# Reduction of the group scheme of $p^n$-th roots of unity and its torsors

Matthieu Romagny

July 2, 2012

Conference "Galois covers and deformations", Bordeaux, 25–29 June 2012

## Lecture 1 : Reduction of varieties and torsors

## 1 A bit of motivation

**1.1 Reduction.** Let $K$ be a field with a discrete valuation, $R$ its ring of integers, $k$ the residue field and $p$ its characteristic. Each algebraic $K$-variety $X_K$ has plenty of models ( $\stackrel{\text{df}}{=}$ faithfully flat $R$-schemes $X$ with generic fibre $X \otimes_R K$ isomorphic to $X_K$) with for each of them a special fibre $X_k := X \otimes_R k$. Studying the reduction of $X_K$ means looking for models $X$ with the nicest possible special fibre $X_k$; that special fibre is called the *reduction* of $X_K$. The reasons why people are interested in this activity is basically that the reduction of an object brings information on the object itself; in fact, it is in some sense *a part* of the object itself. For example, consider the simplest $K$-variety: the *point* $X_K = \mathrm{Spec}(K)$. Assume that $K$ is a local field and you are interested in the abelianized fundamental group of $X$ which is just $\Gamma_K^{\mathrm{ab}}$, the abelianized absolute Galois group of $K$. Let $\rho : \Gamma_K \to \Gamma_k \simeq \widehat{\mathbb{Z}}$ be the reduction map and $\epsilon_p : \Gamma_K \to \mathbb{Z}_p^\times$ the $p$-adic cyclotomic character. The local Kronecker-Weber theorem states that $\rho \times \epsilon_p : \Gamma_K^{\mathrm{ab}} \to \Gamma_k^{\mathrm{ab}} \times \mathbb{Z}_p^\times$ is an isomorphism. Thus we see that the reduction $\Gamma_k^{\mathrm{ab}}$ is a direct factor of the original object $\Gamma_K^{\mathrm{ab}}$. (For a nice description of $G_K$ by generators and relations see Neukirch, Schmitt, Wingberg, *Cohomology of number fields*, chap. VII, thm. 7.5.10.)

**1.2 Torsors.** In these lectures, we will be concerned with the reduction of torsors $Y_K \to X_K$ under finite groups viewed as $K$-algebraic groups. Torsors appear naturally in many contexts. For example, the moduli algebraic stack of curves $\mathscr{M}_g$ has useful torsors $M_g(n)$ which are moduli spaces for curves with full level $n$ structure, and are representable by schemes. (A *full level $n$ structure* on a curve $C$ is an isomorphism $H^1_{\text{ét}}(C, \mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^{2g}$ and thus the Galois group of $M_g(n) \to \mathscr{M}_g$ is $\mathrm{GL}_{2g}(\mathbb{Z}/n\mathbb{Z})$.) Another example comes from twisted forms of a fibration $P \to S$ (here $S$ may be simply the spectrum of a field), that is, fibrations $P' \to S$ that locally over $S$ are isomorphic to $P$. Assume for simplicity that the automorphism functor $G = \mathrm{Aut}_S(P)$ is representable by a flat finitely presented $S$-group scheme. Then the category of such twisted forms is equivalent to that of $G$-torsors on $S$:

- to $P' \to S$ one associates the $G$-torsor $I = \mathrm{Isom}_S(P', P)$,

- to a $G$-torsor $I \to S$ one associates the *contracted product* $P' = P \stackrel{G}{\times} I$, that is, the quotient of $P \times I$ by the action of $G$ given by $g(p, i) = (gp, gi)$. (The problem of existence of this quotient is not a big issue and in any case is not our concern here.)

For instance, the group schemes that are fppf twisted forms of the group scheme of roots of unity $\mu_{n,S}$ are in bijection with torsors under $G = (\mathbb{Z}/n\mathbb{Z})_S^\times$, i.e. they are classified by the flat cohomology group $H^1(S, (\mathbb{Z}/n\mathbb{Z})^\times)$. Note that if $G$ is commutative, then such cohomology groups are particular cases of groups $H^i(S, G)$ which are interesting linear-algebra invariants.

**1.3 Fundamental groups.** The étale torsors of a given variety or scheme $X_K$ are fruitfully studied as a whole via the *étale fundamental group* $\pi_1^{\text{ét}}(X_K,x)$, for a choice of a geometric base point $x$. The *specialization theorem* of Grothendieck says that if $X_K$ is the generic fibre of a morphism $X\to\mathrm{Spec}(R)$ which is proper with geometrically connected fibres, then the fundamental group of the reduction $X_k$ is a quotient of the fundamental group of $X_K$. The torsors under finite, maybe non-étale groups may be studied similarly with the help of the *fundamental $K$-group scheme* $\pi_1(X_K,x)$ defined by Nori, which in positive characteristic is a richer and more complicated object than its étale predecessor. Finally, another related object is given by $p$-divisible groups: start from an elliptic curve $E_K$ defined over $K$ and consider the $p^n$-torsion group $E_K[p^n](\bar{K})$ where $\bar{K}$ is an algebraic closure of $K$. One can also pass to the limit over $n$ to get the Tate module $T_pE_K$, a free finite rank $\mathbb{Z}_p$-module. This is an extremely interesting representation of the Galois group $\Gamma_K$. Flat $R$-models of the group schemes give rise to integral structures on these abelian groups, and their reduction reveals again some information.

**1.4 Degeneration.** It is often the case that during the reduction process, objects acquire singularities. Roughly speaking, this is because moduli spaces for smooth objects usually fail to be projective or proper, and have compactifications whose boundary divisors (classifying singular objects) tend to have positivity properties so that every proper curve in them intersects the boundary. The moduli space of stable curves $\bar{M}_g$ is a typical example. This phenomenon is to be expected also for torsors and their structure groups.

## 2 A few examples of models of varieties

We review some examples of varieties that are known to have nice models. We also consider the models obtained after possible finite base change $K'/K$. These are designed to study the *potential reduction type* which is relevant when one does not care too much about the arithmetic constraint coming from the base field. In all cases, the existence of the model is the result of a (usually big) theorem.

1) Models of curves. The most important ones are the *minimal regular models* over $R$, and the *stable models* over a finite extension $R'/R$.

2) Models of abelian varieties. The most important are the *Néron models* over $R$ and the *semistable models* over a finite extension.

