Models of group schemes of roots of unity

Ariane Mézard, Matthieu Romagny, Dajano Tossici

Work in progress – 10 February 2011

1 Introduction

Let $K$ be a $p$-adic field with ring of integers $O_K$. The object of the present paper is the determination of all possible models over $O_K$ 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 $(\mathbb{Z}/p^n\mathbb{Z})_K$. We aim at the most complete possible description, including the precise situation of these groups in the general theory but also their most down-to-earth features, e.g. their equations.

We briefly indicate two of our motivations. Firstly, in the study of the representations of the Galois group of a $p$-adic local field $K$, finite flat group schemes and $p$-divisible groups are extremely important examples of crystalline representations. Results of Fontaine, Breuil and Kisin have culminated into a fairly nice description of these groups in terms of modules with semilinear Frobenius. This description remains however very abstract and does not allow an easy manipulation of the group schemes, making it impossible to compute with them and to implement the results of the general theory (e.g. filtrations – Abbes-Saito and Harder-Narasimhan-Fargues...) We would like to be able to perform such computations for $\mu_{p^n}$ and $\mathbb{Z}/p^n\mathbb{Z}$. Secondly, we are interested in the reduction problem for Galois covers of $K$-varieties. The most classical examples are covers of curves (isogenies of elliptic curves Katz-Mazur [KaMa], or in higher genus see Abramovich-Corti-Vistoli [ACV], Abramovich-Olsson-Vistoli 2008 (1)). It is visible already for isogenies of elliptic curves that it is necessary to let degenerate, along with the varieties, also the Galois group. The existence of such group degenerations is studied more precisely in [Ro]. 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 group schemes, since any finite flat commutative group scheme becomes isomorphic to a product of such after a finite field extension.

Our results are made possible by the interplay between two different approaches, namely that of Breuil-Kisin and that of Sekiguchi-Suwa. The possibility to mix these approaches was suggested to us by work of the third-named author (completed by an appendix of X. Caruso) on models of $\mu_{p^n, K}$, see [To].

Let us fix our notations. Let $p$ be a prime number and $k$ a perfect field of characteristic $p$. We denote by $W = W(k)$ (resp. $W_n = W_n(k)$) the ring of Witt vectors (resp. of truncated Witt vectors) with coefficients in $k$, and we set $S = W[[u]]$ (resp. $S_n = W_n[[u]]$). The rings $S$ and $S_n$ are endowed with a ring endomorphism $\phi$ continuous for the $u$-adic topology, defined as the usual Frobenius on $W_n$ and by $\phi(u) = u^p$. Let $K_0$ be the fraction field of $W$ and fix a totally ramified extension $K$ of $K_0$ of degree $e$ and a uniformizer $\pi$ of $K$. We denote by $E(u)$ the minimal polynomial of $\pi$ over $K_0$ and by $R$ the ring of integers of $K$.

Let us describe briefly the content of this paper. It is divided into two parts: the first part ($\S$2-6) is devoted to Breuil-Kisin theory. First we apply Breuil-Kisin theory in order to

\[\text{1 Improve these citations}\]
parametrize models of $\mu_{p^n}$ in terms of Breuil-Kisin modules ($\S 2$). Then we develop the theory of loop of lattice matrices ($\S 3$) allowing us to rewrite Breuil-Kisin modules in matricial terms ($\S 4$). The main result of this first part is Theorem [?] which is a computable interpretation of Breuil-Kisin theory. As a first application, we complete the parametrization of models of $\mu_{p^n}$. The second part is devoted to Sekiguchi-Suwa theory ($\S 7-9$). We recall their theory ($\S 7$) and we give a computable presentation of their results ($\S 8$). Then we proceed with the explicit computation of models of $\mu_{p^n}$. As a conclusion ($\S 10$), we compare the two approaches and suggest many open questions.

2 Breuil-Kisin modules

2.1 Breuil-Kisin modules and finite flat group schemes

In recent papers, Kisin has proven a classification theorem for finite flat $R$-group schemes, in terms of the category $(\text{Mod}/\mathcal{S})$ described as follows:

- objects are $\mathcal{S}$-modules $\mathcal{M}$ of projective dimension 1, killed by some power of $p$, and endowed with a $\phi$-semilinear map $\phi_{\mathcal{M}} : \mathcal{M} \to \mathcal{M}$ such that $E(u)\mathcal{M}$ is contained in the $\mathcal{S}$-module generated by $\phi_{\mathcal{M}}(\mathcal{M})$.

- morphisms are $\mathcal{S}$-linear maps compatible with $\phi$.

The classification of Breuil-Kisin (see [Ki3], thm. 0.7 for $p > 2$ and thm. 0.8 for connected groups for $p = 2$) extended to $p = 2$ by Lau and Liu (see [La], [Li]) is the following:

2.1.1 Theorem. There is a contravariant exact equivalence of categories between $(\text{Mod}/\mathcal{S})$ and the category of finite flat $R$-group schemes of $p$-power order.

One may compose with the Cartier duality functor to get a covariant equivalence.

In the sequel, we will very often write simply $\phi$ for $\phi_{\mathcal{M}}$, $\mathcal{M}'$ for the module $\phi^*\mathcal{M} := \mathcal{M} \otimes_{\mathcal{S}} \mathcal{S}$ and $\phi' : \mathcal{M}' \to \mathcal{M}$ for the linear map associated to $\phi$.

2.2 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 $(\text{Mod}/\mathcal{S})$ of modules killed by $p^n$, based on the following lemma.

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

Proof: It follows from [Ki2], lemma 2.3.2 that $\mathcal{M}$ has projective dimension 1 if and only if it is an iterated extension of finite free $\mathcal{S}/p\mathcal{S}$-modules. By induction, it is immediate that this is equivalent to the fact that $\mathcal{M}$ is a finite $\mathcal{S}_n$-module without $u$-torsion.

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

- objects are finite $\mathcal{S}_n$-modules $\mathcal{M}$ with no $u$-torsion endowed with a $\phi$-semilinear map $\phi : \mathcal{M} \to \mathcal{M}$ such that $\text{coker}(\phi')$ is killed by $E(u)$.

- morphisms are $\mathcal{S}_n$-linear maps compatible with $\phi$. 

2
We now study more closely this category. In the sequel, we use without mention the following basic fact.

2.2.2 **Lemma.** For any object $\mathfrak{M}$ of $(\text{Mod }/\mathcal{S})_n$ the map $\phi' : \mathfrak{M} \to \mathfrak{M}$ is injective.

