endomorphisms of a lift $F$ of $F_0$ to $\mathcal{O}_C$.

***Corollary 2.4***. — *Let $F$ be a lift $F$ of $G$ to $\mathcal{O}_C$ with $q = q(F,r) \in H(\mathcal{O}_C)$. Then there are two cases:*

*(i) If the annihilator of $q$ in $\mathcal{O}_K$ is zero then the endomorphism ring of $F$ equals $\mathcal{O}_K$.*

*(ii) If the annihilator of $q$ in $\mathcal{O}_K$ is $\mathfrak{p}^s$ for some $0 \le s < \infty$ then the endomorphism ring of $F$, as a subring of the ring of endomorphisms of $G$, is strictly bigger then $\mathcal{O}_K$ and is isomorphic to*

$$\mathrm{End}_{\mathcal{O}_K,\mathcal{O}_C}(F) \cong \{(z_0, z_1) \in \mathcal{O}_K \times \mathcal{O}_K | z_0 - z_1 \in \mathfrak{p}^s\} \subseteq \mathcal{O}_K \times \mathcal{O}_K.$$

*Proof.* — This follows directly from the proposition with $q = q'$. Note that in this case

$$(z_1 \cdot_H q) -_H (z_0 \cdot_H q) = (z_1 - z_0) \cdot_H q = 0 \in H(R). \quad \square$$

## 3. Quasi-canonical lifts in the split case

We now show that the results on canonical and quasi-canonical liftings in [**Ww1**] and [**G**] have analogues in the present case. To bring out this analogy we introduce the following definitions:

***Definition 3.1***
(i) Set $L = K \times K$ and $\mathcal{O}_L = \mathcal{O}_K \times \mathcal{O}_K$. Embed $K$ resp. $\mathcal{O}_K$ diagonally into $L$ resp. $\mathcal{O}_L$.

(ii) From Lemma 1.5 we get an $\mathcal{O}_K$-linear isomorphism

$$\kappa\colon \mathcal{O}_L \xrightarrow{\cong} \mathrm{End}_{\mathcal{O}_K,k}(G).$$

(iii) The "completion of the maximal unramified extension" of $L$ is given by $M_L = M \times M$ whose "separable closure" is $M_L^{\mathrm{sep}} = M^{\mathrm{sep}} \times M^{\mathrm{sep}}$.

(iv) Set

$$\Gamma_L = \mathrm{Gal}(M_L^{\mathrm{sep}}|M_L) = \mathrm{Gal}(M^{\mathrm{sep}}|M) \times \mathrm{Gal}(M^{\mathrm{sep}}|M).$$

By Lubin-Tate theory we have a reciprocity isomorphism

$$\rho_K^{\mathrm{ab}}\colon\ \mathrm{Gal}(M^{\mathrm{sep}}|M)^{\mathrm{ab}} \xrightarrow{\cong} \mathcal{O}_K^\times.$$

It induces a reciprocity isomorphism

$$\rho_L^{\mathrm{ab}} = (\rho_K^{\mathrm{ab}}, \rho_K^{\mathrm{ab}})\colon \Gamma_L^{\mathrm{ab}} \xrightarrow{\cong} \mathcal{O}_L^\times.$$

(v) For any integer $s \geq 0$ let

$$\mathcal{O}_s = \mathcal{O}_K + \mathfrak{p}^s\mathcal{O}_L = \{(z_0, z_1) \in \mathcal{O}_L | z_0 - z_1 \in \mathfrak{p}^s\}$$

be the "order" containing $\mathcal{O}_K$ of conductor $\mathfrak{p}^s$ or level $s$ in $\mathcal{O}_L$.

(vi) For $s \geq 1$ let $M_s|M$ be the fixed field in $M^{\mathrm{sep}}$ of the inverse image under the reciprocity isomorphism $\rho_K^{\mathrm{ab}}$ of $(1+\mathfrak{p}^s) \subset \mathcal{O}_K^\times$ in $\mathrm{Gal}(M^{\mathrm{sep}}|M))$, *i.e.*, such that reciprocity gives an isomorphism

$$\rho_K^{\mathrm{ab}}\colon\ \mathrm{Gal}(M_s|M) \xrightarrow{\cong} \mathcal{O}_K^\times/(1+\mathfrak{p}^s).$$