3) Models of surfaces, see [KSB88]. Ideas from the Minimal Model Program lead Kollár and Shepherd-Barron to a good notion of stable model for surfaces of general type. The outcome is this: a *stable surface* is a geometrically integral projective surface $X$ with semi-log-canonical (slc) singularities and ample dualizing sheaf $\omega_X$. We won't unravel all the definitions, but recall that $X$ has *slc singularities* if it is Cohen-Macaulay, its only singularities in codimension 1 are of double normal crossing type $(xy=0)\subset\mathbb{A}^3$, the pair $(X^\nu,\Delta^\nu)$ has log-canonical (lc) singularities (here $X^\nu$ is the normalization and $\Delta^\nu$ is the preimage of the one-dimensional part $\Delta$ of the singular locus), and for some $N>0$ the reflexive power $\omega_X^{[N]}:=(\omega_X^{\otimes N})^{\vee\vee}$ is invertible. Surfaces with lc singularities are defined in terms of discrepancies (ramification multiplicities) in a resolution. Resolutions of singularities of surfaces exist in all characteristics $p\geqslant 0$, hence the definition makes sense for all $p$. But while the moduli space of stable surfaces is known to be proper for $p=0$, this is not known for $p>0$. Note that stable surfaces need not be normal, just like stable curves.

## 3 Models of torsors and groups

Here, we will not give particular examples of models of torsors; rather, we will state a result whose interest is that it shows that all models of a finite $K$-group scheme are potentially structure groups of models of torsors. This is relevant for the content of the second and third lectures, where we shall study all models of a fixed group scheme – the group scheme $\mu_{p^n,K}$ of $p^n$-th roots of unity.

Let us consider torsors $Y_K \to X_K$ whose structure group $G_K$ is the group scheme $\Gamma_K$ defined by a finite group $\Gamma$ of order $n$. A *model of* $G_K$ is by definition a finite flat $R$-group scheme $G$ with an isomorphism $G \otimes K \simeq G_K$. A *model of the torsor* is a finite flat morphism $Y \to X$ between suitable models of $X_K, Y_K$ and which is a torsor under some model $G$. In the case where $p$ is prime to $n$, one can usually hope to find models under the constant $R$-group $\Gamma_R$, but we are especially interested in the case where $p$ divides $n$ and then other models of $G_K$ are needed.

**Example.** Assume that $R$ contains a primitive $p$-th root of unity $\zeta$. Then the group scheme of roots of unity $\mu_{p,K}$ is isomorphic to $(\mathbb{Z}/p\mathbb{Z})_K$ and is the structure group for the well-known Kummer torsor $\mathbb{G}_{m,K} \to \mathbb{G}_{m,K}$. There are natural models $\mathbb{G}_{m,R}$ for the two copies of $\mathbb{G}_{m,K}$. The original torsor extends to a torsor $\mathbb{G}_{m,R} \to \mathbb{G}_{m,R}$ under the non-étale group $\mu_{p,R}$ but *not* under $(\mathbb{Z}/p\mathbb{Z})_R$.

For the existence of a model of $G_K$ acting faithfully on a model $Y$, that $Y$ must not be too pathological. For instance if $Y$ has empty special fibre, then no finite model acts faithfully. For the same reasons, if $Y_K$ has irreducible components that are closed in $Y$, the same problem arises. It turns out that by considering (in the nonreduced case) not only generic points of irreducible components but also all associated points of $Y_K$, one gets a good, geometrically meaningful condition:

**Definition.** Let $Y$ be an $R$-scheme of finite type. Let $K^s$ be a separable closure of $K$. We say that $Y$ is *pure* if for all associated points $y \in \mathrm{Ass}(Y_{K^s})$, the closure of $y$ meets the special fibre $Y_k$.

The condition of purity was introduced by Raynaud around 1970. We see that it is a kind of weak valuative criterion of properness. Pure schemes are quite common; for example, proper $R$-schemes, and faithfully flat $R$-schemes with geometrically integral generic fibre, are pure. In fact, virtually all schemes that one encounters in concrete situations are pure. Then we have the following theorem (see [Ro12]):

**Theorem.** *Let $Y$ be a faithfully flat, finite type, separated, pure $R$-scheme. Let $G_K$ be a finite $K$-group scheme acting faithfully on $Y_K$. If $G_K$ has a model $G$ acting on $Y$, then it has a model $G'$ acting faithfully on $Y$, namely the schematic closure of $G_K$ in the fppf sheaf of automorphisms* $\mathrm{Aut}_R(Y)$.

We end the lecture with some comments on the theorem and its proof.

**Remarks.** (1) If $\mathrm{Aut}_R(Y)$ is representable by a scheme, the theorem is easy. The difficulty in the theorem is that $\mathrm{Aut}_R(Y)$ is a sheaf which is *not* a scheme in general.
(2) If $G_K = \Gamma_K$ is defined by a constant abstract group $\Gamma$, then the condition that $G_K$ has a model acting on $Y$ is not restrictive. Indeed, by blowing-up in the special fibre of $Y$ one can find a model $Y' \to Y$ such that all elements of $\Gamma$ extend to automorphisms of $Y'$. Then the $R$-group scheme $\Gamma_R$ acts on $Y'$.
(3) The rough idea of the proof of the theorem is that it is easy if $Y$ is finite over $R$ (because in that case $\mathrm{Aut}_R(Y)$ is a scheme and the result is straightforward), and in general one somehow reduces to the finite case by showing that the finite flat subschemes of a flat and pure $R$-scheme are dense in a very strong sense (schematically, and universally after any base change on $R$).

## Lecture 2 : Construction of models of $\mu_{p^n}$

The content of Lectures 2 and 3 is joint work with A. Mézard and D. Tossici, see [MRT12].

# 4 The Sekiguchi-Suwa exact sequence

## 4.1 Statement

We let $R = \mathbb{Z}_{(p)}[\zeta_{p^n}]$ be the valuation ring obtained by adding a primitive $p^n$-th root of unity $\zeta_{p^n}$ to the ring of integers localized at $p$. This root of unity $\zeta_{p^n}$ singles out an isomorphism $(\mathbb{Z}/p^n\mathbb{Z})_K \simeq \mu_{p^n,K}$. The following result is due to Sekiguchi and Suwa (see [SS99]).

**Theorem.** *There exists an exact sequence denoted $\mathscr{S}_n$ of affine flat $R$-group schemes*

$$0 \longrightarrow (\mathbb{Z}/p^n\mathbb{Z})_R \longrightarrow \mathcal{W}_n \longrightarrow \mathcal{V}_n \longrightarrow 0$$

*whose generic fibre is the Kummer-type exact sequence*

$$0 \longrightarrow \mu_{p^n,K} \longrightarrow (\mathbb{G}_m)^n \xrightarrow{\Theta} (\mathbb{G}_m)^n \longrightarrow 0,$$

*whose special fibre is the Artin-Schreier-Witt exact sequence*

$$0 \longrightarrow (\mathbb{Z}/p^n\mathbb{Z})_k \longrightarrow W_n \xrightarrow{F-\mathrm{id}} W_n \longrightarrow 0,$$

*and such that each cyclic étale $p^n$-covering* $\mathrm{Spec}(T) \to \mathrm{Spec}(S)$ *where $S$ is a local flat $R$-algebra is obtained by base change from $\mathcal{W}_n \to \mathcal{V}_n$. Moreover, there is a natural extension of short exact sequences:*

$$0 \longrightarrow \mathscr{S}_1 \longrightarrow \mathscr{S}_n \longrightarrow \mathscr{S}_{n-1} \longrightarrow 0.$$

The map $\Theta : (\mathbb{G}_m)^n \to (\mathbb{G}_m)^n$ above is given by $\Theta(x_1, \dots, x_n) = (x_1^p, x_2^p x_1^{-1}, \dots, x_n^p x_{n-1}^{-1})$. Kummer theory is usually formulated with the isogeny $\mathbb{G}_m \to \mathbb{G}_m$, $x \mapsto x^{p^n}$ but it can equally well be formulated with the map $\Theta$. The latter is of course best suited for the realization of the Kummer isogeny as the generic fibre of an integral isogeny like in the theorem, since the Artin-Schreier-Witt sequence involves groups of dimension $n$.

