Classification of integral models of $(\mathbb{Z}/p^2\mathbb{Z})_K$ via Breuil-Kisin theory

Appendix to [4]

by Xavier Caruso[1]

In this appendix, we show how the theory presented by Breuil in [1] and developed by Kisin in [2] and [3] gives us the possibility to obtain very quickly a analogue statement to Corollary 3.50 of [4]. Although our approach is certainly more efficient, it has at least two defects. First, it forces us to assume R complete and its residue field perfect. Therefore, the situation that we will considerer in this appendix is slightly less general than the one discussed in the paper. Second, we do not obtain an explicit description of models of $(\mathbb{Z}/p^2\mathbb{Z})_K$, but instead we describe some objects of linear algebra which correspond to these models through Breuil-Kisin theory.

Statement of the main theorem. Let us fix notation. Let p be a prime number (not necessarily odd) and k a perect field of characteristic p. We denote by $W = W(k)$ (resp. $W_n = W_n(k)$) the ring of Witt vectors (resp. of truncated Witt vectors) with coefficients in k and K_0 its fraction field of W. For any integer n, $W_n[[u]]$ is endowed with a continuous (for the u-adic topology) rings endomorphism ϕ defined as the usual Frobenius on W_n and by $\phi(u) = u^p$. Let's fix a totally ramified extension K of K_0 of degree e and an uniformizer π of K. We denote by $E(u)$ the minimal polynomial of π over K_0 and R the ring of integers of K. This one corresponds to the d.v.r. considered as base ring in Tossici's paper.

Let $\mathrm{Mod}^{\phi}_{/W_2[[u]]}$ denote the following category:

- objects are $W_2[[u]]$-modules $\mathfrak{M}$ with no u-torsion endowed with a continuous (for the u-adic topology) ϕ-semi-linear endomorphism (called Frobenius) $\phi_{\mathfrak{M}} : \mathfrak{M} \to \mathfrak{M}$ whose image generates a sub-module containing $E(u)\mathfrak{M}$;
- morphisms are the $W_2[[u]]$-linear maps which commute with Frobenius.

In [2] and [3], Kisin have constructed an anti-equivalence of categories between $\mathrm{Mod}^{\phi}_{/W_2[[u]]}$ and the category of finite, flat and commutative R-group schemes annihilated by p^2. For our aims, an important property of the latter anti-equivalence will be the following: if $\mathfrak{M}$ is the object of $\mathrm{Mod}^{\phi}_{/W_2[[u]]}$ associated to a group scheme G, then $\mathfrak{M}[1/u]$ completely determines the Galois representation $G(\bar{K})$ (where $\bar{K}$ is an algebraic closure of K), *i.e.* the generic fiber of G. From this fact, it is easy to prove that G is a model of $(\mathbb{Z}/p^2\mathbb{Z})_K$ if and only if $\mathfrak{M}[1/u]$ is isomorphic to $W_2((u))$ endowed with the usual Frobenius. We are going to prove the following result, which is the exact analogue in our context of Corollary 3.50 of [4].

Theorem 1. *Let $\mathfrak{M}$ be the object $Mod^{\phi}_{/W_2[[u]]}$ associated to a finite flat R-group scheme whose generic fiber is isomorphic to $(\mathbb{Z}/p^2\mathbb{Z})_K$. Then, there exist $n, m \in \mathbb{N}$, $a \in k[[u]]$ satisfying $\frac{e}{p-1} \geq m \geq n \geq 0$ and*

$$\phi(a) \equiv 0 \pmod{u^n} \tag{1}$$

$$u^{e-m(p-1)}\phi(a) - u^e a \equiv F(u)u^m \pmod{u^{pn}} \tag{2}$$

together with two elements e_1 and e_2 in $\mathfrak{M}$ such that:

i) *$\mathfrak{M}$ is generated over $W_2[[u]]$ by e_1 and e_2 with the unique relation $u^{m-n}e_1 = pe_2$;*

ii) *Frobenius is given by $\phi(e_1) = u^{n(p-1)}e_1$ and $\phi(e_2) = u^{m(p-1)}e_2 + \big[u^{-n}\phi(a) - u^{m(p-1)-n}a\big]e_1$.*

Furthermore n, m and $(a \mod u^n)$ are uniquely determined by the isomorphism class of $\mathfrak{M}$.

Conversely, any triple (n, m, a) satisfying (1) and (2) comes from a finite flat R-group scheme whose generic fiber is isomorphic to $(\mathbb{Z}/p^2\mathbb{Z})_K$.