**Proof:** This is [Kil], lemma 1.1.9. □

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

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

By theorem 2.1.1, there is on $(\text{Mod }/\mathcal{S})_n$ a contravariant exact involutive equivalence given by Cartier duality. It follows that $(\text{Mod }/\mathcal{S})_n$ has cokernels and coimages. □

2.2.4 **Remark.** In general, for a morphism $f : \mathfrak{M} \to \mathfrak{N}$ the objects $\text{coker}(\text{ker}(f))$ and $\text{ker}(\text{coker}(f))$ are not isomorphic. In the category $(\text{Mod }/\mathcal{S})_n$ 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 $\text{ker}(u) = \text{coker}(u) = 0$ even though $u$ is not an isomorphism.

2.3 **Breuil-Kisin modules of models of $\mu_{p^n}$**

The $\mathcal{S}$-module associated to the group scheme $\mu_{p^n,R}$ via the Breuil-Kisin theory is $\mathfrak{M} = \mathcal{S}_n$ with its usual Frobenius. Moreover, for two group schemes $G,G'$ with modules $\mathcal{S},\mathcal{S}'$, if we denote by $\overline{K}$ an algebraic closure of $K$ then 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 of $K$. From this we deduce that $\mathfrak{M}$ is the module associated to a model of $\mu_{p^n,R}$ if and only if $\mathfrak{M}[1/u]$ is isomorphic to $\mathcal{S}_n[1/u] = W_n((u))$ with its Frobenius. Since $\mathfrak{M}$ has no $u$-torsion, we may see it as a submodule of $W_n((u))$. This leads us to consider lattices that is to say finite sub-$W_n[[u]]$-modules $\mathfrak{M} \subset W_n((u))$ such that $\mathfrak{M}[1/u] = W_n((u))$. Then for the classification of models of $\mu_{p^n,R}$ it is enough to consider the following category $\mathcal{C}_n$:

- objects are lattices $\mathfrak{M} \subset W_n((u))$ such that $E(u)\mathfrak{M} \subset \langle \phi(\mathfrak{M}) \rangle \subset \mathfrak{M}$;
- morphisms are the inclusions.

Here $\phi$ is simply the Frobenius endomorphism of $W_n((u))$. There is a natural embedding $\mathcal{C}_n \to (\text{Mod }/\mathcal{S})_n$ whose essential image is the subcategory of modules whose associated group scheme is a model of $\mu_{p^n}$. 

3
3 The loop of lattice matrices

In this section, we present the algebraic machinery necessary for an efficient manipulation of lattices.

Let $\mathfrak{R}$ be a perfect ring of characteristic $p$ and let $W(\mathfrak{R})$ (resp. $W_n(\mathfrak{R})$) be the ring of infinite Witt vectors (resp. $n$-truncated Witt vectors).

3.1 Teichmüller representatives of Witt vectors

We recall that there exists a sequence of universal polynomials $S_i = S_i(X_0, \ldots, X_i) \in \mathbb{Z}[X_0, X_1, X_2, \ldots]$, for $i \geq 0$, giving the addition of two vectors $a = (a_0, a_1, a_2, \ldots)$ and $b = (b_0, b_1, b_2, \ldots)$ in the ring $W(\mathfrak{R})$ by the rule

$$a + b = (S_0(a, b), S_1(a, b), S_2(a, b), \ldots).$$

Moreover, all elements have $p$-adic expansions

$$a = (a_0, a_1, a_2, \ldots) = [a_0] + [a_1/p] p + [a_2/p^2] p^2 + \ldots$$

where $[x] := (x, 0, 0, \ldots)$ is the Teichmüller lift of $x \in \mathfrak{R}$. (Note that in the sequel, we will rather write $p$-adic expansions in the form $a = [a_0] + [a_1] p + [a_2] p^2 + \ldots$) Hence the functions $S_i$ defined by $S_i(a, b) := S_i(a, b)^{1/p^i}$ satisfy

$$a + b = [S_0(a, b)] + [S_1(a, b)] p + [S_2(a, b)] p^2 + \ldots$$

In fact, we can define functions $S_i$ in any number $r$ of variables by the identity

$$a_1 + \cdots + a_r = [S_0(a_1, \ldots, a_r)] + [S_1(a_1, \ldots, a_r)] p + [S_2(a_1, \ldots, a_r)] p^2 + \ldots$$

3.2 Teichmüller representatives of series and matrices

We wish to extend the formalism of $p$-adic expansions to the ring of Laurent series $W(\mathfrak{R})((u))$. For this, we extend the definition of Teichmüller lifts to elements $x \in \mathfrak{R}((u))$ as follows: if $x = \sum_{i \gg -\infty} x_i u^i$ ($x_i \in \mathfrak{R}$), we set

$$[x] = \sum_{i \gg -\infty} [x_i] u^i.$$

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

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

Let $a = \sum_{i \gg -\infty} a_i u^i$ and $b = \sum_{i \gg -\infty} b_i u^i$ be Laurent series with coefficients in $\mathfrak{R}$. We extend the definition of $S_i$ by setting

$$S_i(a, b) = \sum_{j \gg -\infty} S_i(a_j, b) u^j$$

and one verifies immediately that the formula $a + b = \sum_{i \gg 0} [S_i(a, b)] p^i$ remains valid.

The multiplicativity formula $[a][b] = [ab]$ valid for $a, b \in \mathfrak{R}$ does not hold any more if $a, b$ are Laurent series. (One notable case when the formula still holds is when $a$ or $b$ is a monomial.) In fact, there are functions $P_i$ such that for any $r$ series $a_s = \sum_{i \gg -\infty} a_{s,i} u^i$ with coefficients in $\mathfrak{R}((u))$ we have

$$[a_1] \ldots [a_r] = [P_0(a_1, \ldots, a_r)] + [P_1(a_1, \ldots, a_r)] p + [P_2(a_1, \ldots, a_r)] p^2 + \ldots$$
It is a simple exercise to verify that

\[ P_j(a_1, \ldots, a_r) = \sum_i S_j(\ldots, a_{1,i_1} \cdots a_{r,i_r}, \ldots) u^i \]

where as an argument of \( S_j \) enter all the finitely many possible products \( a_{1,i_1} \cdots a_{r,i_r} \) indexed by \((i_1, \ldots, i_r)\) such that \( i_1 + \cdots + i_r = i \). For example, if \( a \) and \( b \) are power series \( x, y \) (i.e. Laurent series with nonnegative \( u \)-valuation) we have

\[ P_j(a, b) = \sum_i S_j(a_0 b_i, \ldots, a_i b_0) u^i. \]

There are plenty of formulas relating the \( S_i \) and the \( P_j \), coming from associativity and distributivity of the sum and product of Witt vectors. Here are simple examples:

\[ S_1(x, y, z) = S_1(x, y) + S_1(x + y, z) \]

by associativity of the sum. Also

\[ S_1(x, y - x) = S_1(x, -y) . \]

Indeed, this can be proven over \( \mathbb{Z} \), where it is straightforward using the formula \( S_1(x, y) = \frac{1}{p} (x^p + y^p - (x + y)^p) \).