## 4.2 Indications on the construction

In dimension $n = 1$, the groups $\mathcal{W}_1$ and $\mathcal{V}_1$ are models of $\mathbb{G}_m$ and these can be described easily. For each $\lambda \in R$, let $i : \mathrm{Spec}(R/\lambda) \to \mathrm{Spec}(R)$ be the closed immersion. On the small flat site of $\mathrm{Spec}(R)$, reduction modulo $\lambda$ defines a surjective morphism of sheaves $\mathbb{G}_{m,R} \to i_*\mathbb{G}_{m,R/\lambda}$ and an exact sequence:

$$(\star) \qquad 0 \longrightarrow \mathcal{G}^\lambda \xrightarrow{\alpha} \mathbb{G}_{m,R} \longrightarrow i_*\mathbb{G}_{m,R/\lambda} \longrightarrow 0.$$

The kernel $\mathcal{G}^\lambda = \mathrm{Spec}(R[x, (1+\lambda x)^{-1}])$ is an affine smooth $R$-group scheme whose group law is given on the points by $x_1 \star x_2 = x_1 + x_2 + \lambda x_1 x_2$. One proves that all models of $\mathbb{G}_m$ with geometrically connected fibers are of this form. It is easy to see that $\mathcal{G}^\lambda$ depends only on the valuation of $\lambda$ up to isomorphism; hence the $\lambda$'s are discrete parameters. If a uniformizer $\pi \in R$ is chosen and $\lambda := \pi^\ell$, we may write $\mathcal{G}^\ell$ instead of $\mathcal{G}^\lambda$. For $\lambda_1 := \zeta_p - 1$, the Kummer sequence over $K$ extends to an exact sequence over $R$ which turns out to be $\mathscr{S}_1$:

$$0 \longrightarrow (\mathbb{Z}/p\mathbb{Z})_R \longrightarrow \mathcal{G}^{\lambda_1} \longrightarrow \mathcal{G}^{\lambda_1^p} \longrightarrow 0.$$

In dimension $n \geqslant 2$, the existence of the extension $0 \to \mathscr{S}_1 \to \mathscr{S}_n \to \mathscr{S}_{n-1} \to 0$ implies that the groups $\mathcal{W}_n$ and $\mathcal{V}_n$ are iterated extensions of copies of the group $\mathcal{G}^{\lambda_1}$. This extension structure is the basic starting point of the construction.

# 5 Filtered group schemes

In this section, we present a construction from [SS99].

## 5.1 Definition

For the construction of models of $\mu_{p^n,K}$, we use the framework of Sekiguchi and Suwa. One minor point is that if we do not insist that $\mu_{p^n,K}$ should be isomorphic to $(\mathbb{Z}/n\mathbb{Z})_K$, the root of unity $\zeta_n$ is useless and we can let the base ring $R$ be *any* mixed characteristic dvr. Another point is that there is no reason a priori to rule out extensions of groups $\mathcal{G}^\lambda$ with different $\lambda$'s. (We abandon the notation $\lambda_1 = \zeta_p - 1$ and $\lambda_1, \lambda_2, \dots$ may now denote arbitrary elements of $R$.)

**Definition.** *A* filtered group scheme *of dimension $n$ and type $(\lambda_1, \dots, \lambda_n)$ is a collection of extensions $0 \to \mathcal{G}^{\lambda_i} \to \mathcal{E}_i \to \mathcal{E}_{i-1} \to 0$, for $1 \leqslant i \leqslant n$. It is often denoted by the symbol $\mathcal{E}_n$ alone.*

It is very likely that filtered group schemes are exactly all the models of split tori with geometrically connected fibres, but we made no serious attempt to prove it.

**Remark.** We shall see that for each choice of discrete parameters $\lambda_i$, the extensions are parameterized by $n(n-1)/2$ continuous parameters. For the purpose of constructing $\mathcal{W}_n$, one single choice of these parameters is relevant but for the construction of models of $\mu_{p^n,K}$ we allow as much choices as possible.

## 5.2 Deformed exponentials

It is not too hard to prove that if $\mathcal{E}$ is a filtered group scheme, then $\mathrm{Ext}^1_R(\mathcal{E}, \mathbb{G}_m) = 0$. Thus the long exact sequence in cohomology derived from $(\star)$ induces an exact sequence

$$\mathrm{Hom}(\mathcal{E}, \mathbb{G}_{m,R}) \longrightarrow \mathrm{Hom}(\mathcal{E}, i_*\mathbb{G}_{m,R/\lambda}) \longrightarrow \mathrm{Ext}^1(\mathcal{E}, \mathcal{G}^\lambda) \longrightarrow 0.$$

This gives a presentation of $\mathrm{Ext}^1(\mathcal{E}, \mathcal{G}^\lambda)$. The heart of the theory of Sekiguchi and Suwa is the complete description of the middle Hom-set. More precisely, homomorphisms $\mathcal{E} \to i_*\mathbb{G}_{m,R/\lambda}$, or equivalently homomorphisms $i^*\mathcal{E} \to \mathbb{G}_{m,R/\lambda}$, will be given by the power series we introduce now (see [SS$_4$]).

**Definition.** *Let $A$ be a $\mathbb{Z}_{(p)}$-algebra and $\lambda \in A$. For each $a \in A$, we define an element of $A[[T]]$ by:*

$$E_p(a, \lambda, T) = (1 + \lambda T)^{\frac{a}{\lambda}} \prod_{k \geqslant 1} (1 + \lambda^{p^k} T^{p^k})^{\frac{1}{p^k}\left(\left(\frac{a}{\lambda}\right)^{p^k} - \left(\frac{a}{\lambda}\right)^{p^{k-1}}\right)}.$$

*For each Witt vector $\underline{a} = (a_0, a_1, a_2, \dots) \in W(A)$, we define an element of $A[[T]]$ by:*

$$E_p(\underline{a}, \lambda, T) = \prod_{\ell=0}^{\infty} E_p(a_\ell, \lambda^{p^\ell}, T^{p^\ell}).$$

**Remarks.** (1) *A priori* the coefficients of $E_p(a, \lambda, T)$ lie in $\mathbb{Q}[a, \lambda]$ and the fact that they are integral at $p$ requires a proof. The corresponding fact for $E_p(\underline{a}, \lambda, T)$ follows immediately.

