ANNALES DE L'INSTITUT FOURIER

ANNALES

DE

L'INSTITUT FOURIER

A. MÉZARD, M. ROMAGNY & D. TOSSICI

Models of group schemes of roots of unity

Tome 63, 3 (2013), p. 1055-1135.

<http://aif.cedram.org/item?id=AIF_2013__63_3_1055_0>

Ann. Inst. Fourier, Grenoble
63, 3 (2013) 1055-1135

MODELS OF GROUP SCHEMES OF ROOTS OF UNITY

by **A. MÉZARD, M. ROMAGNY & D. TOSSICI**

ABSTRACT. — Let $\mathcal{O}_K$ be a discrete valuation ring of mixed characteristics $(0,p)$, with residue field k. Using work of Sekiguchi and Suwa, we construct some finite flat $\mathcal{O}_K$-models of the group scheme $\mu_{p^n,K}$ of p^n-th roots of unity, which we call *Kummer group schemes*. We carefully set out the general framework and algebraic properties of this construction. When k is perfect and $\mathcal{O}_K$ is a complete totally ramified extension of the ring of Witt vectors $W(k)$, we provide a parallel study of the Breuil-Kisin modules of finite flat models of $\mu_{p^n,K}$, in such a way that the construction of Kummer groups and Breuil-Kisin modules can be compared. We compute these objects for $n \leqslant 3$. This leads us to conjecture that all finite flat models of $\mu_{p^n,K}$ are Kummer group schemes.

RÉSUMÉ. — Soit $\mathcal{O}_K$ un anneau de valuation discrète de caractéristique mixte $(0,p)$, de corps résiduel k. Utilisant un travail de Sekiguchi et Suwa, nous construisons des modèles finis plats sur $\mathcal{O}_K$ du schéma en groupes $\mu_{p^n,K}$ des racines p^n-ièmes de l'unité, que nous appelons *schémas en groupes de Kummer*. Nous développons soigneusement le cadre général et les propriétés algébriques de cette construction. Lorsque k est parfait et $\mathcal{O}_K$ est une extension complète totalement ramifiée de l'anneau des vecteurs de Witt $W(k)$, nous étudions en parallèle les modules de Breuil-Kisin des modèles finis plats de $\mu_{p^n,K}$, de telle manière que les constructions des groupes de Kummer et des modules de Breuil-Kisin peuvent être comparées. Nous calculons ces objets pour $n \leqslant 3$. Cela nous mène à conjecturer que tous les modèles finis plats de $\mu_{p^n,K}$ sont des schémas en groupes de Kummer.

1. Introduction

1.1. Context. Let k be a perfect field of characteristic p, $W(k)$ its ring of Witt vectors, K_0 the fraction field of $W(k)$, K/K_0 a finite totally ramified field extension, and $\mathcal{O}_K$ its ring of integers. The aim of the present paper is the determination of the models over $\mathcal{O}_K$ of the group scheme $\mu_{p^n,K}$ of roots of unity, or what is the same by Cartier duality, of the cyclic group scheme

Keywords: group schemes, roots of unity, Breuil-Kisin module.
Math. classification: 14L15.

$(\mathbb{Z}/p^n\mathbb{Z})_K$. Apart from the intrinsic interest of the problem, a first motivation for doing this lies in the study of the representations of the absolute Galois group of K. Indeed, finite flat group schemes and p-divisible groups are extremely important examples of crystalline representations. Work of Fontaine, Breuil and Kisin has culminated into a fairly nice description of these groups using modules with semilinear Frobenius. This description remains however very abstract and many arithmetico-geometric properties of the group schemes do not have an easy translation in terms of modules. Thus, one is in search of concrete examples witnessing the constructions and conjectures of the general theory, like the filtrations defined by Abbes-Saito [1] and Fargues [10]. We wish to provide such explicit examples and test these general constructions.

Another important motivation is to understand the reduction of Galois covers of K-varieties. In the case of covers of curves, it is visible already for isogenies of elliptic curves (Katz-Mazur [15]) but also in higher genus (Abramovich-Romagny [2]) that it is necessary to let degenerate, along with the varieties, also the Galois group of the covers. The existence of such group degenerations is studied more precisely in [23] and [30]. In the particular case of cyclic covers, this leads to the question of understanding the models of $\mathbb{Z}/p^n\mathbb{Z}$. Here it is worth emphasizing that whereas in the context of Galois representations one is by choice sticking to the original field K, in the context of reduction of covers it is natural to allow finite extensions K'/K. This enhances the importance of cyclic K-group schemes, since any finite flat commutative group scheme becomes isomorphic to a product of such after a finite field extension.

A third motivation comes from the problem of finding an explicit description of the Hopf algebras of group schemes over a discrete valuation ring with prescribed generic fiber G, in other words the Hopf orders of the algebra $K[G]$. The most studied and best-known case is that of $G = \mu_{p^n,K}$. Going beyond the Tate-Oort classification [29], work in this trend is due mainly to Larson [18], Greither [12], Byott [5], Underwood [32] and Childs [7]. As a result, one has a complete classification of Hopf orders for $n = 1, 2$ and a wealth of examples for $n = 3$. One difference between our approach and some of these constructions is that we shall find descriptions which offer information about the cohomology of the associated group schemes. Another important feature of our constructions is that they require no assumption on the discretely valued field K, whereas the results obtained by the above authors are valid for K complete, with perfect residue field, containing a primitive p^n-th root of unity.

1.2. Our approach. In this text, building on work of Sekiguchi and Suwa, we present a family of finite flat models of $\mu_{p^n,K}$ which we call *Kummer group schemes*. For this, we consider models of $(\mathbb{G}_{m,K})^n$ constructed by successive extensions of affine, smooth, one-dimensional models of $\mathbb{G}_{m,K}$ with connected fibres, called *filtered group schemes*. Kummer group schemes are defined as the kernels G of some well-chosen isogenies $\mathcal{E} \to \mathcal{F}$ between filtered group schemes, and their name comes from the fact that the exact sequence $0 \to G \to \mathcal{E} \to \mathcal{F} \to 0$ is an integral model of the usual Kummer isogeny. This sequence is especially well-suited for the description of torsors under the group schemes at hand, which as we said before is one of our motivations. We also point out that the isogenies are given by explicit equations, and hence so are the kernels. We formulate the following conjecture:

CONJECTURE. — *Any model of $\mu_{p^n,K}$ over $\mathcal{O}_K$ is a Kummer group scheme.*

Our aim is to give strong evidence for this statement. We remark that this conjecture is true, without assuming the discrete valuation ring complete with perfect residue field, in the case $n \leqslant 2$ (for $n = 1$ see e.g. [33], discussion after Theorem 2.5, and for $n = 2$ see [31]). In order to explain why we think it is true in general and what we actually do, let us first consider the category of finite flat models of $\mu_{p^n,K}$. Using scheme-theoretic closures, it is not hard to see that any morphism $G \to G'$ between finite flat $\mathcal{O}_K$-group schemes factors as the composition $G \twoheadrightarrow G/N \to H \hookrightarrow G'$ of the quotient by a finite flat subgroup scheme, a morphism which is an isomorphism on the generic fibre (a so-called *model map*) and the closed immersion of a finite flat subgroup scheme. Models of $\mu_{p^n,K}$ are special because they have a unique (finite, flat) subgroup and quotient of a given order. Thus the category of models of $\mu_{p^n,K}$ may be completely described by the subcategory of groups with model maps as morphisms, which is just a partially ordered set $(\mathscr{C}_n, \geqslant)$, and the two families of functors $Q_i, S_i : \mathscr{C}_n \to \mathscr{C}_i$ given by the finite flat quotient of degree p^{n+1-i}, and the finite flat subgroup of degree p^{n+1-i}, for $i \in \{1, \dots, n+1\}$.

Now let us describe what we do. As we said, we take up and extend a construction of Sekiguchi and Suwa, and use it to produce models of μ_{p^n}, the Kummer group schemes. These group schemes are parametrized by matrices with coefficients in the ring of Witt vectors $W(\mathcal{O}_K)$. The choice of a uniformizer π for $\mathcal{O}_K$ allows to single out a certain set $\mathscr{M}_n$ of upper triangular matrices with an interesting structure: it is embedded in a bigger set of matrices endowed with a non-associative product, giving rise to a

natural order $\succ$. This set has also operators $\mathcal{U}^i$ and $\mathcal{L}^i$ that take a matrix to its "upper left" and "lower right" square submatrices.

Then, we study Breuil-Kisin modules of models of $\mu_{p^n,K}$. They can be identified with u-integral lattices of the ring of Laurent series $W_n(k)((u))$, where k is the residue field of K. The set $\mathscr{L}_n$ of lattices is ordered by inclusion and is endowed with functors $K_i, I_i : \mathscr{L}_n \to \mathscr{L}_i$ given by the kernel and image of the endomorphisms p^{n+1-i} and p^{i-1} of a given lattice. The lattices have unique distinguished systems of generators whose p-adic coefficients can be put together into an upper triangular matrix. In this way, we obtain a set $\mathscr{G}_n$ of matrices with coefficients in $k((u))$, with a non-associative product very similar to that of $\mathscr{M}_n$ and giving rise to a natural order $\succ$. This set also has functors $\mathcal{U}^i$ and $\mathcal{L}^i$.

Although not quite "isomorphic", the partially ordered sets $(\mathscr{C}_n, \geqslant)$, $(\mathscr{M}_n, \succ)$ and $(\mathscr{G}_n, \succ)$ with their pairs of functors have strong analogies. There are natural functors $\mathscr{M}_n \to \mathscr{C}_n \xrightarrow{\sim} \mathscr{G}_n$ given by mapping a matrix to the Kummer group scheme it defines, and then to the Breuil-Kisin module of that group. The second functor is an equivalence, constructed in [16]. The basic idea to prove the conjecture above is to compute the Breuil-Kisin modules of Kummer groups and check that all modules can be obtained in this way. Unfortunately, there is no direct way to compute Breuil-Kisin modules. However, computations for $n = 2$ (done by Caruso in [31] Appendix A) and $n = 3$ (done in the present article) show a surprising phenomenon: it seems that if we replace π by u in the matrix of a Kummer group, we obtain the matrix of its Breuil-Kisin lattice. In fact, we set up a precise, nontrivial dictionary that indicates how to translate the congruences in a discrete valuation ring of characteristic 0 on one side, into congruences in a discrete valuation ring of characteristic p on the other side. The reader may be inspired by a look at the tables in 8.2.6 (comparison for $n = 2$) and 8.3.5 (comparison for $n = 3$ under a simplifying assumption). She/he will see for her/himself how striking the correspondence is. However, we wish to say that writing the dictionary already for $n = 3$ in the general case seems challenging.

Finally we observe that in particular we prove that Breuil-Kisin modules of models of μ_{p^n} are classified by $\frac{n(n+1)}{2}$ parameters, as conjectured, in [13] and [8], more generally for all models of a fixed group scheme of order p^n. Moreover the Kummer group schemes we constructed form a family with exactly this number of parameters.

1.3. Summary of contents. Here is a short overview of the contents of the article; each section starts with a more detailed introduction. The

article is divided in two parts written to be readable independently (to a reasonable extent). The first part (§§2-5) is devoted to Breuil-Kisin Theory over a complete discrete valuation ring with perfect residue field. We apply that theory in order to parametrize the models of μ_{p^n} in terms of Breuil-Kisin modules (§2). Then we explain the algebraic structure (called a *loop*) of a certain set of matrices (§3) allowing us to rewrite Breuil-Kisin modules in matricial terms (§4). The main result of this first part is Theorem 4.2.2 which is a computable interpretation of Breuil-Kisin Theory (§4.2). The second part (§§6-8) is devoted to Sekiguchi-Suwa Theory over a general discrete valuation ring of unequal characteristics. We recall the construction of *filtered group schemes* and formalize it in matricial terms (§6). Then we describe the conditions for certain model maps of filtered group schemes to be isogenies, whose kernels are by definition the Kummer group schemes (§7). Finally we proceed with the explicit computation of models of μ_{p^3} (§8) with a comparison of the congruences coming from Breuil-Kisin Theory and Sekiguchi-Suwa Theory (8.2.6 an 8.3.5).

1.4. Acknowledgements. We thank Xavier Caruso, Marco Garuti, Noriyuki Suwa and Angelo Vistoli for interesting conversations related to this article. We are also grateful to Christophe Breuil for valuable comments on the genesis of the classification of finite flat group schemes and to Lindsay Childs who kindly sent us a version of the paper [13]. We thank the referee for his careful reading which allowed to correct several inaccuracies. The first and second authors especially enjoyed a stay in the Scuola Normale Superiore di Pisa where part of this work was done. The third author had fruitful stays at the MPIM in Bonn, at the IHES in Bures-sur-Yvette, and spent some time in Paris to work on this project invited by the University Paris 6, the University of Versailles Saint-Quentin and the IHP, during the Galois Trimester. The three authors also spent a very nice week in the CIRM in Luminy. We thank all these institutions for their support and hospitality.

2. Breuil-Kisin modules and μ-lattices

In this section, we recall the description due to Breuil and Kisin of the category of finite flat group schemes (understood commutative, of p-power order) in terms of modules with Frobenius. Then, we specialize to the subcategory of models of the group scheme μ_{p^n} of roots of unity.

We fix the following notations. Let k be a perfect field of characteristic p, $W = W(k)$ the ring of Witt vectors with coefficients in k, and $\mathfrak{S} = W[[u]]$. We write $W_n = W_n(k)$ the ring of Witt vectors of length n and $\mathfrak{S}_n = W_n[[u]]$. The rings $\mathfrak{S}$ and $\mathfrak{S}_n$ are endowed with a ring endomorphism ϕ which is continuous for the u-adic topology, defined as the usual Frobenius on $W_n(k)$ and by $\phi(u) = u^p$. Let K_0 be the fraction field of $W(k)$, let K/K_0 be a totally ramified extension of degree e and $\mathcal{O}_K$ its ring of integers. We fix a uniformizer π of K and denote by $E(u)$ its minimal polynomial over K_0 and v the p-adic valuation with $v(\pi) = 1$. We always use the phrase *finite flat group scheme* as a shortcut for *commutative finite flat group scheme of p-power order*. We denote by $(\mathrm{Gr}/\mathcal{O}_K)$ the corresponding category.

2.1. Breuil-Kisin modules of finite flat group schemes

2.1.1. — The Breuil-Kisin Theorem. In recent papers, Breuil and Kisin have proven a classification theorem for finite flat $\mathcal{O}_K$-group schemes, in terms of the category $(\mathrm{Mod}/\mathfrak{S})$ described as follows:

- the objects of $(\mathrm{Mod}/\mathfrak{S})$ are the finitely generated $\mathfrak{S}$-modules $\mathfrak{M}$ of projective dimension 1, killed by some power of p, and endowed with a ϕ-semilinear map $\phi_{\mathfrak{M}} : \mathfrak{M} \to \mathfrak{M}$ such that $E(u)\mathfrak{M}$ is contained in the $\mathfrak{S}$-module generated by $\phi_{\mathfrak{M}}(\mathfrak{M})$.
- the morphisms in $(\mathrm{Mod}/\mathfrak{S})$ are the $\mathfrak{S}$-linear maps compatible with ϕ.

For any $\mathfrak{M} \in (\mathrm{Mod}/\mathfrak{S})$, the map $\phi_{\mathfrak{M}}$ is called the *Frobenius* and most often written simply ϕ. Note that to ϕ is associated a *linear* map $\phi^*\mathfrak{M} \to \mathfrak{M}$, where $\phi^*\mathfrak{M} := \mathfrak{M} \otimes_{\mathfrak{S},\phi} \mathfrak{S}$. The classification of Breuil and Kisin is the following:

2.1.2. — Theorem. *There is a contravariant exact equivalence of categories* $(\mathrm{Gr}/\mathcal{O}_K) \to (\mathrm{Mod}/\mathfrak{S})$.

One may compose with Cartier duality to get a covariant equivalence, and in this paper this is what we will do.

The category $(\mathrm{Mod}/\mathfrak{S})$ was introduced in [3]. To be more precise, Breuil required moreover that the underlying $\mathfrak{S}$-module of an object $(\mathrm{Mod}/\mathfrak{S})$ should be a finite direct sum of modules $\mathfrak{S}/p^{n_i}\mathfrak{S}$. He conjectured the existence of an equivalence between $(\mathrm{Mod}/\mathfrak{S})$ and the category of finite flat group schemes whose p^m-kernels are finite flat for all m, and he proved the conjecture for group schemes killed by p, when $p > 2$. After that, Kisin realized that arbitrary finite flat group schemes could be taken into account

by requiring the underlying modules merely to have projective dimension 1, and he proceeded to prove the conjecture in general (see [16], Thm 0.5) for $p > 2$. Later Lau [19] and Liu [20] independently proved that the statement also holds for $p = 2$, which in fact was the original motivation of the note of Breuil [3].

For the convenience of the reader, here is a very rough sketch of how the equivalence of the theorem works. Let S denote the p-adic completion of the divided power envelope of $W[u]$ with respect to the ideal generated by $E(u)$. There is a natural inclusion $\mathfrak{S} \to S$ but one has to notice that the ring S is much more complicated than $\mathfrak{S}$. Breuil introduces a category (Mod/S) whose objects are S-modules with a 1-step filtration and a semi-linear Frobenius. On the syntomic site of the formal scheme $\mathrm{Spf}(\mathcal{O}_K)$, all finite flat group schemes define abelian sheaves. Breuil constructs another abelian sheaf $\mathcal{O}^{\mathrm{cris}}_{\mathscr{C},\pi}$. This sheaf plays the role of a sort of dualizing object: Breuil shows that there is a contravariant equivalence $(\mathrm{Gr}/\mathcal{O}_K) \to (\mathrm{Mod}/S)$ that takes a group scheme G to the module $\mathrm{Hom}(G, \mathcal{O}^{\mathrm{cris}}_{\mathscr{C},\pi})$, with a quasi-inverse that takes a module $\mathcal{M}$ to the group scheme that represents the syntomic sheaf $\mathfrak{X} \mapsto \mathrm{Hom}(\mathcal{M}, \mathcal{O}^{\mathrm{cris}}_{\mathscr{C},\pi}(\mathfrak{X}))$. Now there is a covariant functor $(\mathrm{Mod}/\mathfrak{S}) \to (\mathrm{Mod}/S)$ given by tensoring with the map $\phi : \mathfrak{S} \to S$. Kisin proves that for any $\mathcal{M} \in (\mathrm{Mod}/S)$ there is a unique sub-$\mathfrak{S}$-module $\mathfrak{M} \subset \mathcal{M}$ such that $E(u)\mathfrak{M} \subset \langle \phi(\mathfrak{M}) \rangle \subset \mathfrak{M}$. Moreover we can recover $\mathcal{M}$ from this submodule in the sense that $\mathcal{M} \simeq \mathfrak{M} \otimes_{\mathfrak{S},\phi} S$ so that $(\mathrm{Mod}/\mathfrak{S}) \to (\mathrm{Mod}/S)$ is an equivalence.

2.1.3. — Group schemes killed by p^n. The modules killed by p^n correspond to the group schemes killed by p^n. We will use a somewhat different description of the full subcategory of $(\mathrm{Mod}/\mathfrak{S})$ of modules killed by p^n, based on the following lemma.

2.1.4. — Lemma. *Let $\mathfrak{M}$ be an $\mathfrak{S}$-module endowed with a ϕ-semilinear map $\phi : \mathfrak{M} \to \mathfrak{M}$ such that* $\mathrm{coker}(\phi^*\mathfrak{M} \to \mathfrak{M})$ *is killed by $E(u)$. Assume that $\mathfrak{M}$ is killed by p^n. Then $\mathfrak{M}$ is an $\mathfrak{S}$-module of projective dimension 1 if and only if $\mathfrak{M}$ is a finite $\mathfrak{S}_n$-module without u-torsion.*

Proof. — It follows from [16], Lemma 2.3.2 that $\mathfrak{M}$ has projective dimension 1 if and only if it is an iterated extension of finite free $\mathfrak{S}/p\mathfrak{S}$-modules. By induction, it is immediate that this is equivalent to the fact that $\mathfrak{M}$ is a finite $\mathfrak{S}_n$-module without u-torsion. □

Therefore, the full subcategory of $(\mathrm{Mod}/\mathfrak{S})$ of modules killed by p^n is the category $(\mathrm{Mod}/\mathfrak{S})_n$ defined as follows:

- the objects of $(\mathrm{Mod}/\mathfrak{S})_n$ are the finite $\mathfrak{S}_n$-modules $\mathfrak{M}$ with no u-torsion endowed with a ϕ-semilinear map $\phi : \mathfrak{M} \to \mathfrak{M}$ such that $\mathrm{coker}(\phi^*\mathfrak{M} \to \mathfrak{M})$ is killed by $E(u)$.
- the morphisms in $(\mathrm{Mod}/\mathfrak{S})_n$ are the $\mathfrak{S}_n$-linear maps compatible with ϕ.

We now record some basic facts concerning $(\mathrm{Mod}/\mathfrak{S})_n$.

2.1.5. — Lemma. *For any object $\mathfrak{M}$ of $(\mathrm{Mod}/\mathfrak{S})_n$ the map $\phi^*\mathfrak{M} \to \mathfrak{M}$ is injective.*

Proof. — This is [17], Lemma 1.1.9. □

2.1.6. — Lemma. *The category $(\mathrm{Mod}/\mathfrak{S})_n$ has kernels, cokernels, images and coimages. Kernels and images are given as the kernels and images in the category of $\mathfrak{S}$-modules.*

Proof. — Let us prove first that $(\mathrm{Mod}/\mathfrak{S})_n$ has kernels and images. For a morphism $f : \mathfrak{M} \to \mathfrak{N}$, let $\mathfrak{K}$ and $\mathfrak{I}$ be the kernel and the image in the category of $\mathfrak{S}_n$-modules. It is easy to see that $\mathfrak{K}$ and $\mathfrak{I}$ are finite $\mathfrak{S}_n$-modules, stable under ϕ, with no u-torsion. Also note that the map $f' := \phi^* f : \phi^*\mathfrak{M} \to \phi^*\mathfrak{N}$ has kernel $\phi^*\mathfrak{K}$ (since ϕ is flat) and image $\phi^*\mathfrak{I}$. The main point is to see that $E(u)$ kills the cokernels of the maps $\phi^*\mathfrak{K} \to \mathfrak{K}$ and $\phi^*\mathfrak{I} \to \mathfrak{I}$. We start with the kernel. For any $x \in \mathfrak{K}$ we have $x \in \mathfrak{M}$ and since the cokernel of $\phi^*\mathfrak{M} \to \mathfrak{M}$ is killed by $E(u)$ there exists $y \in \mathfrak{M}'$ such that $E(u)x = \phi(y)$. Then $f'(y)$ maps to 0 in $\mathfrak{N}$ and hence is 0 in $\phi^*\mathfrak{N}$. It follows that $y \in \phi^*\mathfrak{K}$, as desired. We come to the image. Let $x \in \mathfrak{I}$ so that $x = f(y)$ for some $y \in \mathfrak{N}$. Then there exists $z \in \phi^*\mathfrak{N}$ such that $E(u)y = \phi(z)$. Therefore $E(u)x = \phi(f'(z))$ with $f'(z) \in \phi^*\mathfrak{I}$, as desired.

By Theorem 2.1.2, there is on $(\mathrm{Mod}/\mathfrak{S})_n$ a contravariant exact involutive equivalence given by Cartier duality. It follows that $(\mathrm{Mod}/\mathfrak{S})_n$ has cokernels and coimages. □

2.1.7. — *Remark.* In general, for a morphism $f : \mathfrak{M} \to \mathfrak{N}$ the objects $\mathrm{coker}(\ker(f))$ and $\ker(\mathrm{coker}(f))$ are not isomorphic. In the category $(\mathrm{Mod}/\mathfrak{S})_n$ this is not so easy to see, because we have not worked out the description of cokernels. Things are a little easier in the category of finite flat group schemes. There, the kernel of a map $u : G \to H$ is the scheme-theoretic closure of the kernel of the generic fibre $u_K : G_K \to H_K$ inside G, and the cokernel is the Cartier dual of the kernel of the dual of u. For example, if R contains a primitive p-th root of unity and $u : (\mathbb{Z}/p\mathbb{Z})_R \to \mu_{p,R}$ is an isomorphism on the generic fibre, then $\ker(u) = \mathrm{coker}(u) = 0$ even though u is not an isomorphism.

2.2. Lattices of $W_n((u))$

We shall see in 2.3 that the Breuil-Kisin modules of models of μ_{p^n} can be identified with lattices in the $W_n[[u]]$-module $W_n((u))$. For this reason, it is useful to collect some basic facts on these lattices; knowing their generating systems will be particularly important in Section 4. Since the lattices we are interested in are Breuil-Kisin modules, for simplicity we keep the letters $\mathfrak{M}, \mathfrak{N}$ (etc.) to denote them.

2.2.1. — Definition. A *lattice* $\mathfrak{M}$ is a finitely generated sub-$W_n[[u]]$-module of $W_n((u))$ such that $\mathfrak{M}[1/u] = W_n((u))$. We denote by $\mathscr{L}_n$ the partially ordered set of lattices with inclusions between them. If a lattice $\mathfrak{M}$ is contained in $W_n[[u]]$, we say that it is *positive* and we write $\mathfrak{M} \geqslant 0$.

Note that it is simpler here not to follow british mathematical usage, so we say *positive* instead of *non-negative*.

For any two lattices $\mathfrak{M}, \mathfrak{N}$, there exists $\alpha \in \mathbb{N}$ such that $u^\alpha \mathfrak{N} \subset \mathfrak{M}$. We define the *volume (or index) of* $\mathfrak{M}$ *with respect to* $\mathfrak{N}$ as

$$\mathrm{vol}(\mathfrak{M}, \mathfrak{N}) = u^{n\alpha - \mathrm{lg}(\mathfrak{M}/u^\alpha \mathfrak{N})}$$

where lg denotes the length as a $W_n[[u]]$-module. Using the fact that $\mathrm{lg}(\mathfrak{N}/u^\alpha\mathfrak{N}) = n\alpha$, one sees that the definition is indeed independent of α. Although our base ring is not a Dedekind ring, this is the analogue of the symbol $\chi(\mathfrak{M}, \mathfrak{N})$ of [10], déf. 5 and [27], chap. III, no. 1. The *volume (or index) of* $\mathfrak{M}$ is defined by $\mathrm{vol}(\mathfrak{M}) = \mathrm{vol}(\mathfrak{M}, W_n[[u]])$, and we have $\mathrm{vol}(\mathfrak{M}, \mathfrak{N}) = \mathrm{vol}(\mathfrak{M})/\mathrm{vol}(\mathfrak{N})$.

2.2.2. — Kernels and images of p. For any lattice $\mathfrak{M}$ and any integer i with $1 \leqslant i \leqslant n+1$, we define $\mathfrak{M}[i] = \ker(p^{n+1-i} : \mathfrak{M} \to \mathfrak{M})$ and $\mathfrak{M}(i) = \mathrm{im}(p^{i-1} : \mathfrak{M} \to \mathfrak{M})$. We have $\mathfrak{M}(i) \subset \mathfrak{M}[i]$ and these submodules fit into compatible decreasing filtrations:

$$\begin{array}{ccccccccc}
\mathfrak{M} = & \mathfrak{M}[1] & \supsetneq & \cdots & \supsetneq & \mathfrak{M}[n] & \supsetneq & \mathfrak{M}[n+1] = 0 \\
& \cup & & & & \cup & & \cup & \\
\mathfrak{M} = & \mathfrak{M}(1) & \supsetneq & \cdots & \supsetneq & \mathfrak{M}(n) & \supsetneq & \mathfrak{M}(n+1) = 0\ .
\end{array}$$

For any two submodules $\mathfrak{N}, \mathfrak{N}'$ of $W_n((u))$, consider the ideal

$$(\mathfrak{N} : \mathfrak{N}') = \{x \in W_n[[u]]\ ,\ x\mathfrak{N}' \subset \mathfrak{N}\}.$$

Let $1 \leqslant i \leqslant j \leqslant n+1$ be integers. One can see easily, by inverting u, that

$$(\mathfrak{M}[j] : \mathfrak{M}[i]) = (\mathfrak{M}(j) : \mathfrak{M}(i)) = p^{j-i} W_n[[u]].$$

Besides, since $\mathfrak{M}$ has no u-torsion then $\mathfrak{M}[i] \cap \mathfrak{M}[j][1/u] = \mathfrak{M}[j]$ and the map

$$\mathfrak{M}[i]/\mathfrak{M}[j] \longrightarrow \mathfrak{M}[i][1/u]/\mathfrak{M}[j][1/u]$$

is injective. Since

$$\mathfrak{M}[i][1/u] = p^{i-1}W_n((u))$$

and

$$p^{i-1}W_n((u))/p^{j-1}W_n((u)) = W_{j-i}((u)),$$

this proves that $\mathfrak{M}[i]/\mathfrak{M}[j]$ is canonically a lattice of $W_{j-i}((u))$. Exactly the same arguments show that $\mathfrak{M}(i)/\mathfrak{M}(j)$ is canonically a lattice of $W_{j-i}((u))$. In particular, for $j = n+1$ this says that $\mathfrak{M}[i]$ and $\mathfrak{M}(i)$ are lattices of $W_{n+1-i}((u))$.

2.2.3. — Generating sets. For each $x \in k$, let $[x] \in W(k)$ be its *Teichmüller representative* (see 3.1 for a reminder on this notion). The map $x \mapsto [x]$ is the unique multiplicative section of the projection onto the residue field. If $e_1, \dots, e_n$ is a set of generators for $\mathfrak{M}$, then we will call *T-combination* a linear combination $t_1e_1 + \cdots + t_ne_n$ where $t_1, \dots, t_n$ are Teichmüller representatives. In the following result, and in other places of the paper, we use the same letter for the valuation of a discrete valuation ring and for the induced function on its artinian quotients.

2.2.4. — Lemma. *Let $\mathfrak{M}$ be a lattice of $W_n((u))$ and let $e_1, \dots, e_n$ be a system of generators. Let v_p denote the p-adic valuation on W_n. Then the following conditions are equivalent:*

(1) *For $1 \leqslant i \leqslant n$, we have $v_p(e_i) = i-1$ and $pe_i \in \langle e_{i+1}, \dots, e_n\rangle$.*
(2) *For $1 \leqslant i \leqslant n$, we have $\mathfrak{M}[i] = \langle e_i, \dots, e_n\rangle$.*
(3) *For $1 \leqslant i \leqslant n$, we have $v_p(e_i) = i-1$ and each element $x \in \mathfrak{M}$ can be written in a unique way as a T-combination $x = [x_1]e_1 + \cdots + [x_n]e_n$ with $x_i \in k[[u]]$.*

Proof. — (1) $\Rightarrow$ (2). Set $\mathfrak{N}_i = \langle e_i, \dots, e_n\rangle$. It is obvious that $\mathfrak{N}_i \subset \mathfrak{M}[i]$, so we only prove the opposite inclusion. Since $v_p(e_i) = i-1$, we have $\mathfrak{N}_i[1/u] = p^{i-1}W_n((u))$. Let $x \in \mathfrak{M}[i]$ and write

$$x = x_1'e_1 + \cdots + x_n'e_n$$

for some coefficients $x_i' \in W_n[[u]]$. The fact that $pe_i \in \mathfrak{N}_{i+1}$ implies that this linear combination may be transformed into a T-combination $x = [x_1]e_1 + \cdots + [x_n]e_n$. If $x \neq 0$ there exists ν minimal such that $x_\nu \neq 0$. Then the assumption that $x \in \mathfrak{M}[i]$ gives $[x_\nu]e_\nu \in \mathfrak{M}[i] + \mathfrak{N}_{\nu+1}$. After

tensoring with $W_n((u))$ we obtain

$$p^{\nu-1}W_n((u)) \subset p^{i-1}W_n((u)) + p^{\nu}W_n((u)) = p^{\min(i-1,\nu)}W_n((u))$$

hence $\nu \geqslant i$, so that $x \in \mathfrak{N}_i$.

(2) $\Rightarrow$ (3). From $\mathfrak{M}[i][1/u] = p^{i-1}W_n((u))$ we deduce by decreasing induction on i that $v_p(e_i) = i-1$. Now fix $x \in \mathfrak{M}$. Since $p\mathfrak{M}[i] \subset \mathfrak{M}[i+1]$, we have $pe_i \in \langle e_{i+1}, \dots, e_n\rangle$ for all i. Using this, we may as above write x as a T-combination $x = [x_1]e_1 + \cdots + [x_n]e_n$ with $x_i \in k[[u]]$. Moreover, if $[x_1]e_1 + \cdots + [x_n]e_n = [x'_1]e_1 + \cdots + [x'_n]e_n$ are two expressions for x, then $([x_1] - [x'_1])e_1 \in \mathfrak{M}[2]$. From the fact that $(\mathfrak{M}[2] : \mathfrak{M}[1]) = pW_n[[u]]$ it follows that $[x_1] - [x'_1] \in pW_{n+1}[[u]]$ and hence $x_1 - x'_1 = 0$. By induction we get similarly $x_i = x'_i$ for all i.

(3) $\Rightarrow$ (1). Since $v_p(e_i) = i-1$, the p-valuation of a nonzero element $[x_1]e_1 + \cdots + [x_n]e_n$ is equal to $\nu - 1$ where ν is the least integer such that $x_\nu \neq 0$. For $x = pe_i$ we find $\nu = i+1$, so that $pe_i \in \langle e_{i+1}, \dots, e_n\rangle$. □

2.2.5. — Definition. A set of generators $e_1, \dots, e_n$ of a lattice $\mathfrak{M}$ satisfying the equivalent conditions of Lemma 2.2.4 is called a *Teichmüller basis*, or a *T-basis* for short.