**3.2.1 Lemma.** Let \( a \) and \( b \) be two power series in \( k[[u]] \). Then we have

\[ \text{val}_u (S_1(a, b)) \geq \max(\text{val}_u(a), \text{val}_u(b)) . \]

**Proof:** This comes from the fact that whenever \( a_i = 0 \) or \( b_i = 0 \), we have \( S_j(a_i, b_i) = 0 \). \( \square \)

### 3.3 Teichmüller representatives 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 \( \mathbb{R}(\!(u)\!) \) (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 \( W(\mathbb{R})(\!(u)\!) \), but we will have no need for this. For us, the most important vector will be

\[ p^* = \begin{pmatrix} 1 \\ p \\ p^2 \\ \vdots \end{pmatrix} \]

which for convenience may denote a vector with finitely, or infinitely many, coefficients. Thus if \( x \in W_n(\mathbb{R})(\!(u)\!)^n \) is a vector with components \( x_1, \ldots, x_n \) we have

\[ t x p^* = x_1 + x_2 p + \cdots + x_n p^{n-1} . \]

If the \( x_i \) are Teichmüller representatives, then this linear combination is called a \( T \)-combination. Of course, any linear combination is equal to a \( T \)-combination:
3.3.1 Lemma. There is a map \( \rho \) that associates to any rectangular matrix \( A \) with entries in \( W_n(\mathcal{R})(\!(u)\!) \) the unique matrix \( \rho(A) \) of the same size with entries in \( \mathcal{R}(\!(u)\!) \) such that

\[
Ap^* = [\rho(A)]p^*.
\]

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 \( Ap^* = [\rho(A)]p^* \) 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 \( A = (a_1 \ldots a_n) \). 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 \( \rho(A) = (a'_1 \ldots a'_n) \). The remaining assertions are clear. \( \square \)

There is an algorithmic point of view on the computation of \( \rho(A) \) that will be useful. It can be stated for arbitrary square matrices with entries in \( W(\mathcal{R})(\!(u)\!) \), but we will mainly manipulate particular square upper-triangular matrices and hence specialize to this case. For the statement, we introduce some convenient terminology. For a coefficient in position \((i,j)\) in a square matrix, we will call \textit{index} the difference \( j - i \). We call \textit{k-diagonal} the set of coefficients on the line \( j - i = k \). Thus the 0-diagonal is just the usual diagonal, and the index \( k \) is a measure of the distance to the diagonal.

3.3.2 Lemma. Let \( E \) be the set of upper-triangular square matrices of size \( n \) with entries in \( W(\mathcal{R})(\!(u)\!) \) with Teichmüller diagonal entries. Define a function \( F : E \to E \) 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 \( a_{i,v} \) and write the truncated \( p \)-adic expansion

\[
a_{i,v}p^{v-1} = [a'_{i,v}] p^{v-1} + \cdots + [a'_{i,n}] p^{n-1} \mod p^n.
\]

Then replace \( a_{i,v} \) by \( [a'_{i,v}] \) and for \( j > i \) replace \( a_{ij} \) by \( a_{ij} + [a'_{ij}] \). After the step \( i = n \) has been accomplished, call the result \( F(A) \). Then, for all \( k \geq 0 \) we have:

- the coefficients of index \( \leq k \) of the matrix \( F^k(A) \) are Teichmüller.

- \( F^k(A) p^* = A p^* \).

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

Proof: This is obvious. \( \square \)

3.4 The loop of lattice matrices

We start with some definitions from quasigroup theory. A \textit{magma} is a set \( X \) endowed with a binary operation \( X \times X \to X \), \((x,y) \mapsto xy\) usually called multiplication. A \textit{submagma} is a subset \( Y \subset X \) that is closed under multiplication. A \textit{quasigroup} is a magma where left and right division are always possible, i.e. 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 \textit{loop} 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. The notion of a magma homomorphism is defined in the obvious way, and a quasigroup homomorphism or a loop homomorphism is a magma homomorphism.

The lattices involved in the Breuil-Kisin classification appear naturally as objects in a certain loop which we call the loop of lattice matrices and denote by \( \mathcal{G}_n((u)) \). As a set, it is composed of the upper-triangular matrices of the form

\[
M(l, a) = \begin{pmatrix}
  u^{l_1} & a_{12} & a_{13} & \cdots & a_{1n} \\
  u^{l_2} & a_{23} & a_{24} & \cdots & a_{2n} \\
  \ddots & \ddots & \ddots & \ddots & \vdots \\
  u^{l_{n-1}} & a_{n-1,n} & \cdots & \cdots & a_{nn} \\
  0 & 0 & 0 & \cdots & u^{l_n}
\end{pmatrix}
\]

with \( l = (l_1, \ldots, l_n) \in \mathbb{Z}^n \) and \( a = (a_{ij})_{1 \leq i < j \leq n} \) where \( a_{ij} \in \mathfrak{R}((u)) \). There is a natural subset \( \mathcal{G}_n[u, u^{-1}] \) composed of matrices with coefficients in \( \mathfrak{R}[u, u^{-1}] \).

Note that as a general rule, we write \( a_{ij} \) instead of \( a_{i,j} \), unless this can disturb comprehension like for \( a_{np,n} \). In order to keep the notation light, we do not specify the coefficient ring \( \mathfrak{R} \) in the symbols \( \mathcal{G}_n((u)) \) and \( \mathcal{G}_n[u, u^{-1}] \).

If \( A, B \) are square matrices with entries in \( \mathfrak{R}((u)) \), we set \( A \ast B = \rho([A][B]) \) where \( \rho \) is the map from lemma 3.3.1. This matrix is characterized by the equality

\[
\]

By lemma 3.3.1, if \( A, B \) are in \( \mathcal{G}_n((u)) \) resp. in \( \mathcal{G}_n[u, u^{-1}] \), then \( A \ast B \) also. It is clear that the identity matrix is a neutral element for this multiplication. Thus the triple \( (\mathcal{G}_n((u)), \ast, \text{Id}) \) is a magma with identity. At this point, the reader may wish to have a look at the shape of the multiplication \( \ast \) in the examples of 3.7 below.