(2) These series are called *deformed Artin-Hasse exponentials*, or briefly *deformed exponentials*, because $E_p(1, 0, T)$ is the usual $p$-adic Artin-Hasse exponential.

**Notations.** Let $F : W(A) \to W(A)$ be the Frobenius endomorphism. For $x \in A$, denote by $[x]$ both the Teichmüller representative $(x, 0, 0, \dots) \in W(A)$ and the multiplication-by-$[x]$ on $W(A)$. Let us write $\widehat{W}(A) \subset W(A)$ the subset of Witt vectors which are *finite* (i.e. with all components 0 except a finite number) and *nilpotent* (i.e. with all components nilpotent).

**Crucial property.** *Let $A$ be a $\mathbb{Z}_{(p)}$-algebra. For each $\lambda \in A$ and $\underline{a} \in \ker(F - [\lambda^{p-1}])$ we have:*

$$E_p(\underline{a}, \lambda, T_1 + T_2 + \lambda T_1 T_2) = E_p(\underline{a}, \lambda, T_1) E_p(\underline{a}, \lambda, T_2).$$

This says that the deformed exponentials define morphisms of $A$-formal groups $\widehat{\mathcal{G}}^{\lambda} \to \widehat{\mathbb{G}}_m$. It is not hard to see that they define morphisms of (algebraic) $A$-group schemes if $\underline{a} \in \widehat{W}(A)$.

### 5.3 The main theorem

In dimension 1, the main theorem is just the crucial property above:

**Theorem ($n = 1$).** *Let $\lambda_1, \lambda_2 \in R$ have positive valuation (for simplicity) and let $U^1$ be the endomorphism $F - [\lambda_1^{p-1}] : \widehat{W}(R/\lambda_2) \to \widehat{W}(R/\lambda_2)$. Then the homomorphism*

$$E_p(-, \lambda_1, -) : \ker(U^1) \longrightarrow \mathrm{Hom}_{R/\lambda_2}(\mathcal{G}^{\lambda_1}, \mathbb{G}_m)$$

*is an isomorphism.*

In the following, we use the short notation $x_{1..n} := (x_1, \ldots, x_n)$ for tuples.

**Theorem ($n \geqslant 2$).** *Let $\lambda_1, \ldots, \lambda_{n+1} \in R$ have positive valuation (for simplicity). Let $\mathcal{E}_n$ be a filtered group scheme of type $(\lambda_1, \ldots, \lambda_n)$, constructed from some finite Witt vectors $\underline{a}_i^{j+1} \in W(R)$ whose reduction mod $\lambda_{j+1}$ is in $\ker(U^j)$. Then there exist:*

*- a power series in $n$ variables $E_p(\underline{a}_{1..n}^{n+1}, \lambda_{1..n}, T_{1..n})$ with parameters $\underline{a}_{1..n}^{n+1} \in W(R/\lambda_{n+1})^n$,*

*- an endomorphism $U^n : \widehat{W}(R/\lambda_{n+1})^n \to \widehat{W}(R/\lambda_{n+1})^n$,*

*such that $E_p(-, \lambda_{1..n}, -)$ induces an isomorphism $\ker(U^n) \to \mathrm{Hom}_{R/\lambda_{n+1}}(\mathcal{E}_n, \mathbb{G}_m)$.*

Starting from an $n$-dimensional filtered group scheme $\mathcal{E}_n$ and elements $\underline{a}_i^j$, here is how we get an $n+1$-dimensional filtered group scheme $\mathcal{E}_{n+1}$. A choice of $n$ finite Witt vectors $\underline{a}_i^{n+1} \in W(R)$ whose reduction mod $\lambda_{n+1}$ is in $\ker(U^n)$ defines an exponential $D_n(T_1, \ldots, T_n) = E_p(\underline{a}_{1..n}^{n+1}, \lambda_{1..n}, T_{1..n})$ which we view as a morphism of $R/\lambda_{n+1}$-group schemes $D_n : \mathcal{E}_n \to i_* \mathbb{G}_{m,R/\lambda_{n+1}}$. We obtain $\mathcal{E}_{n+1}$ by pullback from the extension ($\star$) as follows:

$$\begin{tikzcd}
0 \arrow[r, dotted] & \mathcal{G}^{\lambda_{n+1}} \arrow[r, dotted] \arrow[d, dotted, "\mathrm{id}"'] & \mathcal{E}_{n+1} \arrow[r, dotted] \arrow[d, dotted, "D_n + \lambda_{n+1} T_{n+1}"'] & \mathcal{E}_n \arrow[r, dotted] \arrow[d, "D_n"] & 0 \\
0 \arrow[r] & \mathcal{G}^{\lambda_{n+1}} \arrow[r] & \mathbb{G}_m \arrow[r] & i_* \mathbb{G}_{m,R/\lambda_{n+1}} \arrow[r] & 0
\end{tikzcd}$$

It follows immediately by induction that

$$\mathcal{E}_{n+1} = \mathrm{Spec}\left( R\left[ T_1, \ldots, T_{n+1}, \frac{1}{D_0 + \lambda_1 T_1}, \ldots, \frac{1}{D_n + \lambda_{n+1} T_{n+1}} \right] \right).$$

We can collect the parameters $\underline{a}_i^j$ into a matrix. It is useful to normalize things a bit by setting $\lambda_i = \pi^{\ell_i}$ where $\pi$ is a fixed uniformizer of $R$. Thus each filtered group scheme is determined by a matrix of the form

$$A = \begin{pmatrix} \pi^{\ell_1} & \underline{a}_1^2 & \ldots & \underline{a}_1^n \\ 0 & \pi^{\ell_2} & \ddots & \vdots \\ \vdots & \ddots & \ddots & \underline{a}_{n-1}^n \\ 0 & \ldots & 0 & \pi^{\ell_n} \end{pmatrix}.$$

### 5.4 Comments. A glance at the dust we've been sweeping under the carpet

The construction is quite complicated for (at least) two reasons:

1) the construction of the exponentials is recursive, so starting from $E_p$ which is a quite sophisticated object, we obtain something which is really terrible. More precisely, we have:

$$E_p(\underline{a}^{n+1}_{1..n}, \lambda_{1..n}, T_{1..n}) = \prod_{i=1}^{n} E_p\left(\underline{a}^{n+1}_i, \lambda_i, \frac{T_i}{E_p(\underline{a}^n_{1..n-1}, \lambda_{1..n-1}, T_{1..n-1})}\right).$$