2.2.6. — *Remark.* Let $e_1, \dots, e_n$ be a T-basis of $\mathfrak{M}$ and for each i, let l_i be the u-adic valuation of the class of e_i in $\mathfrak{M}[i]/\mathfrak{M}[i+1]$ which is a lattice of $k((u))$. Then, we have $l_1 \geqslant l_2 \geqslant \cdots \geqslant l_n$. Indeed, by the definition of l_i, we have $e_i = \alpha_i p^{i-1} \mod p^i$ with $\mathrm{val}_u(\alpha_i) = l_i$. Therefore $pe_i = \alpha_i p^i \mod p^{i+1}$ and $e_{i+1} = \alpha_{i+1}p^i \mod p^{i+1}$. Since $pe_i \in \langle e_{i+1}, \dots, e_n\rangle$, it follows at once that $l_i \geqslant l_{i+1}$.

2.2.7. — Proposition. *Let $\mathfrak{M}$ be a lattice of $W_n((u))$. Then there exists a unique T-basis $e_1, \dots, e_n$ of the form:*

$$e_i = u^{l_i}p^{i-1} + [a_{i,i+1}]\,p^i + [a_{i,i+2}]\,p^{i+1} + \cdots + [a_{in}]\,p^{n-1}$$

where $a_{ij} \in k[u, u^{-1}]$ is such that $\deg_u(a_{ij}) < l_j$ for all i, j. Moreover, we have $l_1 \geqslant l_2 \geqslant \cdots \geqslant l_n$. Finally $\mathfrak{M}$ is positive if and only if $l_n \geqslant 0$ and $a_{ij} \in k[u]$ for all i, j.

Proof. — Existence: we construct the e_i by decreasing induction on i, starting from $i = n$. The module $\mathfrak{M}[n]$ is isomorphic via a canonical isomorphism to a lattice of $W_1((u)) = k((u))$, hence generated by u^{l_n} for a unique $l_n \in \mathbb{Z}$. The preimage via this isomorphism of this generator is $e_n = u^{l_n}p^{n-1}$. For $i < n$, assume by induction that $e_{i+1}, \dots, e_n$ have been constructed. The module $\mathfrak{M}[i]/\mathfrak{M}[i+1]$ is again canonically a lattice of $k((u))$, generated by u^{l_i} for a unique $l_i \in \mathbb{Z}$. Since $\mathfrak{M}[i] \subset p^iW_n((u))$, a lift

in $\mathfrak{M}[i]$ of this generator may be written in the form

$$e_i = u^{l_i} p^{i-1} + [a_{i,i+1}]\, p^i + [a_{i,i+2}]\, p^{i+1} + \cdots + [a_{in}]\, p^{n-1}$$

for some Laurent series $a_{ij} \in k((u))$. Now write $a_{i,i+1} = a'_{i,i+1} + u^{l_{i+1}} a''_{i,i+1}$ where $a'_{i,i+1} \in k[u, u^{-1}]$ is the truncation of $a_{i,i+1}$ in degrees $\geqslant l_{i+1}$. Replacing e_i by $e_i - [a''_{i,i+1}]e_{i+1}$, and rewriting the p-adic expansion of the tail $e_i - [a''_{i,i+1}]\, p^i$, we can fulfill the condition $\deg_u(a_{i,i+1}) < l_{i+1}$. Applying the same process to $a_{i,i+s}$ for $s = 1, \ldots, n-i$ we can fulfill the conditions $\deg_u(a_{ij}) < l_j$ for all j. This finishes the construction of e_i, and by induction, of $e_1, \ldots, e_n$. The elements e_i are such that $\mathfrak{M}[i] = \langle e_i, \ldots, e_n \rangle$ by construction.

Uniqueness: the choice of the generator of $\mathfrak{M}[i]/\mathfrak{M}[i+1]$ in the previous induction is normalized by the fact that we are looking for generators e_i with leading coefficients $u^{l_i} p^{i-1}$. The choice of the remaining coefficients of e_i is imposed by the condition on the degrees. This proves that the system $e_1, \ldots, e_n$ is unique. Finally the inequalities between the l_i are given by Remark 2.2.6 and the statement about positivity is obvious. □

2.2.8. — Definition. The T-basis of Lemma 2.2.7 is called the *distinguished basis* of $\mathfrak{M}$.

2.2.9. — *Remark.* Let $\mathfrak{M}$ be a lattice with distinguished basis $e_1, \ldots, e_n$. Then there exist series $b_{ij} \in k[[u]]$ and a set of equalities

$$R_i : \quad pe_i = [b_{ii}]\, e_{i+1} + \cdots + [b_{i,n-1}]\, e_n$$

for $1 \leqslant i \leqslant n$. It can be proven that in fact

$$\langle\, e_1, \ldots, e_n \mid R_1, \ldots, R_n \,\rangle$$

is a presentation by generators and relations of $\mathfrak{M}$ as a $W_n[[u]]$-module. We will not need this.

2.3. Breuil-Kisin modules of models of $\mu_{p^n,K}$

We finally specialize to our main object of interest, namely, the finite flat models of $\mu_{p^n,K}$.

2.3.1. — Models and μ-lattices. The natural morphisms between models are the *model maps*, which are by definition morphisms of R-group schemes inducing an isomorphism on the generic fibre. Let us see how the category of models of $\mu_{p^n,K}$ with model maps can be described concretely in terms of Breuil-Kisin modules.

Let $\overline{K}$ be an algebraic closure of K. For any two finite flat group schemes G, G' with associated Breuil-Kisin modules $\mathfrak{M}, \mathfrak{M}'$, we have:

$$G_K \simeq G'_K \iff G(\overline{K}) \simeq G'(\overline{K}) \iff \mathfrak{M}[1/u] \simeq \mathfrak{M}'[1/u]$$

where $G(\overline{K})$ and $G'(\overline{K})$ are viewed as representations of the absolute Galois group $\mathrm{Gal}(\overline{K}/K)$. The first equivalence is clear, let us explain briefly the second. If we introduce the Kummer extension $K_\infty = \cup_{n\geqslant 0} K(\sqrt[p^n]{\pi})$, then a result of Fontaine says that the module $\mathfrak{M}[1/u]$ determines the $\mathrm{Gal}(\overline{K}/K_\infty)$-representation associated to G (see [11], Remark A.3.4.1). By a result of Breuil ([4], Theorem 3.4.3), this representation in turn determines the crystalline $\mathrm{Gal}(\overline{K}/K)$-representation $G(\overline{K})$.

Recall that we are using the covariant equivalence $(\mathrm{Gr}/\mathcal{O}_K) \to (\mathrm{Mod}/\mathfrak{S})$ given by 2.1.2 and Cartier duality. Thus the $\mathfrak{S}$-module associated to the group scheme $\mu_{p^n,R}$ is $\mathfrak{M} = \mathfrak{S}_n$ with its usual Frobenius. From this, we deduce that $\mathfrak{M}$ is the module associated to a model of $\mu_{p^n,K}$ if and only if $\mathfrak{M}[1/u]$ is isomorphic to $\mathfrak{S}_n[1/u] = W_n(k)((u))$ with its Frobenius. Since $\mathfrak{M}$ has no u-torsion, we may then see it as a submodule of $W_n(k)((u))$. As far as the morphisms are concerned, the model maps correspond to *inclusions* between submodules of $W_n(k)((u))$. We are lead to the following notions.

2.3.2. — Definitions. A *μ-lattice* is a lattice $\mathfrak{M} \subset W_n((u))$ such that $E(u)\mathfrak{M} \subset \langle \phi(\mathfrak{M})\rangle \subset \mathfrak{M}$, where ϕ is the Frobenius of $W_n((u))$. We denote by $\mathscr{L}_n^\mu$ the partially ordered set of μ-lattices with inclusions between them.

The letter 'μ' reminds us of μ_{p^n}. Note that since a μ-lattice $\mathfrak{M}$ is stable under Frobenius, it is positive, for otherwise there would exist an element $x \in \mathfrak{M}$ with negative u-valuation and then the valuation of $\phi^n(x)$ would tend to $-\infty$, in contradiction with the finite generation of $\mathfrak{M}$. What has been said before means that the Breuil-Kisin classification gives an equivalence of categories between $\mathscr{L}_n^\mu$ and the category of models of μ_{p^n} with model maps.

2.3.3. — Kernels and images of p. Let G be a model of $\mu_{p^n,K}$. For $1 \leqslant i \leqslant n+1$, define:

- $G[i]$ the scheme-theoretic closure of $\ker(p^{n+1-i} : G_K \to G_K)$ in G,
- $G(i)$ the scheme-theoretic closure of $\mathrm{im}(p^{i-1} : G_K \to G_K)$ in G.

These are finite flat models of $\mu_{p^{n+1-i}}$. By definition, there are exact sequences:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & G[n+2-i] & \longrightarrow & G & \longrightarrow & G(i) & \longrightarrow & 0 \\ & & & & \downarrow{\scriptstyle p^{i-1}} & \swarrow & & & \\ 0 & \longrightarrow & G[i] & \longrightarrow & G & \longrightarrow & G(n+2-i) & \longrightarrow & 0 \end{array}$$

On the generic fibre, the vertical map $p^{i-1} : G \to G$ vanishes on $G[n+2-i]$ and its image is a subscheme of $G[i]$. By taking closures, the same is true everywhere. Therefore, this map induces a morphism of R-group schemes $G(i) \to G[i]$ which is a model map.

Let $\mathfrak{M}$ be the μ-lattice associated to G. Starting from the exact sequences above and using the fact that the Breuil-Kisin equivalence is exact, we see that $\mathfrak{M}[i]$ is the μ-lattice of $G[i]$ and $\mathfrak{M}(i)$ is the μ-lattice of $G(i)$. Moreover, the inclusion $\mathfrak{M}(i) \subset \mathfrak{M}[i]$ and the model map $G(i) \to G[i]$ correspond to each other.

3. The loop of μ-matrices

In 2.2, we have seen that lattices have "nice" systems of generators. The p-adic coefficients of such systems of generators may be put together into "nice" matrices, called μ-matrices. We will come back to this in more detail in Section 4. In the present section, we focus on the abstract algebra of the set of μ-matrices. This set has a natural operation $(A, B) \mapsto A * B$ whose meaning is that if $i : \mathfrak{M} \to \mathfrak{N}$ is an inclusion of lattices, if A is a matrix associated with a generating system of $\mathfrak{M}$ and if B is a matrix associated with the inclusion i, then $A * B$ is a matrix associated with a generating system of $\mathfrak{N}$. The operation $*$ is unfortunately neither associative nor commutative. Still, a good surprise is that μ-matrices all lie naturally in a set where the operation $*$ becomes invertible on the left and on the right; this set plays the same role as the symmetrization of a commutative monoid. The structure that we obtain, called a *loop*, was considered by Manin [21] in his study of rational points on cubic hypersurfaces, essentially because the analogue of the addition of elliptic curves in higher dimensions fails to be associative.

The key to everything in this section is the use of p-adic expansions, which exist as soon as the coefficient ring of the Witt vectors is a perfect ring of characteristic p. Thus we fix such a perfect ring throughout Section 3. For simplicity we denote it by the letter k, but note that it need not be a field. As before, we set $W = W(k)$ and $W_n = W_n(k)$.

Finally we point out that the role of Witt vectors will be very different in Sections 6 to 8, where we will consider arbitrary $\mathbb{Z}_{(p)}$-algebras as coefficient rings. We will emphasize this in due time.

3.1. p-adic expansions

3.1.1. — p-ADIC EXPANSIONS OF WITT VECTORS. Recall that the ring structure of W is given by universal polynomials with coefficients in $\mathbb{Z}$ in countably many variables $X_0, X_1, X_2, \dots$ For example, there are polynomials $S_i = S_i(X_0, \dots, X_i)$ and $P_i = P_i(X_0, \dots, X_i)$, for $i \geqslant 0$, giving the addition and the multiplication of two vectors $a = (a_0, a_1, a_2, \dots)$ and $b = (b_0, b_1, b_2, \dots)$ by the rules:

$$a + b = (S_0(a,b), S_1(a,b), S_2(a,b), \dots),$$
$$ab = (P_0(a,b), P_1(a,b), P_2(a,b), \dots).$$

Moreover, since k is perfect all elements have p-adic expansions:

$$a = (a_0, a_1, a_2, \dots) = [a_0] + [a_1^{1/p}]\, p + [a_2^{1/p^2}]\, p^2 + \dots$$

where $[x] := (x, 0, 0, \dots)$ is the Teichmüller lift of $x \in k$. Hence the functions $\mathbb{S}_i$ and $\mathbb{P}_i$ defined by $\mathbb{S}_i(a,b) := S_i(a,b)^{1/p^i}$ and $\mathbb{P}_i(a,b) := P_i(a,b)^{1/p^i}$ satisfy

$$a + b = [\mathbb{S}_0(a,b)] + [\mathbb{S}_1(a,b)]\, p + [\mathbb{S}_2(a,b)]\, p^2 + \dots,$$
$$ab = [\mathbb{P}_0(a,b)] + [\mathbb{P}_1(a,b)]\, p + [\mathbb{P}_2(a,b)]\, p^2 + \dots$$

In fact, we can define functions $\mathbb{S}_i$ and $\mathbb{P}_i$ in any number r of variables by the identities

$$a_1 + \dots + a_r = [\mathbb{S}_0(a_1, \dots, a_r)] + [\mathbb{S}_1(a_1, \dots, a_r)]\, p + [\mathbb{S}_2(a_1, \dots, a_r)]\, p^2 + \dots,$$
$$a_1 \dots a_r = [\mathbb{P}_0(a_1, \dots, a_r)] + [\mathbb{P}_1(a_1, \dots, a_r)]\, p + [\mathbb{P}_2(a_1, \dots, a_r)]\, p^2 + \dots$$

3.1.2. — p-ADIC EXPANSIONS OF SERIES. We wish to extend the formalism of p-adic expansions to the ring of Laurent series $W((u))$. For this, we extend the definition of Teichmüller lifts to elements $x \in k((u))$ as follows: if $x = \sum_{j \gg -\infty} x_j u^j$ with $x_j \in k$, we set

$$[x] = \sum_{j \gg -\infty} [x_j]\, u^j\ .$$

Then it is easy to see that for a Laurent series $a = \sum_{j \gg -\infty} a_j u^j$ in $W((u))$, by writing down p-adic expansions of its coefficients one obtains a p-adic expansion

$$a = [a_0] + [a_1]\, p + [a_2]\, p^2 + \dots$$

Let $a = \sum_{j \gg -\infty} a_j u^j$ and $b = \sum_{j \gg -\infty} b_j u^j$ be Laurent series with coefficients in W. We extend the definition of $\mathbb{S}_i$ by setting

$$\mathbb{S}_i(a,b) = \sum_{j \gg -\infty} \mathbb{S}_i(a_j, b_j) u^j = \left(\sum_{j \gg -\infty} S_i(a_j, b_j) u^{jp^i} \right)^{1/p^i}$$

and one verifies immediately that the formula $a + b = \sum_{i \geqslant 0} [\mathbb{S}_i(a,b)]\, p^i$ remains valid. Similarly, one extends the definition of $\mathbb{S}_i(a_1, \dots, a_r)$ for Laurent series $a_s \in W((u))$ in an obvious way. We now come to products. There are functions $\mathbb{P}_i$ such that for any r Laurent series $a_s = \sum_{i \gg -\infty} a_{s,i} u^i$ with coefficients in W we have

$$a_1 \dots a_r = [\mathbb{P}_0(a_1, \dots, a_r)] + [\mathbb{P}_1(a_1, \dots, a_r)]\, p + [\mathbb{P}_2(a_1, \dots, a_r)]\, p^2 + \dots$$

It is a simple exercise to verify that

$$\mathbb{P}_i(a_1, \dots, a_r) = \sum_j \mathbb{S}_i(\dots\,,\, a_{1,j_1} \cdots a_{r,j_r}\,,\, \dots)\, u^i$$

where the arguments of $\mathbb{S}_j$ are all the finitely many possible products $a_{1,j_1} \cdots a_{r,j_r}$ indexed by r-tuples $(j_1, \dots, j_r)$ such that $j_1 + \dots + j_r = j$. For example, if a and b are power series (i.e. Laurent series with nonnegative u-valuation) we have:

$$\mathbb{P}_i(a,b) = \sum_j \mathbb{S}_i(a_0 b_j, \dots, a_j b_0)\, u^j \ .$$

3.1.3. — A warning on the use of $\mathbb{S}_i$ and $\mathbb{P}_i$. In the sequel, we will most often use $\mathbb{S}_i$ and $\mathbb{P}_i$ for Teichmüller elements $a_i = [x_i]$. In this case, we will usually write $\mathbb{S}_i(x_1, \dots, x_r)$ and $\mathbb{P}_i(x_1, \dots, x_r)$ instead of $\mathbb{S}_i([x_1], \dots, [x_r])$ and $\mathbb{P}_i([x_1], \dots, [x_r])$. This is not dangerous, but for $x, y \in k((u))$ one must be careful to distinguish between the sum $x + y$ in $k((u))$ and the sum $[x] + [y]$ of their Teichmüller representatives in $W((u))$. For example, the associativity of the sum of Witt vectors gives for any elements $a, b, c \in W((u))$ the formula $\mathbb{S}_1(a, b, c) = \mathbb{S}_1(a + b, c)$, and here the sum $a + b$ takes place in $W((u))$. The reader is invited to compare with formula 3.1.4(1) below. Among the many formulas relating the $\mathbb{S}_i$ and the $\mathbb{P}_i$, most of them coming from associativity and distributivity of the sum and product of Witt vectors, we give a few examples:

3.1.4. — Lemma. *Let $a, b, c \in k((u))$ and let* val *denote the u-valuation. We have:*

(1) $\mathbb{S}_1(a, b, c) = \mathbb{S}_1(a, b) + \mathbb{S}_1(a + b, c)$.
(2) $\mathbb{S}_1(a, b - a) = \mathbb{S}_1(a, -b)$.
(3) $\mathrm{val}\,(\mathbb{S}_i(a,b)) \geqslant \max(\mathrm{val}(a), \mathrm{val}(b))$ *for all* $i \geqslant 1$.

(4) $[a][b] = [ab]$ *if a or b is a monomial.*

Note that the multiplicativity formula $[a][b] = [ab]$ for $a, b \in k$ does not hold in full generality if $a, b \in k((u))$.

Proof. — (1) This comes from the associativity of the sum of Witt vectors.

(2) It is enough to prove that $S_1(a, b-a) = S_1(a, -b)$. This can be proven over $\mathbb{Z}$, where it follows from the formula $S_1(x, y) = \frac{1}{p}(x^p + y^p - (x+y)^p)$.

(3) This comes from the fact that if we write $a = \sum a_j u^j$ and $b = \sum b_j u^j$, then $\mathbb{S}_i(a_j, b_j) = 0$ as soon as $a_j = 0$ or $b_j = 0$.

(4) This is clear. □

3.1.5. — p-ADIC EXPANSIONS OF VECTORS AND MATRICES. For the computations inside lattices, we will use the notations of linear algebra. The vectors are all column vectors. If A is a rectangular matrix with entries a_{ij} in $k((u))$ (for example A could be a column vector), we will denote by $[A]$ the matrix whose entries are the Teichmüller representatives $[a_{ij}]$. Thus the entries of $[A]$ are (possibly truncated) Witt vectors. We may as above consider p-adic expansions of matrices with entries in $W((u))$, but we will have no need for this. For us, the most important vector will be

$$p^\star = \begin{pmatrix} 1 \\ p \\ p^2 \\ \vdots \end{pmatrix}$$

which for convenience may denote a vector with finitely, or infinitely many, coefficients. Thus if $x \in W_n((u))^n$ is a vector with components $x_1, \dots, x_n$ we have:

$$^t x p^\star = x_1 + x_2 p + \cdots + x_n p^{n-1} \ .$$

If the x_i are Teichmüller representatives, then this linear combination is called a *T-combination*. Of course, any linear combination can be transformed into a T-combination:

3.1.6. — LEMMA. *For any rectangular matrix A with entries in $W_n((u))$ with n columns, there is a unique matrix $\rho(A)$ of the same size with entries in $k((u))$ such that*

$$A p^\star = [\rho(A)]\, p^\star \ .$$

If the entries of A are power series in u, or Laurent polynomials, or polynomials, then so are the entries of $\rho(A)$. If A is upper triangular (resp. with Teichmüller diagonal entries), then so is $\rho(A)$.

Proof. — The equality $Ap^\star = [\rho(A)]\,p^\star$ is equivalent to finitely many equalities, one for each line of A. Thus it is enough to consider the case where A has only one line $A = (a_1 \dots a_n)$. Write the p-adic expansion

$$a_1 + a_2 p + \cdots + a_n p^{n-1} = [a_1'] + [a_2']\,p + \cdots + [a_n']\,p^{n-1}\ .$$

Obviously the desired matrix is $\rho(A) = (a_1' \dots a_n')$. The remaining assertions are clear. □

There is an algorithmic point of view on the computation of $\rho(A)$ that will be useful. In order to explain this, for a coefficient in position (i,j) in an upper triangular square matrix, let us call the difference $j - i$ the *distance to the diagonal*.

3.1.7. — Lemma. *Let $\mathscr{E}$ be the set of upper triangular square matrices of size n with entries in $W((u))$ with Teichmüller diagonal entries. Define a function $F : \mathscr{E} \to \mathscr{E}$ as follows. Given a matrix A, for $i = 1$ to n apply the following rule to the i-th line:*

- *Find the first non-Teichmüller coefficient $a_{i,\nu}$.*
- *Write the truncated p-adic expansion $a_{i,\nu}p^{\nu-1} = [a_{i,\nu}']\,p^{\nu-1} + \cdots + [a_{i,n}']\,p^{n-1} \mod p^n$.*
- *Replace $a_{i\nu}$ by $[a_{i\nu}']$ and for $j > i$ replace a_{ij} by $a_{ij} + [a_{ij}']$.*

After the step $i = n$ has been completed, call the result $F(A)$. Then, for all $k \geqslant 0$ we have:

- *the coefficients with distance to the diagonal $\leqslant k$ of the matrix $F^k(A)$ are Teichmüller, where F^k is the k-th iterate of F.*
- *$F^k(A)\,p^\star = A\,p^\star$.*

In particular $F^{n-1}(A) = \rho(A)$.

Proof. — This is obvious. □

3.2. The loop of μ-matrices

3.2.1. — Quasigroups and loops. We start with some definitions from quasigroup theory, referring to the book of Smith [28] for more details. A *magma* is a set X endowed with a binary operation $X \times X \to X$, $(x,y) \mapsto xy$ usually called *multiplication*. A *submagma* is a subset $Y \subset X$ that is closed under multiplication. A *quasigroup* is a magma where left and right division are always possible, in the sense that left multiplications L_x and right multiplications R_y are bijections. Given $x, y \in X$, the unique element a such that $ax = y$ is denoted y/x (read "y over x") and the unique element b such that $xb = y$ is denoted $x\backslash y$ (read "x into y"). A *loop*

(*boucle* in French, and... *loop* in Italian) is a quasigroup with an identity element, i.e. an element $e \in X$ such that $ex = xe = x$ for all $x \in X$. Thus a loop is a group if and only if the operation is associative. A *magma homomorphism* is a map $f : X \to X'$ such that $f(x_1x_2) = f(x_1)f(x_2)$ for all $x_1, x_2 \in X$. *Quasigroup homomorphisms* and *loop homomorphisms* are just magma homomorphisms.

3.2.2. — The loop $\mathscr{G}_n((u))$. In Section 4, to lattices of $W_n((u))$ we will attach matrices. The matrices coming in this way appear naturally as objects in a certain loop which we call the *loop of μ-matrices* and denote by $\mathscr{G}_n((u))$. As a set, it is composed of the upper triangular matrices of the form

$$M(\boldsymbol{l}, \boldsymbol{a}) = \begin{pmatrix} u^{l_1} & a_{12} & a_{13} & \cdots & a_{1n} \\ & u^{l_2} & a_{23} & & a_{2n} \\ & & \ddots & \ddots & \vdots \\ & & & u^{l_{n-1}} & a_{n-1,n} \\ 0 & & & & u^{l_n} \end{pmatrix}$$

with $\boldsymbol{l} = (l_1, \ldots, l_n) \in \mathbb{Z}^n$ and $\boldsymbol{a} = (a_{ij})_{1 \leqslant i < j \leqslant n}$ where $a_{ij} \in k((u))$. There is a natural subset $\mathscr{G}_n[u, u^{-1}]$ composed of matrices with coefficients in $k[u, u^{-1}]$. In order to keep the notation light, we do not specify the coefficient ring k in the symbols $\mathscr{G}_n((u))$ and $\mathscr{G}_n[u, u^{-1}]$. Note also that as a general rule, we write a_{ij} instead of $a_{i,j}$, unless this can disturb comprehension, for example when we write $a_{np,n}$.

If A, B are square matrices with entries in $k((u))$, we set $A * B = \rho([A][B])$ where ρ is the map from Lemma 3.1.6. This matrix is characterized by the equality:

$$[A][B]\, p^\star = [A * B]\, p^\star \ .$$

By Lemma 3.1.6, if A, B are in $\mathscr{G}_n((u))$ resp. in $\mathscr{G}_n[u, u^{-1}]$, then $A * B$ also. It is clear that the identity matrix is a neutral element for this multiplication. Thus the triple $(\mathscr{G}_n((u)), *, \mathrm{Id})$ is a magma with identity, and $(\mathscr{G}_n[u, u^{-1}], *, \mathrm{Id})$ is a submagma. At this point, the reader may wish to have a look at the shape of the multiplication $*$ in the examples of 3.3 below.

We will now prove that $(\mathscr{G}_n((u)), *, \mathrm{Id})$ is a loop.

3.2.3. — Proposition. *Let $A = M(\boldsymbol{l}, \boldsymbol{a})$ and $B = M(\boldsymbol{m}, \boldsymbol{b})$ be elements of $\mathscr{G}_n((u))$.*

(1) *Any coefficient in position (i,j) of $A * B$ with distance to the diagonal $j-i \geqslant 1$ has the form:*

$$u^{m_j} a_{ij} + u^{l_i} b_{ij} + \left(\begin{array}{c} \text{terms depending on coefficients } a_{i'j'} \text{ and } b_{i'j'} \\ \text{whose distance to the diagonal is } j'-i' < j-i. \end{array} \right).$$

(2) *The maps $L_A : B \mapsto A * B$ and $R_B : A \mapsto A * B$ are bijections. Thus, the triple $(\mathscr{G}_n((u)), *, \mathrm{Id})$ is a loop.*

Proof. — (1) The entry of $[A][B]$ in position (i,j) is

$$u^{l_i}[b_{ij}] + \left(\sum_{k=i+1}^{j-1} [a_{ik}][b_{kj}] \right) + [a_{ij}] u^{m_j} .$$

The coefficients $[a_{ik}]$ and $[b_{kj}]$ in the middle sum have distance to the diagonal strictly less than $j-i$. When applying the algorithm of Lemma 3.1.7 to compute $A * B$, at each step the entry (i,j) is replaced by itself plus some terms involving coefficients a_{st} and b_{st} of distance to the diagonal $t-s < j-i$. This proves the claim.

(2) The argument is the same for L_A and R_B so we do only the case of L_A. Assume that $A * B = C$ with $A = M(\boldsymbol{l}, \boldsymbol{a})$, $B = M(\boldsymbol{m}, \boldsymbol{b})$, $C = M(\boldsymbol{n}, \boldsymbol{c})$. We fix A and C and try to solve for B. We determine its entries by increasing induction on the distance to the diagonal, called k. For $k = 0$ it is clear that we have $m_i = n_i - l_i$. By induction, using point (1), it follows directly that the coefficients b_{ij} of distance to the diagonal k are determined by the entries of A, C and the coefficients $b_{i'j'}$ of lower distance to the diagonal. □

3.2.4. — Some subloops. The homomorphisms $\mathcal{U}$ and $\mathcal{L}$. There are some important examples of subloops and loop homomorphisms. Of course $\mathscr{G}_n[u, u^{-1}]$ is a subloop of $\mathscr{G}_n((u))$. Another example is the subloop of matrices with diagonal entries equal to 1. This is in fact the kernel of the morphism of loops $\varphi : \mathscr{G}_n((u)) \to \mathbb{Z}^n$ to the additive group $\mathbb{Z}^n$ that maps A to the tuple of its diagonal exponents.

For any square matrix A of size n with entries in some ring, we denote by $\mathcal{U}A$ the upper left square submatrix of size $n-1$, i.e. the matrix obtained by deleting the last row and the last column of A. Similarly we denote by $\mathcal{L}A$ the lower right square submatrix of size $n-1$, obtained by deleting the first row and the first column of A.

3.2.5. — Lemma. *The mappings $\mathcal{U} : \mathscr{G}_n((u)) \to \mathscr{G}_{n-1}((u))$ and $\mathcal{L} : \mathscr{G}_n((u)) \to \mathscr{G}_{n-1}((u))$ are commuting loop homomorphisms.*

Proof. — Let $\tau_{\mathcal{U}}$ be the truncation map that takes a vector v with n components to the vector whose components are the first $n-1$ components

of v. Thus $\tau_{\mathcal{U}} p^\star$ is the vector analogous to $p^\star$ in dimension one less. Then simple matrix formulas yield:

$$\begin{aligned}[\mathcal{U}(A * B)]\,\tau_{\mathcal{U}} p^\star &= (\mathcal{U}[A * B])\,\tau_{\mathcal{U}} p^\star = \tau_{\mathcal{U}}([A * B]\,p^\star) = \tau_{\mathcal{U}}([A][B]\,p^\star) \\ &= \mathcal{U}[A] \cdot \mathcal{U}[B]\,\tau_{\mathcal{U}} p^\star = [\mathcal{U}A][\mathcal{U}B]\,\tau_{\mathcal{U}} p^\star = [\mathcal{U}A * \mathcal{U}B]\,\tau_{\mathcal{U}} p^\star\ .\end{aligned}$$

It follows that $\mathcal{U}(A * B) = \mathcal{U}A * \mathcal{U}B$, that is, $\mathcal{U}$ is a loop homomorphism.

Let $\tau_{\mathcal{L}}$ be the truncation taking a vector v with n components to the vector whose components are the last $n-1$ components of v. Thus $\tau_{\mathcal{L}} p^\star$ is the column vector with components $p, p^2, \dots, p^{n-1}$. It is still true that if two square matrices A, B of size $n-1$ with coefficients in $k((u))$ satisfy $[A]\,\tau_{\mathcal{L}} p^\star = [B]\,\tau_L p^\star$ then $A = B$. Then a similar computation as before shows that $[\mathcal{L}(A*B)]\,\tau_{\mathcal{L}} p^\star = [\mathcal{L}A*\mathcal{L}B]\,\tau_{\mathcal{L}} p^\star$, so $\mathcal{L}$ is a loop homomorphism.

Finally, the fact that $\mathcal{U}$ and $\mathcal{L}$ commute is clear. □

3.2.6. — Positive matrices. We say that a matrix $A \in \mathscr{G}_n((u))$ is *positive*, and we write $A \geqslant 0$, if its entries are in $k[[u]]$. (Here, as in 2.2.1, we say *positive* instead of *non-negative* for simplicity.) We denote by $\mathscr{G}_n[[u]]$ the subset of positive elements of $\mathscr{G}_n((u))$. It is a submagma, but not a subloop. Similarly $\mathscr{G}_n[u, u^{-1}]$ has a submagma $\mathscr{G}_n[u] = \mathscr{G}_n[u, u^{-1}] \cap \mathscr{G}_n[[u]]$.

3.3. Examples

Here is what the operation $*$ looks like for $n = 4$. The product $P = A * B$ is given by

$$P = \begin{pmatrix} u^{l_1+m_1} & u^{l_1} b_{12} + u^{m_2} a_{12} & p_{13} & p_{14} \\ 0 & u^{l_2+m_2} & u^{l_2} b_{23} + u^{m_3} a_{23} & p_{24} \\ 0 & 0 & u^{l_3+m_3} & u^{l_3} b_{34} + u^{m_4} a_{34} \\ 0 & 0 & 0 & u^{l_4+m_4} \end{pmatrix}.$$

with

$$\begin{aligned} p_{13} &= u^{l_1} b_{13} + a_{12} b_{23} + u^{m_3} a_{13} + \mathbb{S}_1(u^{l_1} b_{12}, u^{m_2} a_{12}) \\ p_{24} &= u^{l_2} b_{24} + a_{23} b_{34} + u^{m_4} a_{24} + \mathbb{S}_1(u^{l_2} b_{23}, u^{m_3} a_{23}) \\ p_{14} &= u^{l_1} b_{14} + a_{12} b_{24} + a_{13} b_{34} + a_{14} u^{m_4} + \mathbb{S}_2(u^{l_1} b_{12}, u^{m_2} a_{12}) + \\ &\quad + \mathbb{S}_1(u^{l_1} b_{13}, a_{12} b_{23}, u^{m_3} a_{13}, \mathbb{S}_1(u^{l_1} b_{12}, u^{m_2} a_{12})) + \mathbb{P}_1(a_{12}, b_{23})\ . \end{aligned}$$

Applying the homomorphism $\mathcal{U}$ (Lemma 3.2.5), these formulas contain also the formulas of multiplication for $n \leqslant 4$.