The last assertion of the Theorem is easy: one just need to check that the ϕ-module $\mathfrak{M}$ defined by conditions i) and ii) is actually an object of $\mathrm{Mod}^{\phi}_{/W_2[[u]]}$. From now on, we concentrate ourselves to the proof of the rest of the Theorem.

[1]IRMAR, Université de Rennes 1, Campus de Beaulieu, 35042 Rennes Cedex, France
Email address: xavier.caruso@normalesup.org

Proof of existence. Let $\mathfrak{M}$ be a ϕ-module over $W_2[[u]]$ such that $\mathfrak{M}[1/u]$ is isomorphic to $W_2((u))$ endowed with the usual Frobenius. Let us denote by $\mathfrak{M}_1$ the kernel of the multiplication by p on $\mathfrak{M}$ and $\mathfrak{M}_2 = \mathfrak{M}/\mathfrak{M}_1$. It is easy to verify that they are both modules over $W_1[[u]] = k[[u]]$ with no u-torsion. Moreover they inherit endomorphisms $\phi_{\mathfrak{M}_1}$ and $\phi_{\mathfrak{M}_2}$ whose images still generate a module which contains $E(u)\mathfrak{M}_1 = u^e\mathfrak{M}_1$ and $E(u)\mathfrak{M}_2 = u^e\mathfrak{M}_2$ respectively. In the following, we will write ϕ for $\phi_{\mathfrak{M}}$, $\phi_{\mathfrak{M}_1}$ and $\phi_{\mathfrak{M}_2}$.

Lemma 2. *The module $\mathfrak{M}_1$ is free of rank 1 over $k[[u]]$. Moreover, there exists a base (e_1) of $\mathfrak{M}_1$ and an integer $n \in [0, \frac{e}{p-1}]$ such that $\phi(e_1) = u^{n(p-1)}e_1$.*

Proof. Since $k[[u]]$ is a discrete valuation ring, the fact that $\mathfrak{M}_1$ has no u-torsion implies that its freeness. Moreover, it is certainly of rank 1 because $\mathfrak{M}_1[1/u]$ is isomorphic to the kernel of the multiplication by p on $W_2((u))$, that is $k((u))$. Let x be any basis of $\mathfrak{M}_1$. From above it follows that we can consider it as an element of $k((u))$. We can write $x = u^n y$ where y is invertible in $k[[u]]$. Then, if we set $e_1 = u^n$, it is a basis of $\mathfrak{M}_1$ and we have $\phi(e_1) = u^{np} = u^{n(p-1)}e_1$ as expected. □

In the same way it is possible to prove that $\mathfrak{M}_2 = k[[u]]\bar{e}_2$ with $\phi(\bar{e}_2) = u^{m(p-1)}\bar{e}_2$ for some integer $m \in [0, \frac{e}{p-1}]$. Let $e_2 \in \mathfrak{M}$ be any lifting of $\bar{e}_2$. Clearly it is a generator of $\mathfrak{M}[1/u]$ as $W_2((u))$-module. We deduce that

$$e_1 = pu^{-\delta}\alpha e_2 \tag{3}$$

where δ is an integer and α is invertible in $W_2[[u]]$. In fact, α is defined modulo $pW_2[[u]]$, so that we may (and will) consider it as an element of $k[[u]]$. The fact that e_1 generates $\mathfrak{M}_1$ easily implies $\delta \geq 0$. Moreover, since $\phi(e_2) \equiv u^{m(p-1)}e_2 \pmod{p}$, applying ϕ to (3), we obtain

$$\phi(e_1) = pu^{-p\delta}\phi(\alpha)\phi(e_2) = pu^{m(p-1)-p\delta}\phi(\alpha)e_2.$$

Therefore $\phi(e_1) = u^{(m-\delta)(p-1)}\frac{\phi(\alpha)}{\alpha}e_1$. Comparing with $\phi(e_1) = u^{n(p-1)}e_1$, we obtain $m-\delta = n$ and $\phi(\alpha) = \alpha$. The first condition gives $\delta = m - n$ (and in particular $m \geq n$), while the second one implies $\alpha \in \mathbb{F}_p^\star$. So, up to replacing e_1 by $\frac{e_1}{\alpha}$, we may assume $\alpha = 1$.