2) the definition of $U^n$ and hence the construction of $\mathcal{E}_{n+1}$ depends on all the parameters used to construct $\mathcal{E}_1, \ldots, \mathcal{E}_n$. This makes a lot of bookkeeping. In fact, by the choice of $\underline{a}^j_i$, there exists $\underline{b}^j_i$ such that

$$U^{j-1}\begin{pmatrix} \underline{a}^j_1 \\ \vdots \\ \underline{a}^{j-1}_1 \end{pmatrix} = \lambda_j \begin{pmatrix} \underline{b}^j_1 \\ \vdots \\ \underline{b}^{j-1}_1 \end{pmatrix}$$

and the inductive definition is

$$U^n = \begin{pmatrix} F^{\lambda_1} & -T_{\underline{b}^2_1} & -T_{\underline{b}^3_1} & \ldots & -T_{\underline{b}^n_1} \\ 0 & F^{\lambda_2} & -T_{\underline{b}^3_2} & \ldots & -T_{\underline{b}^n_2} \\ \vdots & 0 & \ddots & \ddots & \vdots \\ 0 & 0 & \ddots & \ddots & -T_{\underline{b}^n_{n-1}} \\ 0 & 0 & \ldots & 0 & F^{\lambda_n} \end{pmatrix}.$$

This is a matrix whose entries are endomorphisms of $W(A)$ (with $A = R/\lambda_{n+1}$ in the present case):
- $F^\lambda := F - [\lambda^{p-1}]$,
- $T_{\underline{b}} : W(A) \to W(A)$ is defined by $T_{\underline{b}}(\underline{x}) = \sum_{k=0}^{\infty} V^k([a_k]\underline{x})$, for Witt vectors $\underline{b}, \underline{x} \in W(A)$, where $V : W(A) \to W(A)$ is the Verschiebung endomorphism.

## 6 Kummer group schemes

In this section, we present work of [MRT12] consisting of elaborations on the constructions of [SS99].

The construction of filtered group schemes with successive choices of parameters $\underline{a}^j_i$ gives a little more: each $n$-dimensional filtered group scheme $\mathcal{E} = \mathcal{E}_n$ comes with a morphism of $R$-group schemes $\alpha = \alpha_n : \mathcal{E} \to (\mathbb{G}_m)^n$ which is a *model map*, that is, an isomorphism on the generic fibre. (Indeed, by definition the group $\mathcal{G}^{\lambda_1}$ comes with a model map to $\mathbb{G}_m$, and by induction if $\mathcal{E}_n$ comes with a model map $\alpha_n : \mathcal{E}_n \to (\mathbb{G}_m)^n$ then wee see that $\alpha_{n+1} = (\alpha_n, D_n + \lambda_{n+1}T_{n+1}) : \mathcal{E}_{n+1} \to (\mathbb{G}_m)^{n+1}$ is a model map.) We would like to insert $\alpha$ into a commutative diagram with finite flat $G$:

$$\begin{tikzcd} 0 \arrow[r] & G \arrow[r] \arrow[d, "\alpha"] & \mathcal{E} \arrow[r] \arrow[d, "\alpha"] & \mathcal{E}' \arrow[r] \arrow[d, "\alpha'"] & 0 \\ 0 \arrow[r] & \mu_{p^n,R} \arrow[r] & (\mathbb{G}_m)^n \arrow[r, "\Theta"] & (\mathbb{G}_m)^n \arrow[r] & 0. \end{tikzcd}$$

**Remarks.** Some easy remarks :
1) as usual the subgroup $G$ and the isogeny $\mathcal{E} \to \mathcal{E}'$ determine each other up to isomorphism,

2) if they exist then they are unique, since $G$ is the schematic closure of $\alpha^{-1}(\mu_{p^n,K}) \subset \mathcal{E}_K$ inside $\mathcal{E}$, and $\mathcal{E} \to \mathcal{E}'$ is determined by it generic fibre which is $\Theta$,
3) it is not hard to see that $\mathcal{E}'$ is filtered of type $\lambda_{1..n}^p$ where $\lambda_{1..n}$ is the type of $\mathcal{E}$.

**Theorem** ($n = 1$). *If $\mathcal{E} = \mathcal{G}^\lambda$ then the flat closure $G$ is finite if and only if $e := v(p) \geqslant (p-1)v(\lambda)$.*

In fact $\alpha_n^{-1}(\mu_{p,K})$ is defined by the equation $(1+\lambda x)^p - 1 = 0$ and $G$ is defined by the equation obtained by dividing by the highest possible power $s$ of a uniformizer of $R$. Then $G$ is finite if and only if the result is a monic polynomial, that is if $s = pv(\lambda)$, i.e. $pv(\lambda) \leqslant e + v(\lambda)$, q.e.d.

For the inductive step, we start from filtered group schemes $\mathcal{E}_n$ and $\mathcal{E}'_n$ constructed from families of Witt vectors $\underline{a}_i^j$, $\underline{a}_i'^j$, and we denote by $U^n$ and $U'^n$ their associated endomorphisms.

**Theorem** ($n \geqslant 2$). *Let $\lambda_1, \dots, \lambda_{n+1} \in R$ have positive valuation (for simplicity). Let $\mathcal{E}_n$ be a filtered group scheme such that the flat closure $G_n$ is finite and let $\mathcal{E}'_n = \mathcal{E}_n/G_n$. Then there exists a matrix $\Upsilon^n : \ker(U'^n) \to \ker(U^n)$, which is the matrix representation of the pullback*

$$\mathrm{Hom}_{R/\lambda_{n+1}}(\mathcal{E}'_n, \mathbb{G}_m) \to \mathrm{Hom}_{R/\lambda_{n+1}}(\mathcal{E}_n, \mathbb{G}_m),$$

*such that for $\underline{a}_{1..n}^{n+1} \in \ker(U^n)$ defining $\mathcal{E}_{n+1}$ we have: the flat closure $G_{n+1}$ is finite if and only if*

$$p\underline{a}_{1..n}^{n+1} - (\underline{a}_{1..n-1}^n, [\lambda_n]) \in \mathrm{im}(\Upsilon^n) \mod (\lambda_{n+1})^p.$$

**Remarks.** (1) An element $\underline{a}'^{n+1}_{1..n}$ such that $p\underline{a}_{1..n}^{n+1} - (\underline{a}_{1..n-1}^n, [\lambda_n]) = \Upsilon^n(\underline{a}'^{n+1}_{1..n}) \mod (\lambda_{n+1})^p$ defines the group $\mathcal{E}'_{n+1} = \mathcal{E}_{n+1}/G_{n+1}$.
(2) In the expression $p\underline{a}_i^{n+1} - (\underline{a}_i^n, [\lambda_n])$ we can recognize the map $\Theta$.
(3) There is an inductive construction of $\Upsilon^n$, like for $U^n$... I skip this.
(4) The congruences in the theorem imply, for instance, that if $G_n$ is finite then $v(\lambda_1) \geqslant \dots \geqslant v(\lambda_n)$.
(5) We shall write down the congruences for $n = 3$ in the end of the next lecture.