3.3.1. — Failure of associativity. For $n = 2$, the loop $\mathscr{G}_2$ is a group: in fact the multiplication $*$ is the ordinary multiplication of matrices. For $n \geqslant 3$, the multiplication $*$ is not associative. Let us check this. We have

$$A * B = \begin{pmatrix} u^{l_1+m_1} & u^{l_1}b_{12} + u^{m_2}a_{12} & (A*B)_{13} \\ 0 & u^{l_2+m_2} & u^{l_2}b_{23} + u^{m_3}a_{23} \\ 0 & 0 & u^{l_3+m_3} \end{pmatrix}$$

with

$$(A * B)_{13} = u^{l_1}b_{13} + a_{12}b_{23} + u^{m_3}a_{13} + \mathbb{S}_1(u^{l_1}b_{12}, u^{m_2}a_{12}) \ .$$

We now examine the coefficients in position $(1, 3)$:

$$\begin{aligned}((A * B) * C)_{13} = {} & u^{l_1+m_1}c_{13} + (u^{l_1}b_{12} + u^{m_2}a_{12})c_{23} \\ & + u^{n_3}\big(u^{l_1}b_{13} + a_{12}b_{23} + u^{m_3}a_{13} + \mathbb{S}_1(u^{l_1}b_{12}, u^{m_2}a_{12})\big) \\ & + \mathbb{S}_1\big(u^{l_1+m_1}c_{12}, u^{n_2}(u^{l_1}b_{12} + u^{m_2}a_{12})\big)\end{aligned}$$

and

$$\begin{aligned}(A * (B * C))_{13} = {} & u^{l_1}\big(u^{m_1}c_{13} + b_{12}c_{23} + u^{n_3}b_{13} + \mathbb{S}_1(u^{m_1}c_{12}, u^{n_2}b_{12})\big) \\ & + a_{12}(u^{m_2}c_{23} + u^{n_3}b_{23}) + u^{m_3+n_3}a_{13} \\ & + \mathbb{S}_1\big(u^{l_1}(u^{m_1}c_{12} + u^{n_2}b_{12}), u^{m_2+n_2}a_{12}\big) \ .\end{aligned}$$

Using the formula $\mathbb{S}_1(x, y, z) = \mathbb{S}_1(x, y) + \mathbb{S}_1(x + y, z)$ from Lemma 3.1.4, we compute the difference:

$$\begin{aligned}&((A * B) * C)_{13} - (A * (B * C))_{13} \\ &\quad = \ \mathbb{S}_1\big(u^{l_1+n_3}b_{12}, u^{m_2+n_3}a_{12}\big) + \mathbb{S}_1\big(u^{l_1+m_1}c_{12}, u^{n_2}(u^{l_1}b_{12} + u^{m_2}a_{12})\big) \\ &\qquad - \mathbb{S}_1(u^{l_1+m_1}c_{12}, u^{l_1+n_2}b_{12}\big) \\ &\qquad\quad - \mathbb{S}_1\big(u^{l_1}(u^{m_1}c_{12} + u^{n_2}b_{12}), u^{m_2+n_2}a_{12}\big) \\ &\quad = \ (u^{n_3} - u^{n_2})\mathbb{S}_1\big(u^{l_1}b_{12}, u^{m_2}a_{12}\big) \ .\end{aligned}$$

This is not zero so $*$ is not associative.

However, we see that this is zero on the subloop $\ker\phi : \mathscr{G}_3((u)) \to \mathbb{Z}^3$, which then is a group. Let us verify that for $n \geqslant 4$, the multiplication $*$ is not associative even if we restrict it to the subloop $\ker\phi : \mathscr{G}_4((u)) \to \mathbb{Z}^4$. We shall check this only for $n = 4$. We make the following observation: the multiplication of $\mathscr{G}_n((u))$ differs from that of the underlying group of matrices by terms coming from the operations of Witt vectors, i.e. involving the sum and product functions $\mathbb{S}_i$ and $\mathbb{P}_j$. Since the ordinary multiplication of matrices is associative, the terms of the entries in $(A*B)*C$ and $A*(B*C)$ that do not involve $\mathbb{S}_i$ or $\mathbb{P}_j$ are equal. Consequently when we question

associativity it is enough to look at the terms that contain $\mathbb{S}_i$ or $\mathbb{P}_j$. Once this is said, let us compare the entries in position $(1,4)$ of $(A*B)*C$ and $A*(B*C)$. Looking at the above formulas, we see that among the terms involving $\mathbb{S}_i$ or $\mathbb{P}_j$ the coefficient c_{34} is present in $((A*B)*C)_{14}$ whereas it is absent from $(A*(B*C))_{14}$. Then one can easily specialize the parameters to obtain an example where $((A*B)*C) \neq ((A*B)*C)$. We can also see that $*$ is not *diassociative* (i.e. the subloops generated by two elements are not associative), and hence not a *Moufang loop* like the loops considered by Manin in his book on cubic forms [21].

3.3.2. — Formulas for left and right division. Finally, we let $C = A*B$ and give the formulas for $A = C/B$ and $B = A\backslash C$ for $n = 3$. We use the notations $A = M(\boldsymbol{l}, \boldsymbol{a})$, $B = M(\boldsymbol{m}, \boldsymbol{b})$, $C = M(\boldsymbol{n}, \boldsymbol{c})$.
The matrix $A = C/B$ is determined by $l_i = n_i - m_i$ for $i = 1, 2, 3$ and:

$$a_{12} = \frac{c_{12} - u^{n_1-m_1} b_{12}}{u^{m_2}}$$

$$a_{23} = \frac{c_{23} - u^{n_2-m_2} b_{23}}{u^{m_3}}$$

$$a_{13} = \frac{c_{13} - u^{n_1-m_1} b_{13} - \frac{c_{12}-u^{n_1-m_1}b_{12}}{u^{m_2}} b_{23} - \mathbb{S}_1(u^{n_1-m_1}b_{12}, c_{12} - u^{n_1-m_1}b_{12})}{u^{m_3}}$$

The matrix $B = A\backslash C$ is determined by $m_i = n_i - l_i$ for $i = 1, 2, 3$ and:

$$b_{12} = \frac{c_{12} - u^{n_2-l_2} a_{12}}{u^{l_1}}$$

$$b_{23} = \frac{c_{23} - u^{n_3-l_3} a_{23}}{u^{l_2}}$$

$$b_{13} = \frac{c_{13} - a_{12}\frac{c_{23}-u^{n_3-l_3}a_{23}}{u^{l_2}} - u^{n_3-l_3} a_{13} - \mathbb{S}_1(c_{12} - u^{n_2-l_2}a_{12}, u^{n_2-l_2}a_{12})}{u^{l_1}}$$

When C is the identity matrix, we see that left inverse and right inverse coincide.

4. Relating lattices and matrices

In this section, we consider matrices adapted to well-chosen systems of generators of lattices. More precisely, we define subsets

$$\mathscr{G}_n^{\mu}((u)) \subset \mathscr{G}_n^{d}((u)) \subset \mathscr{G}_n^{T}((u)) \subset \mathscr{G}_n((u))$$

whose relation to lattices is the following. The set $\mathscr{G}_n^{T}((u))$ of *T-matrices* corresponds to the nice systems of generators of lattices which we called T-bases. The set $\mathscr{G}_n^{d}((u))$ of *distinguished matrices* corresponds to the distinguished T-bases, that is, to the lattices themselves. Finally the set $\mathscr{G}_n^{\mu}((u))$

of *μ-matrices* corresponds to the μ-lattices. The final result is Theorem 4.2.2 which formulates the classification of models of $\mu_{p^n,K}$ in terms of matrices, well-suited for computations.

From now on, the ring of coefficients k is a perfect field and $W = W(k)$, $W_n = W_n(k)$.

4.1. Matrices and lattices

Recall that lattices, T-bases and distinguished bases are defined in 2.2.

4.1.1. — Definition. For each $A \in \mathscr{G}_n((u))$ we consider the column vector $e_\star = [A]\, p^\star$, its components $e_1, \dots, e_n$, and the lattice $\mathfrak{M} = \mathfrak{M}(A)$ they generate.

(1) We say that A is a *T-matrix* if $e_1, \dots, e_n$ is a T-basis of $\mathfrak{M}$.

(2) We say that A is *distinguished* if $e_1, \dots, e_n$ is the distinguished basis of $\mathfrak{M}$.

We denote by $\mathscr{G}_n^T((u))$, resp. $\mathscr{G}_n^d((u))$, the set of T-matrices, resp. distinguished matrices, in $\mathscr{G}_n((u))$. We have similar subsets $\mathscr{G}_n^*[[u]] \subset \mathscr{G}_n[[u]]$, $\mathscr{G}_n^*[u, u^{-1}] \subset \mathscr{G}_n[u, u^{-1}]$, $\mathscr{G}_n^*[u] \subset \mathscr{G}_n[u]$ with $* \in \{T, d\}$.

Let $\mathscr{L}_n$ be the set of lattices of $W_n((u))$. We have a well-defined map

$$\mathscr{G}_n((u)) \to \mathscr{L}_n \quad , \quad A \mapsto \mathfrak{M}(A).$$

Denote by $A(\mathfrak{M})$ the matrix whose coefficients are the p-adic coefficients of the distinguished basis of $\mathfrak{M}$. Then we have a section

$$\mathscr{L}_n \to \mathscr{G}_n^T[u, u^{-1}] \subset \mathscr{G}_n((u)) \quad , \quad \mathfrak{M} \mapsto A(\mathfrak{M}).$$

4.1.2. — Lemma. *Let $A \in \mathscr{G}_n((u))$ and $\mathfrak{M} = \mathfrak{M}(A)$. Then:*

(1) *A is a T-matrix if and only if $\mathcal{U}A/\mathcal{L}A \geqslant 0$, i.e. $\mathcal{U}A = B * \mathcal{L}A$ for some $B \in \mathscr{G}_n[[u]]$.*

(2) *$A \geqslant 0$ if and only if $\mathfrak{M} \geqslant 0$.*

Proof. — (1) Set $e_\star = [A]\, p^\star$. Due to the shape of matrices in $\mathscr{G}_n((u))$, we have $v_p(e_i) = i - 1$. It follows from (1) of Lemma 2.2.4 that $e_\star$ is a T-basis if and only if $pe_i \in \langle e_{i+1}, \dots, e_n \rangle$ for all i. This is in turn equivalent to the existence of elements $b_{ij} \in k[[u]]$ such that

$$pe_i = [b_{ii}]\, e_{i+1} + \cdots + [b_{i,n-1}]\, e_n$$

for all i. Let B be the upper triangular matrix with diagonal entries $u^{l_i - l_{i+1}}$ and other entries $b_{ij} \in k[[u]]$. It is simple to see that the set of equalities above is equivalent to $\mathcal{U}A = B * \mathcal{L}A$.

(2) We have $\mathfrak{M} \geqslant 0$ if and only if $e_i \in W_n[[u]]$ for all i. Since $e_i = u^{l_i}p^{i-1} + [a_{i,i+1}]\,p^i + \cdots + [a_{in}]\,p^{n-1}$, this means that u^{l_i} and a_{ij} belong to $k[[u]]$ for all i, j. □

The construction of the distinguished basis in Lemma 2.2.7 shows that the volume of a lattice (defined in 2.3) can be computed from a T-matrix giving rise to it:

4.1.3. — Lemma. *For $A \in \mathscr{G}_n^T((u))$ and $\mathfrak{M} = \mathfrak{M}(A)$, we have* $\mathrm{vol}(\mathfrak{M}) = \det(A)$.

Proof. — Let α be an integer such that $u^\alpha\mathfrak{M} \subset W_n[[u]]$. Replacing $\mathfrak{M}$ by $u^\alpha\mathfrak{M}$ and A by $u^\alpha A$, we may assume that $\alpha = 0$. To simplify the notation, we write $\mathfrak{M}^+ = W_n[[u]]/\mathfrak{M}$. Write $A = M(\boldsymbol{l}, \boldsymbol{a})$. We have the following diagram with exact rows and columns:

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathfrak{M}[i+1] & \longrightarrow & \mathfrak{M}[i] & \longrightarrow & \mathfrak{M}[i]/\mathfrak{M}[i+1] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & W_{n-i}[[u]] & \longrightarrow & W_{n-i+1}[[u]] & \longrightarrow & W_1[[u]] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathfrak{M}[i+1]^+ & \longrightarrow & \mathfrak{M}[i]^+ & \longrightarrow & (\mathfrak{M}[i]/\mathfrak{M}[i+1])^+ & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

Since $A \in \mathscr{G}_n[[u]]$, we have $\mathfrak{M}[i]/\mathfrak{M}[i+1] \simeq u^{l_i}k[[u]]$ and $(\mathfrak{M}[i]/\mathfrak{M}[i+1])^+ \simeq k[u]/(u^{l_i})$ of length l_i. Then the result follows by induction, using the additivity of the length. □

Let us now look at some natural lattices associated to a lattice $\mathfrak{M}$. We defined the kernel $\mathfrak{M}[i]$ and the image $\mathfrak{M}(i)$ in 2.2.2. The ring $W_n((u))$ is endowed with a Frobenius endomorphism ϕ whose restriction to W_n is the Frobenius of the Witt vectors, and such that $\phi(u) = u^p$. This gives rise to another interesting lattice, namely the lattice generated by $\phi(\mathfrak{M})$. Also, for a polynomial $E(u) \in W_n[u]$ we can consider the lattice $E(u)\mathfrak{M}$. If $\mathfrak{M} = \mathfrak{M}(A)$, we wish to express the matrices associated to these lattices in terms of A. We will shortly give the result, but we first need a bit of notation.

4.1.4. — **Notation.** We denote by $\mathcal{P}$ the matrix operator taking a square matrix M of size r to the square matrix of size $r+1$ whose upper right block of size r is M and whose other entries are zero. In pictures,

$$\mathcal{P}M = \begin{pmatrix} 0 & \vdots & M \\ \cdots & & \\ 0 & 0 & \end{pmatrix}.$$

The operator $\mathcal{P}^i$ takes a matrix M of size r to the matrix of size $r+i$ whose upper right block is M and whose other blocks are zero.

4.1.5. — Definition. Let $A \in \mathscr{G}_n((u))$ be a matrix and $E(u) \in W_n[u]$ a polynomial, with p-adic expansion $E(u) = [E_0(u)] + [E_1(u)]\,p + \cdots + [E_{n-1}(u)]\,p^{n-1}$. With the notation of 4.1.4, we define:
(1) $E(u)\diamond A = \rho\big(\sum_{i=0}^{n-1} [E_i\,\mathrm{Id} * \mathcal{P}^i\mathcal{U}^i A]\big)$, where ρ is the map from Lemma 3.1.6.
(2) $\phi(A)$ is the matrix obtained by applying Frobenius to all the entries of A.

The two operations $\phi(-)$ and $E(u)\diamond -$ are compatible with $\mathcal{U}$ and $\mathcal{L}$ in the following sense.

4.1.6. — Lemma. *For all matrices $A \in \mathscr{G}_n((u))$ and polynomials $E(u) \in W_n[u]$, we have:*
(1) $\mathcal{U}(\phi(A)) = \phi(\mathcal{U}(A))$ *and* $\mathcal{L}(\phi(A)) = \phi(\mathcal{L}(A))$.
(2) $\mathcal{U}(E(u)\diamond A) = E(u)\diamond\mathcal{U}(A)$, *and* $\mathcal{L}(E(u)\diamond A) = E(u)\diamond\mathcal{L}(A)$,
where in $E(u)\diamond\mathcal{U}(A)$ and $E(u)\diamond\mathcal{L}(A)$ it is the image of $E(u)$ in $W_{n-1}[u]$ that is involved.

Proof. — (1) is obvious and we only prove (2). Let $\tau_{\mathcal{U}}$ be the truncation map that takes a vector v with n components to the vector whose components are the first $n-1$ components of v, so $\tau_{\mathcal{U}}p^\star$ is the vector analogous to $p^\star$ in dimension one less, as in the proof of Lemma 3.2.5. Since $\mathcal{P}\mathcal{U}A$ is the matrix obtained from $\mathcal{U}\mathcal{P}A$ by replacing the last line by 0, we have: $[\mathcal{P}\mathcal{U}A]\,\tau_{\mathcal{U}}p^\star = \tau_{\mathcal{U}}[\mathcal{P}A]\,p^\star$. It follows that

$$\begin{aligned}\tau_{\mathcal{U}}p^\star &= \sum_{i=0}^{n-2} [E_i][\mathcal{P}^i\mathcal{U}^{i+1}A]\,\tau_{\mathcal{U}}p^\star = \tau_{\mathcal{U}}\left(\sum_{i=0}^{n-1} [E_i][\mathcal{P}^i\mathcal{U}^i A]\,p^\star\right)\\ &= \tau_{\mathcal{U}}\Big([E(u)\diamond A]\,p^\star\Big).\end{aligned}$$

But it is exactly the defining property of $M = \mathcal{U}(E(u)\diamond A)$ that $[M]\,\tau_{\mathcal{U}}p^\star = \tau_{\mathcal{U}}([E(u)\diamond A]\,p^\star)$. This proves that $\mathcal{U}(E(u)\diamond A) = E(u)\diamond\mathcal{U}(A)$. The proof for

the commutation with $\mathcal{L}$ is similar: $\mathcal{P}\mathcal{L}A$ is the matrix obtained from $\mathcal{L}\mathcal{P}A$ by replacing the first line by 0, etc. □

4.1.7. — Lemma. *Let $A \in \mathscr{G}_n((u))$ and $\mathfrak{M} \in \mathscr{L}_n$.*

(1) *If $\mathfrak{M} = \mathfrak{M}(A)$ then:*

(a) $\mathfrak{M}(i) = \mathfrak{M}(\mathcal{U}^{i-1}A)$,
(b) $\mathfrak{M}[i] = \mathfrak{M}(\mathcal{L}^{i-1}A)$,
(c) $\langle\phi(\mathfrak{M})\rangle = \mathfrak{M}(\phi(A))$,
(d) $E(u)\mathfrak{M} = \mathfrak{M}(E(u)\diamond A)$.

(2) *If A is a T-matrix then $\mathcal{U}^{i-1}A$, $\mathcal{L}^{i-1}A$, $\phi(A)$, $E(u)\diamond A$ are also T-matrices.*

(3) *If A is distinguished then $\mathcal{U}^{i-1}A$, $\mathcal{L}^{i-1}A$, $\phi(A)$ are also distinguished.*

It is not true in general that if A is distinguished then $E(u)\diamond A$ is distinguished. There are obvious counter-examples for $n = 2$ as soon as $l_1 \geqslant l_2+1$.

Proof. — (1) Let $e_\star = [A]\,p^\star$. Let us fix $i \in \{1, \dots, n\}$ and define:

(a) $f_j = p^{i-1}e_j$ for $1 \leqslant j \leqslant n+1-i$,
(b) $g_j = e_{j+i-1}$ for $1 \leqslant j \leqslant n+1-i$,
(c) $h_j = \phi(e_j)$ for $1 \leqslant j \leqslant n$,
(d) $\ell_j = E(u)e_j$ for $1 \leqslant j \leqslant n$,

The elements f_j generate $\mathfrak{M}(i)$ and we have $f_\star = [\mathcal{U}^{i-1}A]\,p^\star$, hence $\mathfrak{M}(i) = \mathfrak{M}(\mathcal{U}^{i-1}A)$. The elements g_j generate $\mathfrak{M}[i]$ and satisfy $g_\star = [\mathcal{L}^{i-1}A]\,p^\star$, so that $\mathfrak{M}[i] = \mathfrak{M}(\mathcal{L}^{i-1}A)$. The elements h_j generate $\langle\phi(\mathfrak{M})\rangle$ and satisfy $h_\star = [\phi(A)]\,p^\star$ so $\langle\phi(\mathfrak{M})\rangle = \mathfrak{M}(\phi(A))$. Finally the elements ℓ_j generate $E(u)\mathfrak{M}$ and moreover a simple matrix computation shows that $p^i[A]\,p^\star = [\mathcal{P}^i\mathcal{U}^iA]\,p^\star$ so

$$\begin{aligned} E(u)e_\star &= \big(\sum [E_i]p^i\big)[A]\,p^\star = \sum [E_i][\mathcal{P}^i\mathcal{U}^iA]\,p^\star \\ &= \big[\rho\big(\sum E_i\,\mathrm{Id} *\mathcal{P}^i\mathcal{U}^iA\big)\big]\,p^\star = [E(u)\diamond A]\,p^\star\ . \end{aligned}$$

It follows that $E(u)\mathfrak{M} = \mathfrak{M}(E(u)\diamond A)$.

(2) Using the characterization 1) in Lemma 2.2.4, it is very easy to prove that $f_\star$, $g_\star$, $h_\star$, $\ell_\star$ are T-bases.

(3) It is immediate that the matrices $\mathcal{U}^{i-1}A$, $\mathcal{L}^{i-1}A$ and $\phi(A)$ have Laurent polynomial entries and satisfy the condition on the degrees required to be distinguished. □

4.1.8. — Lemma. *Let A, A' be in $\mathscr{G}_n((u))$ and $\mathfrak{M} = \mathfrak{M}(A)$, $\mathfrak{M}' = \mathfrak{M}(A')$.*

(1) *Assume that $A' \in \mathscr{G}_n^T((u))$. Then $\mathfrak{M} \subset \mathfrak{M}'$ if and only if $A/A' \geqslant 0$.*

(2) *In particular, the T-matrices are the minimal elements among the matrices $A \in \mathscr{G}_n((u))$ such that $\mathfrak{M}(A) = \mathfrak{M}$, in the sense that for any two matrices A, A' with $\mathfrak{M}(A) = \mathfrak{M}(A') = \mathfrak{M}$, if A' is a T-matrix then $A/A' \geqslant 0$.*
(3) *Assume that $A, A' \in \mathscr{G}_n^T((u))$. Then $\mathfrak{M} = \mathfrak{M}'$ if and only if A/A' is positive and unipotent.*

Proof. — Let $e_\star = [A]\, p^\star$ and $e'_\star = [A']\, p^\star$ be the associated generating sets. Then $\mathfrak{M} \subset \mathfrak{M}'$ if and only if for each i we have $e_i \in \mathfrak{M}'[i]$. This means that there exist scalars $b_{ij} \in k[[u]]$ such that

$$e_i = [b_{ij}]\, e'_i + [b_{i,i+1}]\, e'_{i+1} + \cdots + [b_{i,n}]\, e_n \ .$$

Let B be the upper triangular matrix with coefficients b_{ij}. These equalities amount to $e_\star = [B]\, e'_\star$, in other words $[A]\, p^\star = [B][A']\, p^\star = [B * A']\, p^\star$. Thus $A/A' = B \geqslant 0$ and this proves (1). Now (2) and (3) follow immediately. □

4.1.9. — *Remark.* It follows from this lemma that the relation $\succ$ on $\mathscr{G}_n^T((u))$ defined by $A \succ B$ if and only if $A/B \geqslant 0$ is reflexive and transitive.

4.2. Matricial description of Breuil-Kisin modules

Finally we arrive at the description in terms of matrices of the Breuil-Kisin modules corresponding to a group scheme which is a model of μ_{p^n}. We recall that K is a finite totally ramified field extension of K_0, the fraction field of the Witt ring $W = W(k)$ of a perfect field k of characteristic $p > 0$, and that $E(u)$ is the Eisenstein polynomial of a fixed uniformizer $\pi \in \mathcal{O}_K$.

4.2.1. — Definition. We say that $A = M(\boldsymbol{l}, \boldsymbol{a}) \in \mathscr{G}_n((u))$ is a *μ-matrix* if it is distinguished and if
(1) $\phi(A)/A \geqslant 0$,
(2) $(E(u) \diamond A)/\phi(A) \geqslant 0$.
We denote by $\mathscr{G}_n^\mu((u))$ the set of μ-matrices in $\mathscr{G}_n((u))$.

With the induced order of $\mathscr{G}_n^T((u))$ (*cf* Remark 4.1.9), the set $\mathscr{G}_n^\mu((u))$ is an ordered set. Since $\mathcal{U}$ and $\mathcal{L}$ are loop homomorphisms (3.2.5), take positive matrices to positive matrices (obvious), and commute with ϕ and $E(u) \diamond -$ (4.1.6), one sees that if $A \in \mathscr{G}_n((u))$ is a μ-matrix, then $\mathcal{U}A$ and $\mathcal{L}A$ are also μ-matrices.

4.2.2. — Theorem. *The maps $G \mapsto \mathfrak{M}(G)$ and $\mathfrak{M} \mapsto A(\mathfrak{M})$ give bijections between:*

- *the set of isomorphism classes of R-models of $\mu_{p^n,K}$,*
- *the set $\mathscr{L}_n^\mu$ of μ-lattices, i.e. finitely generated sub-$W_n[[u]]$-modules of $W_n((u))$ satisfying $E(u)\mathfrak{M} \subset \langle\phi(\mathfrak{M})\rangle \subset \mathfrak{M}$,*
- *the set $\mathscr{G}_n^\mu((u))$ of μ-matrices, i.e. matrices*

$$A = \begin{pmatrix} u^{l_1} & a_{12} & a_{13} & \dots & a_{1n} \\ & u^{l_2} & a_{23} & & a_{2n} \\ & & \ddots & \ddots & \vdots \\ & & & u^{l_{n-1}} & a_{n-1,n} \\ 0 & & & & u^{l_n} \end{pmatrix}$$

where $l = (l_1, \dots, l_n) \in \mathbb{N}^n$ and $a_{ij} \in k[u]$ for all i, j, such that:

(1) $\deg_u(a_{ij}) < l_j$ *whenever* $1 \leqslant i < j \leqslant n$,
(2) $\mathcal{U}A/\mathcal{L}A \geqslant 0$,
(3) $\phi(A)/A \geqslant 0$,
(4) $(E(u)\diamond A)/\phi(A) \geqslant 0$.

These bijections are increasing: if G, G' are models of $\mu_{p^n,K}$ with associated lattices $\mathfrak{M}, \mathfrak{M}'$ and distinguished matrices A, A', then the following conditions are equivalent:

- *there exists a model map $G \to G'$,*
- *$\mathfrak{M} \subset \mathfrak{M}'$,*
- *$A/A' \geqslant 0$.*

Finally, these bijections are "compatible with quotients and kernels":

- *$G(i)$, $\mathfrak{M}(i)$ and $\mathcal{U}^{i-1}A$ correspond to each other, and*
- *$G[i]$, $\mathfrak{M}[i]$ and $\mathcal{L}^{i-1}A$ correspond to each other.*

Proof. — The increasing bijection between models of μ_{p^n} and μ-lattices is the Breuil-Kisin equivalence. The map $\mathfrak{M} \mapsto A(\mathfrak{M})$ is the map taking a lattice to its distinguished matrix, so that $A = A(\mathfrak{M}) = M(\boldsymbol{l}, \boldsymbol{a})$ satisfies the conditions (1) and (2). It remains to prove that the additional conditions satisfied by a μ-lattice translate into the additional conditions (3) and (4) in the theorem. Indeed, the condition (3) is a translation of the fact that $\langle\phi(\mathfrak{M})\rangle \subset \mathfrak{M}$ and the condition (4) is a translation of the fact that $E(u)\mathfrak{M} \subset \mathfrak{M}$. Moreover, since $\mathfrak{M}$ is positive (see 2.3), then so is A and hence $l_i \geqslant 0$. This gives the refinement in the statement of the theorem. The fact that the bijection between μ-lattices and μ-matrices is increasing is Lemma 4.1.8. The fact that the bijections are compatible with quotients and kernels comes from Lemma 4.1.7 and the fact that $\mathcal{U}$ and $\mathcal{L}$ preserve μ-matrices. □

4.2.3. — *Remark.* Let us recapitulate some of the information we have on the parameters.

(1) We have $l_1 \geqslant l_2 \geqslant \cdots \geqslant l_n$ since $\mathcal{U}A/\mathcal{L}A \geqslant 0$ (A is a T-matrix). In fact, the positivity of $\mathcal{U}A/\mathcal{L}A$ corresponds to the existence of the model maps $G(i) \to G[i]$ of 2.3.3, for all i.
(2) We have $l_i \geqslant 0$ and $\mathrm{val}_u(a_{i,i+1}) \geqslant l_{i+1}/p$, for all i. Indeed, since $\phi(A)/A \geqslant 0$ there exists a positive matrix $B = M(\boldsymbol{m}, \boldsymbol{b})$ such that $\phi(A) = B * A$. Comparing the diagonal entries, we get $(p-1)l_i = m_i \geqslant 0$ thus $l_i \geqslant 0$. Comparing the entries at distance 1 from the diagonal, we get $(a_{i,i+1})^p = u^{(p-1)l_i} a_{i,i+1} + u^{l_{i+1}} b_{i,i+1}$. Thus $(a_{i,i+1})^p \equiv 0 \mod u^{l_{i+1}}$.
(3) We have $e/(p-1) \geqslant l_1$ since $(E(u) \diamond A)/\phi(A) \geqslant 0$. Indeed, the upper left entry of $E(u) \diamond A$ is u^{e+l_1} and the upper left entry of $\phi(A)$ is u^{pl_1}. The result follows.

Theorem 4.2.2 gives already very precise information on the structure of the set of models of μ_{p^n}. In a naive way, it is parametrized by n integers $0 \leqslant l_n \leqslant \cdots \leqslant l_1 \leqslant e/(p-1)$ and at most $\sum_{i=1}^{n-1} i l_i$ elements of k (the coefficients a_{ij}), as follows from condition (1) in Theorem 4.2.2.

4.2.4. — Definition. The parameters $(l_1, \ldots, l_n)$ of a model of μ_{p^n} are called the *type* of the model.

The geometric interpretation of the type of a model of μ_{p^n} is quite clear. Theorem 4.2.2 gives a precise geometric interpretation for the other (somehow more mysterious) parameters of the Breuil-Kisin modules: some of them parametrize flat subgroup schemes or quotients, and some others parametrize extensions between such subquotients, models of μ_{p^s} and μ_{p^r} for $1 \leqslant r, s \leqslant n-1$.

4.2.5. — *Remark.* A remaining open question is the structure of this set of parameters. The explicit computation of relations is completed for $n = 3$ in Section 5. Since the functions $\mathbb{S}_i$ and $\mathbb{P}_i$ involved in the operation $A * B$ are defined by exponentiation with respect to negative powers of p, a high enough power of Frobenius transforms the constraints defining μ-matrices into polynomial relations between the coefficients of the a_{ij}. Hence up to Frobenius, we can easily define the variety of models of μ_{p^n}. The study of the dimension and irreducible components of this variety has to be compared to the works of Imai and Caruso ([6], [14]) on Kisin's moduli space of models of μ_{p^n} ([17]).

5. Computation of μ-matrices for $n = 3$

Since the bijections in Theorem 4.2.2 are compatible with quotients and kernels, the matricial formulas for the models of μ_{p^n} contain the matricial formulas for the models of μ_{p^i} for all $i \leqslant n$. In this section, we work out the conditions in Theorem 4.2.2 for $n = 3$ and $p \geqslant 3$. We stress that they include also the case $n = 1, 2$. And in these cases one gets the formulas obtained by Caruso in [31], Appendix A.