***Remark 3.2***. — One easily sees that the map $\mathcal{O}_L^\times \to \mathcal{O}_K^\times$ given by sending $(x, y) \in \mathcal{O}_L^\times$ to the quotient $xy^{-1} \in \mathcal{O}_K^\times$ induces an isomorphism

$$\mathcal{O}_L^\times/\mathcal{O}_s^\times \xrightarrow{\cong} \mathcal{O}_K^\times/(1+\mathfrak{p}^s).$$

If we let $\Gamma_s \subset \Gamma_L^{\mathrm{ab}}$ be the inverse image of $\mathcal{O}_s^\times$ in $\Gamma_L^{\mathrm{ab}}$ under $\rho_L^{\mathrm{ab}}$, then we have the following commutative diagram

$$\begin{tikzcd}
\Gamma_L^{\mathrm{ab}} \arrow[r, "\rho_L^{\mathrm{ab}}", "\cong"'] \arrow[d, two heads] & \mathcal{O}_L^\times \arrow[d, two heads] \\
\Gamma_L^{\mathrm{ab}}/\Gamma_s \arrow[r, "\cong"] \arrow[d, "(\sigma,\tau)\mapsto\sigma\tau^{-1}"', "\cong"] & \mathcal{O}_L^\times/\mathcal{O}_s^\times \arrow[d, "\cong"', "(x,y)\mapsto xy^{-1}"] \\
\mathrm{Gal}(M_s|M) \arrow[r, "\cong"'] & \mathcal{O}_K^\times/(1+\mathfrak{p}^s)
\end{tikzcd}$$

where "$\cong$" denotes isomorphisms. In this sense we may consider $M_s|M$ to be the "ring class field" of the "order" $\mathcal{O}_s \subseteq \mathcal{O}_L$.

***Definition 3.3***. — A quasi-canonical lift of $G$ of level $s \geq 0$ ( with respect to $\kappa$) is a lift $F$ of $G$ to $\mathcal{O}_C$ already defined over the ring of integers of some finite extension of $M$, together with an $\mathcal{O}_K$-algebra isomorphism $\mathcal{O}_s \xrightarrow{\cong} \mathrm{End}_{\mathcal{O}_K,\mathcal{O}_C}(F')$. A quasi-canonical lift of level $s = 0$ is also called canonical.

***Proposition 3.4*** **(compare [Ww1, §1.3])**. — *Let $F$ be a lift of $G$. Then the following statements are equivalent:*

*(1) The lift $F$ is canonical,* i.e., *defined over some finite extension of $M$ and such that* $\mathrm{End}_{\mathcal{O}_K,\mathcal{O}_C}(F) = \mathrm{End}_{\mathcal{O}_K,k}(G) \cong \mathcal{O}_K \times \mathcal{O}_K$.

*(2) The lift $F$ is isomorphic to $H_{\mathcal{O}_M} \times (K/\mathcal{O}_K)_{\mathcal{O}_M}$.*

*In particular there exists a canonical lift and it is unique up to unique isomorphism. The formal modulus of a canonical lift $F_{can}$ is $q(F_{can}) = 0$ and thus independent of the chosen isomorphism $r$.*

*Proof.* — Clearly, the lift $F = H_{\mathcal{O}_M} \times (K/\mathcal{O}_K)_{\mathcal{O}_M}$ is canonical. To show that any canonical lift is isomorphic to the product, note that the endomorphism ring of a canonical lift contains the images $e_{\mathrm{inf}}$ and $e_{\mathrm{et}}$ of $(1,0) \in \mathcal{O}_L$ and $(0,1) \in \mathcal{O}_L$. They satisfy $e_{\mathrm{inf}}^2 = e_{\mathrm{et}}^2 = 1$ and $e_{\mathrm{inf}} + e_{\mathrm{et}} = 1$ and hence define a splitting

$$F \cong \mathrm{Im}(e_{\mathrm{inf}}) \times \mathrm{Im}(e_{\mathrm{et}})$$

as claimed. Given two canonical lifts, the element $(1,1) \in \mathcal{O}_L$ induces a canonical isomorphism. For the last claim simply observe that the split extension is the image of $0 \in H(\mathcal{O}_C)$ under $\delta_{\mathcal{O}_C}$ by construction. □