Let us come back to the models of $\mu_{p^n,K}$. Assume that we construct a filtered group scheme $\mathcal{E}_n$ with parameters $\underline{a}_i^j$ and write

$$\alpha_n : \mathcal{E}_n \to (\mathbb{G}_m)^n , \qquad (t_1, \dots, t_n) \mapsto (1 + \lambda_1 t_1, D_1 + \lambda_2 t_2, \dots, D_{n-1} + \lambda_n t_n)$$

where $D_j = D_j(t_1, \dots, t_j) = E_p(\underline{a}_{1..n}^{j+1}, \lambda_{1..j}, t_{1..j})$ are the exponentials. Provided it exists, the finite flat model $G$ is described as the closed subscheme of affine $n$-space defined by the equations:

$$\frac{(1+\lambda_1 T_1)^p - 1}{\lambda_1^p}, \ \frac{(D_1 + \lambda_2 T_2)^p (1+\lambda_1 T_1)^{-1} - 1}{\lambda_2^p} \quad , \dots , \quad \frac{(D_{n-1} + \lambda_n T_n)^p (D_{n-2} + \lambda_{n-1} T_{n-1})^{-1} - 1}{\lambda_n^p}.$$

## Lecture 3 : Breuil-Kisin modules of models of $\mu_{p^n}$

In this lecture, we shall use the classification of finite flat group schemes due to Breuil [Br00] and Kisin [Ki09] for our models of $\mu_{p^n,K}$.

In the sequel, we assume that $R$ is complete and that the residue field $k$ is perfect. We denote by $W = W(k)$ the ring of infinite Witt vectors of $k$, $K_0$ its fraction field, $\phi : W \to W$ the Frobenius and $W_n = W/p^n$. We write $\mathfrak{S} = W[[u]]$ and $\mathfrak{S}_n = W_n[[u]]$ the rings of power series in $u$. The Frobenius $\phi$ on $W$ extends to an endomorphism $\phi$ of $\mathfrak{S}$ such that $\phi(u) = u^p$, and similarly for $\mathfrak{S}_n$. Finally we fix a uniformizer $\pi \in R$ and we denote by $E = E(u)$ its minimal polynomial over $K_0$.

## 7 The Breuil-Kisin classification

### 7.1 Finite flat group schemes and Breuil-Kisin modules

We are interested in the category $\mathrm{Gr}_n$ of finite flat commutative $R$-group schemes killed by $p^n$. On the other hand let $\mathrm{Mod}_n$ be the category of finite $\mathfrak{S}_n$-modules without $u$-torsion $\mathfrak{M}$ endowed with a $\phi$-semi-linear map $\phi_{\mathfrak{M}} : \mathfrak{M} \to \mathfrak{M}$ such that $E(u)\mathfrak{M} \subset \langle \phi_{\mathfrak{M}}(\mathfrak{M}) \rangle \subset \mathfrak{M}$. (Note that a semi-linear map is the same thing as a linear map $\phi^*\mathfrak{M} \to \mathfrak{M}$.) In the sequel we write $\phi$ instead of $\phi_{\mathfrak{M}}$.

There is on the syntomic site of the formal scheme $\mathrm{Spf}(R)$ a certain abelian sheaf $\mathcal{O}^{\mathrm{cris}}_{\infty,\pi}$ that plays the same role as the functor of Witt covectors plays in the Dieudonné-Fontaine theory.

**Theorem (Breuil, Kisin)** *For each $G \in \mathrm{Gr}_n$ there is a unique sub-$\mathfrak{S}$-module $\mathfrak{M}$ in $\mathrm{Hom}(G, \mathcal{O}^{\mathrm{cris}}_{\infty,\pi})$ such that $E(u)\mathfrak{M} \subset \langle \phi(\mathfrak{M}) \rangle \subset \mathfrak{M}$. The functor $G \mapsto \mathfrak{M}$ induces an anti-equivalence of categories from $\mathrm{Gr}_n$ to $\mathrm{Mod}_n$.*

It is more convenient to work with an equivalence (i.e. a covariant functor). We do this by composing the anti-equivalence with the Cartier dual functor.

Then one proves that a group $G$ is a model of $\mu_{p^n,K}$ if and only if its module $\mathfrak{M}$ is such that $\mathfrak{M}[1/u]$ is isomorphic to the $W_n((u))$-module $W_n((u))$ itself endowed with its usual Frobenius. Since $\mathfrak{M}$ has no $u$-torsion, the map $\mathfrak{M} \to \mathfrak{M}[1/u]$ is injective and the outcome is that we may view $\mathfrak{M}$ as a *lattice* inside $W_n((u))$ (a finitely generated sub-$\mathfrak{S}_n$-module such that $\mathfrak{M}[1/u] = W_n((u))$) satisfying $E(u)\mathfrak{M} \subset \langle \phi(\mathfrak{M}) \rangle \subset \mathfrak{M}$ where now $\phi$ is the ambient Frobenius.

**Remark.** Such a $\phi$-stable lattice is necessarily included in $W_n[[u]]$, because if $x \in \mathfrak{M}$ has negative $u$-valuation then $\mathrm{val}_u(\phi^n x) \to -\infty$, in contradiction with the finite generation of $\mathfrak{M}$.

### 7.2 Breuil-Kisin modules and matrices

Let us extend the Teichmüller map $[-] : k \to W_n$ to power series by $[\sum a_i u^i] = \sum [a_i] u^i$. For a lattice $\mathfrak{M}$, let us say that a system of generators $e_1, \dots, e_n$ is a *$T$-basis* if $v_p(e_i) = i - 1$ and each element $x \in \mathfrak{M}$ can be written in a unique way $x = [x_1]e_1 + \dots + [x_n]e_n$ with $x_i \in k[[u]]$.