5.1. Computation of the matrices

We have

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

$$\mathcal{L}A = \begin{pmatrix} u^{l_2} & a_{23} \\ 0 & u^{l_3} \end{pmatrix}.$$

Using Examples 3.3 we find

$$\mathcal{U}A/\mathcal{L}A = \begin{pmatrix} u^{l_1-l_2} & \frac{a_{12}-u^{l_1-l_2}a_{23}}{u^{l_3}} \\ 0 & u^{l_2-l_3} \end{pmatrix}.$$

Moreover we have

$$\phi(A) = \begin{pmatrix} u^{pl_1} & a_{12}^p & a_{13}^p \\ 0 & u^{pl_2} & a_{23}^p \\ 0 & 0 & u^{pl_3} \end{pmatrix}$$

and

$$\phi(A)/A = \begin{pmatrix} u^{(p-1)l_1} & \frac{a_{12}^p-u^{(p-1)l_1}a_{12}}{u^{l_2}} & p_{13} \\ 0 & u^{(p-1)l_2} & \frac{a_{23}^p-u^{(p-1)l_2}a_{23}}{u^{l_3}} \\ 0 & 0 & u^{(p-1)l_3} \end{pmatrix}$$

where

$$p_{13} = \frac{a_{13}^p - u^{(p-1)l_1}a_{13} - \frac{a_{12}^p-u^{(p-1)l_1}a_{12}}{u^{l_2}}a_{23} - \mathbb{S}_1(u^{(p-1)l_1}a_{12}, -a_{12}^p)}{u^{l_3}}.$$

Finally we compute $E(u)\diamond A$. Note that for $n=3$ we have $E_i\,\mathrm{Id}\,{*}\mathcal{P}^i\mathcal{U}^iA = E_i\mathcal{P}^i\mathcal{U}^iA$ for all i, but this is false already for $n=4$, because of the failure of multiplicativity of Teichmüller representatives of polynomials (see Lemma 3.1.4). Thus

$$E(u)\diamond A = \begin{pmatrix} u^{e+l_1} & u^e a_{12} + u^{l_1}E_1 & u^e a_{13} + a_{12}E_1 + \mathbb{S}_1(u^e a_{12}, u^{l_1}E_1) + u^{l_1}E_2 \\ 0 & u^{e+l_2} & u^e a_{23} + u^{l_2}E_1 \\ 0 & 0 & u^{e+l_3} \end{pmatrix}.$$

and

$$(E(u)\diamond A)/\phi(A) = \begin{pmatrix} u^{e-(p-1)l_1} & \frac{u^e a_{12} + u^{l_1}E_1 - u^{e-(p-1)l_1}a_{12}^p}{u^{pl_2}} & q_{13} \\ 0 & u^{e-(p-1)l_2} & \frac{u^e a_{23} + u^{l_2}E_1 - u^{e-(p-1)l_2}a_{23}^p}{u^{pl_3}} \\ 0 & 0 & u^{e-(p-1)l_3} \end{pmatrix}$$

where

$$q_{13} = \frac{u^e a_{13} + a_{12}E_1 + \mathbb{S}_1(u^e a_{12}, u^{l_1}E_1) + u^{l_1}E_2 - u^{e-(p-1)l_1}a_{13}^p}{u^{pl_3}}$$

$$- \frac{\frac{u^e a_{12} + u^{l_1}E_1 - u^{e-(p-1)l_1}a_{12}^p}{u^{pl_2}}a_{23}^p - \mathbb{S}_1(u^{e-(p-1)l_1}a_{12}^p, u^e a_{12} + u^{l_1}E_1 - u^{e-(p-1)l_1}a_{12}^p)}{u^{pl_3}}.$$

5.2. Translation of the conditions of the theorem

- Condition (1) yields:

$$\boxed{\deg_u(a_{12}) \leqslant l_2 - 1} \quad , \quad \boxed{\deg_u(a_{13}) \leqslant l_3 - 1} \quad \text{and} \quad \boxed{\deg_u(a_{23}) \leqslant l_3 - 1}.$$

- Condition (2) yields:

$$\boxed{l_1 \geqslant l_2 \geqslant l_3} \quad \text{and} \quad \boxed{a_{12} - u^{l_1 - l_2}a_{23} \equiv 0 \mod u^{l_3}}.$$

- Condition (3) yields:

$$a_{12}^p - u^{(p-1)l_1}a_{12} \equiv 0 \mod u^{l_2},$$

$$a_{23}^p - u^{(p-1)l_2}a_{23} \equiv 0 \mod u^{l_3}$$

and

$$a_{13}^p - u^{(p-1)l_1}a_{13} - \frac{a_{12}^p - u^{(p-1)l_1}a_{12}}{u^{l_2}}a_{23} - \mathbb{S}_1(u^{(p-1)l_1}a_{12}, -a_{12}^p) \equiv 0 \mod u^{l_3}.$$

Since $(p-1)l_1 \geqslant l_2$, the first two are equivalent to:

$$\boxed{a_{12}^p \equiv 0 \mod u^{l_2}} \quad \text{and} \quad \boxed{a_{23}^p \equiv 0 \mod u^{l_3}}\,.$$

Concerning the third, observe that since $(p-1)l_1 \geqslant l_3$ the term $u^{(p-1)l_1}a_{13}$ can be neglected. Also since $\mathrm{val}_u(\mathbb{S}_1(x,y)) \geqslant \max(\mathrm{val}_u(x), \mathrm{val}_u(y))$ by Lemma 3.1.4, we see that the $\mathbb{S}_1$ term can be neglected. Finally the term $u^{(p-1)l_1-l_2}a_{12}a_{23}$ can also be neglected: indeed $pl_1 \geqslant 2l_1 \geqslant l_2 + l_3$ implies that its valuation is at least

$$\big((p-1)l_1 - l_2\big) + \frac{l_2}{p} + \frac{l_3}{p} = \frac{1}{p}\big((p-1)(pl_1 - l_2) + l_3\big) \geqslant \frac{1}{p}\big((p-1)l_3 + l_3\big) = l_3\,.$$

So the third condition is equivalent to:

$$\boxed{a_{13}^p - u^{-l_2}a_{12}^p a_{23} \equiv 0 \mod u^{l_3}}\,.$$

- Condition (4) yields:

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

$$\boxed{u^e a_{23} + u^{l_2}E_1 - u^{e-(p-1)l_2}a_{23}^p \equiv 0 \mod u^{pl_3}}$$

and

$$u^e a_{13} + a_{12}E_1 + \mathbb{S}_1(u^e a_{12}, u^{l_1}E_1) + u^{l_1}E_2 - u^{e-(p-1)l_1}a_{13}^p$$

$$- \tfrac{u^e a_{12} + u^{l_1}E_1 - u^{e-(p-1)l_1}a_{12}^p}{u^{pl_2}} a_{23}^p - \mathbb{S}_1(u^{e-(p-1)l_1}a_{12}^p, -u^e a_{12} - u^{l_1}E_1) \equiv 0 \mod u^{pl_3}.$$

Finally the last but one boxed congruence implies that

$$\mathbb{S}_1(u^{e-(p-1)l_1}a_{12}^p, u^e a_{12} + u^{l_1}E_1 - u^{e-(p-1)l_1}a_{12}^p) \equiv 0 \mod u^{pl_2}.$$

Hence it vanishes also modulo u^{pl_3} and we obtain:

$$\boxed{\begin{aligned} u^e a_{13} + a_{12}E_1 + \mathbb{S}_1(u^e a_{12}, u^{l_1}E_1) + u^{l_1}E_2 - u^{e-(p-1)l_1}a_{13}^p \\ - \tfrac{u^e a_{12} + u^{l_1}E_1 - u^{e-(p-1)l_1}a_{12}^p}{u^{pl_2}} a_{23}^p \equiv 0 \mod u^{pl_3} \end{aligned}}\,.$$

5.2.1. — Corollary. *Let $p \geqslant 3$. Let $\mathfrak{M} \in (\mathrm{Mod}/\mathfrak{S})_3$ be the Breuil-Kisin module of a finite flat R-model of $\mu_{p^3,K}$. Then there exists a unique family of parameters $(l_1, l_2, l_3, a_{12}, a_{13}, a_{23})$ composed of three integers $0 \leqslant l_3 \leqslant l_2 \leqslant l_1 \leqslant e/(p-1)$ and three polynomials $a_{12}, a_{13}, a_{23} \in k[u]$ satisfying:*

(i) $\deg_u a_{12} \leqslant l_2 - 1$, $\deg_u a_{13} \leqslant l_3 - 1$, $\deg_u a_{23} \leqslant l_3 - 1$,

(ii) $a_{12} - u^{l_1 - l_2}a_{23} \equiv 0 \mod u^{l_3}$, $a_{12}^p \equiv 0 \mod u^{l_2}$, $a_{23}^p \equiv 0 \mod u^{l_3}$,

(iii) $a_{13}^p - u^{-l_2}a_{12}^p a_{23} \equiv 0 \mod u^{l_3}$,

(iv) $u^e a_{12} + u^{l_1} E_1 - u^{e-(p-1)l_1} a_{12}^p \equiv 0 \mod u^{pl_2}$ *and* $u^e a_{23} + u^{l_2} E_1 - u^{e-(p-1)l_2} a_{23}^p \equiv 0 \mod u^{pl_3}$,

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

such that $\mathfrak{M} = \mathfrak{M}(A)$ *with*

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

5.3. The tamely ramified case

In the tamely ramified case $(e,p) = 1$, some of these congruences can be simplified. To begin with, let us prove that

$$\boxed{l_1 \geqslant pl_2} \quad \text{and} \quad \boxed{l_2 \geqslant pl_3}\,.$$

Let us prove the first inequality. If $l_2 = 0$ there is nothing to show. Otherwise we have $l_2 > 0$ and we claim that the only monomial of degree l_1 in the polynomial

$$u^e a_{12} + u^{l_1} E_1 - u^{e-(p-1)l_1} a_{12}^p$$

is $u^{l_1} E_1(0)$. Indeed the first term has valuation

$$\mathrm{val}(u^e a_{12}) \geqslant e + l_2/p > e \geqslant (p-1)l_1 \geqslant l_1\ .$$

Moreover since a_{12}^p is a p-th power, the degrees of the monomials of $u^{e-(p-1)l_1} a_{12}^p$ are of the form

$$e - (p-1)l_1 + ip = e + l_1 - p(l_1 - i)$$

for some integer i. Since $(e,p) = 1$, this degree is not congruent to l_1 modulo p. This proves that $u^{l_1} E_1(0)$ is the only monomial of degree l_1 and then the congruence

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

forces $l_1 \geqslant pl_2$. The proof that $l_2 \geqslant pl_3$ is similar.

It follows that the condition given by the congruence $a_{12} - u^{l_1 - l_2} a_{23} \equiv 0 \mod u^{l_3}$ is empty since we already know that both terms have valuation at least l_3.

It follows also that the congruences implied by condition (4) become:

$$\boxed{u^{e-(p-1)l_1} a_{12}^p \equiv 0 \mod u^{pl_2}} \quad , \quad \boxed{u^{e-(p-1)l_2} a_{23}^p \equiv 0 \mod u^{pl_3}}$$

and

$$\boxed{a_{12}E_1 - u^{e-(p-1)l_1}a_{13}^p - \frac{u^e a_{12} + u^{l_1}E_1 - u^{e-(p-1)l_1}a_{12}^p}{u^{pl_2}}a_{23}^p \equiv 0 \mod u^{pl_3}}\,.$$

Then, in the tamely ramified case, the parametrisation of models of $\mu_{p^3,K}$ is much easier:

5.3.1. — Corollary. *In the tamely ramified case* $(e,p)=1$, *the models of* μ_{p^3} *over* $\mathcal{O}_K$ *are classified by three integers* $0 \leqslant p^2 l_3 \leqslant pl_2 \leqslant l_1 \leqslant e/(p-1)$ *and three polynomials* $a_{12}, a_{13}, a_{23} \in k[u]$ *satisfying:*

(i) $\deg_u a_{12} \leqslant l_2 - 1$, $\deg_u a_{13} \leqslant l_3 - 1$, $\deg_u a_{23} \leqslant l_3 - 1$,

(ii) $u^{e-(p-1)l_1}a_{12}^p \equiv 0 \mod u^{pl_2}$, $u^{e-(p-1)l_2}a_{23}^p \equiv 0 \mod u^{pl_3}$,

(iii) $a_{12}E_1 - u^{e-(p-1)l_1}a_{13}^p - \frac{u^e a_{12} + u^{l_1}E_1 - u^{e-(p-1)l_1}a_{12}^p}{u^{pl_2}}a_{23}^p \equiv 0 \mod u^{pl_3}$.

5.3.2. — *Remark.* The tamely ramified case seems to be easy to compute in higher dimension. In Corollary 5.2.1, even for $n=3$, we can see that ramification intervenes in the computation in a very delicate way: not only through the coefficient E_2 of the Eisenstein polynomial but also through the lifting modulo p^2 of the parameters via $\mathbb{S}_1(u^e a_{12}, u^{l_1}E_1)$.

6. Sekiguchi-Suwa Theory

In this section, we recall and complement some aspects of Sekiguchi-Suwa Theory. The main definitions and results are given in Subsections 6.1, 6.2, 6.3. For an extended version, see [22]. We also give an interpretation of these results from a matricial point of view: we introduce the set $\mathscr{M}_n$ of matrices parametrizing filtered group schemes, and study its basic properties. This is the topic of Subsection 6.4.

6.1. Some definitions about Witt vectors

6.1.1. — The maps V, F, T. We recall here some definitions about Witt vectors. We emphasize that in contrast with Sections § 2 to § 5, we consider Witt vectors with coefficients in an arbitrary ring, not necessarily perfect of characteristic p. In particular, we need to consider quotients of a discrete valuation ring of unequal characteristics. For $r \geqslant 0$, we recall the definition of the r-th Witt polynomial:

$$\Phi_r(X_0, \ldots, X_r) = X_0^{p^r} + pX_1^{p^{r-1}} + \cdots + p^r X_r.$$

Then for each ring A the following maps are defined:

- Verschiebung:

$$V : W(A) \longrightarrow W(A)$$
$$(a_0, a_1, a_2, \dots) \longmapsto (0, a_0, a_1, a_2, \dots)$$

- Frobenius:

$$F : W(A) \longrightarrow W(A)$$
$$\boldsymbol{a} = (a_0, a_1, a_2, \dots) \longmapsto (F_0(\boldsymbol{a}), F_1(\boldsymbol{a}), F_2(\boldsymbol{a}), \dots)$$

where the polynomials $F_r(\mathbb{X}) = F_r(X_0, \dots, X_r) \in \mathbb{Z}[X_0, \dots, X_{r+1}]$ are defined inductively by

$$\Phi_r(F_0(\mathbb{X}), F_1(\mathbb{X}), \dots, F_r(\mathbb{X})) = \Phi_{r+1}(X_0, \dots, X_{r+1}).$$

- T map:

$$T : W(A) \times W(A) \longrightarrow W(A)$$
$$(\boldsymbol{a}, \boldsymbol{x}) \longmapsto T_{\boldsymbol{a}}\boldsymbol{x} = (T_0(\boldsymbol{a}, \boldsymbol{x}), T_1(\boldsymbol{a}, \boldsymbol{x}), T_2(\boldsymbol{a}, \boldsymbol{x}), \dots)$$

where the polynomials $T_r(\mathbb{A}, \mathbb{X}) = T_r(A_0, \dots, A_r, X_0, \dots, X_r) \in \mathbb{Z}[A_0, \dots, A_r, X_0, \dots, X_r]$ are defined inductively by

$$\Phi_n(T_0, \dots, T_n) = \sum_{i=0}^{n} p^{n-i} (A_{n-i})^{p^i} \Phi_i(X_0, \dots, X_i).$$

Since $\Phi_n(T_0, \dots, T_n)$ is linear in the variables $\Phi_i(X_0, \dots, X_i)$, we see that for fixed $\boldsymbol{a}$ the map $T_{\boldsymbol{a}}$ is a morphism of additive groups. Moreover, it is easy to see that for any ring A and Witt vectors $\boldsymbol{a}, \boldsymbol{x} \in W(A)$ with $\boldsymbol{a} = (a_0, \dots, a_n, \dots)$ we have explicitly $T_{\boldsymbol{a}}\boldsymbol{x} = \sum_{k=0}^{\infty} V^k([a_k]\boldsymbol{x})$ (see [25], Lemma 4.2). For instance if $\boldsymbol{a} = [a_0]$ is a Teichmüller element then $T_{\boldsymbol{a}}$ is nothing else than left multiplication by $[a_0]$, and in particular T_1 is the identity. If $\boldsymbol{x} = [x_0]$ is Teichmüller then $T_{\boldsymbol{a}}([x_0]) = (a_0x_0, a_1x_0, a_2x_0, \dots)$. For each ring A an element $\lambda \in A$, we set

$$\lambda.\boldsymbol{a} \overset{\text{df}}{=} (\lambda a_0, \lambda a_1, \lambda a_2, \dots) = T_{\boldsymbol{a}}([\lambda]).$$

Clearly $\lambda_1.(\lambda_2.\boldsymbol{a}) = (\lambda_1\lambda_2).\boldsymbol{a}$ which will usually be written $\lambda_1\lambda_2.\boldsymbol{a}$. The ideal $\lambda.W(A)$ is the kernel of the morphism of rings $W(A) \to W(A/\lambda A)$. If two vectors $\boldsymbol{a}, \boldsymbol{b}$ are congruent modulo $\lambda.W(A)$, we sometimes write simply $\boldsymbol{a} \equiv \boldsymbol{b} \mod \lambda$. We will also have to consider the following type of Witt vectors with coefficients in the ring $A[1/\lambda]$:

$$\frac{\boldsymbol{a}}{\lambda} \overset{\text{df}}{=} \left(\frac{a_0}{\lambda}, \frac{a_1}{\lambda}, \frac{a_2}{\lambda}, \dots\right).$$

The notations $\frac{1}{\lambda}\boldsymbol{a}$ or $\boldsymbol{a}/\lambda$ may also be used when it is convenient.

6.1.2. — Definition. For any ring A, we define the *subfunctor of finite Witt vectors* by

$$W^f(A) = \big\{(a_0, a_1, a_2, \dots) \in W(A)\ ;\ a_i = 0 \text{ for } i \gg 0\big\}$$

and the *completion* of $W(A)$ by

$$\widehat{W}(A) = \big\{(a_0, a_1, a_2, \dots) \in W(A)\ ;\ a_i = 0 \text{ for } i \gg 0 \text{ and } a_i \text{ is nilpotent for all } i\big\}.$$

Note that $W^f(A)$ is not a subgroup of $W(A)$, but $\widehat{W}(A)$ is an ideal in $W(A)$ which is stable under F and V (see [22], 2.2.1, 2.2.3, 2.2.4).

6.1.3. — The T-multiplication. We shall define a new product between matrices whose entries are Witt vectors. We need to start with some elementary properties of the map T when one of the variables is fixed.

6.1.4. — Lemma. *Let A be a ring and $\boldsymbol{a} = (a_0, a_1, a_2, \dots) \in W(A)$ with a_0 not a zero divisor. Then the morphism $T_{\boldsymbol{a}}$ is injective. If a_0 is invertible then it is an isomorphism.*

Proof. — Let us suppose that a_0 is not a zero divisor and that $T_{\boldsymbol{a}}\boldsymbol{x} = 0$ with $\boldsymbol{x} = (x_0, x_1, \dots) \in W(A)$. We prove, by induction, that $x_n = 0$ for any n. Since $\Phi_0(T_{\boldsymbol{a}}\boldsymbol{x}) = a_0 x_0 = 0$ and since a_0 is not a zero divisor then $x_0 = 0$. We now suppose that $x_i = 0$ for $i \leqslant n$. This means that $\boldsymbol{x} = V^{n+1}\boldsymbol{y}$ with $\boldsymbol{y} = (x_{n+1}, \dots, x_r, \dots) \in W(A)$. Therefore

$$T_{\boldsymbol{a}}\boldsymbol{x} = \sum_{k=0}^{\infty} V^k([a_k]V^{n+1}(\boldsymbol{y})) = V^{n+1}(\sum_{k=0}^{\infty} V^k([a_k^{p^{n+1}}]\boldsymbol{y})) = 0.$$

In particular we have $a_0^{p^{n+1}} x_{n+1} = 0$. Since a_0 is not a zero divisor then $x_{n+1} = 0$.

Let us now suppose that a_0 is invertible. Let $\boldsymbol{y} \in W(A)$. Let $p_n : W(A) \to W_n(A)$ and $p_{n,k} : W_n(A) \to W_k(A)$, if $n \geqslant k$, the natural projections. We now prove that for any $n \in \mathbb{N}$ there exist $\boldsymbol{x}_n \in W_n(A)$ such that $T_{p_n(\boldsymbol{a})}\boldsymbol{x}_n = p_n(\boldsymbol{y})$ and $p_{n,n-1}(\boldsymbol{x}_n) = \boldsymbol{x}_{n-1}$. This clearly implies that there exists $\boldsymbol{x} \in W(A)$ such that $T_{\boldsymbol{a}}\boldsymbol{x} = \boldsymbol{y}$.

We prove the above statement by induction. Clearly $\boldsymbol{x}_0 = (x_0) = (\frac{y_0}{a_0}) \in A$. Let us suppose that there exists $\boldsymbol{x}_n = (x_0, \dots, x_n)$ such that $T_{p_n(\boldsymbol{a})}\boldsymbol{x}_n = p_n(\boldsymbol{y})$. The required $\boldsymbol{x}_{n+1}$ is given by $(x_0, \dots, x_{n+1})$ with x_{n+1} such that

$$V^{n+1}[a_0 x_{n+1}] = p_{n+1}(\boldsymbol{y}) - \sum_{i=1}^{n+1} V^i([a_i](x_0, \dots, x_n, 0)) - [a_0](x_0, \dots, x_n, 0).$$

The existence of x_{n+1} is ensured by the fact that a_0 is invertible and by the fact that the projection of the right hand side on W_n is zero by induction. □

6.1.5. — LEMMA. *For any $\boldsymbol{x} = (x_0, x_1, x_2, \dots) \in W(A)$ with x_0 not a zero divisor, the map $T_\bullet \boldsymbol{x}$ is injective. If x_0 is invertible then it is bijective.*

Proof. — Let $\boldsymbol{a} = (a_0, a_1, a_2, \dots)$ and $\boldsymbol{b} = (b_0, b_1, b_2, \dots)$ as above. We will prove by induction that $a_n = b_n$ for any n. If $T_{\boldsymbol{a}}\boldsymbol{x} = T_{\boldsymbol{b}}\boldsymbol{x}$ in particular $a_0 x_0 = b_0 x_0$. Since x_0 is not a zero divisor them $a_0 = b_0$. Now let us suppose that $a_i = b_i$ for $i \leqslant n$. We prove $a_n = b_n$. By hypothesis, we have

$$T_{\boldsymbol{a}}\boldsymbol{x} - T_{\boldsymbol{b}}\boldsymbol{x} = T_{\boldsymbol{a}}\boldsymbol{x} = \sum_{k=0}^{\infty} V^k(([a_k] - [b_k])\boldsymbol{x}) = \sum_{k=n+1}^{\infty} V^k(([a_k] - [b_k])\boldsymbol{x}) = 0$$

In particular we have $a_{n+1}x_0 = b_{n+1}x_0$ which implies $a_{n+1} = b_{n+1}$ since x_0 is not a zero divisor. To prove the surjectivity when x_0 is invertible one proceeds in a similar way as in the previous lemma and it is even simpler. □

We now introduce a new, nonassociative product between matrices with Witt vector entries.

6.1.6. — DEFINITION. Let $M = (\boldsymbol{m}_i^j)$ and N be two matrices belonging to $M_n(W(A))$. We define the T-multiplication by

$$M \star_T N := T_M(N)$$

where T_M is the matrix of operators $(T_{\boldsymbol{m}_i^j})_{1 \leqslant i,j \leqslant n}$.

Endowed with this composition law, $M_n(W(A))$ is a magma and the identity matrix is a two-sided unit element. We will now consider the set $\mathscr{H}_n(W(A)) \subseteq M_n(W(A))$ of upper triangular matrices of the form

$$\begin{pmatrix} \boldsymbol{a}_1^1 & \boldsymbol{a}_1^2 & \boldsymbol{a}_1^3 & \dots & \boldsymbol{a}_1^n \\ 0 & \boldsymbol{a}_2^2 & \boldsymbol{a}_2^3 & \dots & \boldsymbol{a}_2^n \\ \vdots & & & & \vdots \\ & & 0 & \boldsymbol{a}_{n-1}^{n-1} & \boldsymbol{a}_{n-1}^n \\ & & & 0 & \boldsymbol{a}_n^n \end{pmatrix}$$

with $\boldsymbol{a}_i^j = (a_{i0}^j, a_{i1}^j, a_{i2}^j, \dots)$ and a_{i0}^i not a zero divisor. We refer to 3.2.4 for the definition of the operators $\mathcal{U}$ and $\mathcal{L}$, taking a square matrix to its upper left and lower right codimension 1 submatrices.

6.1.7. — LEMMA. *The set $\mathscr{H}_n(W(A))$ is a submagma of $M_n(W(A))$ and the cancellation laws hold, i.e. if $M \star_T N = M' \star_T N$ then $M = M'$ and if $M \star_T N = M \star_T N'$ then $N = N'$. Moreover if A is a field then $\mathscr{H}_n(W(A))$ is a loop.*

Proof. — It is easy to prove that $\mathscr{H}_n(W(A))$ is stable under $\star_T$. We now prove that the cancellation laws hold by induction on n. For $n = 1$ this is just lemmas 6.1.4 and 6.1.5. Let us suppose that the cancellation laws hold in $\mathscr{H}_n(W(A))$ and prove them for $\mathscr{H}_{n+1}(W(A))$. We observe that for any $M, N \in \mathscr{H}_{n+1}(W(A))$ we have

$$\mathcal{U}(M \star_T N) = \mathcal{U}(M) \star_T \mathcal{U}(N)$$

and

$$\mathcal{L}(M \star_T N) = \mathcal{L}(M) \star_T \mathcal{L}(N).$$

Therefore if $M \star_T N = M' \star_T N$ we have, by induction, that $\mathcal{U}(M) = \mathcal{U}(M')$ and $\mathcal{L}(M) = \mathcal{L}(M')$. Similarly if $M \star_T N = M \star_T N'$ then $\mathcal{U}(N) = \mathcal{U}(N')$ and $\mathcal{L}(N) = \mathcal{L}(N')$. It remains to prove that $\boldsymbol{m}_1^{n+1} = {\boldsymbol{m}'}_1^{n+1}$ and $\boldsymbol{n}_1^{n+1} = {\boldsymbol{n}'}_1^{n+1}$. We begin with the first. From

$$(M \star_T N)_1^{n+1} = (M' \star_T N)_1^{n+1}$$

it follows that

$$\sum_{j=1}^{n+1} T_{\boldsymbol{m}_1^j} \boldsymbol{n}_j^{n+1} = \sum_{j=1}^{n+1} T_{{\boldsymbol{m}'}_1^j} \boldsymbol{n}_j^{n+1}.$$

Since $\boldsymbol{m}_1^j = {\boldsymbol{m}'}_1^j$ for $j = 1, \ldots, n$ it follows that

$$T_{\boldsymbol{m}_1^{n+1}} \boldsymbol{n}_{n+1}^{n+1} = T_{{\boldsymbol{m}'}_1^{n+1}} \boldsymbol{n}_{n+1}^{n+1}$$

which implies $\boldsymbol{m}_1^{n+1} = {\boldsymbol{m}'}_1^{n+1}$ by Lemma 6.1.4. Now from

$$(M \star_T N)_1^{n+1} = (M \star_T N')_1^{n+1}$$

it follows that

$$\sum_{j=1}^{n+1} T_{\boldsymbol{m}_1^j} \boldsymbol{n}_j^{n+1} = \sum_{j=1}^{n+1} T_{\boldsymbol{m}_1^j} {\boldsymbol{n}'}_j^{n+1}.$$

Since $\boldsymbol{n}_1^j = {\boldsymbol{n}'}_1^j$ for $j = 1, \ldots, n$ it follows that

$$T_{\boldsymbol{m}_1^1} \boldsymbol{n}_1^{n+1} = T_{\boldsymbol{m}_1^1} {\boldsymbol{n}'}_1^{n+1}$$

which implies $\boldsymbol{n}_1^{n+1} = {\boldsymbol{n}'}_1^{n+1}$ by Lemma 6.1.5.

To prove the fact that $\mathscr{H}_n(W_n(A))$ is a loop if A is a field one proceeds similarly, using the second part of Lemmas 6.1.4 and 6.1.5. □

6.2. Deformed Artin-Hasse exponentials

In this section we introduce some deformations of Artin-Hasse exponentials which we will need in the following.

6.2.1. — Definition. Given indeterminates Λ, U and T, we define a formal power series in T with coefficients in $\mathbb{Q}[\Lambda, U]$ by

$$E_p(U,\Lambda,T) = (1+\Lambda T)^{\frac{U}{\Lambda}} \prod_{k=1}^{\infty} (1+\Lambda^{p^k} T^{p^k})^{\frac{1}{p^k}\left(\left(\frac{U}{\Lambda}\right)^{p^k} - \left(\frac{U}{\Lambda}\right)^{p^{k-1}}\right)}.$$

It satisfies basic properties such as $E_p(0,\Lambda,T)=1$ and $E_p(MU,M\Lambda,T) = E_p(U,\Lambda,MT)$, where M is another indeterminate. It is a deformation of the classical Artin-Hasse exponential $E_p(T) = \prod_{k=0}^{\infty} \exp(T^{p^k}/p^k)$ in the sense that $E_p(1,0,T) = E_p(T)$. To see this it is sufficient to observe that, for any k, the series $(1+\Lambda^{p^k}T^{p^k})^{\frac{1}{p^k}\left(\frac{1}{\Lambda^{p^k}} - \frac{1}{\Lambda^{p^{k-1}}}\right)}$ is equal to $\left((1+\Lambda^{p^k}T^{p^k})^{\frac{1}{\Lambda^{p^k}}}\right)^{\frac{1-\Lambda^p}{p^k}}$, and this gives $\exp(T^{p^k}/p^k)$ for $\Lambda = 0$.

6.2.2. — Definition. Given a vector of indeterminates $\mathbb{U} = (U_0, U_1, \dots)$, we define a power series in T with coefficients in $\mathbb{Q}[\Lambda, U_0, U_1, \dots]$ by

$$E_p(\mathbb{U},\Lambda,T) = \prod_{\ell=0}^{\infty} E_p(U_\ell, \Lambda^{p^\ell}, T^{p^\ell}).$$

We have the following fundamental lemma.

6.2.3. — Lemma. *The series $E_p(U,\Lambda,T)$ and $E_p(\mathbb{U},\Lambda,T)$ are integral at p, that is, they have their coefficients in $\mathbb{Z}_{(p)}[\Lambda,U]$ and $\mathbb{Z}_{(p)}[\Lambda,U_0,U_1,\dots]$ respectively.*

Proof. — See [26], Corollary 2.5. □

It follows from this lemma that given a $\mathbb{Z}_{(p)}$-algebra A, elements $\lambda, a \in A$ and $\boldsymbol{a} = (a_0, a_1, \dots) \in A^{\mathbb{N}}$, we have specializations $E_p(a,\lambda,T)$ and $E_p(\boldsymbol{a},\lambda,T)$ which are power series in T with coefficients in A. We usually consider $\boldsymbol{a}$ as a Witt vector, i.e. as an element in $W(A)$.

6.2.4. — *Remark.* Let $\mathbb{A}^1 = \mathrm{Spec}(\mathbb{Z}_{(p)}[\Lambda])$ be the affine line over the ring of p-integers $\mathbb{Z}_{(p)}$, with coordinate Λ, and write $W_{\mathbb{A}^1}$ for the scheme of Witt vectors over $\mathbb{A}^1$. We remark (see [26], Corollary 2.9.1) that, generalizing what happens for the Artin-Hasse exponential, the deformed exponential of Definition 6.2.2 gives a homomorphism

$$W_{\mathbb{A}^1} \longrightarrow \mathbf{\Lambda}_{\mathbb{A}^1}$$

where $\mathbf{\Lambda}_{\mathbb{A}^1} = \mathrm{Spec}(\mathbb{Z}_{(p)}[\Lambda, X_1, \dots, X_n, \dots])$ is the $\mathbb{A}^1$-group scheme whose group of R-points, for any $\mathbb{Z}_{(p)}[\Lambda]$-algebra R, is the abelian multiplicative group $1 + TR[[T]]$. (We hope that the difference between the symbols Λ and $\mathbf{\Lambda}$ is visible enough.) The above homomorphism is in fact a closed immersion. We also note that there is an isomorphism:

$$\prod_{p\nmid k} W_{\mathbb{A}^1} \simeq \mathbf{\Lambda}_{\mathbb{A}^1}$$

which works as follows. With any $\mathbb{Z}_{(p)}$-algebra R, any element $\lambda \in R$, and any family of Witt vectors $\boldsymbol{a}_k = (a_{k0}, a_{k1}, a_{k2}, \dots) \in W(A)$ indexed by the prime-to-p integers k, this isomorphism associates the series $F(T) = \prod_{p\nmid k} E_p(\boldsymbol{a}_k, \lambda, T^k)$ (see [22], Lemma 3.1.2). □

Here are a couple more definitions which will be useful in the sequel. We set

$$\widetilde{p}E_p(\mathbb{U}, \Lambda, T) = E_p(V(U_0^p, U_1^p, \dots), \Lambda, T).$$

where V is the Verschiebung. Using the isomorphism $\prod_{k\nmid p} W_{\mathbb{A}^1} \simeq \mathbf{\Lambda}_{\mathbb{A}^1}$ described above, one extends this definition to any element of

$$1 + T\mathbb{Z}_{(p)}[U_1, \dots, U_n, \Lambda][[T]].$$

The result is a group scheme endomorphism

$$\widetilde{p} : \mathbf{\Lambda}_{\mathbb{A}^1} \longrightarrow \mathbf{\Lambda}_{\mathbb{A}^1}.$$

In [25] this operator is called $[p]$, but we prefer $\widetilde{p}$ to avoid confusion with Teichmüller representatives. Also, we define an additive endomorphism $F^{\Lambda} := F - [\Lambda^{p-1}] : W_{\mathbb{A}^1} \to W_{\mathbb{A}^1}$. For each element λ in a $\mathbb{Z}_{(p)}$-algebra R, this gives an endomorphism $F^{\lambda} : W_R \to W_R$. When R is a discrete valuation ring with uniformizer π and $\lambda = \pi^l$ for some $l > 0$, we will sometimes write $F^{(l)}$ instead of F^{π^l} (see e.g. the statement of Theorem 6.3.4).

6.2.5. — Definition. Let Λ_2 be another indeterminate. For any H in $1 + T\mathbb{Z}_{(p)}[U_1, \dots, U_n, \Lambda][[T]]$ we define the series

$$\widetilde{E}_p(\mathbb{W}, \Lambda_2, H) = H^{\frac{W_0}{\Lambda_2}} \prod_{r=1}^{\infty} \left(\widetilde{p}^r H\right)^{\frac{1}{p^r \Lambda_2^{p^r}} \Phi_{r-1}(F^{\Lambda_2}(\mathbb{W}))}. \tag{6.1}$$

From the definition, one sees that $\widetilde{E}_p(\mathbb{W}, \Lambda, H)$ gives a bilinear group scheme homomorphism

$$W_{\mathbb{A}^1} \times \mathbf{\Lambda}_{\mathbb{A}^1} \to \mathbf{\Lambda}_{\mathbb{A}^1}.$$

With some quite simple computations one shows the following lemma.

6.2.6. — Lemma. *In the group* $1+T\mathbb{Z}_{(p)}[\mathbb{W},\frac{\mathbb{U}}{\Lambda_2},\Lambda,\Lambda_2][[T]]$, *we have*

$$\widetilde{E}_p(\mathbb{W},\Lambda_2,E_p(\mathbb{U},\Lambda;T))=E_p(T_{\mathbb{U}/\Lambda_2}\mathbb{W},\Lambda;T).$$

Proof. — See [25], Proposition 4.11. □

In particular, we have $\widetilde{E}_p(\mathbb{W},\Lambda,1+\Lambda T)=E_p(\mathbb{W},\Lambda;T)$. Finally we define the following series.

6.2.7. — Definition. For any H as above, we define

$$G_p(\mathbb{W},\Lambda_2,H)$$
$$=\prod_{r=1}^{\infty}\left(\frac{1+(H-1)^{p^r}}{\widetilde{p}^r H}\right)^{\frac{1}{p^r\Lambda_2^{p^r}}\Phi_{r-1}(\mathbb{W})}\in 1+T\mathbb{Q}[\mathbb{W},\mathbb{U},\Lambda,\Lambda_2,\frac{1}{\Lambda_2}][[T]].$$

Using [26], Lemma 2.8, one sees immediately that

$$G_p(F^{\Lambda_2}(\mathbb{W}),\Lambda_2,H)=\frac{E_p(\mathbb{W},\Lambda_2;\frac{H-1}{\Lambda_2})}{\widetilde{E}_p(\mathbb{W},\Lambda_2,H)}. \tag{6.2}$$

We remark that for any H as above we have

$$G_p(\mathbb{W},\Lambda_2,H)\,G_p(\mathbb{W}',\Lambda_2,H)$$
$$=G_p(\mathbb{W}+\mathbb{W}',\Lambda_2,H)\in 1+T\mathbb{Q}[\mathbb{W},\mathbb{W}',\mathbb{U},\Lambda,\Lambda_2\frac{1}{\Lambda_2}][[T]] \tag{6.3}$$

where $\mathbb{W}+\mathbb{W}'$ is the sum of Witt vectors. We finally have the following lemma.

6.2.8. — Lemma. *We have*

$$G_p(\mathbb{W},\Lambda_2,E_p(\mathbb{U},\Lambda_2;T))\in\mathbb{Z}_{(p)}[\mathbb{W},\frac{\mathbb{U}}{\Lambda_2},\Lambda,\Lambda_2][[T]].$$

Proof. — See [25], Proposition 4.12. □

It is quite simple to verify the following equality.