***Proposition 3.5*** **(compare [Ww1, §3] and [G, Prop.5.3])**

*(1) Quasi-canonical liftings $F_s$ exist for all levels $s \geq 0$.*

*(2) Liftings of level $s$ are rational over the ring of integers $\mathcal{O}_{M_s}$ of $M_s$. Their isomorphism classes are permuted simply transitively under the action of the Galois group*

$$\mathrm{Gal}(M_s|M) \cong \mathcal{O}_L^\times/\mathcal{O}_s^\times \cong (\mathcal{O}_L/\mathfrak{p}^s\mathcal{O}_L)^\times/(\mathcal{O}_K/\mathfrak{p}^s)^\times$$

*which has order*

$$|\operatorname{Gal}(M_s|M)| = \begin{cases} q^s\left(1-\frac{1}{q}\right) & : \quad s \geq 1 \\ 1 & : \quad s = 0 \end{cases}$$

*In particular $M_s$ is the smallest extension of $M$ over which a quasi-canonical lift can be defined.*

*(3) The formal modulus $q(F_s) \in H(\mathcal{O}_{M_s}) = H(\mathcal{O}_C)$ of a quasi-canonical lift of level $s$ is a uniformizing element of $\mathcal{O}_{M_s}$. In particular, for $s \geq 1$ the $\mathcal{O}_K$-modules $F_s$ and $F_{can}$ are not isomorphic over $\mathcal{O}_{M_s}/\mathfrak{m}_{M_s}^2$.*

*Proof.* — For the first point recall that it follows from Lubin-Tate theory that $H(\mathcal{O}_C)_{\text{torsion}} \cong K/\mathcal{O}_K$ as $\mathcal{O}_K$-modules. Thus there are elements $q_s \in H(\mathcal{O}_C)$ with annihilator $\mathfrak{p}^s$ for any given $s \geq 0$. This implies the existence of a lift $F_s/\mathcal{O}_C$ with formal modulus $q_s$. By Corollary 2.4 the endomorphism ring of $F_s$ is isomorphic to $\mathcal{O}_s$. If $s = 0$ then $F_{can} = H \times K/\mathcal{O}_K$ is a canonical lift and it is clearly defined over $M$. If $s \geq 1$ then the stabilizer of the formal modulus $q_s$, *i.e.*, $1 + \operatorname{Ann}(q_s)$, equals $1 + \mathfrak{p}^s \subset \mathcal{O}_K^\times$. Thus again by Lubin-Tate theory its isomorphism class is stable under the Galois group $\operatorname{Gal}(M^{\text{sep}}|M_s)$ since the identification of $\mathcal{D}_{F_0}(\mathcal{O}_C)$ with $H(\mathcal{O}_C)$ is compatible with the action of $\operatorname{Gal}(M^{\text{sep}}|M)$. Since deformations have no non-trivial automorphisms, this induces a Galois action on the chosen lift $F_s/\mathcal{O}_C$ itself. It follows that $F_s$ descends to a formal $\mathcal{O}_K$-module over $\mathcal{O}_{M_s} = \mathcal{O}_C \cap M_s$.

For the second point note that the first isomorphism follows from Remark 3.2. One checks easily that the natural map

$$\mathcal{O}_L^\times/\mathcal{O}_s^\times \longrightarrow (\mathcal{O}_L/\mathfrak{p}^s\mathcal{O}_L)^\times/(\mathcal{O}_K/\mathfrak{p}^s)^\times$$

is an isomorphism. For $s \geq 1$ it follows from Lubin-Tate theory that

$$|\mathcal{O}_K^\times/1+\mathfrak{p}^s| = N(\mathfrak{p})^{s-1}(N(\mathfrak{p})-1) = |\operatorname{Gal}(M_s|M)|$$

as claimed .