**Lemma.** *Let $\mathfrak{M}$ be a sublattice of $W_n[[u]]$. Then there exists a unique $T$-basis of $\mathfrak{M}$ of the form*

$$e_i = u^{l_i} p^{i-1} + [a_{i,i+1}]p^i + \dots + [a_{in}]p^{n-1}$$

*with $l_i \geqslant 0$, $a_i \in k[u]$ and $\deg(a_{ij}) < l_j$.*

It is easy to see why this is so. Let us introduce the submodules $\mathfrak{M}[i] = \ker(p^{n+1-i} : \mathfrak{M} \to \mathfrak{M})$ forming a filtration $0 = \mathfrak{M}[n+1] \subset \mathfrak{M}[n] \subset \dots \subset \mathfrak{M}[1] = \mathfrak{M}$. We have the following sublemma whose proof is easy and omitted:

**Sublemma.** *Consider the natural inclusion $\mathfrak{M}[i] \subset p^{i-1}W_n((u))$. The induced map*

$$\begin{aligned} \mathfrak{M}[i]/\mathfrak{M}[i+1] \longrightarrow p^{i-1}W_n((u))/p^iW_n((u)) &\simeq k((u)) \\ p^{i-1}x &\mapsto x \end{aligned}$$

*is an injection that identifies $\mathfrak{M}[i]/\mathfrak{M}[i+1]$ with a lattice of $k((u))$.*

Thus $\mathfrak{M}[n]$ is isomorphic to a lattice of $k((u))$ hence has a unique generator of the form $u^{l_n}$, with $l_n \geqslant 0$ because of the remark above (stability under Frobenius). The preimage of $u^{l_n}$ in $\mathfrak{M}$ is

$e_n = p^{n-1}u^{l_n}$. Now similarly $\mathfrak{M}[n-1]/\mathfrak{M}[n]$ has a unique generator of the form $u^{l_{n-1}}$ with $l_{n-1} \geqslant 0$, whose preimage in $\mathfrak{M}$ may be written in $p$-adic expansion:

$$e_{n-1} = u^{l_{n-1}}p^{n-2} + [a_{n-1,n}]p^{n-1}.$$

Of course, we may alter $e_{n-1}$ by a multiple of $e_n$. Writing the euclidean division $a_{n-1,n} = u^{l_n}q + r$ and changing $e_{n-1}$ into $e_{n-1} - qe_n$ allows to fulfill the condition $\deg(a_{n-1,n}) < l_n$ and is the unique way to do it. The construction of $e_{n-2}, \dots, e_1$ proceeds similarly. End proof lemma.

Thus to each lattice we can associate an upper-triangular matrix:

$$A = \begin{pmatrix} u^{l_1} & a_{12} & \dots & a_{1n} \\ 0 & u^{l_2} & \ddots & \vdots \\ \vdots & \ddots & \ddots & a_{n-1,n} \\ 0 & \dots & 0 & u^{l_n} \end{pmatrix}.$$

We can translate inclusions of lattices in terms of matrices as follows. To each $n$-tuple $L = (a_1 \dots a_n)$ of elements of $W_n((u))$, associate the $n$-tuple $L' = (a'_1 \dots a'_n)$ where $a_1 + pa_2 + \dots + p^{n-1}a_n = [a'_1] + p[a'_2] + \dots + p^{n-1}[a'_n]$ is the $p$-adic expansion. To each square matrix $A$ with entries in $W_n((u))$, associate the matrix $A'$ obtained by replacing each of its lines $L$ by the line $L'$. Finally if $A, B$ are two matrices with entries in $k((u))$, let $A * B = ([A][B])'$ be the result of taking the Teichmüller representatives of the elements of the matrices, multiplying them as matrices with entries in $W_n((u))$ and then applying $(-)'$. Then, we have:

**Lemma.** *If $\mathfrak{M}_1$ and $\mathfrak{M}_2$ are lattices with matrices $A_1$ and $A_2$ then $\mathfrak{M}_1 \subset \mathfrak{M}_2$ if and only if $A_1$ is right divisible by $A_2$, that is, there exists a matrix $B$ such that $A_1 = B * A_2$.*

This allows to translate the conditions $E(u)\mathfrak{M} \subset \langle \phi(\mathfrak{M}) \rangle \subset \mathfrak{M}$ in terms of matrices and finally in terms of congruences (modulo powers of $u$) on the entries of $A$. These congruences are quite messy and in the end of the lecture, we shall restrict to the case $n = 3$.

### 7.3 The case $n = 3$

Here, we will compare the matrices associated to Breuil-Kisin lattices and the matrices arising from the Sekiguchi-Suwa construction. The main difficulty is that the former, resp. the latter, have entries in truncations of a dvr of equal characteristics, resp. unequal characteristics. Just for fun, the upshot of the comparison might be called the KASWSSBK theory, where

$$\text{KASWSSBK} := \text{Kummer-Artin-Schreier-Witt-Sekiguchi-Suwa-Breuil-Kisin}.$$

In the article *Models of group schemes of roots of unity*, we compared the two sides only under the additional assumption that $l_1 \geqslant pl_3$ because without this assumption, the computations on the Sekiguchi-Suwa side are really scary. Thus we make this assumption here also.

**7.3.1 Breuil-Kisin.** Recall that $R \simeq W[u]/(E)$ where $E = E(u)$ is the minimal polynomial of a chosen uniformizer $\pi \in R$, an Eisenstein polynomial. We can write a $p$-adic expansion $E = [E_0] + [E_1]p + \dots + [E_{n-1}]p^{n-1}$ where $E_i \in k[u]$. We saw that each finite flat model of $\mu_{p^3,K}$ is determined by a lattice of $W_3((u))$, itself described by a matrix

$$A = \begin{pmatrix} u^{l_3} & a_{12} & a_{13} \\ 0 & u^{l_2} & a_{23} \\ 0 & 0 & u^{l_n} \end{pmatrix}$$

satisfying some conditions. These conditions are expressed by congruences on the entries that we sort in five sets:

**A:** $a_{12}^p \equiv 0 \mod u^{l_2}$, $a_{23}^p \equiv 0 \mod u^{l_3}$

**B:** $\begin{cases} u^e a_{12} + u^{l_1} E_1 - u^{e-(p-1)l_1} a_{12}^p \equiv 0 \mod u^{pl_2} \\ u^e a_{23} + u^{l_2} E_1 - u^{e-(p-1)l_2} a_{23}^p \equiv 0 \mod u^{pl_3} \end{cases}$

**C:** $a_{12} - u^{l_1 - l_2} a_{23} \equiv 0 \mod u^{l_3}$

**D:** $u^{l_2} a_{13}^p - a_{12}^p a_{23} \equiv 0 \mod u^{l_2+l_3}$

**E:** $u^e a_{13} + a_{12} E_1 + \mathbb{S}_1(u^e a_{12}, u^{l_1} E_1) + u^{l_1} E_2 - u^{e-(p-1)l_1} a_{13}^p - \frac{u^e a_{12} + u^{l_1} E_1 - u^{e-(p-1)l_1} a_{12}^p}{u^{pl_2}} a_{23}^p \equiv 0 \mod u^{pl_3}$

In the last equation is used the two-variable function $\mathbb{S}_1(x, y) = [\frac{1}{p}(x^p + y^p - (x+y)^p)]^{1/p}$.