We will now prove that \( \mathcal{G}_n((u)), \ast, \text{Id} \) is a loop.

3.4.1 Lemma. Let \( A = M(l, a) \) and \( B = M(m, b) \) be in \( \mathcal{G}_n((u)) \). Then a coefficient \( (i, j) \) of index \( j - i \geq 1 \) of \( A \ast B \) has the following form:

\[
u^{m_j}a_{ij} + u^{l_i}b_{ij} + \text{terms containing coefficients } a_{i'j'} \text{ and } b_{i'j'} \text{ of index } j' - i' < j - i .
\]

Proof: The entry of \([A][B]\) in position \((i, j)\) is

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

The coefficients \([a_{ik}]\) and \([b_{kj}]\) in the middle sum have index strictly less than \( j - i \). When applying the algorithm of lemma 3.3.2 to compute \( A \ast B \), at each step the entry \((i, j)\) is replaced by itself plus some terms involving coefficients \( a_{st} \) and \( b_{st} \) of index \( t - s < j - i \). This proves the claim.

3.4.2 Lemma. For \( A, B \in \mathcal{G}_n \) the maps \( L_A : B \mapsto A \ast B \) and \( R_B : A \mapsto A \ast B \) are bijections, thus the triple \( (\mathcal{G}_n((u)), \ast, \text{Id}) \) is a loop.

Proof: The argument is the same for \( L_A \) and \( R_B \) so we do only the case of \( L_A \). Assume that \( A \ast B = C \) with \( A = M(l, a) \), \( B = M(m, b) \), \( C = M(n, c) \). We fix \( A \) and \( C \) and try to solve for \( B \). We determine its entries by increasing induction on the index \( k \). For \( k = 0 \) it is clear that
we have \( m_i = n_i - l_i \). By induction, using lemma 3.4.1, it follows directly that the coefficients \( b_{ij} \) of index \( k \) are determined by the entries of \( A, C \) and the coefficients \( b_{ij'} \) of lower index. □

There is a morphism of loops \( \varphi : \mathcal{G}_n((u)) \to \mathbb{Z}^n \) to the additive group \( \mathbb{Z}^n \) that maps \( A \) to the tuple of its diagonal exponents. The kernel \( \mathcal{U}_n((u)) = \ker(\varphi) \) is a subloop \(^2\), and \( \mathcal{U}_n[u, u^{-1}] = \mathcal{U}_n((u)) \cap \mathcal{U}_n[u, u^{-1}] \) is a subloop of \( \mathcal{U}_n[u, u^{-1}] \).

### 3.5 Positive elements

There is a natural subset \( \mathcal{G}_n[[u]] \subset \mathcal{G}_n((u)) \) composed of matrices with entries in \( \mathcal{R}[[u]] \). It is a submagma, but not a subloop. If \( A \in \mathcal{G}_n[[u]] \) then we say that \( A \) is positive and we write \( A \geq 0 \). Similarly there are submagmas of positive elements \( \mathcal{G}_n[u] = \mathcal{G}_n[u, u^{-1}] \cap \mathcal{G}_n[[u]] \), \( \mathcal{U}_n[u] = \mathcal{U}_n[u, u^{-1}] \cap \mathcal{G}_n[[u]] \) and, \( \mathcal{U}_n[[u]] = \mathcal{U}_n[u, u^{-1}] \cap \mathcal{G}_n[[u]] \). It is easy to verify that in fact \( \mathcal{U}_n[u] \) and \( \mathcal{U}_n[[u]] \) are loops. As we shall see below, for \( n = 3 \) the loop \( \mathcal{U}_3((u)) \) is a group but this is not true any more for \( n \geq 4 \).

An element of \( \mathcal{G}_n[[u]] \) is right invertible if and only if it is left invertible if and only if it lies in the subloop \( \mathcal{U}_n[[u]] \).

### 3.6 The homomorphisms \( U \) and \( L \)

For any square matrix \( A \) of size \( n \) with entries in some ring, we denote by \( U A \) (resp. \( LA \)) the upper left (lower right) square submatrix of size \( n - 1 \), i.e. the matrix obtained by deleting the last (first) row and the last (first) column of \( A \).

#### 3.6.1 Lemma. The mappings \( U : \mathcal{G}_n((u)) \to \mathcal{G}_{n-1}((u)) \) and \( L : \mathcal{G}_n((u)) \to \mathcal{G}_{n-1}((u)) \) are commuting loop homomorphisms.

**Proof:** Let \( \tau_U \) 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 \( \tau_U p^* \) is the vector analogous to \( p^* \) in dimension one less. Then simple matrix formulas yield:

\[
\]

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

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

Finally, the fact that \( U \) and \( L \) commute is clear. □

### 3.7 Examples

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

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

\(^2\)The letter \( \mathcal{U} \) is chosen for “unipotent”. For the moment, it seems that we do not need \( \mathcal{U}_n((u)) \). In the end we do not use it, we will maybe drop it from the paper.
Looking at the above formulas, we see that among the terms involving $S$ and the subloop $U$, the multiplication of $P_1(a_{12}, b_{23})$. It follows that this is zero on the subloop $U$. Question associativity it is enough to look at the terms that contain coming from the operations of Witt vectors, i.e. involving the sum and product functions $S(A, B)$, $S(B, C)$, and $S(C, D)$, with $n$ of matrices. Applying the homomorphism $U$ (lemma 3.6.1), these formulas contain also the formulas for multiplication for $n \leq 4$.

For $n = 2$, the multiplication $*$ is the ordinary multiplication of matrices.