6.2.9. — Lemma. *We have*

$$\widetilde{E}_p(\mathbb{W},\Lambda_3,G_p(\mathbb{U},\Lambda_2;H))=G_p(T_{\mathbb{U}/\Lambda_3}\mathbb{W},\Lambda_2;H).$$

Proof. — See [25], Proposition 4.13. □

6.3. Main theorems of Sekiguchi-Suwa Theory

In this section, we briefly recall the main results of Sekiguchi-Suwa Theory, stated in [25]. One can also find a summary of this theory in wider generality in [22]. From now on, we denote by R a discrete valuation ring of unequal characteristics. We stress that, in contrast with Sections § 2 to § 5 we do not assume that R is complete and neither that its residue field is perfect. We will denote by π a fixed uniformizer of R and by v the valuation of R.

6.3.1. — Definition. Let $l, l_1, \dots, l_n$ be integers.
(1) We let $\mathcal{G}^{(l)}$ be the group scheme $\mathrm{Spec}(R[T, 1/(\pi^l T + 1)])$ with group law $T * T' = T + T' + \pi^l TT'$, the unique group law such that the morphism $\alpha : \mathrm{Spec}(R[T, 1/(\pi^l T+1)]) \to \mathbb{G}_m = \mathrm{Spec}(R[T, 1/T])$ given by $T \mapsto 1+\pi^l T$ is a group scheme homomorphism.
(2) Let $\mathcal{E}$ be a flat R-group scheme. If there exist exact sequences of flat R-group schemes

$$0 \longrightarrow \mathcal{G}^{(l_i)} \longrightarrow \mathcal{E}_i \longrightarrow \mathcal{E}_{i-1} \longrightarrow 0$$

for $1 \leqslant i \leqslant n$, with $\mathcal{E}_0 = 0$ and $\mathcal{E}_n = \mathcal{E}$, we call the sequence of flat R-group schemes

$$\mathcal{E}_1 = \mathcal{G}^{(l_1)}, \mathcal{E}_2, \dots, \mathcal{E}_n = \mathcal{E}$$

or, sometimes, simply $\mathcal{E}$, a filtered R-group scheme of type $(l_1, \dots, l_n)$.

6.3.2. — *Remark.* One can define a group scheme $\mathcal{G}^{(\lambda)}$ for each $\lambda \in R$, in such a way that $\mathcal{G}^{(l)} := \mathcal{G}^{(\pi^l)}$ is just the group scheme defined in 6.3.1. In this article, we care only about the isomorphism class of $\mathcal{G}^{(\lambda)}$ which depends only on λ up to units, so we prefer to adopt the more compact notation.

6.3.3. — Theorem. *Let $\mathcal{E} = (\mathcal{E}_1, \dots, \mathcal{E}_n)$ be a filtered group scheme of type $(l_1, \dots, l_n)$, with $l_i > 0$ for each i. Then there are compatible open immersions of $\mathcal{E}_i \to \mathbb{A}^i$ and elements*

$$D_i \in H^0(\mathbb{A}^i_R, \mathcal{O}_{\mathbb{A}^i_R}) = R[T_1, \dots, T_i]$$

such that, for each $1 \leqslant i \leqslant n$, the Hopf algebra of $\mathcal{E}_i$ is given by

$$R[\mathcal{E}_i] = R\Big[T_1, \dots, T_i, \frac{1}{1+\pi^{l_1}T_1}, \frac{1}{D_1(T_1)+\pi^{l_2}T_2}, \dots, \frac{1}{D_{i-1}(T_1, \dots, T_{i-1})+\pi^{l_i}T_i}\Big]$$

The group law of $\mathcal{E}_i$ is the one which makes the morphism

$$\alpha_{\mathcal{E}_i} : \mathcal{E}_i \longrightarrow (\mathbb{G}_{m,R})^i$$
$$(T_1, \dots, T_i) \longmapsto (1+\pi^{l_1}T_1, D_1(T_1)+\pi^{l_2}T_2, \dots, D_{i-1}(T_1, \dots, T_{i-1})+\pi^{l_i}T_i)$$

a group-scheme homomorphism and the reduction modulo $\pi^{l_{i+1}}$ of the function $D_i : \mathbb{A}^i_R \to \mathbb{A}^1_R$ factors into a group scheme homomorphism $D_{i|\mathcal{E}_i} : \mathcal{E}_{i,R/\pi^{l_{i+1}}R} \to \mathbb{G}_{m,R/\pi^{l_{i+1}}R} \subseteq \mathbb{A}^1_{R/\pi^{l_{i+1}}R}$.

Moreover if l_{n+1} is a positive integer and $D_n : \mathbb{A}^n_R \to \mathbb{A}^1_R$ is a function whose reduction modulo $\pi^{l_{n+1}}$ factors into a group scheme homomorphism

$$D_{n|\mathcal{E}_n} : \mathcal{E}_{n,R/\pi^{l_{n+1}}R} \to \mathbb{G}_{m,R/\pi^{l_{n+1}}R} \subseteq \mathbb{A}^1_{R/\pi^{l_{n+1}}R}$$

then

$$R[\mathcal{E}_{n+1}] := R[\mathcal{E}_n]\left[T_{n+1}, 1/(D_n(T_1,\dots,T_n) + \pi^{l_{n+1}}T_{n+1})\right]$$

is the Hopf algebra of a filtered group scheme $\mathcal{E}_{n+1}$ of type $(l_1,\dots,l_{n+1})$, where the group scheme structure is the only one which turns into a group scheme homomorphism the morphism $\alpha_{\mathcal{E}_{n+1}} : \mathcal{E}_{n+1} \to (\mathbb{G}_{m,R})^{n+1}$ which extends $\alpha_{\mathcal{E}_n}$ and sends T_{n+1} to $D_n(T_1,\dots,T_n) + \pi^{l_{n+1}}T_{n+1}$.

Finally, a polynomial $D'_n \in R[T_1,\dots,T_n]$ with the same reduction modulo $\pi^{l_{n+1}}$ as D_n gives the same filtered group scheme up to isomorphism.

Proof. — See [25], Theorem 3.2 and Theorem 3.3. □

In fact one can describe very explicitly the polynomials which appear in the above theorem. In the next statement and in the rest of the article, we sometimes write $f : X \circlearrowleft$ for a map $f : X \to X$ from some set to itself.

6.3.4. — Theorem. *Let $\mathcal{E}$ be a filtered group scheme of type $(l_1,\dots,l_n)$ with $l_i > 0$ for each i. Then there exist elements $\boldsymbol{a}_i^j \in W^f(R)$ with $1 \leqslant i < j \leqslant n$, whose reductions modulo π^{l_j} are in $\widehat{W}(R/\pi^{l_j}R)$, such that*

- *one can take, for any $j = 1,\dots,n-1$, $D_j(T_1,\dots,T_j)$ as the truncation of*

$$E_p((\boldsymbol{a}_i^{j+1})_{1\leqslant i\leqslant j}, (\pi^{l_k})_{1\leqslant k\leqslant j}; T_1,\dots,T_j)$$

in degree r, where $E_p\big((\boldsymbol{a}_i^{j+1})_{1\leqslant i\leqslant j}, (\pi^{l_k})_{1\leqslant k\leqslant j}; T_1,\dots,T_j\big)$ is the series defined by induction

$$\prod_{i=1}^{j} E_p\left(\boldsymbol{a}_i^{j+1}, \pi^{l_i}; \frac{T_i}{E_p((\boldsymbol{a}_s^i)_{1\leqslant s\leqslant i-1}, (\pi^{l_k})_{1\leqslant k\leqslant i-1}; T_1,\dots,T_{i-1})}\right)$$

and r is the degree of the reduction of this series modulo $\pi^{l_{j+1}}$, which is a polynomial;

- *the reduction modulo π^{l_j} of each $(\boldsymbol{a}_i^j)_{1\leqslant i\leqslant j-1}$ is in the kernel of the operator*

$$U^{j-1} : \widehat{W}(R/\pi^{l_j}R)^{j-1} \circlearrowleft$$

defined as follows: U^1 *is defined as* $F^{(l_1)} := F - \left[\pi^{(p-1)l_1}\right]$ *and we define*

$$U^n = \begin{pmatrix} F^{(l_1)} & -T_{\boldsymbol{b}_1^2} & -T_{\boldsymbol{b}_1^3} & \dots & -T_{\boldsymbol{b}_1^n} \\ 0 & F^{(l_2)} & -T_{\boldsymbol{b}_2^3} & \dots & -T_{\boldsymbol{b}_2^n} \\ \vdots & 0 & \ddots & \ddots & \vdots \\ 0 & 0 & \ddots & \ddots & -T_{\boldsymbol{b}_{n-1}^n} \\ 0 & 0 & \dots & 0 & F^{(l_n)} \end{pmatrix}$$

where $\mathfrak{U}(U^n) = U^{n-1}$ *and* $\mathfrak{L}(U^n)$ *are defined by induction and*

$$\boldsymbol{b}_1^n := \frac{1}{\pi^{l_n}} \left(F^{(l_1)} \boldsymbol{a}_1^n - \sum_{t=2}^{n-1} T_{\boldsymbol{b}_1^t} \boldsymbol{a}_t^n \right) = \frac{U^{n-1}(\boldsymbol{a}_i^n)_{1 \leqslant i \leqslant n-1}}{\pi^{l_n}};$$

- *for any* $l \in \mathbb{N}$, *we have an isomorphism*

$$\ker \left(U^n : \widehat{W}(R/\pi^l R)^n \circlearrowleft \right) \longrightarrow \mathrm{Hom}_{R/\pi^l R\text{-Gr}}(i^*\mathcal{E}, \mathbb{G}_{m,R/\pi^l R}),$$

given by

$$\boldsymbol{c}^n \longmapsto E_p(\boldsymbol{c}^n, (\pi^{l_j})_{1 \leqslant j \leqslant n}, T_1, \dots, T_n),$$

where i *is the closed immersion* $\mathrm{Spec}(R/\pi^l R) \to \mathrm{Spec}(R)$.

Proof. — See [25], Theorem 5.1 and Theorem 5.2. □

6.4. Sekiguchi-Suwa Theory from a matricial point of view

Our purpose here is to introduce "simple" matrices parametrizing filtered group schemes (6.4.1) and to translate in matricial terms the main operations on group schemes: quotients and subgroups (6.4.5) and model maps (6.4.7). In the following, we always suppose that the parameters l_i of the filtered group schemes we are considering are positive ($l_i > 0$).

Let $\mathscr{H}_n(W(K))$ be the loop constructed in 6.1.7. For matrices $A, B \in \mathscr{H}_n(W(K))$ we will make use of the notations A/B and $A\backslash B$ as defined in 3.2.1. In a similar way as in 3.2.6 we will say that a matrix A in $\mathscr{H}_n(W(K))$ is *positive*, and we will write $A \geqslant 0$, if it belongs to $\mathscr{H}_n(W(R))$.

6.4.1. — The set $\mathscr{M}_n$. To start with, we need a technical remark allowing to reformulate the congruences in Theorem 6.3.4. We consider an

upper triangular matrix of the following form:

$$A = \begin{pmatrix} [\pi^{l_1}] & \boldsymbol{a}_1^2 & \boldsymbol{a}_1^3 & \dots & \boldsymbol{a}_1^n \\ & [\pi^{l_2}] & \boldsymbol{a}_2^3 & & \vdots \\ & & \ddots & \ddots & \vdots \\ & & & [\pi^{l_{n-1}}] & \boldsymbol{a}_{n-1}^n \\ 0 & & & & [\pi^{l_n}] \end{pmatrix} \in M_n(W^f(R)) \text{ , all } l_i > 0.$$

6.4.2. — Lemma. *For each matrix A as above, let $F(A)$ be the matrix obtained by applying Frobenius to all entries. Then the following conditions are equivalent:*

(1) *for each $j \in \{1, \dots, n\}$, the reduction of $(\boldsymbol{a}_i^j)_{1 \leqslant i \leqslant j-1}$ belongs to $\widehat{W}(R/\pi^{l_j}R)^{j-1}$ and*

$$U^{j-1}(\boldsymbol{a}_i^j)_{1 \leqslant i \leqslant j-1} \equiv 0 \mod \pi^{l_j}$$

where U^{j-1} is defined by induction in Theorem 6.3.4.
(2) *$F(A)/A \geqslant 0$.*

Note that the operator U^{j-1} in (1) depends only on the vectors $\boldsymbol{a}^k \in W(R)^k$ with $1 \leqslant k \leqslant j-1$.

Proof. — In fact, we have

$$F(A)/A = \begin{pmatrix} [\pi^{(p-1)l_1}] & \boldsymbol{b}_1^2 & \boldsymbol{b}_1^3 & \dots & \boldsymbol{b}_1^n \\ 0 & [\pi^{(p-1)l_2}] & \boldsymbol{b}_2^3 & \dots & \boldsymbol{b}_2^n \\ \vdots & \ddots & \ddots & & \vdots \\ \vdots & & \ddots & [\pi^{(p-1)l_{n-1}}] & \boldsymbol{b}_{n-1}^n \\ 0 & \dots & \dots & 0 & [\pi^{(p-1)l_n}] \end{pmatrix} \in \mathscr{H}_n(W(K))$$

where the $\boldsymbol{b}_i^j$ are defined as in 6.3.4. By the definition of $\boldsymbol{b}_i^j$, this matrix is in $\mathscr{H}_n(W(R))$ if and only if the congruences in (1) are satisfied. It remains to prove that if $F(A)/A \geqslant 0$ then for each j the reduction of $(\boldsymbol{a}_i^j)_{1 \leqslant i \leqslant j-1}$ belongs to $\widehat{W}(R/\pi^{l_j}R)^{j-1}$. We prove this by induction on n. We observe that since the entries of A are in $W^f(A)$, then this condition simply means that the entries of A are congruent to 0 modulo π, i.e. $A/[\pi]\,\mathrm{Id}$ is positive. For $n = 1$ there is nothing to prove. Let us suppose the statement true for

n and prove it for $n+1$. Then one has

$$F(A)/A = \begin{pmatrix} \mathcal{U}F(A)/\mathcal{U}A & \frac{F((\boldsymbol{a}_i^{n+1})_{1\leqslant i\leqslant n}) - T_{(\mathcal{U}F(A)/\mathcal{U}A)}(\boldsymbol{a}_i^{n+1})_{1\leqslant i\leqslant n}}{\pi^{l_{n+1}}} \\ 0 \quad \dots \quad 0 & [\pi^{(p-1)l_{n+1}}] \end{pmatrix} \tag{6.4}$$

and

$$F(A)/A = \begin{pmatrix} [\pi^{(p-1)l_{n+1}}] & \frac{F((\boldsymbol{a}_1^j)_{2\leqslant j\leqslant n+1}) - T_{(\mathcal{L}F(A)/\mathcal{L}A)}(\boldsymbol{a}_1^j)_{2\leqslant j\leqslant n+1}}{\pi^{l_j}} \\ 0 & \\ \vdots & \mathcal{L}F(A)/\mathcal{L}A \\ 0 & \end{pmatrix}$$

where we use the notation $T_M(N)$ from Definition 6.1.6. By the inductive hypothesis, the matrices $\mathcal{U}A/[\pi]\,\mathrm{Id}$ and $\mathcal{L}A/[\pi]\,\mathrm{Id}$ are positive. Therefore it remains to prove that $\boldsymbol{a}_1^{n+1} \equiv 0 \mod \pi$. Since $F(A)/A$ is positive and $l_{n+1} > 0$ then from (6.4) we derive

$$F(\boldsymbol{a}_1^{n+1}) \equiv T_{(\mathcal{U}F(A)/\mathcal{U}A)}(\boldsymbol{a}_i^{n+1})_{1\leqslant i\leqslant n} \mod \pi.$$

Since by induction $\boldsymbol{a}_i^{n+1} \equiv 0 \mod \pi^{l_{n+1}}$ for $i = 2, \dots, n$ and $\mathcal{U}^n F(A)/\mathcal{U}^n A = ([\pi^{(p-1)l_1}])$ with $l_1 > 0$, then we have

$$F(\boldsymbol{a}_1^{n+1}) \equiv [\pi^{(p-1)l_1}]\boldsymbol{a}_1^{n+1} \equiv 0 \mod \pi.$$

This implies that $\boldsymbol{a}_1^{n+1} \equiv 0 \mod \pi$. □

Theorems 6.3.3 and 6.3.4 imply that to any matrix satisfying the equivalent conditions of Lemma 6.4.2 one can attach a unique filtered group scheme $\mathcal{E}(A)$. Conversely, for any filtered group scheme $\mathcal{E}$ one can find a matrix A satisfying these conditions such that $\mathcal{E} = \mathcal{E}(A)$. This leads us to introduce the relevant set of matrices. Note that if $\mathcal{E}$ is given, then a matrix A such that $\mathcal{E} = \mathcal{E}(A)$ is not unique. So we have to identify the equivalence relation saying that two matrices define the same filtered group; this will be done in 6.4.7.

6.4.3. — Definition. Let $n \in \mathbb{N}$ and $\boldsymbol{l} = (l_1, \dots, l_n) \in (\mathbb{N}_{>0})^n$. We define

$$\mathscr{M}_n^{\boldsymbol{l}} := \big\{A = (\boldsymbol{a}_i^j) \in M_n(W^f(R)), \text{upper triangular}, \boldsymbol{a}_i^i = [\pi^{l_i}] \text{ for } 1 \leqslant i \leqslant n \text{ and } F(A)/A \geqslant 0\big\}$$

and $\mathscr{M}_n := \bigcup \mathscr{M}_n^{\boldsymbol{l}}$, the union being over all $\boldsymbol{l} \in (\mathbb{N}_{>0})^n$.

6.4.4. — *Remark.* If $A \in \mathscr{M}_n$, then it is not necessarily the case that $F(A) \in \mathscr{M}_n$. There are counterexamples already for $n = 2$, with $l_2 \gg l_1$.

By Theorems 6.3.3, 6.3.4 and Lemma 6.4.2, one can associate with any $A \in \mathscr{M}_n^{\boldsymbol{l}}$ a filtered group scheme $\mathcal{E}(A)$ of type $(l_1, \dots, l_n)$. It is constructed by successive extensions defined by deformed exponentials $D_j(T_1, \dots, T_j)$ equal to the truncation of $E_p((\boldsymbol{a}_i^{j+1})_{1 \leqslant i \leqslant j}, (\pi^{l_k})_{1 \leqslant k \leqslant j}; T_1, \dots, T_j)$ in degree r, where $r = r_i$ is the degree of the reduction modulo $\pi^{l_{i+1}}$ of this series. We call D_j the *truncated exponential* associated with $(\boldsymbol{a}_i^{j+1})_{1 \leqslant i \leqslant j}$. (Note that similar truncated exponentials appear in the work [13].) With the vocabulary introduced in the article [22] (see especially 3.2 and 4.3 there), the vectors $\boldsymbol{a}^j$ are *frames* for the filtered group $\mathcal{E}(A)$, and the matrix A may be called a *matrix of frames*.

6.4.5. — Operators $\mathcal{U}$ and $\mathcal{L}$ versus quotients and subgroups. It is clear that for each $A \in \mathscr{M}_n$ and $i \in \{1, \dots, n\}$ we have $\mathcal{U}^{n-i}A \in \mathscr{M}_i$ and $\mathcal{L}^i A \in \mathscr{M}_{n-i}$. Here is the precise meaning of the operators $\mathcal{U}$ and $\mathcal{L}$ for filtered group schemes.

6.4.6. — Proposition. *Let $\mathcal{E} = (\mathcal{E}_1, \dots, \mathcal{E}_n)$ be a filtered group scheme of type $\boldsymbol{l} = (l_1, \dots, l_n)$, and $A \in \mathscr{M}_n^{\boldsymbol{l}}$. For $1 \leqslant i \leqslant n-1$ consider the exact sequence $0 \to \mathcal{S}_{n-i} \to \mathcal{E}_n \to \mathcal{Q}_i \to 0$ where $\mathcal{Q}_i := \mathcal{E}_i$ (quotient of dimension i) and $\mathcal{S}_{n-i} := \ker(\mathcal{E}_n \to \mathcal{E}_i)$ (subgroup of codimension i). Then:*

(1) *$\mathcal{Q}_i$ is a filtered group scheme of type $(l_1, \dots, l_i)$. If $\mathcal{E} = \mathcal{E}(A)$ then $\mathcal{Q}_i = \mathcal{E}(\mathcal{U}^{n-i}A)$.*

(2) *$\mathcal{S}_{n-i}$ is a filtered group scheme of type $(l_{i+1}, \dots, l_n)$. If $\mathcal{E} = \mathcal{E}(A)$ then $\mathcal{S}_{n-i} = \mathcal{E}(\mathcal{L}^i A)$.*

Proof. — Assertion (1) comes from the inductive construction of $\mathcal{E}_n$. For the proof of (2), we set $\mathcal{K}_d = \ker(\mathcal{E}_d \to \mathcal{E}_i)$ for each $d \geqslant i+1$. First, we show by induction on d that $\mathcal{K}_d$ is a filtered group scheme of type $(l_{i+1}, \dots, l_d)$. The initialization at $d = i+1$ is clear and the inductive step is verified since the morphism $\nu_d : \mathcal{E}_{d+1} \to \mathcal{E}_d$ with kernel $\mathcal{G}^{(l_{d+1})}$ induces an exact sequence:

$$0 \longrightarrow \mathcal{G}^{(l_{d+1})} \longrightarrow \mathcal{K}_{d+1} \xrightarrow{\nu_d} \mathcal{K}_d \longrightarrow 0.$$

In order to prove that $\mathcal{S}_{n-i} = \mathcal{E}(\mathcal{L}^i A)$ if $\mathcal{E} = \mathcal{E}(A)$, we examine more closely the way these extensions are built. The extension $\mathcal{E}_{d+1}$ is constructed from $\mathcal{E}_d$ using a morphism $D_d : \mathcal{E}_d \to i_* \mathbb{G}_m$ where $i : \mathrm{Spec}(R/\pi^{l_{d+1}}R) \hookrightarrow \mathrm{Spec}(R)$ is the closed immersion. This morphism is the deformed exponential defined by the coefficients $\boldsymbol{a}_i^{d+1}$ in the $(d+1)$-th column of A. The extension $\mathcal{K}_{d+1}$ is constructed from $\mathcal{K}_d$ using the morphism $D_d|_{\mathcal{K}_d} : \mathcal{K}_d \to i_* \mathbb{G}_m$. In the coordinates $T_1, \dots, T_d$ of 6.3.4, the closed subgroup scheme $\mathcal{K}_d \subset \mathcal{E}_d$

is defined by the vanishing of the coordinates $T_1, \dots, T_i$. It follows that $D_d|_{\mathcal{K}_d}$ is obtained from the deformed Artin-Hasse exponential D_d by setting $\boldsymbol{a}_1^{d+1} = \boldsymbol{a}_2^{d+1} = \cdots = \boldsymbol{a}_i^{d+1} = 0$. Hence the matrix of coefficients that defines $\mathcal{K}_d$ is the boxed middle matrix:

$$A = \begin{pmatrix} \ddots & & * & & * \\ & [\pi^{l_i}] & & & \\ & & \boxed{\begin{matrix} [\pi^{l_{i+1}}] & & \\ & \ddots & \\ & & [\pi^{l_d}] \end{matrix}} & & * \\ 0 & & & & \\ & & & [\pi^{l_{d+1}}] & \\ 0 & & 0 & & \ddots \end{pmatrix}$$

In symbols, $\mathcal{K}_d = \mathcal{E}(\mathcal{U}^{n-d}\mathcal{L}^i A)$. For $d = n$, we get $\mathcal{S}_{n-i} = \mathcal{K}_n = \mathcal{E}(\mathcal{L}^i A)$. □

6.4.7. — Positive matrices versus model maps. We use the word *unitriangular* as a synonym for *upper triangular unipotent*.

6.4.8. — Proposition. *Let $\mathcal{E} = \mathcal{E}(A)$ and $\mathcal{E}' = \mathcal{E}(A')$ be two filtered group schemes, with $A, A' \in \mathscr{M}_n$.*

- *There exists a (unique) model map $\mathcal{E} \to \mathcal{E}'$ which commutes with $\alpha_{\mathcal{E}}$ and $\alpha_{\mathcal{E}'}$ if and only if $A/A' \geqslant 0$. In particular, the relation $\succ$ in $\mathscr{M}_n$ given by $A \succ A'$ if and only if $A/A' \geqslant 0$, is transitive. Moreover $\mathcal{E}$ and $\mathcal{E}'$ are isomorphic if and only if A/A' is positive and unitriangular.*
- *If $\varphi : \mathcal{E} \to \mathcal{E}'$ is such a model map, the morphism of groups*

$$\varphi^* : \mathrm{Hom}_{R/\pi^l R\text{-Gr}}(i^*\mathcal{E}', \mathbb{G}_{m,R/\pi^l R}) \longrightarrow \mathrm{Hom}_{R/\pi^l R\text{-Gr}}(i^*\mathcal{E}, \mathbb{G}_{m,R/\pi^l R})$$

is given, using the isomorphism of Theorem 6.3.4, by the operator $T_{A/A'}$.

Proof. — We prove by induction on the dimension n the following more precise statements:

- There exists a (unique) model map $\mathcal{E} \to \mathcal{E}'$ which commutes with $\alpha_{\mathcal{E}}$ and $\alpha_{\mathcal{E}'}$ if and only if $A/A' \geqslant 0$.
- Let $D_1, \dots, D_{n-1}$ (resp. $D'_1, \dots, D'_{n-1}$) be the truncated polynomials determined by A (resp. A'). If a model map $\varphi^n : \mathcal{E} \to \mathcal{E}'$ exists

then it is given by $\varphi^n = (\varphi_i)_{1\leqslant i\leqslant n}$, where $\varphi_1(T_1) = \pi^{l_1'-l_1}$ and

$$\varphi_i(T_1,\dots,T_i) = \frac{D_{i-1}(T_1,\dots,T_{i-1}) - D'_{i-1}(\varphi_1(T_1),\dots,\varphi_{i-1}(T_1,\dots,T_{i-1}))}{\pi^{l_i'}} + \pi^{l_i-l_i'}T_i$$

for all $i > 1$.

- Write $A = (\boldsymbol{a}_i^j)$ and $A' = (\boldsymbol{a}'^j_i)$ in $\mathscr{M}_n$ with $\boldsymbol{a}_i^i = [\pi^{l_i}]$ and $\boldsymbol{a}_i'^i = [\pi^{l_i'}]$ for $1 \leqslant i \leqslant n$. Let $(\boldsymbol{w}_i^n)_{1\leqslant i\leqslant n} \in W(R)^n$ be a vector whose reduction modulo π^l belongs to

$$\ker(U^n : \widehat{W}(R/\pi^l R)^n \circlearrowleft).$$

Let $H_1 = 1 + \pi^{l_1}T_1$ and

$$H_n = \frac{E_p\big((\boldsymbol{a}_i^n)_{1\leqslant i\leqslant n-1}, (\pi^{l_i})_{1\leqslant i\leqslant n-1}, \mathbb{T}\big)\big(1 + \pi^{l_n}\frac{T_n}{E_p((\boldsymbol{a}_i^n)_{1\leqslant i\leqslant n-1}, (\pi^{l_i})_{1\leqslant i\leqslant n-1}, \mathbb{T})}\big)}{E_p((\boldsymbol{a}'^n_i)_{1\leqslant i\leqslant n-1}, (\pi^{l_1})_{1\leqslant i\leqslant n}, \varphi^n(\mathbb{T}))}$$

for $n > 1$. Then

$$E_p(\boldsymbol{w}^n, (\pi^{l_1},\dots,\pi^{l_n}), \varphi^n(\mathbb{T})) = E_p(T_{A/A'}(\boldsymbol{w}^n), (\pi^{l_1},\dots,\pi^{l_n}), \mathbb{T}) \times \prod_{2\leqslant r\leqslant n} G_p(U_r^n(\boldsymbol{w}^n), \pi^{l_r}; H_{r-1}) \tag{6.5}$$

where U_r^n is the r-th row of U^n, and

$$H_n = \frac{E_p\left((\boldsymbol{a}_i^n)_{1\leqslant i\leqslant n-1} - T_{\mathcal{U}A/\mathcal{U}A'}(\boldsymbol{a}'^n_i)_{1\leqslant i\leqslant n-1}, (\pi^{l_1},\dots,\pi^{l_{n-1}}); \mathbb{T}\right)}{\prod_{2\leqslant r\leqslant n} G_p(U_r^n(\boldsymbol{w}^n), \pi^{l_r'}; H_{r-1})} \times E_p\left([\pi^{l_n}], \pi^{l_n}; \frac{\mathbb{T}}{E_p((\boldsymbol{a}'^n_i)_{1\leqslant i\leqslant n-1}, (\pi^{l_i})_{1\leqslant i\leqslant n-1}, \varphi^n(\mathbb{T}))}\right). \tag{6.6}$$

Note that (6.5) implies that φ^* is given by the operator $T_{A/A'}$, as asserted in the statement of the proposition.

If $n = 1$ we have $\mathcal{E} = \mathcal{G}^{(l_1)}$ and $\mathcal{E}' = \mathcal{G}^{(l_1')}$ for some positive integers l_1, l_1'. In this case $A/A' \geqslant 0$ simply means $l_1 \geqslant l_1'$ and the above statement is known: see [24], Proposition 1.4 for the first part and second part and [26], Remark 3.8 for the third part.

We now suppose that the three statements hold true for some $n \geqslant 1$ and we prove them for $n+1$. We have

$$A/A' = \begin{pmatrix} & \mathcal{U}A/\mathcal{U}A' & & \frac{(\boldsymbol{a}_i^{n+1})_{1\leqslant i\leqslant n} - T_{\mathcal{U}A/\mathcal{U}A'}((\boldsymbol{a}'^{n+1}_i)_{1\leqslant i\leqslant n})}{\pi^{l'_{n+1}}} \\ 0 & \dots & 0 & [\pi^{l_{n+1}-l'_{n+1}}] \end{pmatrix}.$$

Let $D_1, \dots, D_{n+1}$ (resp. $D'_1, \dots, D'_n$) be the truncated exponentials that define $\mathcal{E}$ (resp. $\mathcal{E}'$). The model map φ_{n+1} which we are looking for should commute with $\alpha_{\mathcal{E}}$ and $\alpha_{\mathcal{E}'}$, so if it exists it is unique. So one sees immediately that it exists if and only if there exists a model map $\mathcal{E}_n \to \mathcal{E}'_n$ and, if we write $\varphi^{n+1} = (\varphi_i)_{1 \leqslant i \leqslant n+1}$, the polynomial

$$\begin{aligned}&\varphi_{n+1}(T_1, \dots, T_{n+1})\\ &\quad = \frac{D_n(T_1, \dots, T_n) - D'_n(\varphi_1(T_1), \dots, \varphi_n(T_1, \dots, T_n))}{\pi^{l'_{n+1}}} + \pi^{l_{n+1} - l'_{n+1}} T_{n+1}\end{aligned}$$

belongs to $R[T_1, \dots, T_n]$. Therefore, by the inductive hypothesis, there exists a model map between $\mathcal{E}$ and $\mathcal{E}'$ if and only if $\mathcal{U}A/\mathcal{U}A'$ is positive, $l_{n+1} \geqslant l'_{n+1}$ and

$$D_n(T_1, \dots, T_n) \equiv D'_n(\varphi_1(T_1), \dots, \varphi_n(T_1, \dots, T_n)) \mod \pi^{l'_{n+1}}. \tag{6.7}$$

By induction we have that

$$\begin{aligned}\varphi^* : \operatorname{Hom}_{R/\pi^l R\text{-}\,\mathrm{Gr}}(i^*\mathcal{E}(\mathcal{U}(A')), \mathbb{G}_{m,R/\pi^l R})&\\ \longrightarrow \operatorname{Hom}_{R/\pi^l R\text{-}\,\mathrm{Gr}}(i^*\mathcal{E}(\mathcal{U}(A)), \mathbb{G}_{m,R/\pi^l R})&\end{aligned}$$

is given by the operator $T_{\mathcal{U}A/\mathcal{U}A'}$. This means that the equation (6.7) is equivalent to

$$(\boldsymbol{a}_i^{n+1})_{1 \leqslant i \leqslant n} \equiv T_{\mathcal{U}A/\mathcal{U}A'}\big((\boldsymbol{a}_i^{n+1})_{1 \leqslant i \leqslant n}\big) \mod \pi^{l'_{n+1}}.$$

Thus we have proved the first and second part of the statement for $n+1$.