**7.3.2 Sekiguchi-Suwa.** It will be enough to restrict to matrices $A$ like in 5.3 whose entries are Teichmüller representatives, that is $\underline{a}_i^j = [a_i^j]$. Thus

$$A = \begin{pmatrix} \pi^{\ell_1} & [a_1^2] & [a_1^3] \\ 0 & \pi^{\ell_2} & [a_2^3] \\ 0 & 0 & \pi^{\ell_3} \end{pmatrix}.$$

Here again, the entries must satisfy congruences that can be sorted in five sets:

**A:** $(a_1^2)^p \equiv 0 \mod \pi^{l_2}$, $(a_2^3)^p \equiv 0 \mod \pi^{l_3}$

**B:** $\begin{cases} pa_1^2 - \pi^{l_1} - \frac{p}{\pi^{(p-1)l_1}}(a_1^2)^p \equiv 0 \mod \pi^{pl_2} \\ pa_2^3 - \pi^{l_2} - \frac{p}{\pi^{(p-1)l_2}}(a_2^3)^p \equiv 0 \mod \pi^{pl_3} \end{cases}$

**C:** ???

**D:** $\pi^{l_2}(a_1^3)^p \equiv a_2^3 (a_1^2)^p \mod \pi^{l_2+l_3}$

**E:** $\frac{p}{\pi^{(p-1)l_1}}(a_1^3)^p \equiv pa_1^3 - a_1^2 - (a_2^3)^p \, \frac{pa_1^2 - \pi^{l_1} - \frac{p}{\pi^{(p-1)l_1}}(a_1^2)^p}{\pi^{pl_2}} \mod \pi^{pl_3}$

**7.3.3 Comparison.** Since $R$ is complete with perfect residue field, its elements have $\pi$-adic expansions and we can define a map:

$$\begin{gathered} k[[u]] \longrightarrow R \\ c = \sum c_i u^i \longmapsto c^* = \sum [c_i] \pi^i. \end{gathered}$$

This is a bijection, which is neither additive nor multiplicative in general. It is an isometry, in the sense that for each $l$ the ideals $(u^l)$ and $(\pi^l)$ are mapped onto each other, and it induces bijections $k[[u]]/(u^l) \to R/(\pi^l)$. (In fact we shall need only the maps on the truncations; these can be defined without the assumption that $R$ is complete. Note that the Teichmüller representative $k \to R/(\pi^l)$ exists since $R/(\pi^l)$ is complete, see e.g. Serre, *Corps Locaux*.) The map $(-)^*$ can be used to associate to a matrix

$$A = \begin{pmatrix} u^{l_1} & a_{12} & a_{13} \\ 0 & u^{l_2} & a_{23} \\ 0 & 0 & u^{l_3} \end{pmatrix}$$

with entries in $k[[u]]$ the matrix

$$A^* = \begin{pmatrix} [\pi^{l_1}] & [a_{12}^*] & [a_{13}^*] \\ 0 & [\pi^{l_2}] & [a_{23}^*] \\ 0 & 0 & [\pi^{l_3}] \end{pmatrix}.$$

with entries Teichmüller elements in $W(R)$. The basic thing we want to do is to check that if $A$ is a matrix satisfying the Breuil-Kisin congruences, then $A^*$ is a matrix satisfying the Sekiguchi-Suwa congruences. Although we do not really know if the map $(-)^*$ computes the Breuil-Kisin equivalence (or its inverse), if we pretend it does, then this will show that all models of $\mu_{p^3,K}$ satisfying $l_1 \geqslant pl_3$ are those we have constructed.

There seems to be an extra condition **C** on the Breuil-Kisin side, but in fact its image $\mathbf{C}^*$ holds on the Sekiguchi-Suwa side because it can be proved easily that it is a consequence of the others.

Checking the compatibility of the conditions **A** is immediate; for **B** we will indicate how it works; for **C** there is nothing to say, as we indicated; checking conditions **D** and **E** is more tedious but can be done.

Thus we just have a glimpse on **B**, in order to see what the whole computation looks like. If we take the image under $(-)^*$ of the first of the congruences in **B**:

$$u^e a_{12} + u^{l_1} E_1 - u^{e-(p-1)l_1} a_{12}^p \equiv 0 \mod u^{pl_2},$$

we obtain

$$\pi^e a_{12}^* + \pi^{l_1}[E_1](\pi) - \pi^{e-(p-1)l_1}(a_{12}^*)^p \equiv 0 \mod \pi^{pl_2}.$$

Since $E$ is Eisenstein, we have $E(u) \equiv u^e + [E_1(u)]p \mod p^2$ with $\deg(E_1(u)) < e$ and $E_1(0) \neq 0$. Since $E(\pi) = 0$, we obtain $\pi^e + p[E_1](\pi) \equiv 0 \mod p^2$. Given that $p^2 \equiv 0 \mod \pi^{pl_2}$, we can replace $\pi^e$ by $-p[E_1](\pi)$ in the above congruence. Working a little bit, one finds that this is exactly the first congruence **B** on the Sekiguchi-Suwa side satisfied by the parameters $a_i^j := a_{ij}^*$.

In order to conclude, it is important to emphasize that we do not know if the map $(-)^*$ really computes the functor $\mathrm{Gr}_n \to \mathrm{Mod}_n$ of Breuil and Kisin. This is why we write *almost sure* instead of *true* in the following statement. Recall that the Kummer group schemes are the models of $\mu_{p^n,K}$ constructed using the Sekiguchi-Suwa theory in section 6.

**Theorem.** *It is almost sure that for $l_1 \geqslant pl_3$, all models of $\mu_{p^3,K}$ are Kummer group schemes.*

However, the formalism for the comparison has been settled for all $n$ and the evidence for the following conjecture seems quite solid.

**Conjecture.** *For all $n \geqslant 1$, all models of $\mu_{p^n,K}$ are Kummer group schemes.*

## References


[Br00] Ch. Breuil, *Groupes p-divisibles, groupes finis et modules filtrés*, Ann. of Math. 2000.

[Ki09] M. Kisin, *Moduli of finite flat group schemes, and modularity*, Ann. of Math. 2009.

[KSB88] J. Kollár, N. Shepherd-Barron, *Threefolds and deformations of surface singularities*, Invent. Math. 1988.

[MRT12] A. Mézard, M. Romagny, D. Tossici, *Models of group schemes of roots of unity*, Ann. Inst. Fourier, to appear.

[Ro12] M. Romagny, *Effective models of group schemes*, J. of Algebraic Geom., to appear.

[$\mathrm{SS}_i$], T. Sekiguchi, N. Suwa, *A note on extensions of algebraic and formal groups $i = 1 \ldots 5$*, Math. Z. 1991, Math. Z. 1994, Tôhoku Math. J. 1997, Tôhoku Math. J. 2001, Japanese J. of Math. 2003.

[SS99], T. Sekiguchi, N. Suwa, *On the unified Kummer-Artin-Schreier-Witt theory*, Univ. Bordeaux 1 preprint series, 1999.