For $n \geq 3$, the multiplication $*$ is not associative. Quite anecdotically, it turns out that for $n = 3$ the restriction of $*$ to the subloop $\mathcal{W}_3((u))$ is associative, i.e. that subloop is a subgroup. Let us see this. We have

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

with

$$(A \ast B)_{13} = u^{l_1}b_{13} + a_{12}b_{23} + u^m a_{13} + S_1(u^{l_1}b_{12}, u^m a_{12})$$

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

$$((A \ast B) \ast C)_{13} = u^{l_1+m_1}c_{13} + (u^{l_1}b_{12} + u^m a_{12})c_{23} + u^{m_3}(u^{l_1}b_{13} + a_{12}b_{23} + u^m a_{13} + S_1(u^{l_1}b_{12}, u^m a_{12})) + S_1(u^{l_1+m_1}c_{12}, u^m(u^{l_1}b_{12} + u^m a_{12}))$$

and

$$(A \ast (B \ast C))_{13} = u^{l_1}(u^{m_1}c_{13} + b_{12}c_{23} + u^m b_{13} + S_1(u^{m_1}c_{12}, u^m b_{12}) + a_{12}(u^m b_{23} + u^m c_{23}) + u^{m_3+n_3}a_{13} + S_1(u^{l_1+m_1}c_{12}, u^m(u^{l_1}b_{12} + u^m b_{12}), u^{m_2+n_2}a_{12})$$

Then, using the formula $S_1(x, y, z) = S_1(x, y) + S_1(x + y, z)$ we compute the difference

$$((A \ast B) \ast C)_{13} - (A \ast (B \ast C))_{13} = S_1(u^{l_1+n_3}b_{12}, u^{m_2+n_3}a_{12}) + S_1(u^{l_1+m_1}c_{12}, u^m(u^{l_1}b_{12} + u^m b_{12})) - S_1(u^{l_1+m_1}c_{12}, u^{l_1+n_2}b_{12}) - S_1(u^{l_1}(u^{m_1}c_{12} + u^m b_{12}), u^{m_2+n_2}a_{12})$$

$$= (u^{n_3} - u^{n_2})S_1(u^{l_1}b_{12}, u^{m_2}a_{12})$$

It follows that this is zero on the subloop $\mathcal{W}_3((u))$, which then is a group.

Now we verify that for $n \geq 4$, the multiplication $*$ is not associative even if we restrict it to the subloop $\mathcal{W}_n((u))$. We shall check this only for $n = 4$. We make the following observation: the multiplication of $\mathcal{W}_n((u))$ 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 $S_i$ and $P_j$. Since the ordinary multiplication of matrices is associative, the terms of the entries in $(A \ast B) \ast C$ and $A \ast (B \ast C)$ that do not involve $S_i$ or $P_j$ are equal. Consequently when we question associativity it is enough to look at the terms that contain $S_i$ or $P_j$.

Once this is said, let us compare the entries in position $(1,4)$ of $(A \ast B) \ast C$ and $A \ast (B \ast C)$. Looking at the above formulas, we see that among the terms involving $S_i$ or $P_j$ the coefficient

$$p_{13} = u^{l_1}b_{13} + a_{12}b_{23} + u^{m_3}a_{13} + S_1(u^{l_1}b_{12}, u^{m_2}a_{12})$$

$$p_{24} = u^{l_2}b_{24} + a_{23}b_{34} + u^{m_4}a_{24} + S_1(u^{l_2}b_{23}, u^{m_3}a_{23})$$

$$p_{14} = u^{l_1}b_{14} + a_{12}b_{24} + a_{13}b_{34} + a_{14}u^{m_4} + S_2(u^{l_1}b_{12}, u^{m_2}a_{12}) + S_1(u^{l_1}b_{13}, a_{12}b_{23}, u^{m_3}a_{13}, S_1(u^{l_1}b_{12}, u^{m_2}a_{12})) + P_1(a_{12}, b_{23})$$
We use the notations \( A \) where \( \lg \) denotes the length as a \( W \) exponents. Then:

\[
\begin{align*}
A_{12} & = c_{12} - u^{n_1-m_1}b_{12} \\
A_{23} & = c_{23} - u^{n_2-m_2}b_{23} \\
A_{13} & = c_{13} - u^{n_1-m_1}b_{13} - c_{12} - u^{n_1-m_1}b_{12}b_{23} - S_1(u^{n_1-m_1}b_{12}, c_{12} - u^{n_1-m_1}b_{12}) \\
b_{12} & = c_{12} - u^{n_2-l_2}a_{12} \\
b_{23} & = c_{23} - u^{n_3-l_3}a_{23} \\
b_{13} & = c_{13} - a_{12} - u^{n_3-l_3}a_{23} - u^{n_3-l_3}a_{13} - S_1(c_{12} - u^{n_2-l_2}a_{12}, u^{n_2-l_2}a_{12})
\end{align*}
\]

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

4 Lattices

From now on, the ring of coefficients \( \mathcal{R} \) is a perfect field \( k \). We use the simplified notations \( W = W(k) \) and \( W_n = W_n(k) \).

4.1 Notations on lattices

We fix an integer \( n \geq 1 \). A lattice of \( W_n((u)) \) is a finitely generated sub-\( W_n([u]) \)-module \( \mathcal{M} \) of \( W_n((u)) \) such that \( \mathcal{M}[1/u] = W_n((u)) \).

We say that a lattice is positive if \( \mathcal{M} \subset W_n([u]) \). In general, there is always an \( \alpha \in \mathbb{Z} \) such that \( u^\alpha \mathcal{M} \subset W_n([u]) \). We define the volume of \( \mathcal{M} \) as

\[
\text{vol(} \mathcal{M} \text{)} = u^{\text{lg}(W_n([u])/u^\alpha \mathcal{M}) - \alpha}
\]

where \( \lg \) denotes the length as a \( W_n([u]) \)-module. Using the fact that \( \text{lg}(W_n([u])/u^\alpha) = n \alpha \), one checks that the definition is indeed independent of \( \alpha \). If \( \mathcal{M} \subset \mathcal{R} \) are lattices then the volume of \( \mathcal{M} \) in \( \mathcal{R} \) is defined as \( \text{vol}_{\mathcal{R}}(\mathcal{M}) = \text{vol}(\mathcal{M})/\text{vol}(\mathcal{R}) \).

For any lattice \( \mathcal{M} \), we define

\[
\mathcal{M}[i] := \ker(p^{n+1-i}: \mathcal{M} \to \mathcal{M})
\]

and

\[
\mathcal{M}(i) = \text{im}(p^{i-1}: \mathcal{M} \to \mathcal{M})
\]

\(^3\text{We do not really care about Moufang loops, but here is why they are important. There is a much nicer theory for Moufang loops than for arbitrary loops (e.g. there are analogues of the theorems of Sylow, Lagrange, and others, for finite Moufang loops; there is a fairly good Lie theory for differentiable Moufang loops, etc). Moufang loops were considered by Manin [Ma] in his study of rational points on cubic hypersurfaces, essentially because the analogue of the addition of elliptic curves in higher dimensions is not associative.}

10
We have decreasing filtrations
\[
\mathfrak{M} = \mathfrak{M}[1] \supseteq \cdots \supseteq \mathfrak{M}[n] \supseteq \mathfrak{M}[n+1] = 0 \\
\mathfrak{M} = \mathfrak{M}(1) \supseteq \cdots \supseteq \mathfrak{M}(n) \supseteq \mathfrak{M}(n+1) = 0 .
\]