It remains to prove the formulas (6.5) and (6.6) for $n+1$. But the second one clearly follows from the first one, so we just have to prove (6.5). Let us suppose that (6.5) is true for n and prove it for $n+1$. We clearly have

$$\begin{aligned}&E_p((\boldsymbol{w}_r^{n+1})_{1 \leqslant r \leqslant n+1}, (\pi^{l_1}, \dots, \pi^{l_{n+1}}), \varphi^{n+1}(\mathbb{T})) =\\ &E_p\left((\boldsymbol{w}_r^{n+1})_{1 \leqslant r \leqslant n}, (\pi^{l_1}, \dots, \pi^{l_n}), \varphi^n(\mathbb{T})\right) E_p\left(\boldsymbol{w}_{n+1}^{n+1}, \pi^{l_{n+1}}, \frac{\varphi_{n+1}(\mathbb{T})}{E_p((\boldsymbol{a}'^{n+1}_i)_{1 \leqslant i \leqslant n}, (\pi^{l_i})_{1 \leqslant i \leqslant n}, \varphi^n(\mathbb{T}))}\right).\end{aligned} \tag{6.8}$$

Moreover, by induction

$$\begin{aligned}&E_p\big((\boldsymbol{w}_i^{n+1})_{1 \leqslant i \leqslant n}, (\pi^{l_1}, \dots, \pi^{l_n}), \varphi^n(\mathbb{T})\big)\\ &\qquad = E_p\big(T_{\mathcal{U}A/\mathcal{U}A'}(\boldsymbol{w}_i^{n+1})_{1 \leqslant i \leqslant n}, (\pi^{l_1}, \dots, \pi^{l_n}), \mathbb{T}\big)\\ &\qquad\qquad \times \prod_{2 \leqslant r \leqslant n} G_p\big(U_r^n((\boldsymbol{w}_i^{n+1})_{1 \leqslant i \leqslant n}), \pi^{l'_r}; H_{r-1}\big).\end{aligned} \tag{6.9}$$

Now

$$\begin{aligned}
&E_p\Big(\boldsymbol{w}_{n+1}^{n+1}, \pi^{l'_{n+1}}, \frac{\varphi_{n+1}(\mathbb{T})}{E_p((\boldsymbol{a'}_i^{n+1})_{1\leqslant i\leqslant n}, (\pi^{l_i})_{1\leqslant i\leqslant n}, \varphi^n(\mathbb{T}))}\Big)\\
&\quad= E_p\Big(\boldsymbol{w}_{n+1}^{n+1}, \pi^{l_{n+1}}, \frac{H_n-1}{\pi^{l'_{n+1}}}\Big)\\
&\quad\overset{(6.2)}{=} \widetilde{E}_p\Big(\boldsymbol{w}_{n+1}^{n+1}, \pi^{l_{n+1}}, H_n\Big)\, G_p\Big(F^{l_{n+1}}\boldsymbol{w}_{n+1}^{n+1}, \pi^{l_{n+1}}, H_n\Big)\\
&\quad= E_p\Big(T_{\frac{(a_i^{n+1})_{1\leqslant i\leqslant n} - T_{\mathcal{U}A/\mathcal{U}A'}(a'^{n+1}_i)_{1\leqslant i\leqslant n}}{\pi^{l_{n+1}}}}\boldsymbol{w}_{n+1}^{n+1}, (\pi^{l_1},\dots,\pi^{l_n}); \mathbb{T}\Big)\\
&\qquad\times E_p\Big(T_{[\pi^{l_{n+1}-l'_{n+1}}]}\boldsymbol{w}_{n+1}^{n+1}, \pi^{l_{n+1}}; \frac{T_{n+1}}{E_p((\boldsymbol{a}_i^{n+1})_{1\leqslant i\leqslant n-1}, (\pi^{l_i})_{1\leqslant i\leqslant n}, \varphi^n(\mathbb{T}))}\Big)\\
&\qquad\times \prod_{r=2}^{n} G_p\Big(-T_{\frac{U_r^n(a_i^n)_{1\leqslant i\leqslant n-1}}{\pi^{l_{n+1}}}}\boldsymbol{w}_{n+1}^{n+1}, \pi^{l_{n+1}}; H_{r-1}\Big)\, G_p\Big(F^{l_{n+1}}\boldsymbol{w}_{n+1}^{n+1}, \pi^{l_{n+1}}, H_n\Big)
\end{aligned}$$

where in the last equality we have used Equation (6.6), Lemma 6.2.6, Lemma 6.2.9, Equation (6.3) and the fact that $\widetilde{E}_p(\mathbb{W}, \Lambda, H)$ gives a bilinear group scheme homomorphism $W_{\mathbb{A}^1} \times \boldsymbol{\Lambda}_{\mathbb{A}^1} \to \boldsymbol{\Lambda}_{\mathbb{A}^1}$. Now using (6.8) and (6.9) one gets the result.

Finally we remark that if $A/A' \geqslant 0$ and $A'/A \geqslant 0$ then necessarily A/A' and A'/A are unitriangular, as it is very easy to verify. □

The order relation $\succ$ from the previous proposition induces an equivalence relation on $\mathscr{M}_n$:

6.4.9. — Definition. For any $A, A' \in \mathscr{M}_n$ we write $A \sim A'$ if and only if A/A' is positive and unitriangular.

This relation characterizes when two matrices in $\mathscr{M}_n$ define the same filtered group scheme:

6.4.10. — Corollary. *The map $A \mapsto \mathcal{E}(A)$ induces an increasing bijection between the set $\mathscr{M}_n/\sim$ ordered by the relation $\succ$ and the set of isomorphism classes of filtered group schemes of dimension n ordered by the existence of a model map.*

7. Kummer group schemes

In this section, following Sekiguchi and Suwa's approach, we specify Theorem 6.3.4 for filtered R-group schemes containing a model of μ_{p^n}. The main result (7.1.1 below) is a generalization of Theorem 9.4 of [25], which covers the particular case where the finite flat subgroup is the constant group scheme $(\mathbb{Z}/p^n\mathbb{Z})_R$. As it turns out, the main difficulty is to find the

statement of the generalized theorem, for then the proof of [25] carries over smoothly.

We point out an important fact: the computation of successive extensions by groups $\mathcal{G}^{(l)}$, which is the essence of the existence of filtered group schemes, proceeds differently when $l > 0$ and when $l = 0$. The former case is treated by Theorem 7.1.1, and we indicate in Remark 7.1.4 how to handle the easier case $l = 0$.

7.1. Finiteness of closures of finite flat subgroups

Let $\mathcal{E} = \mathcal{E}_n$ be a filtered group scheme of type $(l_1, \dots, l_n)$. Let $\alpha : \mathcal{E} \to (\mathbb{G}_m)^n$ be a morphism of filtered R-group schemes which is an isomorphism on the generic fibre. Let $\Theta^n : (\mathbb{G}_m)^n \to (\mathbb{G}_m)^n$ be the morphism defined by

$$\Theta^n(T_1, \dots, T_n) = (T_1^p, T_2^p T_1^{-1}, \dots, T_n^p T_{n-1}^{-1}).$$

The kernel of Θ^n is a subgroup isomorphic to $\mu_{p^n,R}$ which we call the *Kummer* μ_{p^n} *of* $\mathbb{G}_m^n$. Via the map α, we can see the Kummer $\mu_{p^n,K}$ as a closed subscheme of $\mathcal{E}_K$. We define the *pre-Kummer subgroup* G_n as the scheme-theoretic closure of $\mu_{p^n,K}$ in $\mathcal{E}$, and we call it the *Kummer subgroup* when it is finite over R. In spite of the notation, G_n depends on the choice of α (see Theorem 6.3.3). If G_n is finite, then the quotient $\mathcal{F}_n$ is a filtered group scheme and the quotient map $\Psi^n : \mathcal{E}_n \to \mathcal{F}_n$ is an isogeny. In this case, for each $\mu \in R$ we have a pullback map

$$(\Psi^n)^* : \mathrm{Hom}_{R/\mu R\text{- Gr}}(\mathcal{F}_n, \mathbb{G}_m) \longrightarrow \mathrm{Hom}_{R/\mu R\text{- Gr}}(\mathcal{E}_n, \mathbb{G}_m).$$

We know by Theorem 6.3.4 that using the deformed Artin-Hasse exponentials, the groups on both sides may be identified with suitable kernels of additive operators U^n on Witt vector groups. Once this is done, Sekiguchi and Suwa express $(\Psi^n)^*$ by a matrix called Υ^n. Let us give some details in the case $n = 1$ that initiates the induction. Then we have $\mathcal{E}_1 \simeq \mathcal{G}^{(l_1)}$ and the closure of $\mu_{p,K}$ is finite flat if and only if $v(p) \geqslant (p-1)l_1$, see e.g. [22], Lemma 5.1.1. Moreover $\mathcal{F}_1 = \mathcal{E}_1/G_1 \simeq \mathcal{G}^{(pl_1)}$ and one may check that the pullback $(\Psi^1)^*$ is expressed by the one-term matrix $\Upsilon^1 = (T_{p[\lambda_1]/\lambda_1^p})$. Note that the operator $T_{p[\lambda_1]/\lambda_1^p}$ indeed takes the kernel of $F^{(pl_1)}$ into the kernel of $F^{(l_1)}$, see [22], Lemma 5.2.8. Let us come back to an arbitrary dimension n.

In this setting, we can characterize the situation where the pre-Kummer group scheme G_{n+1} inside a filtered group scheme $\mathcal{E}_{n+1}$ is finite and flat. In the statement below, we will denote by U^i the matrices involved in the

construction of $\mathcal{E}_n$ like in Theorem 6.3.4, and $\overline{U}^i$ the matrices involved in the construction of $\mathcal{F}_n$ (this is the notation of [25]). Note that the inductive construction of $\overline{U}^n$ is included in the statement of the theorem via the vectors $\boldsymbol{u}^n$.

7.1.1. — THEOREM. *Let $n \geqslant 1$, $\boldsymbol{l} = (l_1, \dots, l_{n+1})$ with $l_i > 0$ for each i, and $A \in \mathscr{M}^{\boldsymbol{l}}_{n+1}$. Let $\mathcal{E} = \mathcal{E}(A) = (\mathcal{E}_1, \dots, \mathcal{E}_{n+1})$ be the filtered group scheme of type $\boldsymbol{l}$ defined by A. Assume that $G_n \subset \mathcal{E}_n$ is finite flat. Then, the following conditions are equivalent:*

(i) *G_{n+1} is finite flat,*

(ii) *$v(p) \geqslant (p-1)l_{n+1}$ and there exist vectors $\boldsymbol{u}^{n+1}$ and $\boldsymbol{v}^{n+1}$ in $W^f(R)^n$, with the reduction of $\boldsymbol{u}^{n+1}$ modulo $\pi^{pl_{n+1}}$ lying in $\ker(\overline{U}^n : \widehat{W}(R/\pi^{pl_{n+1}}R)^n \circlearrowleft)$, such that*

$$p\boldsymbol{a}_i^{n+1} - \boldsymbol{c}_i^{n+1} - (\Upsilon^n \boldsymbol{u}^{n+1})_i = \pi^{pl_{n+1}}.\boldsymbol{v}_i^{n+1}$$

for all $1 \leqslant i \leqslant n$, where $\boldsymbol{c}^2 = \boldsymbol{c}_1^2 = [\pi^{l_1}] \in W(R)$, $\boldsymbol{c}^{n+1} = (\boldsymbol{a}^n, [\pi^{l_n}]) \in W(R)^n$ for $n \geqslant 2$, with $\boldsymbol{a}^n = (\boldsymbol{a}_i^n)_{1 \leqslant i < n}$.

In this case, the filtered group scheme $\mathcal{F}_{n+1} = \mathcal{E}_{n+1}/G_{n+1}$ is obtained from $\mathcal{E}_n/G_n$ using the deformed Artin-Hasse exponential defined by $\boldsymbol{u}^{n+1}$. Moreover, if $\Psi^{n+1} : \mathcal{E}_{n+1} \to \mathcal{F}_{n+1}$ is the induced morphism and if $\mu \in R \backslash \{0\}$ then the morphism

$$(\Psi^{n+1})^* : \mathrm{Hom}_{R/\mu R\text{-}\,\mathrm{Gr}}(\mathcal{F}_{n+1}, \mathbb{G}_m) \to \mathrm{Hom}_{R/\mu R\text{-}\,\mathrm{Gr}}(\mathcal{E}_{n+1}, \mathbb{G}_m)$$

is given by

$$\Upsilon^{n+1} = \begin{pmatrix} & \Upsilon^n & & T_{\boldsymbol{v}^{n+1}} \\ 0 & \dots & 0 & T_{p[\pi^{l_{n+1}}]/\pi^{pl_{n+1}}} \end{pmatrix}.$$

Proof. — We make an induction on n. It is convenient to set $\mathcal{E}_0 = \{1\}$ and to start the induction at $n = 0$, in which case the result is known (see e.g. [22], Lemma 5.1.1). For the last statement we will prove something more precise. Write $\mathcal{E}_{n+1} = \mathcal{E}(A)$ and $\mathcal{F}_{n+1} = \mathcal{E}(B)$ with $A = (\boldsymbol{a}_i^j)$ and $B = (\boldsymbol{u}_i^j)$ in $\mathscr{M}_{n+1}$ with $\boldsymbol{a}_i^i = [\pi^{l_i}]$ and $\boldsymbol{u}_i^i = [\pi^{pl_i}]$ for $i = 1, \dots, n+1$. Let

$$K_0 := (1 + \pi^{l_1} T_1)^p = E_p(p[\pi^{l_1}], \pi^{l_1}, T_1)$$

and for $r \geqslant 1$ let

$$K_r := \frac{(E_p(\boldsymbol{a}^{r+1}, (\pi^{l_i})_{1 \leqslant i \leqslant r}, \mathbb{T}) + \pi^{l_{r+1}} T_{r+1})^p}{(E_p(\boldsymbol{a}^r, (\pi^{l_i})_{1 \leqslant i \leqslant r-1}, \mathbb{T}) + \pi^{l_r} T_r)\, E_p(\boldsymbol{u}^{r+1}, (\pi^{l_i})_{1 \leqslant i \leqslant r}, \Psi^r(\mathbb{T}))} \in R[T_1, \dots, T_{r+1}].$$

Given $\boldsymbol{w}^n \in W(R)^n$ whose reduction belongs to $\ker(\overline{U}^n : \widehat{W}(R/\mu R)^n \circlearrowleft)$, we will prove that

$$E_p(\boldsymbol{w}^n, (\pi^{pl_1}, \dots, \pi^{pl_{n+1}}), \Psi^n(\mathbb{T})) = \\ E_p(\Upsilon^n(\boldsymbol{w}^n), (\pi^{l_1}, \dots, \pi^{l_{n+1}}), \mathbb{T}) \prod_{1 \leqslant r \leqslant n} G_p(\overline{U}^n_r(\boldsymbol{w}^n), \pi^{pl_r}, K_{r-1}), \tag{7.1}$$

where $\overline{U}^n_r$ is the r-th row of $\overline{U}^n$. Since $G_p(\overline{U}^n_r(\boldsymbol{w}^n), \pi^{pl_r}; K_{r-1}) \in 1 + TR[[T]]$ for each $r \geqslant 1$ ([25], Prop. 9.3), Equation (7.1) implies

$$K_r = \frac{E_p(p\boldsymbol{a}^r - \boldsymbol{c}^r - \Upsilon^r \boldsymbol{u}^r, (\pi^{l_1}, \dots, \pi^{l_r}); \mathbb{T})\, E_p(p[\pi^{l_{r+1}}], \pi^{l_{r+1}}; \frac{T_{r+1}}{E_p(\boldsymbol{a}^{r+1}, (\pi^{l_i})_{1 \leqslant i \leqslant r}; \mathbb{T})})}{\prod_{i=1}^r G_p(U_i^r(\boldsymbol{u}^r), \pi^{pl_{r+1}}; K_{i-1})}. \tag{7.2}$$

For $n = 1$ the formula (7.1) follows from 6.2.6 and (6.2). We now suppose that the theorem and the formula (7.1) are true for $n-1$ and we prove them for n. We do this in three steps (a)-(b)-(c).

(a) We prove that (i) is equivalent to (ii). Among the objects constructed inductively at the same time as the filtered groups $\mathcal{E}_n, \mathcal{F}_n$, we consider the polynomials D_r, D'_r (truncated exponentials associated respectively to $\mathcal{E}_n$ and $\mathcal{F}_n$) and the isogenies $\Psi^r : \mathcal{E}_r \to \mathcal{F}_r$, for $1 \leqslant r \leqslant n-1$. We also introduce the notation:

$$C_{n+1} = C_{n+1}(T_1, \dots, T_{n+1}) \\ := (D_n(T_1, \dots, T_n) + \pi^{l_{n+1}} T_{n+1})^p (D_{n-1}(T_1, \dots, T_{n-1}) + \pi^{l_n} T_n)^{-1}.$$

We have $K[G_{n+1}] = K[G_n][T_{n+1}]/(C_{n+1} - 1)$. Assume that G_{n+1} is finite over R; then it is finite over G_n. It follows ([9], Prop. 4.1) that $C_{n+1} - 1 \equiv 0$ mod $\pi^{pl_{n+1}}$ and

$$R[G_{n+1}] = R[G_n][T_{n+1}]/\Big(\frac{C_{n+1} - 1}{\pi^{pl_{n+1}}}\Big). \tag{7.3}$$

In particular C_{n+1}, seen as an element of $\mathrm{Hom}_{R/\pi^{pl_{n+1}}R}(G_n, \mathbb{G}_m)$, is the trivial morphism. If we apply the functor $\mathrm{Hom}_{R/\pi^{pl_{n+1}}R}(-, \mathbb{G}_m)$ to the short exact sequence

$$0 \longrightarrow G_n \xrightarrow{i_n} \mathcal{E}_n \xrightarrow{\Psi^n} \mathcal{F}_n \longrightarrow 0,$$

we obtain a long exact sequence

$$0 \longrightarrow \mathrm{Hom}_{R/\pi^{pl_{n+1}}R}(\mathcal{F}_n, \mathbb{G}_m) \xrightarrow{(\Psi^n)^*} \mathrm{Hom}_{R/\pi^{pl_{n+1}}R}(\mathcal{E}_n, \mathbb{G}_m) \\ \xrightarrow{i_n^*} \mathrm{Hom}_{R/\pi^{pl_{n+1}}R}(G_n, \mathbb{G}_m) \longrightarrow \dots$$

As we noticed before, the element C_{n+1} lives in $\ker(i_n^*)$ and hence is equal to $(\Psi^n)^*(D'_n)$ for some $D'_n \in \mathrm{Hom}_{R/\pi^{pl_{n+1}}}(\mathcal{F}_{n+1}, \mathbb{G}_m)$. Now we use the description of groups of homomorphisms from a filtered group scheme to $\mathbb{G}_m$ in terms of vectors, as given by the third point of Theorem 6.3.4. Let $\boldsymbol{u}^{n+1} \in W(R)^n$ be a lift in $W(R)^n$ of a vector corresponding to D'_n. The equality

$$C_{n+1} = (\Psi^n)^*(D'_n)$$

translates to n equalities $p\boldsymbol{a}_i^{n+1} - \boldsymbol{c}_i^{n+1} = (\Upsilon^n \boldsymbol{u}^{n+1})_i$ in $W(R/\pi^{pl_{n+1}}R)^n$, for $1 \leqslant i \leqslant n$. Lifting this to $W(R)^n$ shows that (ii) holds. Conversely, if (ii) holds then C_{n+1} is of the form $(\Psi^n)^*(D'_n)$ for some D'_n, hence it has trivial image under i_n^*. Thus $C_{n+1} \equiv 1 \mod \pi^{pl_{n+1}}$ and the expression (7.3) defines a finite flat group scheme G_{n+1} over R.

(b) Let $\mathcal{F}_{n+1} = \mathcal{E}_{n+1}/G_{n+1}$. Now we prove that $\mathcal{F}_{n+1} = \mathcal{F}'_{n+1}$ where $\mathcal{F}'_{n+1}$ is the filtered group scheme obtained from $\mathcal{F}_n$ using the vector $\boldsymbol{u}^{n+1}$. The R-algebra of $\mathcal{F}'_{n+1}$ is

$$R[\mathcal{F}_n][T_{n+1}, 1/(D'_n + \pi^{pl_{n+1}}T_{n+1})].$$

where $D'_n \in R[T_1, \dots, T_n]$ is the truncation of

$$E_p(\boldsymbol{u}^{n+1}) \prod_{j=1}^{n} E_p(\boldsymbol{u}_j^{n+1}, \pi^{l_j}, T_j / E_p(\boldsymbol{u}^{i-1}, (\pi^{l_i}), \mathbb{T}))$$

as defined in Theorem 6.3.4. Let $\Psi_1, \dots, \Psi_n$ be the polynomials defining the isogeny $\Psi^n : \mathcal{E}_n \to \mathcal{F}_n$. Let

$$\Psi_{n+1}(T_1, \dots, T_n) = \frac{1}{\pi^{pl_{n+1}}} \left(\frac{(D_n(T_1, \dots, T_n) + \pi^{l_{n+1}}T_{n+1})^p}{D_{n-1}(T_1, \dots, T_{n-1}) + \pi^{l_n}T_n} - D'_n(\Psi_1(\mathbb{T}), \dots, \Psi_n(\mathbb{T})) \right).$$

Then the morphism $R[\mathcal{F}_{n+1}] \to R[\mathcal{E}_{n+1}]$, $T_i \mapsto \Psi_i(T_1, \dots, T_i)$ defines an isogeny $\mathcal{E}_{n+1} \to \mathcal{F}'_{n+1}$ with kernel G_{n+1}. Therefore $\mathcal{F}_{n+1}$ is isomorphic to $\mathcal{F}'_{n+1}$ as a filtered group scheme.

(c) We now prove the formula (7.1). We have

$$E_p\left(\boldsymbol{w}^{n+1}, (\pi^{pl_1}, \dots, \pi^{pl_{n+1}}), \Psi^{n+1}(\mathbb{T})\right) = E_p\left((\boldsymbol{w}_r^{n+1})_{1\leqslant r\leqslant n}, (\pi^{pl_1}, \dots, \pi^{pl_n}), \Psi^n(\mathbb{T})\right) E_p\left(\boldsymbol{w}_{n+1}^{n+1}, \pi^{pl_{n+1}}, \frac{\Psi_{n+1}(\mathbb{T})}{E_p(\boldsymbol{u}^{n+1}, (\pi^{l_i})_{1\leqslant i\leqslant n}; \Psi^n(\mathbb{T}))}\right). \tag{7.4}$$

By the induction hypothesis we have

$$E_p\left((\boldsymbol{w}_r^{n+1})_{1\leqslant r\leqslant n},(\pi^{pl_1},\dots,\pi^{pl_n}),\Psi^n(\mathbb{T})\right)= E_p\left(\Upsilon^n\boldsymbol{w}^{n+1},(\pi^{l_1},\dots,\pi^{l_n}),\mathbb{T}\right)\prod_{1\leqslant r\leqslant n}G_p\left(U_r^n((\boldsymbol{w}_s^{n+1})_{1\leqslant s\leqslant n}),\pi^{pl_{n+1}},K_{r-1}\right). \tag{7.5}$$

Moreover we have

$$\begin{aligned}E_p\left(\boldsymbol{w}_{n+1}^{n+1},\pi^{pl_{n+1}},\frac{\Psi_{n+1}(\mathbb{T})}{E_p(\boldsymbol{u}^{n+1},(\pi^{l_i})_{1\leqslant i\leqslant n};\Psi^n(\mathbb{T}))}\right)&= E_p\left(\boldsymbol{w}_{n+1}^{n+1},\pi^{pl_{n+1}},\frac{K_n-1}{\pi^{pl_{n+1}}}\right)\\ &\overset{(6.2)}{=}\widetilde{E}_p\left(\boldsymbol{w}_{n+1}^{n+1},\pi^{pl_{n+1}},K_n\right)G_p\left(F^{(pl_{n+1})}\boldsymbol{w}_{n+1}^{n+1},\pi^{pl_{n+1}},K_n\right)\\ &= E_p\left(T_{\frac{(pa^n-c^{n-1}-\Upsilon^n u^{n+1})}{\pi^{pl_{n+1}}}}\boldsymbol{w}_{n+1}^{n+1},(\pi^{l_1},\dots,\pi^{l_n});\mathbb{T}\right)\\ &\quad\times E_p\left(T_{\frac{p[\pi^{l_{n+1}}]}{\pi^{pl_{n+1}}}}\boldsymbol{w}_{n+1}^{n+1},\pi^{l_{n+1}};\frac{T_{n+1}}{E_p(\boldsymbol{a}^{n+1},(\pi^{l_i})_{1\leqslant i\leqslant n},\mathbb{T})}\right)\\ &\quad\times\prod_{1\leqslant r\leqslant n}G_p\left(-T_{\frac{U_r^n u^{n+1}}{\pi^{pl_{n+1}}}}\boldsymbol{w}_{n+1}^{n+1},\pi^{pl_{n+1}};K_{r-1}\right)\\ &\quad\times G_p\left(F^{(l_{n+1})}\boldsymbol{w}_{n+1}^{n+1},\pi^{pl_{n+1}};K_n\right)\end{aligned}$$

where in the last equality we have used Equation (7.2), Lemma 6.2.6, Lemma 6.2.9, Equation (6.3) and the bilinearity of $\widetilde{E}_p(\mathbb{W},\Lambda,H):W_{\mathbb{A}^1}\times\boldsymbol{\Lambda}_{\mathbb{A}^1}\to\boldsymbol{\Lambda}_{\mathbb{A}^1}$, see 6.2.5. Now using Equations (7.4) and (7.5) one gets the result. □

7.1.2. — Definition. Let $\mathcal{E}(A)=(\mathcal{E}_1,\dots,\mathcal{E}_n)$ be a filtered group scheme. We say that *A satisfies the integrality conditions* if for any $1\leqslant i\leqslant n$, the upper left square submatrix $\mathcal{U}^{n-i}A$ of A satisfies the conditions (ii) in Theorem 7.1.1 applied to an i-dimensional matrix.

In other words, A satisfies the integrality conditions if and only if the pre-Kummer subgroups G_i are finite flat in $\mathcal{E}_i$, for $1\leqslant i\leqslant n$. From the proof of Theorem 7.1.1, we deduce an explicit formula for these models of $\mu_{p^n,K}$.

7.1.3. — Corollary. *Let $\mathcal{E}_n=\mathcal{E}(A)$ be a filtered group scheme given by a family of parameters $A=(\boldsymbol{a}_i^j)$ satisfying the integrality conditions. Let $D_1(T_1)\in R[T_1]$ be any lifting of $E_p(\boldsymbol{a}_1^2,\pi^{l_1},T_1)\mod\pi^{l_2},\dots$, and $D_{n-1}(T_1,\dots,T_{n-1})\in R[T_1,\dots,T_{n-1}]$ be any lifting of*

$$E_p(\boldsymbol{a}^n,(\pi^{l_1},\dots,\pi^{l_{n-1}}),T_1,\dots,T_{n-1})\mod\pi^{l_n}$$

as defined in Theorem 6.3.4. Then G_n is a finite flat R-group scheme, defined in affine n-space in coordinates $T_1, \dots, T_n$ by the n equations:

$$\frac{(1+\pi^{l_1}T_1)^p - 1}{\pi^{pl_1}}, \frac{(D_1 + \pi^{l_2}T_2)^p(1+\pi^{l_1}T_1)^{-1} - 1}{\pi^{pl_2}}, \cdots$$
$$\cdots, \frac{(D_{n-1} + \pi^{l_n}T_n)^p(D_{n-2} + \pi^{l_{n-1}}T_{n-1})^{-1} - 1}{\pi^{pl_n}}.$$

Proof. — This is a translation of Theorem 7.1.1. □

7.1.4. — *Remark.* In the statement of Theorem 7.1.1, it is assumed that $l_i > 0$ for all i. Here is what to do so as to obtain a description of all Kummer group schemes, including the case where some l_i vanish. We make some preliminary observations. First, as it is easy to see from the case $n = 2$, the type of a Kummer group is necessarily ordered: $l_1 \geqslant l_2 \geqslant \cdots \geqslant l_n$ (see 8.2.5). Second, there are no nontrivial extensions of a filtered group scheme by $\mathbb{G}_m$ (see [25], Prop. 3.1). Third, it is easy to see that the only Kummer group scheme of $(\mathbb{G}_m)^n$ with type $(0, \dots, 0)$ is μ_{p^n}. After these preliminaries, it remains to see how to describe Kummer groups of type $\boldsymbol{l}$ with $l_1 \geqslant \cdots \geqslant l_r > l_{r+1} = \cdots = l_n = 0$. Such a Kummer group G lies in a filtered group $\mathcal{E} = \mathbb{G}_m^{n-r} \times \mathcal{E}'(A')$ where $\mathcal{E}'(A')$ is filtered of type $\boldsymbol{l}' = (l_1, \dots, l_r)$. We define $\mathcal{E}(A) := \mathcal{E}$ when

$$A = \begin{pmatrix} A' & 0 \\ 0 & V \end{pmatrix}$$

with V unipotent in $M_{n-r}(W^f(R))$ (therefore equivalent to the identity, since invertible: use Lemma 6.1.4). Moreover, G is an extension of a finite flat Kummer group G' of $\mathcal{E}'$ by $\mu_{p^{n-r}}$. Using the same argument as in [31], Prop. 3.6 there is an exact sequence:

$$0 \longrightarrow \mathbb{Z}/p^r\mathbb{Z} \longrightarrow \mathrm{Ext}^1(G', \mu_{p^{n-r}}) \longrightarrow H^1(S, (G')^\vee) \longrightarrow 0$$

where $S = \mathrm{Spec}(R)$ and $(G')^\vee$ is the Cartier dual of G'. Then with the same proof as in [31], Cor. 3.20 we see that the Kummer subgroups of $\mathcal{E}$ are given by the image of $1 \in \mathbb{Z}/p^r\mathbb{Z}$. They have the following ring of functions:

$$R[G] = \frac{R[G'][T_{r+1}]}{(T_{r+1}^{p^{n-r}}(D_{r-1} + \pi^{l_r}T_r)^{-1} - 1)}.$$

7.2. Matricial translation of the integrality conditions

We translate the previous results on Kummer group schemes in terms of matrices, in order to emphasize the formal similarities with the classification of models of μ_{p^n} by their Breuil-Kisin lattices in 4.2.2. Up to now in Sections §6 and §7, we followed Sekiguchi and Suwa's notation a_i^j for the entries of matrices. However, in order to compare the parameters with those of the Breuil-Kisin classification, we will henceforth write a_{ij}. In the statement of the following result, we use the operator $\mathcal{P}$ introduced in 4.1.4.

7.2.1. — Theorem. *Let G be a Kummer group scheme. Then there exists $\boldsymbol{l} = (l_1, \dots, l_n) \in (\mathbb{N})^n$ and upper triangular matrices*

$$A = \begin{pmatrix} [\pi^{l_1}] & \boldsymbol{a}_{12} & \boldsymbol{a}_{13} & \dots & \boldsymbol{a}_{1n} \\ & [\pi^{l_2}] & \boldsymbol{a}_{23} & & \boldsymbol{a}_{2n} \\ & & \ddots & \ddots & \vdots \\ & & & [\pi^{l_{n-1}}] & \boldsymbol{a}_{n-1,n} \\ 0 & & & & [\pi^{l_n}] \end{pmatrix},$$

$$B = \begin{pmatrix} [\pi^{pl_1}] & \boldsymbol{b}_{12} & \boldsymbol{b}_{13} & \dots & \boldsymbol{b}_{1n} \\ & [\pi^{pl_2}] & \boldsymbol{b}_{23} & & \boldsymbol{b}_{2n} \\ & & \ddots & \ddots & \vdots \\ & & & [\pi^{pl_{n-1}}] & \boldsymbol{b}_{n-1,n} \\ 0 & & & & [\pi^{pl_n}] \end{pmatrix}$$

with entries in $W^f(R)$, satisfying

(1) $F(A)/A \geqslant 0$, $F(B)/B \geqslant 0$,
(2) $(pA - \mathcal{P}\mathcal{U}A)/B \geqslant 0$,

such that G is the kernel of an isogeny $\mathcal{E}(A) \longrightarrow \mathcal{E}(B)$. Moreover when A is chosen, B is unique up to the equivalence relation $\sim$.

If there exists A and B as above then $\mathcal{E}(A)$ contains a finite and flat Kummer subgroup scheme G and $\mathcal{E}/G \simeq \mathcal{E}(B)$.

Proof. — Let us first suppose that $(l_1, \dots, l_n) = (0, \dots, 0)$. Then the unique Kummer scheme of type $(0, \dots, 0)$ is μ_{p^n}. In this case any matrix as in the statement is unipotent and so is equivalent to the identity, since

it is invertible. Therefore such a matrix gives rise to the group scheme μ_{p^n}. Conversely $A = B = Id$ satisfy the conditions of the theorem.

We will now suppose that all the l_i are all strictly positive. The case with some l_i equal to zero can be deduced form this one using Remark 7.1.4.

By definition of a Kummer subgroup, it is embedded in a filtered group scheme $\mathcal{E}(A)$, for some $A \in \mathscr{M}_n$ of type $\boldsymbol{l}$. Moreover by 7.1.1 it is easy to see that

$$pA - \mathcal{PU}A = V_n \star_T B_n$$

where the matrices B_n, V_n are defined by induction:

$$B_{n+1} = \begin{pmatrix} & B_n & & \boldsymbol{u}^{n+1} \\ \\ 0 & \dots & 0 & [\pi^{pl_{n+1}}] \end{pmatrix}$$

and

$$V_{n+1} = \begin{pmatrix} & V_n & & \boldsymbol{v}^{n+1} \\ \\ 0 & \dots & 0 & p[\pi^{l_{n+1}}]/\pi^{pl_{n+1}} \end{pmatrix}$$

with $\boldsymbol{u}^{n+1}$ and $\boldsymbol{v}^{n+1}$ as in the statement of Theorem 7.1.1. It follows from the same theorem that $\mathcal{E}(A)/G \simeq \mathcal{E}(B)$. Similar argument for the converse. □

7.2.2. — *Remark.* One significant difference between this theorem and Theorem 4.2.2 is that here we do not provide a normal form, or distinguished choice, for a matrix A defining a Kummer group scheme. Theorem 4.2.2 suggests that maybe one could choose a pair (A, B) of the form $(A, F(A))$. This is true for instance for $n = 2$ and at least in some cases for $n = 3$, as we will see in the next section.

This theorem should be seen as the analogue in Sekiguchi-Suwa Theory of Theorem 4.2.2 in Breuil-Kisin Theory.

8. Computation of Kummer group schemes for $n = 3$

In this section, we apply the general theory to compute some Kummer group schemes for $n = 3$, that is to say, those models of μ_{p^3} constructed using Sekiguchi-Suwa Theory. From the start, we see that the complexity of the computations with Witt vectors is a serious obstacle. In fact, the difficulty increases with the number of nonzero coefficients of the vectors. It

is therefore interesting to know if in Theorem 7.2.1 we can choose matrices A and B with "short" Witt vector entries. The results of [31] show that in the case $n = 2$, any Kummer group scheme may be described by matrices A, B such that A has *Teichmüller entries*. We could not settle the question whether this is possible for all n, but in our opinion it is not very likely. It is much more plausible that A may be chosen with entries of bounded length; more precisely, it seems reasonable to hope that each Kummer model of μ_{p^n} may be defined by a matrix A all whose entries are Witt vectors of length at most $n-1$. However, it is probably impossible to make simple choices *simultaneously for A and B*, which means that one should not make a priori assumptions on B. Because of these remarks, here we compute the Kummer groups defined by matrices $A, B \in \mathscr{M}_3$ such that A has Teichmüller entries and B is arbitrary.