We have just proved that $\mathfrak{M}$ is generated by two vectors e_1 and e_2 related by (3) with $\alpha = 1$. This is exactly what appears in the statement of Theorem 1. We also know that $\phi(e_1) = u^{n(p-1)}e_1$. It still remains to precise the shape of $\phi(e_2)$. Let z denote the image of $e_2 \in \mathfrak{M}[1/u]$ through the isomorphism $\mathfrak{M}[1/u] \simeq W_2((u))$. From $\phi(\bar{e}_2) = u^{m(p-1)}\bar{e}_2$, we deduce that, up to multiplying e_2 by a $(p-1)$-th root of unity, we can write $z = u^m + pa$, with $a \in k((u))$. After some calculations, we obtain

$$\phi(e_2) = u^{m(p-1)}e_2 + \big[u^{-n}\phi(a) - u^{m(p-1)-n}a\big]e_1 = u^{m(p-1)}e_2 + be_1.$$

Hence RHS have to be in $\mathfrak{M}$, which gives directly (1) (using $m \geq n$). Now, using $E(u)\mathfrak{M} \subset \langle \phi(e_1), \phi(e_2)\rangle$ (where the notation $\langle \cdots \rangle$ means the generated submodule), we find that there exist $x, y \in W_2[[u]]$ such that

$$E(u)e_2 = xu^{n(p-1)}e_1 + y(u^{m(p-1)}e_2 + be_1).$$

Reducing modulo p, we have $y = u^{e-m(p-1)} + py'$ for some $y' \in W_2[[u]]$. Since x and y' are defined modulo p, one may consider them as elements of $k[[u]]$. After some calculations, we get $F(u) = bu^{n-pm+e} + xu^{pn-m} + y'u^{m(p-1)}$ where $F(u)$ is defined by the equality $E(u) = u^e + pF(u)$. As $m \geq n$, we have $m(p-1) \geq pn - m$. This shows that the equality we obtained is equivalent to the congruence $bu^{n-pm-e} \equiv F(u) \pmod{u^{pn-m}}$. Replacing b by its expression, we finally obtain (2). It remains to prove that a is an element of $k[[u]]$ (*a priori*, we only know that it belongs to $k((u))$), but it is clear from (1).

Proof of unicity. Let $\mathfrak{M}$ and $\mathfrak{M}'$ be two ϕ-modules presented as in Theorem 1 with parameters (n, m, a) and (n', m', a') respectively. We want to prove that $\mathfrak{M}$ and $\mathfrak{M}'$ are isomorphic if and only if $n = n'$, $m = m'$ and $a \equiv a' \pmod{u^n}$. Let us assume that there exists an isomorphism $f : \mathfrak{M} \to \mathfrak{M}'$. Since ϕ acts by multiplication by $u^{n(p-1)}$ (resp. $u^{n'(p-1)}$) on $\mathfrak{M}_1 = \ker p_{|\mathfrak{M}}$ (resp. $\mathfrak{M}'_1 = \ker p_{|\mathfrak{M}'}$), we get $n = n'$. In fact, examining the action of ϕ on e_1 and e'_1 it is easy to see that there exists $\alpha \in \mathbb{F}_p^\star$ such that $f(e_1) = \alpha e'_1$. In the same way, regarding actions of ϕ on quotients $\mathfrak{M}/\mathfrak{M}_1$ and $\mathfrak{M}'/\mathfrak{M}'_1$, we have $m = m'$. Then, equalities

$u^{m-n}e_1 = pe_2$ and $u^{m-n}e_1' = pe_2'$ give $f(e_2) = \alpha e_2' + xe_1$ for some element $x \in k[[u]]$. A little calculation shows that the compatibility with ϕ implies

$$\alpha u^{-n}\phi(a') - \alpha u^{m(p-1)-n}a' + \phi(x)u^{n(p-1)} = xu^{m(p-1)} + \alpha u^{-n}\phi(a) - \alpha u^{m(p-1)-n}a,$$

which gives $\phi(t) = u^{m(p-1)}t$ where we set $t = \alpha(a'-a) + u^n x$. Comparing u-adic valuations of both sides, we see that any solution t has to be divisible by u^m. As $m \geq n$, we have $a \equiv a' \pmod{u^n}$ as wanted. Conversely, if $a \equiv a' \pmod{u^n}$, it is sufficient to set $\alpha = 1$ and $x = \frac{a-a'}{u^n}$ to obtain an isomorphism $f : \mathfrak{M} \to \mathfrak{M}'$.

References

[1] C. Breuil, *Schémas en groupes et corps des normes*, unpublished (1998), available at http://www.ihes.fr/ breuil/PUBLICATIONS/groupesnormes.pdf

[2] M. Kisin, *Moduli of finite flat group schemes and modularity*, to appear on Annals of Math.

[3] M. Kisin, *Modularity of* 2*-adic Barsotti-Tate representations*, preprint (2006)

[4] D. Tossici, *Models of* $\mathbb{Z}/p^2\mathbb{Z}$ *over a discrete valuation ring of unequal characteristic*, preprint (2008)