For \( j > i \), consider the ideal
\[
(\mathfrak{M}[j] : \mathfrak{M}[i]) = \{ x \in W_n[[u]] , \, x\mathfrak{M}[i] \subset \mathfrak{M}[j] \} .
\]

One can see easily, by inverting \( u \), that \((\mathfrak{M}[j] : \mathfrak{M}[i]) = p^j W_n[[u]] \). (Similarly \((\mathfrak{M}[j] : \mathfrak{M}[i]) = p^j W_n[[u]] \).) From this follows that the quotients \( \mathfrak{M}[i]/\mathfrak{M}[j] \) and \( \mathfrak{M}(i)/\mathfrak{M}(j) \) are naturally submodules of
\[
p^{j-1} W_n((u))/p^{j-1} W_n((u)) \cong W_{j-i}(u)
\]
and they can be viewed as lattices of \( W_{j-i}(u) \) via this canonical isomorphism. In particular, for \( j = n + 1 \) this says that \( \mathfrak{M}[i] \) and \( \mathfrak{M}(i) \) are submodules of \( p^{j-1} W_n((u)) \) and can be viewed as lattices of \( W_{n+1-j}(u) \).

We now study generating systems of lattices. If \( e_1, \ldots, e_n \) is a set of generators for \( \mathfrak{M} \), then as in 3.3 we will call \( T\)-combination a linear combination \( t_1 e_1 + \cdots + t_n e_n \) where \( t_1, \ldots, t_n \) are Teichmüller representatives.

\section*{4.1.1 Lemma.} Let \( \mathfrak{M} \subset W_n((u)) \) be a lattice and \( e_1, \ldots, e_n \) be elements of \( W_n((u)) \) that generate \( \mathfrak{M} \). Then the following conditions are equivalent:
1) For \( 1 \leq i \leq n \), we have \( v_p(e_i) = i-1 \) and \( pe_i \in \langle e_{i+1}, \ldots, e_n \rangle \).

2) For \( 1 \leq i \leq n \), we have \( \mathfrak{M}[i] = \langle e_i, \ldots, e_n \rangle \).

3) For \( 1 \leq i \leq n \), we have \( v_p(e_i) = i-1 \) and moreover each element \( x \in \mathfrak{M} \) can be written in a unique way \( x = [x_1] e_1 + \cdots + [x_n] e_n \) with \( x_i \in k[[u]] \).

\section*{Proof:} We write \( \mathfrak{N}_i = \langle e_1, \ldots, e_n \rangle \). Note that since \( \mathfrak{M} \) is a lattice, we have \( \mathfrak{M}[i] \otimes W_n((u)) = p^{i-1} W_n((u)) \).

1) \( \Rightarrow \) 2). The fact that \( \mathfrak{N}_i \subset \mathfrak{M}[i] \) is obvious, so we only prove the opposite inclusion. Since \( v_p(e_i) = i-1 \), we have \( \mathfrak{M}[i] \otimes W_n((u)) = p^{i-1} W_n((u)) \). 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 \( \nu \) minimal such that \( x_{\nu} \neq 0 \). Then the assumption that \( x \in \mathfrak{M}[i] \) gives \( [x_\nu] e_\nu \in \mathfrak{M}[i] + \mathfrak{N}_{i+1} \). 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 \( \nu \geq i \), so that \( x \in \mathfrak{N}_i \).

2) \( \Rightarrow \) 3). From \( \mathfrak{M}[i] \otimes W_n((u)) = p^{i-1} W_n((u)) \) 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 \( pe_i \in \langle e_{i+1}, \ldots, e_n \rangle \) 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 \( ([x_1] - [x'_1]) e_1 \in \mathfrak{N}_2 \). From the fact that \( \mathfrak{M}[2] : \mathfrak{M}[1] \) it follows that \( [x_1] - [x'_1] \in p W_{n+1}[[u]] \) 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 \( \nu \) is the least integer such that \( x_\nu \neq 0 \). For \( x = pe_i \) we find \( \nu = i + 1 \), so that \( pe_i \in \langle e_{i+1}, \ldots, e_n \rangle \).
4.1.2 Definition. A set of generators \( e_1, \ldots, e_n \) of a lattice \( \mathcal{M} \) satisfying the equivalent conditions of lemma 4.1.1 is called a \( T \)-basis.

4.1.3 Remark. Let \( \mathcal{M} \) be a lattice. We prove in proposition 4.2.4 below that there exists a \( T \)-basis \( e_1, \ldots, e_n \). For such a generating system, there exist series \( b_{ij} \) and a set of equalities

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

for \( 1 \leq i \leq n \). 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 \( \mathcal{M} \) as an abstract \( W_n[[u]] \)-module. We will not need this.

4.2 Matrices and lattices

Let \( \mathcal{L}_n \) be the set of lattices of \( W_n((u)) \). To a matrix \( A \in \mathcal{G}_n((u)) \) we associate the column vector \( e_* = [A]^p \) with components \( e_1, \ldots, e_n \), and the lattice \( \mathcal{M} = \mathcal{M}(A) \) generated by the \( e_i \). This defines a map

\[
\mathcal{G}_n((u)) \rightarrow \mathcal{L}_n , \quad A \mapsto \mathcal{M}(A).
\]

4.2.1 Definition. We say that \( A \in \mathcal{G}_n((u)) \) is a \( T \)-matrix if \( U\mathcal{A}/\mathcal{L} \mathcal{A} \geq 0 \), that is to say, if there exists a matrix \( B \in \mathcal{G}_n[[u]] \) such that \( U\mathcal{A} = B \mathcal{L} \mathcal{A} \). We denote by \( \mathcal{G}_n((u)), \mathcal{G}_n[[u]], \mathcal{G}_n[u, u^{-1}], \mathcal{G}_n^\star[[u]] \) the various sets of \( T \)-matrices.

4.2.2 Lemma. Let \( A \in \mathcal{G}_n((u)), \quad e_* = [A]^p \), \( \mathcal{M} = \mathcal{M}(A) \). Then:

1) \( e_* \) is a \( T \)-basis of \( \mathcal{M} \) if and only if \( A \) is a \( T \)-matrix;

2) \( A \geq 0 \) if and only if \( \mathcal{M} \geq 0 \).