Even though this is not essential, it will simplify matters to assume throughout that $p \geqslant 3$. Recall that R is a discrete valuation ring of characteristic 0, residue characteristic p, uniformizer π, valuation v and $v(p) = e$. For $l \geqslant 1$, we denote again by v the induced valuation on $R/\pi^l R$. Whenever the context does not allow confusions, we keep the same notation for a Witt vector $\boldsymbol{a} = (a_0, a_1, \dots, a_i \dots) \in W(R)$ and its image in $W(R/\pi^l R)$. Following the comments at the beginning of 7.2 and the notation in 7.2.1, in this section we will write $\boldsymbol{a}_{ij}$ the entries of the matrices.

8.1. Two lemmas

We collect two easy lemmas for future reference.

8.1.1. — Lemma. *Let $l \geqslant 1$ be an integer. Then the following statements hold.*

(1) *If $pe \geqslant (p-1)l$, then for any $\boldsymbol{a} \in \ker(F : \widehat{W}(R/\pi^l R) \circlearrowleft)$ we have $v(a_i) \geqslant l/p$ for all $i \geqslant 0$.*

(2) *For all $\boldsymbol{a}, \boldsymbol{b} \in \widehat{W}(R/\pi^l R)$ such that $v(a_i) \geqslant l/p$ and $v(b_i) \geqslant l/p$ for all $i \geqslant 0$, we have $\boldsymbol{a} + \boldsymbol{b} = (a_0 + b_0, a_1 + b_1, \dots)$.*

Proof. — This is Lemma 2.4 of [31]. More precisely, (1) and (2) are proven in the proof of *loc. cit.* and the assertion of Lemma 2.4 itself is a combination of these statements. □

8.1.2. — Lemma. *Let $\mathbb{X} = (X_0, X_1, X_2, \dots)$ and $\mathbb{Y} = (Y_0, Y_1, Y_2, \dots)$ be sequences of indeterminates and $S_0, S_1, S_2, \dots$ the polynomials giving Witt vector addition (see 3.1).*

(1) *If the variables X_i, Y_i are given the weight p^i, then the polynomial $S_n(\mathbb{X}, \mathbb{Y}) \in \mathbb{Z}[\mathbb{X}, \mathbb{Y}]$ is homogeneous of degree p^n.*
(2) *We have $S_0(\mathbb{X}, \mathbb{Y}) = X_0 + Y_0$,*

$$S_1(\mathbb{X}, \mathbb{Y}) = S_0(X_1, Y_1) + \sigma_1(X_0, Y_0)$$

with

$$\sigma_1(X_0, Y_0) = \frac{X_0^p + Y_0^p - (X_0 + Y_0)^p}{p}$$

and

$$S_2(\mathbb{X}, \mathbb{Y}) = S_0(X_2, Y_2) + \sigma_1(X_1, Y_1) + \sigma_1\Big(X_1 + Y_1, \sigma_1(X_0, Y_0)\Big) + \sigma_2(X_0, Y_0)$$

with

$$\sigma_2(X_0, Y_0) = \frac{X_0^{p^2} + Y_0^{p^2} - (X_0 + Y_0)^{p^2} - p\sigma_1(X_0, Y_0)^p}{p^2}.$$

(3) *We have $\sigma_i(X, -Y) = \sigma_i(X, Y - X)$ and $\sigma_i(X, -Y) = \sigma_i(X, Y - X)$.*
(4) *For any $l \geqslant 1$, $a, b \in R/\pi^l R$ and $i = 1, 2$ we have:*

$$v(\sigma_i(a, b)) \geqslant \min\Big((p^i - 1)v(a) + v(b), (p^i - 1)v(b) + v(a)\Big).$$

(5) *If $p \geqslant 3$, then in the ring $W(\mathbb{Z})$ we have*

$$p = (p, 1 - p^{p-1}, \epsilon_2 p^{p-1}, \epsilon_3 p^{p-1}, \epsilon_4 p^{p-1}, \dots)$$

where $\epsilon_2, \epsilon_3, \epsilon_4, \dots$ are principal p-adic units.

Proof. — (1) is obvious and well-known, (2) is a simple computation, (3) is proven in 3.1.4, (4) follows from (2) with the help of the binomial theorem, and (5) is proven for example in Lemma 5.2.1 of [22]. □

8.2. Computations for $n = 2$

As already said, the case $n = 1$ is well-known (see for instance [22] Lemma 5.1.1). All the models of $\mu_{p,K}$ are given by certain group schemes, called $G_{\pi^l,1}$ with $l \in \mathbb{N}$ such that $\frac{e}{p-1} \geqslant l$. If $l = 0$ we obtain the group scheme $\mu_{p,R} \subset \mathbb{G}_m$. One proves (see [31] § 1) that there exists a model map between $G_{\pi^l,1}$ and $G_{\pi^m,1}$ if and only if $l \geqslant m$. Using Lemma 4.1.8, this implies that for models of $\mu_{p,K}$, the covariant equivalence of Kisin described in § 2.1 is given by $G_{\pi^l,1} \mapsto u^l k[[u]]$. We recall that the matrix associated to the Breuil-Kisin module $u^l k[[u]]$ is the 1×1 matrix (u^l).

We now consider the case $n = 2$. First we recall the following lemma.

8.2.1. — Lemma. *If G is a Kummer group scheme of type (l_1, l_2) then $l_1 \geqslant l_2$.*

Proof. — If G is of type (l_1, l_2), it is an extension of $G_{\pi^{l_1},1}$ by $G_{\pi^{l_2},1}$ so the result follows from [31], Lemma 3.2. Another way to see this is to argue that by 2.3.3 there is a model map $G_{\pi^{l_1},1} \to G_{\pi^{l_2},1}$ and this forces $l_1 \geqslant l_2$, as recalled above. Finally, in the case $l_1, l_2 > 0$ one can also obtain the lemma using Theorem 7.2.1. □

Now fix $l_1, l_2 > 0$. We consider a matrix

$$A = \begin{pmatrix} [\pi^{l_1}] & \boldsymbol{a}_{12} \\ 0 & [\pi^{l_2}] \end{pmatrix} \in M_2(W^f(R)).$$

8.2.2. — Lemma. *The condition $A \in \mathscr{M}_2$, that is to say $F(A)/A \geqslant 0$, is equivalent to the congruence $F^{(l_1)}(\boldsymbol{a}_{12}) \equiv 0 \mod \pi^{l_2}$. Moreover let*

$$A' = \begin{pmatrix} [\pi^{l_1}] & \boldsymbol{a}'_{12} \\ 0 & [\pi^{l_2}] \end{pmatrix} \in M_2(W^f(R)).$$

Then $\boldsymbol{a}'_{12} \equiv \boldsymbol{a}_{12} \mod \pi^{l_2}$ if and only if $A' \in \mathscr{M}_2$ and $\mathcal{E}(A) \simeq \mathcal{E}(A')$.

Proof. — By definition we have $F(A)/A \geqslant 0$ if and only if there exists a positive matrix

$$C = \begin{pmatrix} [\pi^{(p-1)l_1}] & \boldsymbol{c}_{12} \\ 0 & [\pi^{(p-1)l_2}] \end{pmatrix}$$

such that $F(A) = C \star_T A$. The equality of entries in position $(1,2)$ gives $F^{(l_1)}(\boldsymbol{a}_{12}) = \pi^{l_2}.\boldsymbol{c}_{12}$. This is equivalent to $F^{(l_1)}(\boldsymbol{a}_{12}) = 0$ in $W(R/\pi^{l_2}R)$, which is the first assertion. In order to prove the second assertion, let $A' \in M_2(W^f(R))$ be as in the statement. If $\boldsymbol{a}'_{12} \equiv \boldsymbol{a}_{12} \mod \pi^{l_2}$, then:

(i) $F^{(l_1)}(\boldsymbol{a}'_{12}) \equiv F^{(l_1)}(\boldsymbol{a}_{12}) \equiv 0 \mod \pi^{l_2}$,

(ii) there exists $\boldsymbol{r} \in W(R)$ such that $\boldsymbol{a}'_{12} = \boldsymbol{a}_{12} + \pi^{l_2}.\boldsymbol{r}$, so $A' = D \star_T A$ with $D = \left(\begin{smallmatrix} 1 & \boldsymbol{r} \\ 0 & 1 \end{smallmatrix}\right)$.

By (i) and the first assertion of the lemma we have $A' \in \mathscr{M}_2$, and by (ii) and Prop. 6.4.8 we have $\mathcal{E}(A') \simeq \mathcal{E}(A)$. Conversely if $A' \in \mathscr{M}_2$ and $\mathcal{E}(A) \simeq \mathcal{E}(A')$, then by Prop. 6.4.8 there exists a unitriangular matrix D as above such that $A' = D \star_T A$. It follows that $\boldsymbol{a}'_{12} = \boldsymbol{a}_{12} + \pi^{l_2}.\boldsymbol{r}$ and $\boldsymbol{a}'_{12} \equiv \boldsymbol{a}_{12} \mod \pi^{l_2}$. □

Now we use Theorem 7.2.1 in order to tell exactly when A gives rise to a model of μ_{p^2}, in the case A is a matrix with Teichmüller entries.

8.2.3. — Proposition. *Let*

$$A := \begin{pmatrix} [\pi^{l_1}] & [a_{12}] \\ 0 & [\pi^{l_2}] \end{pmatrix}$$

be a matrix with Teichmüller entries and $l_1, l_2 \geqslant 0$. Then A belongs to $\mathscr{M}_2$ and $\mathcal{E}(A)$ contains a finite flat Kummer subgroup G if and only if

(i) $\frac{e}{p-1} \geqslant l_1 \geqslant l_2$,
(ii) $a_{12}^p \equiv 0 \mod \pi^{l_2}$, *and*
(iii) $pa_{12} - \pi^{l_1} - \frac{p}{\pi^{(p-1)l_1}}(a_{12})^p \equiv 0 \mod \pi^{pl_2}$.

In such a case, we have $\mathcal{E}(A)/G \simeq \mathcal{E}(F(A))$. Moreover, if we set $D_1(T) = \sum_{k=0}^{p-1} a_{12}^k T^k/k!$, then

$$G = \operatorname{Spec}\left(R[T_1,T_2]\Big/\Big(\frac{(1+\pi^{l_1}T_1)^p - 1}{\pi^{l_1 p}}, \frac{(D_1(T_1)+\pi^{l_2}T_2)^p(1+\pi^{l_1}T_1)^{-1}-1}{\pi^{pl_2}}\Big)\right).$$

Finally G depends only on the reduction of a_{12} modulo π^{l_2}.

Proof. — If $l_1 = 0$ or $l_2 = 0$, the result comes from the case $n = 1$ (see 7.1.4) and is easy so we suppose that $l_1, l_2 > 0$. By Theorem 7.1.1 and Lemmas 8.2.1 and 8.2.2, the matrix A gives a finite flat Kummer group G if and only $\frac{e}{p-1} \geqslant l_1 \geqslant l_2$, $F^{(l_1)}([a_{12}]) \equiv 0 \mod \pi^{l_2}$ and there exists a vector $\boldsymbol{u} = \boldsymbol{u}_{12} \in W^f(R)$ with reduction in $\ker(F^{(pl_1)} : \widehat{W}(R/\pi^{pl_2}R) \circlearrowleft)$ such that:

$$p[a_{12}] - [\pi^{l_1}] = T_{p[\pi^{l_1}]/\pi^{pl_1}}(\boldsymbol{u}) \mod \pi^{pl_2}. \tag{8.1}$$

Since $l_1 \geqslant l_2$, the congruence $F^{(l_1)}([a_{12}]) \equiv 0 \mod \pi^{l_2}$ is equivalent to $a_{12}^p \equiv 0 \mod \pi^{l_2}$. It remains only to prove that (8.1) and (iii) are equivalent equations.

First, let us consider the left hand side of the congruence (iii). Using the expression $p = (p, 1-p^{p-1}, \dots) \in W(R)$ recalled in 8.1.2(5) and the minoration $v(a_{12}) \geqslant l_2/p$, we find:

$$p[a_{12}] = \big(pa_{12}, (1-p^{p-1})(a_{12})^p, 0, 0, \dots\big) \in W(R/\pi^{pl_2}R).$$

Since $p \geqslant 3$, we have $v(p^{p-1}) = (p-1)e \geqslant (p-1)^2 l_2 \geqslant pl_2$. Thus in fact:

$$p[a_{12}] = (pa_{12}, (a_{12})^p, 0, 0, \dots) \mod \pi^{pl_2}.$$

Using Lemma 8.1.1(2) we obtain

$$p[a_{12}] - [\pi^{l_1}] = (pa_{12} - \pi^{l_1}, (a_{12})^p, 0, 0, \dots) \mod \pi^{pl_2}. \tag{8.2}$$

Now let us turn to the right hand side. We set $\omega := \frac{p}{\pi^{(p-1)l_1}}$. In the same way as before, we obtain

$$\frac{p[\pi^{l_1}]}{\pi^{pl_1}} = (\omega, 1, 0, 0, \dots) \mod \pi^{pl_2}.$$

It follows that $T_{p[\pi^{l_1}]/\pi^{pl_1}} \boldsymbol{u} = [\omega]\boldsymbol{u} + V\boldsymbol{u}$ in $W(R/\pi^{pl_2}R)$. Now note that in $W(R/\pi^{pl_2}R)$ we have $\ker(F^{(pl_1)}) = \ker(F)$, so it follows from Lemma 8.1.1(1) that

$$\boldsymbol{u} \equiv 0 \mod \pi^{l_2},$$

hence also

$$[\omega]\boldsymbol{u} \equiv V\boldsymbol{u} \equiv 0 \mod \pi^{l_2}.$$

Thus by Lemma 8.1.1(2), their sum in $W(R/\pi^{pl_2}R)$ is computed componentwise:

$$T_{p[\pi^{l_1}]/\pi^{pl_1}} \boldsymbol{u} = \left(\omega u_0, \omega^p u_1 + u_0, \omega^{p^2} u_2 + u_1, \omega^{p^3} u_3 + u_2, \dots\right).$$

Since $\boldsymbol{u}$ has finitely many nonzero coefficients, we may call u_k the last of them. It follows from the above that

$$\begin{aligned}(pa_{12} - \pi^{l_1}, (a_{12})^p, 0, \dots) \\ = \left(\omega u_0, \omega^p u_1 + u_0, \omega^{p^2} u_2 + u_1, \dots \omega^{p^3} u_k + u_{k-1}, u_k \dots\right).\end{aligned}$$

This is possible only if $k = 0$, hence $\boldsymbol{u} = (u_0, 0, \dots) = [u_0]$ in $W(R/\pi^{pl_2}R)$. Now if we identify

$$T_{p[\pi^{l_1}]/\pi^{pl_1}} \boldsymbol{u} = (\omega u_0, u_0, 0, 0, \dots) = (pa_{12} - \pi^{l_1}, (a_{12})^p, 0, \dots),$$

we obtain $u_0 \equiv (a_{12})^p \mod \pi^{pl_2}$ and the congruence

$$pa_{12} - \pi^{l_1} - \frac{p}{\pi^{(p-1)l_1}}(a_{12})^p \equiv 0 \mod \pi^{pl_2}.$$

This finishes the proof of the first assertion of the proposition. As a bonus, we see that $\boldsymbol{u} = F([a_{12}])$ is a solution to (8.1). Then Theorem 7.2.1 shows that $\mathcal{E}(A)/G \simeq \mathcal{E}(F(A))$. The final expression for the function ring of G follows from the general theory, which of course provides also the group law. The final statement follows from the above lemma. □

8.2.4. — *Remarks.* (1) In the set of conditions (i)-(ii)-(iii) of the proposition, the inequality $l_1 \geqslant l_2$ is a consequence of the rest. Indeed, if we assume the three conditions satisfied except that $l_1 < l_2$, it is clear that (iii) has no solution.

(2) We recover, with essentially the same proof, all the group schemes exhibited in Tossici's paper [31]. In *loc. cit.* it is also proven with some more work that if (l_1, l_2, a_{12}) and (l_1, l_2, a'_{12}) give rise to isomorphic group

schemes then $a_{12} \equiv a'_{12} \mod \pi^{l_2}$, and that all models of μ_{p^2} are obtained in this way. Moreover Proposition 3.34 in *loc. cit.* can be complemented by saying that the existence of model maps corresponds to the divisibility between their matrices (with Teichmüller entries). All these things works also in characteristic 2.

The following remark is the equivalent of 4.2.3.

8.2.5. — *Remark.* The above results for $n = 2$ have consequences for general n. Let G be a finite flat Kummer group scheme in a filtered group scheme $\mathcal{E}(A)$ of type $(l_1, \dots, l_n) \in \mathbb{N}^n$. Then

(1) $\frac{e}{p-1} \geqslant l_1$,
(2) $l_1 \geqslant l_2 \geqslant \cdots \geqslant l_n$,
(3) if $\boldsymbol{a}_{i,i+1} = (a^0_{i,i+1}, a^1_{i,i+1}, \dots, a^k_{i,i+1}, \dots)$ then $v(a^k_{i,i+1}) \geqslant l_{i+1}/p$ for all i, k.

In fact point (1) is already known (first sentences of 8.2). For $n = 2$, point (2) follows from Lemma 8.2.1 and point (3) follows from Lemmas 8.2.2 and 8.1.1(1). The statement for arbitrary n follows simply by considering the $n-1$ subquotients of G of order p^2, whose matrices are the diagonal blocks of size $(2, 2)$ of the matrix A (see Proposition 6.4.8).

8.2.6. — Comparison Sekiguchi-Suwa Theory / Breuil-Kisin Theory for $n = 2$. The existence of a link between these two theories was already known in [31], Appendix A but in a less precise way. Explaining it in details using our formalism will give an idea of what the problems are for $n > 2$. We shall construct an explicit bijection between the set of matrices parametrizing models of μ_{p^2} viewed as Kummer group schemes, and the set of matrices parametrizing Breuil-Kisin lattices.

We recall the setting: R is a complete discrete valuation ring with perfect residue field k, totally ramified over $W(k)$. We fix a uniformizer $\pi \in R$ and we call $E(u)$ its minimal polynomial over K, so that $u \mapsto \pi$ induces an isomorphism $W(k)[u]/(E(u)) \simeq R$. Note that since $E(u)$ is Eisenstein, we have $E(u) \equiv u^e + p\,[E_1(u)] \mod p^2$ with $E_1(u) \in k[u]$, $\deg(E_1(u)) < e$ and $E_1(0) \neq 0$.

The central point in the dictionary between the two theories is the map $(-)^* : k[[u]] \to R$ sending a power series $c = \sum_{i=0}^{\infty} c_i u^i$ to $c^* = \sum_{i=0}^{\infty} [c_i]\pi^i$. It is an isometry for the u-adic distance on the domain and the π-adic distance on the target, which means simply that $f \equiv g \mod u^l$ if and only if $f^* \equiv g^* \mod \pi^l$, for all $l \geqslant 0$. Moreover, we have the property $(u^n c)^* = \pi^n c^*$. For each $l \geqslant 1$, the map $c \mapsto c^*$ induces a map $k[u]/u^l k[u] \simeq R/\pi^l R$ which for $l \leqslant e$ is an isomorphism of rings but is neither additive nor

multiplicative in general. Now, using $(-)^*$ we map any matrix

$$A = \begin{pmatrix} u^{l_1} & a_{12} \\ 0 & u^{l_2} \end{pmatrix} \in \mathscr{G}_2((u))$$

to the matrix

$$A^* = \begin{pmatrix} [\pi^{l_1}] & [a_{12}^*] \\ 0 & [\pi^{l_2}] \end{pmatrix} \in M_2(W(R)).$$

We claim that A is a μ-matrix if and only if A^* gives rise to a model of μ_{p^2}. In order to prove this, we just have to check that the congruences in the two columns correspond to each other:

Breuil-Kisin (*cf* 5.2.1)	Sekiguchi-Suwa (*cf* 8.2.3)
$\frac{e}{p-1} \geqslant l_1 \geqslant l_2$	$\frac{e}{p-1} \geqslant l_1 \geqslant l_2$
$(a_{12})^p \equiv 0 \mod u^{l_2}$	$(a_{12}^*)^p \equiv 0 \mod \pi^{l_2}$
$u^e a_{12} + E_1(u)u^{l_1} - u^{e-(p-1)l_1}(a_{12})^p \equiv 0 \mod u^{pl_2}$	$pa_{12}^* - \pi^{l_1} - \frac{p}{\pi^{(p-1)l_1}}(a_{12}^*)^p \equiv 0 \mod \pi^{pl_2}$

Since $l_2 \leqslant e$, the equivalence between the congruences in the second line comes from the isomorphism $k[\![u]\!]/u^l k[\![u]\!] \simeq R/\pi^l R$. It remains only to prove the equivalence of the congruences in the third line: this is not immediate since $R/\pi^{pl_2}R$ is not isomorphic to $k[\![u]\!]/u^{pl_2}$ if $pl_2 > e$. So we look at the image under $c \mapsto c^*$ of the Breuil-Kisin congruence

$$u^e a_{12} + E_1(u)u^{l_1} \equiv u^{e-(p-1)l_1}(a_{12})^p \mod u^{pl_2}. \tag{8.3}$$

We compute the image of both sides. Since, for $\alpha, \beta \in k$, the difference $[\alpha+\beta] - [\alpha] - [\beta] \in W(k)$ is a multiple of p, one sees that the difference between $(u^e a_{12} + E_1(u)u^{l_1})^*$ and $\pi^e a_{12}^* + [E_1](\pi)\pi^{l_1}$ is a multiple of $p\pi^e$. Hence using the fact that $2e > pl_2$ we see that

$$(u^e a_{12} + E_1(u)u^{l_1})^* \equiv \pi^e a_{12}^* + [E_1](\pi)\pi^{l_1} \mod \pi^{pl_2},$$

where $[E_1](\pi)$ is the evaluation of the polynomial $[E_1]$ at $u = \pi$. Now using $\mathrm{val}_u(a_{12}) \geqslant l_2/p$ and $\frac{e}{p-1} \geqslant l_2$, one sees using the binomial theorem that $((a_{12})^p)^* = (a_{12}^*)^p \mod \pi^{pl_2}$. Putting things together, it follows that the image of the congruence (8.3) is:

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

Since E vanishes at $u = \pi$, we have $\pi^e + p[E_1](\pi) \equiv 0 \mod p^2$ (beware that $[E_1(u)]$ evaluated at $u = \pi$ is $[E_1](\pi)$). Given that $p^2 \equiv 0 \mod \pi^{pl_2}$, we may replace π^e by $-p[E_1](\pi)$ in the previous congruence and obtain:

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

Since $[E_1](\pi)$ is invertible mod π^{pl_2}, this is indeed equivalent to the equation on the Sekiguchi-Suwa side in the third line. Our claim is thus proved.

As we noticed in 8.2.4(2), the results of [31] imply that in fact the matrices with Teichmüller coefficients that we are considering above on the Sekiguchi-Suwa side are in one-one correspondence with the models of $\mu_{p^2,K}$. Since the map $A \mapsto A^*$ also preserves divisibility between matrices, it follows that we have set up a covariant equivalence between the category of μ-matrices and the category of models of $\mu_{p^2,K}$. We have not proven that this equivalence is the covariant equivalence constructed by Kisin, but it seems natural to conjecture that they are indeed the same.

8.3. Computations for $n = 3$

Fix $l_1, l_2, l_3 > 0$. We consider a matrix:

$$A = \begin{pmatrix} [\pi^{l_1}] & \boldsymbol{a}_{12} & \boldsymbol{a}_{13} \\ 0 & [\pi^{l_2}] & \boldsymbol{a}_{23} \\ 0 & 0 & [\pi^{l_3}] \end{pmatrix} \in \mathscr{H}_3(W^f(R)).$$

8.3.1. — Lemma. *The condition $A \in \mathscr{M}_3$, i.e. $F(A)/A \geqslant 0$, is equivalent to the congruences:*

(1) $F^{(l_1)}(\boldsymbol{a}_{12}) \equiv 0 \mod \pi^{l_2}$, $F^{(l_2)}(\boldsymbol{a}_{23}) \equiv 0 \mod \pi^{l_3}$, *and*
(2) $F^{(l_1)}(\boldsymbol{a}_{13}) \equiv T_{\frac{F^{(l_1)}(a_{12})}{\pi^{l_2}}}(\boldsymbol{a}_{23}) \mod \pi^{l_3}$.

Moreover if $A' = (\boldsymbol{a}'_{ij}) \in \mathscr{M}_3$ then $\mathcal{E}(A') \simeq \mathcal{E}(A)$ as filtered group schemes if and only if $\boldsymbol{a}'_{12} \equiv \boldsymbol{a}_{12} \in W(R/\pi^{l_2}R)$, $\boldsymbol{a}'_{23} \equiv \boldsymbol{a}_{23} \in W(R/\pi^{l_3}R)$ and

$$\boldsymbol{a}'_{13} \equiv \boldsymbol{a}_{13} + T_{\frac{a'_{12}-a_{12}}{\pi^{l_2}}}(\boldsymbol{a}_{23}) \mod \pi^{l_3}. \tag{8.4}$$

If A has Teichmüller entries $[a_{ij}]$ and $l_1 \geqslant l_2 \geqslant l_3$ then $F(A)/A \geqslant 0$ is equivalent to the congruences:

(1) $a_{12}^p \equiv 0 \mod \pi^{l_2}$, $a_{23}^p \equiv 0 \mod \pi^{l_3}$, *and*
(2) $\pi^{l_2}a_{13}^p \equiv a_{23}a_{12}^p \mod \pi^{l_2+l_3}$.

Moreover if $A' = ([a'_{ij}]) \in \mathscr{H}_3(W^f(R))$ *with* $a'_{ii} = \pi^{l_i}$, *then* $A' \in \mathscr{M}_3$ *and* $\mathcal{E}(A) \simeq \mathcal{E}(A')$ *as filtered group schemes if and only if* $a'_{12} \equiv a_{12} \mod \pi^{l_2}$, $a'_{23} \equiv a_{23} \mod \pi^{l_3}$ *and*

$$[a'_{13}] - [a_{13}] \equiv \Big[\frac{(a'_{12} - a_{12})a_{23}}{\pi^{l_2}}\Big] \mod \pi^{l_3}. \tag{8.5}$$

8.3.2. — *Remark.* Here is a remark for later use. Let us suppose that $pe \geqslant (p-1)l_3$ and $l_1, l_2 \geqslant l_3$. Let $\boldsymbol{a}_{i3} = (a^0_{i3}, a^1_{i3}, \dots, a^k_{i3}, \dots)$ for $i = 1, 2$. Then, if $\boldsymbol{a}_{13}$ and $\boldsymbol{a}_{23}$ satisfy the congruences of the first part of the above lemma then $v(a_{13}) \geqslant l_3/p^2$. To prove this we first observe that since $F(\boldsymbol{a}_{23}) \equiv 0 \mod \pi^{l_3}$ it follows from Lemma 8.1.1(1) that $v(a^k_{23}) \geqslant l_3/p$, for any k. Hence from

$$F^{(l_1)}(\boldsymbol{a}_{13}) \equiv T_{\frac{F^{(l_1)}(a_{12})}{\pi^{l_2}}}(\boldsymbol{a}_{23}) \mod \pi^{l_3}$$

it follows that all the components of $F(\boldsymbol{a}_{13})$ have valuation at least l_3/p. Again by Lemma 8.1.1(1) we obtain $v(a^k_{13}) \geqslant l_3/p^2$ for any k.

Proof. — We begin with the general case. By definition we have $F(A)/A \geqslant 0$ if and only if there exists a positive matrix

$$C = \begin{pmatrix} [\pi^{(p-1)l_1}] & \boldsymbol{c}_{12} & \boldsymbol{c}_{13} \\ 0 & [\pi^{(p-1)l_2}] & \boldsymbol{c}_{23} \\ 0 & 0 & [\pi^{(p-1)l_3}] \end{pmatrix}$$

such that $F(A) = C \star_T A$. By the case $n = 2$, this gives the congruences in (i). The equality of entries in position $(1, 3)$ gives:

$$F^{(l_1)}(\boldsymbol{a}_{13}) = T_{\boldsymbol{c}_{12}}(\boldsymbol{a}_{23}) + \pi^{l_3}.\boldsymbol{c}_{13}.$$

The coefficient $\boldsymbol{c}_{12}$ is determined by the equality of entries in position $(1, 2)$, namely it is equal to $\frac{F^{(l_1)}([a_{12}])}{\pi^{l_2}}.\boldsymbol{c}_{12}$. This gives the congruence (ii).

Let A' be another matrix in $\mathscr{M}_3$. Then by 6.4.7 we have $\mathcal{E}(A) \simeq \mathcal{E}(A')$ as filtered group schemes if and only if there exist Witt vectors $\boldsymbol{r}', \boldsymbol{s}', \boldsymbol{t}'$ such that

$$A' := \begin{pmatrix} [\pi^{l_1}] & \boldsymbol{a}'_{12} & \boldsymbol{a}'_{13} \\ 0 & [\pi^{l_2}] & \boldsymbol{a}'_{23} \\ 0 & 0 & [\pi^{l_3}] \end{pmatrix} = \begin{pmatrix} 1 & \boldsymbol{r}' & \boldsymbol{t}' \\ 0 & 1 & \boldsymbol{s}' \\ 0 & 0 & 1 \end{pmatrix} \star_T \begin{pmatrix} [\pi^{l_1}] & \boldsymbol{a}_{12} & \boldsymbol{a}_{13} \\ 0 & [\pi^{l_2}] & \boldsymbol{a}_{23} \\ 0 & 0 & [\pi^{l_3}] \end{pmatrix}.$$

It is easy to see that $\boldsymbol{r}' = \frac{\boldsymbol{a}'_{12} - \boldsymbol{a}_{12}}{\pi^{l_2}}$ and the rest follows.

We now show how things simplify if one supposes that A has Teichmüller entries and $l_1 \geqslant l_2 \geqslant l_3$.

Formulas in (1) are immediate, under these hypothesis, from the general case, and we already found them in the case $n = 2$. Now let us suppose that

$$F^{(l_1)}([a_{13}]) \equiv T_{\frac{F^{(l_1)}([a_{12}])}{\pi^{l_2}}}([a_{23}]) \mod \pi^{l_3}.$$

Since $(p-1)l_1 \geqslant 2l_1 \geqslant l_2 + l_3$, this is equivalent to say

$$a_{13}^p \equiv \frac{a_{12}}{\pi^{l_2}} a_{23} \mod \pi^{l_3},$$

which is equivalent to (2).

We now study when two matrices with Teichmüller entries are equivalent. The assertions about a_{12} and a_{23} clearly come from the general case. Now let us take an upper triangular matrix $A' = ([a'_{ij}]) \in \mathscr{M}_3$. The condition (8.4) reads, in this case,

$$[a'_{13}] \equiv [a_{13}] + T_{\frac{[a'_{12}]-[a_{12}]}{\pi^{l_2}}}([a_{23}]) \mod \pi^{l_3}.$$

Since $a'_{12} = a_{12} + \pi^{l_2} r$ for some $r \in R$, $l_2 \geqslant l_3$ and $v(a_{12}), v(a_{23}) \geqslant \frac{l_3}{p}$ we have

$$T_{\frac{[a'_{12}]-[a_{12}]}{\pi^{l_2}}}([a_{23}]) \equiv \frac{[(a'_{12} - a_{12})a_{23}]}{\pi^{l_2}} \mod \pi^{l_3}.$$

So we get

$$[a'_{13}] \equiv [a_{13}] + \frac{[(a'_{12} - a_{12})a_{23}]}{\pi^{l_2}} \mod \pi^{l_3},$$

as desired. □

We now state our final result for $n = 3$, and we provide some comments after the statement.

8.3.3. — Theorem. *Let $0 \leqslant l_3 \leqslant l_2 \leqslant l_1 \leqslant e/(p-1)$ be integers and $a_{12}, a_{23}, a_{13} \in R$ elements satisfying the congruences:*

$$a_{12}^p \equiv 0 \mod \pi^{l_2} \quad , \quad a_{23}^p \equiv 0 \mod \pi^{l_3} \quad , \quad \pi^{l_2} a_{13}^p \equiv a_{23} a_{12}^p \mod \pi^{l_2+l_3}.$$

Let $A = ([a_{ij}])$ be the matrix with Teichmüller entries of $\mathscr{M}_3$ defined by these parameters (Lemma 8.3.1). Assume that $l_1 \geqslant pl_3$. Then the pre-Kummer subgroup $G \subset \mathcal{E}(A)$ is finite flat if and only if the following congruences are satisfied:

$$pa_{12} - \pi^{l_1} - \frac{p}{\pi^{(p-1)l_1}} a_{12}^p \equiv 0 \mod \pi^{pl_2},$$

$$pa_{23} - \pi^{l_2} - \frac{p}{\pi^{(p-1)l_2}} a_{23}^p \equiv 0 \mod \pi^{pl_3},$$

$$\frac{p}{\pi^{(p-1)l_1}} a_{13}^p \equiv pa_{13} - a_{12} - a_{23}^p \frac{pa_{12} - \pi^{l_1} - \frac{p}{\pi^{(p-1)l_1}} a_{12}^p}{\pi^{pl_2}} \mod \pi^{pl_3}.$$

When this is the case, we have

$$G = \mathrm{Spec}\left(R[T_1,T_2,T_3] \Big/ \left(\begin{array}{l} \frac{(1+\pi^{l_1}T_1)^p}{\pi^{l_1 p}}, \frac{(D_1(T_1)+\pi^{l_2}T_2)^p(1+\pi^{l_1}T_1)^{-1}-1}{\pi^{pl_2}}, \\ \\ \frac{(D_2(T_1,T_2)+\pi^{l_3}T_3)^p(D_1(T_1)+\pi^{l_2}T_2)^{-1}-1}{\pi^{pl_3}} \end{array} \right) \right)$$

where $D_1(T) = E_p(a_{12}T) = \sum_{k=0}^{p-1} a_{12}^k \frac{T^k}{k!}$ *and* $D_2(T_1,T_2)$ *is a lifting of*

$$E_p(a_{13}T_1)E_p\Big(a_{23}\frac{T_2}{D_1(T_1)}\Big) \mod \pi^{l_3},$$

which under the above congruences is a polynomial. Finally if $A' = ([a'_{ij}]) \in \mathscr{M}_3$ *then the finite and flat group scheme of* $\mathcal{E}(A')$ *is isomorphic to* G *if and only if* $a'_{12} \equiv a_{12} \in R/\pi^{l_2}R$, $a'_{23} \equiv a_{23} \in R/\pi^{l_3}R$ *and*

$$[a'_{13}] - [a_{13}] \equiv \Big[\frac{(a'_{12}-a_{12})a_{23}}{\pi^{l_2}}\Big] \mod \pi^{l_3}. \tag{8.6}$$

8.3.4. — *Remark.* (1) This result says that we are able to describe completely the congruences satisfied by matrices with Teichmüller entries giving rise to Kummer group schemes of order p^3, under the (light) assumption that $l_1 \geqslant pl_3$. Removing this assumption would require more work. See the final remarks in 8.5 for more comments on the case $l_1 < pl_3$. However we do not know if Kummer group schemes of order p^3 arising from matrices with Teichmüller entries provide all the Kummer group schemes of order p^3, under the hypothesis $l_1 \geqslant pl_3$.