The last point also follows from Lubin-Tate theory (see [**Me1**]), for one knows that $N_{M_s|M}(-q_s) = \pi$ and hence

$$v_{M_s|M}(q_s) = \frac{1}{[M_s:M]} v_M(N_{M_s|M}(q_s)) = \frac{1}{[M_s:M]}$$

as claimed. Therefore $q_s \in \mathfrak{m}_{M_s} \backslash \mathfrak{m}_{M_s}^2$ for $s \geq 1$. But the canonical lift has formal modulus $q_{can} = 0 \in \mathfrak{m}_{M_s}^2$. It follows that $q_s \not\equiv q_{can} \bmod \mathfrak{m}_{M_s}^2$. □

***Remark 3.6***

(i) The degree formula in the proposition can be written in a uniform way as

$$|\operatorname{Gal}(M_s|M)| = N(\mathfrak{p}^s) \prod_{\mathfrak{l}|\mathfrak{p}^s} \left(1 - \left(\frac{L}{\mathfrak{l}}\right)\frac{1}{N(\mathfrak{l})}\right)$$

where one formally sets

$$\left(\frac{L}{\mathfrak{l}}\right) = +1, -1, 0$$

according as $\mathfrak{l} = \mathfrak{p}$ is split (our case), inert or ramified (the cases treated in [**Ww1**]) in the extension $L|K$.

(ii) Let $E_0$ be an ordinary elliptic curve over $\overline{\mathbb{F}}_p$. Then one knows that its endomorphism ring is isomorphic to some order $\mathcal{O} \subset L$ in some imaginary quadratic field $L$. Let $c_0 \in \mathbb{Z}$ be the conductor of $\mathcal{O}$. It is known that $p$ does not divide $c_0$. Set $c_s = p^s c_0$ and $\mathcal{O}_s = \mathbb{Z} + p^s\mathcal{O}$. Let $M_s|L$ be the ring class field of the order $\mathcal{O}_s$. For example if $c_0 = 1$ and $s = 0$ then $M_s = M$ is the Hilbert class field of $L$, *i.e.*, the maximal unramified abelian extension of $L$. In this situation one has Deuring's lifting theorem (compare [**L**, chap.13,§4,§5]). It guarantees the existence of an elliptic curve $E_s$ over $M_s$ with complex multiplication by $\mathcal{O}_s$ and such that the reduction of $E_s$ at some prime of degree one over $p$ is isomorphic to $E_0$ (same notational conflict as in the local case). The $j$-invariants of the different curves $E_s$ are permuted simply transitively by the Galois group $\mathrm{Gal}(M_s|M)$. By the well known formula for the class numbers of orders in imaginary quadratic fields (see [**S**, exercise 4.12]) the Galois group has order

$$|\operatorname{Gal}(M_s|M)| = \frac{h(\mathcal{O}_s)}{h(\mathcal{O})} = \frac{|\mathcal{O}_s^\times|}{|\mathcal{O}^\times|} \cdot \frac{c_s}{c_0} \prod_{l|\frac{c_s}{c_0}} \left(1 - \left(\frac{L}{l}\right)\frac{1}{l}\right).$$

where the symbol $\left(\frac{L}{l}\right)$ is defined as in (i). The extra factor $\frac{|\mathcal{O}_s^\times|}{|\mathcal{O}^\times|}$ is due to the presence of nontrivial automorphisms in this situation. It is trivial for $L \neq \mathbb{Q}(i)$, $\mathbb{Q}(e^{\frac{2\pi i}{3}})$. This statement of a global nature is thus completely analogous to the local statement of Proposition 3.5.

## References


[CE] H. Cartan & S. Eilenberg – *Homological algebra*, 1956.

[D] V. G. Drinfel'd – Elliptic modules, *Math. USSR, Sb.* **23** (1974), p. 561–592.

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

[K] N. Katz – Serre-Tate local moduli, in *Surfaces algebriques, Sémin. de géométrie algébrique, Orsay 1976-78*, Springer Lect. Notes Math., vol. 868, 1981, p. 138–202.

[L] S. Lang – *Elliptic functions*, Addison-Wesley, 1973.

[Mes] W. Messing – *The crystals associated to Barsotti-Tate groups: with applications to Abelian schemes*, Springer Lect. Notes Math., vol. 264, 1972.

[Me1] V. Meusers – Lubin-Tate formal groups, this volume, p. 49–55.

[Mt] B. Mitchell – *Theory of categories*, 1965.

[S] G. Shimura – *Introduction to the arithmetic theory of automorphic functions*, Princeton Univ. Press, 1971.

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

[Ww1] S. Wewers – Canonical and quasi-canonical liftings, this volume, p. 67–86.

V. Meusers, Mathematisches Institut der Universität Bonn, Beringstr. 1, 53115 Bonn, Germany
*E-mail :* meusers@math.uni-bonn.de