Proof: 1) Due to the shape of matrices in \( \mathcal{G}_n((u)) \), we have \( v_p(e_i) = i - 1 \). It follows from 1) of lemma 4.1.1 that \( e_* \) is a \( T \)-basis if and only if \( pe_i \in \langle e_{i+1}, \ldots, e_n \rangle \) 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 entries \( b_{ij} \in k[[u]] \). It is simple to see that the set of equalities above is equivalent to \( U\mathcal{A} = B \mathcal{L} \mathcal{A} \), i.e. \( A \) is a \( T \)-matrix.

2) We have \( \mathcal{M} \geq 0 \) if and only if \( e_i \in W_n[[u]] \) for all \( i \). Since \( e_i = u^k p^{-1} + [a_{i+1,i}] p^j + \cdots + [a_{i,n}] p^{n-1} \) and expressions as \( T \)-combinations are unique, this means that \( u^k \) and \( a_{ij} \) belong to \( k[[u]] \) for all \( i,j \).

Now we define a section of \( A \rightarrow \mathcal{M}(A) \):

\[
\mathcal{L}_n \rightarrow \mathcal{G}_n^\star[u, u^{-1}] \subset \mathcal{G}_n((u)) , \quad \mathcal{M} \mapsto A(\mathcal{M}).
\]

4.2.3 Definition. We say that \( A = M(l, a) \in \mathcal{G}_n((u)) \) is distinguished if \( A \) is a \( T \)-matrix, its entries are Laurent polynomials, and \( \deg_u(a_{ij}) < l_j \) whenever \( 1 \leq i < j \leq n \).

4.2.4 Proposition. Let \( \mathcal{M} \) be a lattice of \( W_n((u)) \). Then there exists a unique distinguished matrix \( A = A(\mathcal{M}) \) such that \( \mathcal{M}(A) = \mathcal{M} \).
Proof: Since the matrix $A$ that we are looking for is in $G^T_n((u))$, the components of $e_\ast = [A] p^*$ form a $T$-basis. Hence $\mathcal{M}[i]/\mathcal{M}[i+1]$ is generated by the image of $e_i$. This motivates the construction of $e_i = u^{l_i} i^{p-1} + [a_{i+1}] p^i + \cdots + [a_n] p^{n-1}$ by decreasing induction on $i$, as follows. The module $\mathcal{M}[n]$ is isomorphic via a canonical isomorphism to a lattice of $W_1((u)) = k((u))$, hence generated by $u^{l_n}$ for some uniquely defined $l_n \in \mathbb{Z}$. The preimage via this isomorphism of this generator is $e_n = u^{l_n} p^{n-1}$. For $i < n$, assume by induction that $e_{i+1}, \ldots, e_n$ have been constructed. The module $\mathcal{M}[i]/\mathcal{M}[i+1]$ is again isomorphic to a lattice of $k((u))$, generated by $u^{l_i}$ for a unique $l_i \in \mathbb{Z}$. Let $e_i = u^{l_i} p^{i-1} + [a_{i+1}] p^i + \cdots + [a_n] p^{n-1}$ be a lift in $\mathcal{M}[i]$ of this generator. Write $a_{i+1} = a'_{i,i+1} + u^{l_{i+1} + 1} + u^{l_{i+1} + 1}$ where $a'_{i,i+1} \in k[u,u^{-1}]$ is the truncation of $a_{i+1}$ in degree $< l_{i+1}$. Then replacing $e_i$ by $e_i - [a'_{i,i+1}] e_{i+1}$, and rewriting the tail $e_i - [a_{i+1}] p^i$ as a $p$-adic expansion with Teichmüller coefficients, we can fulfill the condition $\deg e_{i+1} < l_{i+1}$. Next we truncate $a_{i,i+2}$ in degree $< l_{i+2}$ and continue as before, etc. This finishes the construction by induction of $e_1, \ldots, e_n$.

The construction in the proof above shows that the volume of a lattice (defined in the beginning of 4.1) can be computed from a $T$-matrix giving rise to it:

4.2.5 Lemma. For $A \in G^T_n((u))$ and $\mathcal{M} = \mathcal{M}(A)$, we have $\text{vol}(\mathcal{M}) = \det(A)$.

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

$$
\begin{array}{ccccccc}
0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 \rightarrow \mathcal{M}[i+1] \rightarrow \mathcal{M}[i] \rightarrow \mathcal{M}[i]/\mathcal{M}[i+1] \rightarrow 0 \\
0 \rightarrow W_{-i}((u)) \rightarrow W_{-i+1}((u)) \rightarrow W_1((u)) \rightarrow 0 \\
0 \rightarrow \mathcal{M}[i+1]^+ \rightarrow \mathcal{M}[i]^+ \rightarrow (\mathcal{M}[i]/\mathcal{M}[i+1])^+ \rightarrow 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0
\end{array}
$$

Since $A \in G_n((u))$, we have $\mathcal{M}[i]/\mathcal{M}[i+1] \simeq u^{l_i} k((u))$ and $(\mathcal{M}[i]/\mathcal{M}[i+1])^+ \simeq k[u]/(u^{l_i})$ 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 $\mathcal{M}$. We have met the kernel $\mathcal{M}[i]$ and the image $\mathcal{M}(i)$ before. The ring $W_n((u))$ is endowed with a Frobenius endomorphism $\varphi$ whose restriction to $W_n$ is the Frobenius of the Witt vectors, and such that $\varphi(u) = u^p$. This gives rise to another interesting lattice, namey the lattice generated by $\varphi(\mathcal{M})$. Also, for a polynomial $E(u) \in W_n[u]$ we can consider the lattice $E(u)\mathcal{M}$. Of course, later on $E(u)$ will be the Eisenstein polynomial of a uniformizer of a totally ramified extension of discrete valuation rings.

If $\mathcal{M} = \mathcal{M}(A)$, we wish to understand the matrices associated to these lattices. For $E(u)\mathcal{M}$, this requires to introduce some notation, before we can explain the result.

4.2.6 Notation. Given a polynomial $E(u) \in W_n[u]$ and a matrix $A \in G_n((u))$, we define a matrix $E(u):A$ as follows. First, for $i \leq n$ we consider the matrix operator $T_i$ taking a square
matrix $M$ of size $r$ to the square matrix of size $r + i$ whose upper right block of size $r$ is $M$ and whose other blocks are zero. In pictures,

$$T_i M = \begin{pmatrix} 0 & M \\ 0 & 0 \end{pmatrix}.$$ 

Then we write the $p$-adic expansion

$$E(u) = [E_0(u)] + [E_1(u)] p + \cdots + [E_{n-1}(u)] p^{n-1}$$

and we set $E(u) : A = \rho(\sum [E_i \text{Id}] * [T_i U^i A])$ where $\rho$ is the map from lemma 3.3.1.