(2) A consequence of the above statement is that in the situation of 8.3.3, we may take $B = F(A)$ in Theorem 7.2.1. See also Remark 7.2.2.

(3) In the third congruence of the second set of congruences, one may in fact remove the term pa_{13} since $e \geqslant l_1 \geqslant pl_3$. But leaving it emphasizes the similarity with the congruences we obtained with the Breuil-Kisin approach, as we will see in 8.3.5.

Proof. — The dependency on the parameters (in the end of the statement) follows from Lemma 8.3.1. The rest is proven by the general theory, except for the precise shape of the congruences. Proposition 8.2.3 gives the congruences for the subgroup and quotient of degree p^2 in G to be finite flat, and fills up the upper left and lower right matrices of size 2. More precisely, we have the congruences:

$$pa_{12} - \pi^{l_1} - \frac{p}{\pi^{(p-1)l_1}}(a_{12})^p \equiv 0 \mod \pi^{pl_2},$$
$$pa_{23} - \pi^{l_2} - \frac{p}{\pi^{(p-1)l_2}}(a_{23})^p \equiv 0 \mod \pi^{pl_3}.$$

With the notations of Theorem 7.2.1, we have:

$$B = B_3 = \begin{pmatrix} [\pi^{pl_1}] & [a_{12}^p] & \boldsymbol{u}_{13} \\ 0 & [\pi^{pl_2}] & [a_{23}^p] \\ 0 & 0 & [\pi^{pl_3}] \end{pmatrix}$$

and

$$V_3 = \begin{pmatrix} p[\pi^{l_1}]/\pi^{pl_1} & \boldsymbol{v}_{12} & \boldsymbol{v}_{13} \\ 0 & p[\pi^{l_2}]/\pi^{pl_2} & \boldsymbol{v}_{23} \\ 0 & 0 & p[\pi^{l_3}]/\pi^{pl_3} \end{pmatrix}$$

where $\boldsymbol{v}_{12} = \boldsymbol{v}_1^2$ and $\boldsymbol{v}_{23} = \boldsymbol{v}_2^3$ are the following vectors of $W(R)$:

$$\boldsymbol{v}_{12} = \frac{1}{\pi^{pl_2}} \left(p[a_{12}] - [\pi^{l_1}] - T_{p[\pi^{l_1}]/\pi^{pl_1}}[a_{12}^p] \right),$$
$$\boldsymbol{v}_{23} = \frac{1}{\pi^{pl_3}} \left(p[a_{23}] - [\pi^{l_2}] - T_{p[\pi^{l_2}]/\pi^{pl_2}}[a_{23}^p] \right).$$

Thus G is finite flat if and only if the previous congruences are satisfied as well as the following last one:

$$p[a_{13}] - [a_{12}] - T_{p[\pi^{l_1}]/\pi^{pl_1}} \boldsymbol{u}_{13} - T_{\boldsymbol{v}_{12}}[a_{23}^p] \equiv 0 \mod \pi^{pl_3}.$$

It only remains to prove that this is equivalent to:

$$\frac{p}{\pi^{(p-1)l_1}} a_{13}^p \equiv pa_{13} - a_{12} - a_{23}^p \frac{pa_{12} - \pi^{l_1} - \frac{p}{\pi^{(p-1)l_1}} a_{12}^p}{\pi^{pl_2}} \mod \pi^{pl_3}.$$

This is done in Subsection 8.4. □

8.3.5. — Comparison Sekiguchi-Suwa Theory / Breuil-Kisin Theory for $n = 3$. We proceed as in 8.2.6 to compare the two theories. Since we conducted the computations only under the additional assumption $l_1 \geqslant pl_3$ on the Sekiguchi-Suwa side, we will stay in this restricted setting. We consider again the map $(-)^* : k[[u]] \to R$, $\sum_{i=0}^{\infty} c_i u^i \mapsto \sum_{i=0}^{\infty} [c_i]\pi^i$

and the induced map on matrices:

$$A = \begin{pmatrix} u^{l_1} & a_{12} & a_{13} \\ 0 & u^{l_2} & a_{23} \\ 0 & 0 & u^{l_3} \end{pmatrix} \in \mathscr{G}_3((u))$$

$$\longmapsto \quad A^* = \begin{pmatrix} [\pi^{l_1}] & [a_{12}^*] & [a_{13}^*] \\ 0 & [\pi^{l_2}] & [a_{23}^*] \\ 0 & 0 & [\pi^{l_3}] \end{pmatrix} \in M_3(W(R)).$$

We want to check that A is a μ-matrix if and only if A^* gives rise to a model of μ_{p^3}. For this we compare the congruences from Breuil-Kisin Theory (*cf* 5.2.1) on the left, and the congruences from Sekiguchi-Suwa Theory (*cf* 8.2.3) on the right.

A

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

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

B

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

$$\begin{aligned} pa_{12}^* - \pi^{l_1} - \tfrac{p}{\pi^{(p-1)l_1}} a_{12}^{*\,p} &\equiv 0 \mod \pi^{pl_2} \\ pa_{23}^* - \pi^{l_2} - \tfrac{p}{\pi^{(p-1)l_2}} a_{23}^{*\,p} &\equiv 0 \mod \pi^{pl_3} \end{aligned}$$

C

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

???

D

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

$$\pi^{l_2} a_{13}^{*\,p} \equiv a_{23}^* a_{12}^{*\,p} \mod \pi^{l_2 + l_3}$$

E

$$\begin{aligned} &u^e a_{13} + a_{12} E_1 + \mathbb{S}_1(u^e a_{12}, u^{l_1} E_1) + u^{l_1} E_2 \\ &-u^{e-(p-1)l_1} a_{13}^p - \tfrac{u^e a_{12} + u^{l_1} E_1 - u^{e-(p-1)l_1} a_{12}^p}{u^{pl_2}} a_{23}^p \equiv 0 \mod u^{pl_3} \end{aligned}$$

$$\tfrac{p}{\pi^{(p-1)l_1}} a_{13}^{*\,p} \equiv pa_{13}^* - a_{12}^* - a_{23}^{*\,p} \tfrac{pa_{12}^* - \pi^{l_1} - \frac{p}{\pi^{(p-1)l_1}} a_{12}^{*\,p}}{\pi^{pl_2}} \mod \pi^{pl_3}$$

One sees immediately that in the Breuil-Kisin side there is one more equation. We will prove below that in fact this congruence is a consequence of the others, so we do not bother considering it for the moment.

In fact, only conditions **D** and **E** need to be compared, since the previous ones match by the case $n = 2$. The equivalence between the congruences in **D** is immediate since the operator $(-)^*$ induces an isomorphism on the truncations of level $l_2 + l_3$, given that $e \geqslant l_2 + l_3$. We pass to **E**. Taking into account our assumption that $l_1 \geqslant pl_3$, on the Breuil-Kisin side we have

$$u^{l_1} E_2 \equiv \mathbb{S}_1(u^e a_{12}, u^{l_1} E_1) \equiv 0 \mod u^{pl_3}.$$

With what remains, we can see that the two equations are equivalent in the same way as in 8.2.6. It is still true that $p^2 \equiv 0 \mod \pi^{pl_3}$. So we have $\pi^e + p[E_1](\pi) \equiv 0 \mod p^2$ (beware that $[E_1(u)]$ evaluated at $u = \pi$ is $[E_1](\pi)$). With no more difficulty than in the case $n = 2$ one shows, using $l_1 \geqslant pl_3$, that $(a_{13}^p)^* \equiv (a_{13}^*)^p \mod \pi^{l_3}$, $(a_{23}^p)^* \equiv (a_{23}^*)^p \mod \pi^{l_3}$ and

$$\big(u^e a_{13} + a_{12}E_1 - \frac{u^e a_{12} + u^{l_1}E_1 - u^{e-(p-1)l_1} a_{12}^p}{u^{pl_2}} a_{23}^p\big)^* \equiv$$
$$\pi^e a_{13}^* + a_{12}^*[E_1](\pi) - \frac{\pi^e a_{12}^* + \pi^{l_1}[E_1](\pi) - \pi^{e-(p-1)l_1} a_{12}^p}{\pi^{pl_2}} (a_{23}^*)^p \mod \pi^{pl_3}.$$

This gives the result.

We now prove that the congruence $a_{12} \equiv u^{l_1 - l_2} a_{23} \mod u^{l_3}$, in the Breuil-Kisin side, is implied by the others. We first observe that by the Breuil Kisin congruence in **E**, and since $a_{23}^p \equiv 0 \mod u^{l_3}$, we have

$$a_{12}E_1 \equiv -u^{e-(p-1)l_1} a_{13}^p \mod u^{l_3}.$$

So, using $a_{13}^p \equiv a_{23} \frac{a_{12}^p}{u^{l_2}} \mod u^{l_3}$, it follows that

$$a_{12}E_1 \equiv -u^{e-(p-1)l_1} a_{23} \frac{a_{12}^p}{u^{l_2}} \mod u^{l_3}. \tag{8.7}$$

But if we divide $u^e a_{12} - u^{l_1} E_1 \equiv u^{e-(p-1)l_1} a_{12}^p \mod u^{l_2 p}$ by u^{l_2}, and we consider what we obtain modulo u^{l_3}, we get

$$-u^{l_1 - l_2} E_1 \equiv u^{e-(p-1)l_1} \frac{a_{12}^p}{u^{l_2}} \mod u^{l_3}.$$

Putting this congruence inside (8.7) one gets the claim. Finally the sets of congruences on the left is equivalent to the set of congruences on the right.

8.4. Five lemmas

The lemmas in this subsection complete the proof of Theorem 8.3.3. We use all the notations introduced in the statement and the proof of the theorem.

8.4.1. — Lemma. *Modulo π^{pl_3}, we have:*

$$\boldsymbol{v}_{12} = \frac{1}{\pi^{pl_2}}\Big(pa_{12} - \pi^{l_1} - \frac{p}{\pi^{(p-1)l_1}}a_{12}^p, \sigma_1(pa_{12}, -\pi^{l_1}) - \sigma_1\big(pa_{12} - \pi^{l_1}, \frac{p}{\pi^{(p-1)l_1}}a_{12}^p\big), 0, \dots\Big).$$

Proof. — We will compute $\pi^{pl_2}\boldsymbol{v}_{12} = p[a_{12}] - [\pi^{l_1}] - T_{p[\pi^{l_1}]/\pi^{pl_1}}[(a_{12})^p]$ modulo $\pi^{p(l_2+l_3)}$. Since $v(a_{12}) \geqslant l_2/p$, we obtain $v(S_i([a_{12}], [a_{12}])) \geqslant l_2 p^{i-1}$ for each $i \in \mathbb{N}$. For $i \geqslant 3$, we have $l_2 p^{i-1} \geqslant l_2 p^2 \geqslant pl_2 + pl_3$, hence

$$p[a_{12}] = \Big(pa_{12}, (1-p^{p-1})(a_{12})^p, *p^{p-1}(a_{12})^{p^2}, \dots\Big) \in \widehat{W}(R/\pi^{p(l_2+l_3)}R),$$

with $v(*) \geqslant 0$. Note that

$$v(p^{p-1}(a_{12})^{p^2}) \geqslant e(p-1) + pl_2 \geqslant l_3(p-1)^2 + pl_2 \geqslant pl_2 + pl_3$$

so finally

$$p[a_{12}] = \big(pa_{12}, (1-p^{p-1})(a_{12})^p, 0, \dots\big) \in \widehat{W}(R/\pi^{p(l_2+l_3)}R).$$

We now compute:

$$\begin{aligned} &p[a_{12}] - [\pi^{l_1}] \\ &\quad = \big(pa_{12} - \pi^{l_1}, (1-p^{p-1})(a_{12})^p + \sigma_1(pa_{12}, -\pi^{l_1}), S_2(p[a_{12}], -[\pi^{l_1}]), \dots\big). \end{aligned}$$

Using the minorations $v(pa_{12}) \geqslant e$, $v(1-p^{p-1})(a_{12})^p \geqslant l_2$, $v(\pi^{l_1}) = l_1$, we obtain $S_i(p[a_{12}], -[\pi^{l_1}]) = 0$ in $R/\pi^{p(l_2+l_3)}R$.

$$\begin{aligned} v(\sigma_2(pa_{12}, -\pi^{l_1})) &\geqslant (p^2-1)l_1 + e \\ &\geqslant (p^2-1)l_1 + (p-1)l_1 = pl_1 + (p^2-2)l_1 \geqslant pl_2 + pl_3 \end{aligned}$$

so finally

$$p[a_{12}] - [\pi^{l_1}] = \big(pa_{12} - \pi^{l_1}, (1-p^{p-1})(a_{12})^p + \sigma_1(pa_{12}, -\pi^{l_1}), 0, \dots\big).$$

The last term contributing to $\boldsymbol{v}_{12}$ is

$$\begin{aligned} &T_{p[\pi^{l_1}]/\pi^{pl_1}}[(a_{12})^p] \\ &\qquad = \left(\frac{p\pi^{l_1}}{\pi^{pl_1}}(a_{12})^p, (1-p^{p-1})(a_{12})^p, 0\dots\right) \in \widehat{W}(R/\pi^{p(l_2+l_3)}R). \end{aligned}$$

We add up and we obtain the lemma. □

8.4.2. — Lemma. *In $\widehat{W}(R/\pi^{pl_3}R)$, we have the equality:*

$$T_{v_{12}}[(a_{23})^p] = \left(\frac{(a_{23})^p}{\pi^{pl_2}} \left(pa_{12} - \pi^{l_1} - \frac{p}{\pi^{(p-1)l_1}}(a_{12})^p \right), \frac{(a_{23})^p}{\pi^{pl_2}} \sigma_1 \left(pa_{12}, -\pi^{l_1} \right), 0, \dots \right).$$

Proof. — Now we can compute, in $\widehat{W}(R/\pi^{pl_3}R)$ this time:

$$T_{v_{12}}[(a_{23})^p] = \left(\frac{(a_{23})^p}{\pi^{pl_2}} \left(pa_{12} - \pi^{l_1} - \frac{p}{\pi^{(p-1)l_1}}(a_{12})^p \right), \right.$$
$$\left. \frac{(a_{23})^p}{\pi^{pl_2}} \sigma_1 \left(pa_{12}, -\pi^{l_1} \right) + \frac{(a_{23})^p}{\pi^{pl_2}} \sigma_1 \left(pa_{12} - \pi^{l_1}, \frac{p}{\pi^{(p-1)l_1}}(a_{12})^p \right), 0, \dots \right).$$

We simplify a little bit. Using the identity $\sigma_1(x,y) = \sigma_1(x, -y-x)$, we get

$$\sigma_1 \left(pa_{12} - \pi^{l_1}, \frac{p}{\pi^{(p-1)l_1}}(a_{12})^p \right) = \sigma_1 \left(pa_{12} - \pi^{l_1}, -\frac{p}{\pi^{(p-1)l_1}}(a_{12})^p + \pi^{l_1} - pa_{12} \right).$$

We use the inequality $v(\sigma_1(a,b)) \geqslant \min((p-1)v(a)+v(b), (p-1)v(b)+v(a))$ from Lemma 8.1.2(4). In our case $a = pa_{12} - \pi^{l_1}$ has valuation l_1 and $b = -\frac{p}{\pi^{(p-1)l_1}}(a_{12})^p + \pi^{l_1} - pa_{12}$ has valuation at least pl_2, and we find

$$v \left(\frac{(a_{23})^p}{\pi^{pl_2}} \sigma_1(a,b) \right) \geqslant l_3 - pl_2 + \min \left((p-1)l_1 + pl_2, l_1 + (p-1)pl_2 \right) \geqslant pl_3$$

so this term vanishes. Finally we obtain the lemma. □

8.4.3. — Lemma. *We have the following equalities in $\widehat{W}(R/\pi^{pl_3}R)$:*

$$\begin{aligned} p[a_{13}] - [a_{12}] - T_{v_{12}}[(a_{23})^p] &= (pa_{13} - a_{12}, (a_{13})^p + \sigma_1(pa_{13}, -a_{12}), 0, \dots) \\ &\quad - \left(\frac{(a_{23})^p}{\pi^{pl_2}} \left(pa_{12} - \pi^{l_1} - \frac{p}{\pi^{(p-1)l_1}}(a_{12})^p \right), \frac{(a_{23})^p}{\pi^{pl_2}} \sigma_1 \left(pa_{12}, -\pi^{l_1} \right), 0, \dots \right) \\ &= (c_0, c_1, c_2, \dots) \end{aligned}$$

with

$$\begin{aligned} c_0 &= pa_{13} - a_{12} - \tfrac{(a_{23})^p}{\pi^{pl_2}} \left(pa_{12} - \pi^{l_1} - \tfrac{p}{\pi^{(p-1)l_1}}(a_{12})^p \right) \\ c_1 &= (a_{13})^p \end{aligned}$$

and $c_i = 0$, $i \geqslant 2$.

Proof. — We have

$$\begin{aligned}&p[a_{13}]-[a_{12}]\\&\quad=(pa_{13},(a_{13})^p,0,\dots)-(a_{12},0,\dots)\\&\quad=(pa_{13}-a_{12},(a_{13})^p+\sigma_1(pa_{13},-a_{12}),\sigma_2(pa_{13},-a_{12}),\dots)\in\widehat{W}(R/\pi^{pl_3}R).\end{aligned}$$

Recall from Lemma 8.1.2(4) that

$$v(\sigma_2(a,b))\geqslant\min\left((p^2-1)v(a)+v(b),(p^2-1)v(b)+v(a)\right).$$

Using this we see immediately that $\sigma_2(pa_{13},-a_{12})\equiv 0 \mod \pi^{pl_3}$ so that

$$p[a_{13}]-[a_{12}]=(pa_{13}-a_{12},(a_{13})^p+\sigma_1(pa_{13},-a_{12}),0,\dots)\in\widehat{W}(R/\pi^{pl_3}R).$$

So c_0 is as in the statement and

$$\begin{aligned}c_1=(a_{13})^p+\sigma_1(pa_{13},-a_{12})-\frac{(a_{23})^p}{\pi^{pl_2}}\sigma_1\left(pa_{12},-\pi^{l_1}\right)\\+\sigma_1\left(pa_{13}-a_{12},-\frac{(a_{23})^p}{\pi^{pl_2}}\left(pa_{12}-\pi^{l_1}-\frac{p}{\pi^{(p-1)l_1}}(a_{12})^p\right)\right).\end{aligned}$$

Then we have $v(\sigma_1(pa_{13},-a_{12}))\geqslant e+(p-1)l_2/p\geqslant(p-1)l_1\geqslant pl_3$,

$$v\left(\tfrac{(a_{23})^p}{\pi^{pl_2}}\sigma_1\left(pa_{12},-\pi^{l_1}\right)\right)\geqslant l_3-pl_2+l_1(p-1)+e+l_2/p\geqslant pl_3,$$

$$v\left(\sigma_1\left(pa_{13}-a_{12},-\tfrac{(a_{23})^p}{\pi^{pl_2}}\left(pa_{12}-\pi^{l_1}-\tfrac{p}{\pi^{(p-1)l_1}}(a_{12})^p\right)\right)\right)\geqslant l_1/p+(p-1)l_3\geqslant pl_3.$$

□

8.4.4. — Lemma. *For $\boldsymbol{u}_{13}=(u_0,u_1,\dots)$, the condition*

$$p[a_{13}]-[a_{12}]-T_{p[\pi^{l_1}]/\pi^{pl_1}}\boldsymbol{u}_{13}-T_{\boldsymbol{v}_{12}}[a_{23}^p]\equiv 0 \mod \pi^{pl_3}.$$

implies in $R/\pi^{pl_3}R$:

$$c_0=\tfrac{p}{\pi^{(p-1)l_1}}u_0$$

$$c_1-u_0=\left(\tfrac{p}{\pi^{(p-1)l_1}}\right)^p u_1$$

$$\sigma_1(c_1,-u_0)-u_1=0.$$

Proof. — Since $\frac{p[\pi^{l_1}]}{\pi^{pl_1}}\equiv\left(\frac{p}{\pi^{(p-1)l_1}},1,0,\dots\right)$ modulo π^{pl_3}, then

$$T_{\frac{p[\pi^{l_1}]}{\pi^{pl_1}}}\boldsymbol{u}_{13}\equiv\left[\frac{p}{\pi^{(p-1)l_1}}\right]\boldsymbol{u}_{13}+V\boldsymbol{u}_{13} \mod \pi^{pl_3}.$$

Then by the condition in the statement it follows

$$\Big[\frac{p}{\pi^{(p-1)l_1}}\Big]\boldsymbol{u}_{13} = -V\boldsymbol{u}_{13} + (c_0, c_1, 0, \dots) = -(0, u_0, u_1, \dots) + (c_0, c_1, 0, \dots).$$

Remark that $v(c_0) \geqslant \frac{l_2}{p}$ and $v(c_1) \geqslant l_3/p$. Also note that by Remark 8.3.2 it follows that $v(u_i) \geqslant l_3/p$, for all $i \geqslant 0$. We deduce:

$$\begin{aligned}&\Big[\frac{p}{\pi^{(p-1)l_1}}\Big]\boldsymbol{u}_{13}\\ &\quad= \Big(c_0, c_1 - u_0, \sigma_1(c_1, -u_0) - u_1, -u_2, \dots, -u_k, 0, \dots\Big) \in \widehat{W}(R/\pi^{pl_3}R)\end{aligned}$$

where u_k is by definition the last nonzero term in $\boldsymbol{u}_{13}$ and $-u_k$ occurs here at the $(k+1)$-th place. On the other hand,

$$\begin{aligned}&\Big[\frac{p}{\pi^{(p-1)l_1}}\Big]\boldsymbol{u}_{13}\\ &= \Big(\frac{p}{\pi^{(p-1)l_1}}u_0, \Big(\frac{p}{\pi^{(p-1)l_1}}\Big)^p u_1, \Big(\frac{p}{\pi^{(p-1)l_1}}\Big)^{p^2} u_2, \dots, \Big(\frac{p}{\pi^{(p-1)l_1}}\Big)^{p^k} u_k, 0, \dots\Big)\end{aligned}$$

where here the term involving u_k occurs at the k-th place. This is not possible if $k \geqslant 2$. Hence $k \leqslant 1$ and $\boldsymbol{u}_{13} = (u_0, u_1, 0, \dots) \in \widehat{W}(R/\pi^{pl_3}R)$. And we obtain the expected formulas. □

8.4.5. — Lemma. *We have $u_1 = 0$. Therefore $u_0 = a_{13}^p$ and the condition of the previous lemma is equivalent to the congruence:*

$$\frac{p}{\pi^{(p-1)l_1}}a_{13}^p \equiv pa_{13} - a_{12} - a_{23}^p\,\frac{pa_{12} - \pi^{l_1} - \frac{p}{\pi^{(p-1)l_1}}a_{12}^p}{\pi^{pl_2}} \mod \pi^{pl_3}.$$

Proof. — We have $u_0 = c_1 - \Big(\frac{p}{\pi^{(p-1)l_1}}\Big)^p \sigma_1(c_1, -u_0)$. Since c_1 divides $\sigma_1(c_1, -u_0) \in R/\pi^{pl_3}R$, $u_0 = c_1u_0'$ with $v(u_0') \geqslant 0$. Write $\beta = c_1\Big(\frac{p}{\pi^{(p-1)l_1}}\Big)$ then

$$c_0 = \beta - \Big(\frac{p}{\pi^{(p-1)l_1}}\Big)\beta^p\sigma_1(1, u_0')$$

and $v(\beta) \geqslant v(c_1) \geqslant l_3/p$. We obtain

$$\begin{aligned}\beta &= c_0 + \Big(\frac{p}{\pi^{(p-1)l_1}}\Big)\sigma_1(1, u_0')(c_0 + \Big(\frac{p}{\pi^{(p-1)l_1}}\Big)\beta^p\sigma_1(1, u_0'))^p\\ &= c_0 + \Big(\frac{p}{\pi^{(p-1)l_1}}\Big)\sigma_1(1, u_0')c_0^p \in R/\pi^{pl_3}R.\end{aligned}$$

Recall that $c_0 = pa_{13} - a_{12} - \frac{(a_{23})^p}{\pi^{pl_2}}\left(pa_{12} - \pi^{l_1} - \frac{p}{\pi^{(p-1)l_1}}(a_{12})^p\right)$. Hence $c_0^p = -a_{12}^p \in R/\pi^{pl_3}R$. Now we come back to the congruence

$$pa_{12} - \pi^{l_1} - \frac{p}{\pi^{(p-1)l_1}}(a_{12})^p \equiv 0 \mod \pi^{pl_2}.$$

If $e+v(a_{12}) \leqslant e-l_1(p-1)+pv(a_{12})$ then $v(a_{12}) \geqslant l_1$ and $a_{12}^p = 0 \in R/\pi^{pl_3}R$. If $e + v(a_{12}) > e - l_1(p-1) + pv(a_{12})$, then $e - l_1(p-1) + pv(a_{12}) \geqslant \min(pl_2, l_1)$ and $\left(\frac{p}{\pi^{(p-1)l_1}}\right)a_{12}^p = 0 \in R/\pi^{pl_3}R$. Hence $\beta = c_0 \in R/\pi^{pl_3}R$. Since $\beta = \left(\frac{p}{\pi^{(p-1)l_1}}\right)c_1$, we obtain the lemma. □

8.5. Conclusion

The case $l_1 < pl_3$ excluded in Proposition 8.3.3 shows the complexity of the ramification. To achieve this case, we should compute the integrality conditions with matrices with non-Teichmüller entries (see the introduction of Section 8). More generally, for $n \geqslant 4$, in order to compute the Breuil-Kisin modules of Kummer groups, we need to define adapted liftings of parameters to R. In view of Theorem 4.2.2, these choices should be related to $E(u) \mod p^n$ in some way.

We have seen that any μ-matrix has to satisfy the condition $\mathcal{U}A/\mathcal{L}A \geqslant 0$. This condition is not present in the context of the classification of Kummer group schemes. And in the case $n = 2$ and $n = 3$ (with $l_1 \geqslant pl_3$ and matrices with Teichmüller entries) we have seen that in fact this condition is consequence of the others. We do not know if we could remove this condition in the classification of μ-matrices.

Let us emphasize that the explicit formulas for Kummer subgroups are relevant not only in the perpective of classification of Hopf orders of rank p^n ([8], [13]) but also for the computation of dimension and irreducible components ([6],[14]) of Kisin's variety parametrizing some group schemes over $\mathcal{O}_K$ ([17]). At last, Kummer group schemes could be useful to give an explicit form for Breuil-Kisin's equivalence of categories between $(\mathrm{Mod}/\mathfrak{S})$ and the category of finite flat group schemes of p-power order.

BIBLIOGRAPHY

[1] A. Abbes & T. Saito, "Ramification of local fields with imperfect residue fields I", *Amer. J. Math.* **124** (2002), p. 879-920.

[2] D. Abramovich & M. Romagny, "Moduli of Galois covers in mixed characteristics", to appear in Algebra and Number Theory.

[3] C. Breuil, "Schémas en groupes et corps des normes", unpublished manuscript, September 1998.

[4] ———, "Integral p-adic Hodge Theory", in *Algebraic geometry 2000, Azumino (Hotaka)*, Adv. Stud. Pure Math., vol. 36, Math. Soc. Japan, 2002, p. 51-80.

[5] N. P. Byott, "Cleft extensions of Hopf algebras", *Proc. London Math. Soc.* **67** (1993), p. 227-307.

[6] X. Caruso, "Estimation des dimensions de certaines variétés de Kisin", preprint, arXiv:1005.2394.

[7] L. N. Childs, *Taming Wild Extensions: Hopf Algebras and Local Galois Module Theory*, Mathematical Surveys and Monographs, vol. 80, American Mathematical Society, 2000.

[8] L. N. Childs & R. G. Underwood, "Cyclic Hopf orders defined by isogenies of formal groups", *Amer. J. of Math.* **125** (2003), p. 1295-1334.

[9] D. Eisenbud, *Commutative algebra with a view toward algebraic geometry*, Graduate Texts in Math., vol. 150, Springer-Verlag, 1995.

[10] L. Fargues, "La filtration de Harder-Narasimhan des schémas en groupes finis et plats", *J. Reine Angew. Math.* **645** (2010), p. 1-39.

[11] J.-M. Fontaine, "Représentations p-adiques des corps locaux I", in *The Grothendieck Festschrift, Vol. II*, Progr. Math., vol. 87, Birkhäuser, 1990, p. 249-309.

[12] C. Greither, "Extensions of finite group schemes, and Hopf Galois theory over a complete discrete valuation ring", *Math. Z.* **210** (1992), p. 37-67.

[13] C. Greither & L. Childs, "p-Elementary group schemes-constructions and Raynaud's Theory", in *Hopf algebra, Polynomial formal Groups and Raynaud Orders*, vol. 136, Mem. Amer. Soc., 1998, p. 91-118.

[14] N. Imai, "On the connected components of moduli spaces of finite flat models", to appear in Amer. J. Math.

[15] N. Katz & B. Mazur, *Arithmetic moduli of elliptic curves*, Annals of Mathematics Studies, vol. 108, Princeton University Press, 1985.

[16] M. Kisin, "Crystalline representations and F-crystals", in *Algebraic geometry and number theory*, Progr. Math., vol. 253, Birkhäuser, 2006, p. 459-496.

[17] ———, "Moduli of finite flat group schemes, and modularity", *Ann. of Math. (2)* **170** (2009), no. 3, p. 1085-1180.

[18] R. Larson, "Hopf algebra orders determined by group valuations", *J. Algebra* **38** (1976), no. 2, p. 414-452.

[19] E. Lau, "A relation between Dieudonné displays and crystalline Dieudonné theory", preprint, arXiv:1006.2720.

[20] T. Liu, "The correspondence between Barsotti-Tate groups and Kisin modules when $p = 2$", preprint, (2011).

[21] Y. I. Manin, *Cubic forms. Algebra, geometry, arithmetic*, second ed., North-Holland, 1986.

[22] A. Mézard, M. Romagny & D. Tossici, "Sekiguchi-Suwa Theory revisited", preprint, (2011).

[23] M. Romagny, "Effective models of group schemes", to appear in the Journal of Algebraic Geometry.

[24] T. Sekiguchi & N. Oort, F. avd Suwa, "On the deformation of Artin-Schreier to Kummer", *Ann. Sci. École Norm. Sup. (4)* **22** (1989), no. 3, p. 345-375.

[25] T. Sekiguchi & N. Suwa, "On the unified Kummer-Artin-Schreier-Witt Theory", no. 111 in the preprint series of the Laboratoire de Mathématiques Pures de Bordeaux (1999).

[26] ———, "A note on extensions of algebraic and formal groups. IV. Kummer-Artin-Schreier-Witt theory of degree p^2", *Tohoku Math. J. (2)* **53** (2001), no. 2, p. 203-240.

[27] J.-P. Serre, *Corps Locaux*, Hermann, 1980.

[28] J. D. H. Smith, *An introduction to quasigroups and their representations*, Studies in Advanced Mathematics, Chapman & Hall, 2007.

[29] J. Tate & F. Oort, "Group schemes of prime order", *Ann. Sci. Ec. Norm. Sup.* **3** (1970), p. 1-21.

[30] D. Tossici, *Effective models and extension of torsors over a discrete valuation ring of unequal characteristic*, Int. Math. Res. Not. IMRN, 2008, Art. ID rnn111, 68 pp.

[31] ———, "Models of $\mu_{p^2,K}$ over a discrete valuation ring. With an appendix by Xavier Caruso", *J. Algebra* **323** (2010), no. 7, p. 1908-1957.

[32] R. Underwood, "R-Hopf algebra orders in KC_p^2", *J. Alg.* **169** (1994), p. 418-440.

[33] W. Waterhouse & B. Weisfeiler, "One-dimensional affine group schemes", *J. Algebra* **66** (1980), no. 2, p. 550-568.

Manuscrit reçu le 4 mai 2011,
accepté le 21 février 2012.

A. MÉZARD
Institut de Mathématiques de Jussieu,
Université Pierre et Marie Curie,
4 place Jussieu,
75252 Paris Cedex 05,
France
mezard@math.jussieu.fr

M. ROMAGNY
Institut de Recherche Mathématique de Rennes,
Université de Rennes 1,
Campus de Beaulieu,
35042 Rennes Cedex,
France
matthieu.romagny@univ-rennes1.fr

D. TOSSICI
Scuola Normale Superiore di Pisa,
Piazza dei Cavalieri 7,
56126 Pisa,
Italy
dajano.tossici@gmail.com