4.2.7 Lemma. Let $A \in \mathcal{G}_n((u))$ and $\mathcal{M} \in \mathcal{L}_n$.

1) If $\mathcal{M} = \mathcal{M}(A)$ then:
   a) $\mathcal{M}(i) = \mathcal{M}(U^{-1}A)$,
   b) $\mathcal{M}(i) = \mathcal{M}(L^{-1}A)$,
   c) $\langle \varphi(\mathcal{M}) \rangle = \mathcal{M}(\varphi(A))$,
   d) $E(u) \mathcal{M} = \mathcal{M}(E(u) : A)$.

2) If $A$ is a $T$-matrix then $U^{-1}A$, $L^{-1}A$, $\varphi(A)$, $E(u) : A$ are also $T$-matrices.

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

4.2.8 Remark. If $A$ is distinguished then it is not true in general that $E(u) : A$ is distinguished. There are obvious counter-examples for $n = 2$ as soon as $l_1 \geq l_2 + 1$.

Proof: Let $e_* = [A] p^*$. We define:

a) $f_j = p^{l-1} e_j$ for $1 \leq j \leq n + 1 - i$,

b) $g_j = e_{j+i-1}$ for $1 \leq j \leq n + 1 - i$,

c) $h_j = \varphi(e_j)$ for $1 \leq j \leq n$,

d) $\ell_j = E(u) e_j$ for $1 \leq j \leq n$.

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

$$E(u) e_* = (\sum [E_i p^*] [A] p^*) = \sum [E_i | T U^{-1} A] p^* = [\rho(\sum E_i \text{Id} * T U^{-1} A)] p^* = [E(u) : A] p^*.$$ 

It follows that $E(u) \mathcal{M} = \mathcal{M}(E(u) : A)$.

2) Using the characterization 1) in lemma 4.1.1, it is very easy to prove that $f_*$, $g_*$, $h_*$, $\ell_*$ are $T$-bases.

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

4.2.9 Lemma. Let $A, A'$ be in $\mathcal{G}_n((u))$ and $\mathcal{M} = \mathcal{M}(A)$, $\mathcal{M}' = \mathcal{M}(A')$.

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

2) In particular, the $T$-matrices are the minimal elements among the matrices $A \in \mathcal{G}_n((u))$ such that $\mathcal{M}(A) = \mathcal{M}$, in the sense that for any two matrices $A, A'$ with $\mathcal{M}(A) = \mathcal{M}(A') = \mathcal{M}$, if $A'$ is a $T$-matrix then $A/A' \geq 0$. 


Proof: Let $e_* = [A]p^*$ and $e'_* = [A']p^*$ be the associated generating sets. Then $\mathcal{M} \subset \mathcal{M}'$ if and only if for each $i$ we have $e_i \in \mathcal{M}'[i]$. 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 $e_* = [B]e'_*$, in other words $[A]p^* = [B][A']p^* = [B + A']p^*$. Thus $A/A' = B \geq 0$ and this proves 1). The proof of 2) follows when $\mathcal{M}' = \mathcal{M}$. □

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

5 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 $\mu_p^n$.

5.0.11 Theorem. The map $BK_n \to \mathcal{G}_n^T[u], \mathcal{M} \mapsto A(\mathcal{M})$ induces a bijection between the set of isomorphism classes of Breuil-Kisin modules of models of $\mu_p^n$ and the set of matrices $A = \begin{pmatrix} u^{l_1} & a_{12} & a_{13} & \cdots & a_{1n} \\ u^{l_2} & a_{23} & & & a_{2n} \\ & \ddots & \ddots & \ddots & \vdots \\ & & \ddots & \ddots & a_{n-1,n} \\ 0 & & & u^{l_{n-1}} & a_{n-1,n} \end{pmatrix}$ where $l = (l_1, \ldots, l_n) \in \mathbb{Z}^n$ and $a_{ij} \in k[[u]]$ for all $i, j$, such that

1) $\deg_u(a_{ij}) < l_j$ whenever $1 \leq i < j \leq n$,
2) $UA/LA \geq 0$,
3) $\varphi(A)/A \geq 0$,
4) $E(u): A/\varphi(A) \geq 0$.

Proof: To a Breuil-Kisin module $\mathcal{M}$ we associate the distinguished matrix $A$ of the underlying lattice. Note that since $\mathcal{M}$ is stable under Frobenius, it is a positive lattice, for otherwise there would exist an element $x \in \mathcal{M}$ with negative $u$-valuation and then the valuation of $\varphi^n(x)$ would tend to $-\infty$, in contradiction with the finite generation of $\mathcal{M}$. Thus $A \geq 0$. The conditions 1) and 2) just say that $A$ is distinguished. In view of lemma 4.2.7 and lemma 4.2.9, condition 3) says that $\langle \varphi(\mathcal{M}) \rangle \subset \mathcal{M}$ and condition 4) says that $E(u)\mathcal{M} \subset \mathcal{M}$. □

5.0.12 Remark. Condition 2) implies in particular that

$$l_1 \geq l_2 \geq \cdots \geq l_n.$$ 

Condition 3) implies in particular that

$$\text{val}_u(a_{i,i+1}) \geq l_{i+1}/p.$$ 

Condition 4) implies in particular that $e/(p-1) \geq l_1$. 

15
6 The case \( n = 3 \)

We work out the conditions in theorem 5.0.11 for \( n = 3 \). Although this case is not as simple as the case \( n = 2 \), still many complications show up only for \( n \geq 4 \).

6.1 Computation of the matrices

We have

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

Using the formulas in 3.7 we find

\[
UA/LA = \begin{pmatrix}
  u^{l_1-l_2} & a_{12}-u^{l_1-l_2}a_{23} \\
  0 & u^{l_2-l_3}
\end{pmatrix} .
\]

Moreover we have

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

and

\[
\varphi(A)/A = \begin{pmatrix}
  u^{(p-1)l_1} & a_{12}^{p-1}u^{(p-1)l_1} & a_{13}^{p-1}u^{(p-1)l_1} \\
  0 & u^{(p-1)l_2} & a_{23}^{p-1}u^{(p-1)l_2} \\
  0 & 0 & u^{(p-1)l_3}
\end{pmatrix}
\]

where

\[
p_{13} = a_{13}^{p-1} - a_{12}^{p-1}a_{12}^{p-1}a_{23} - S_1(u^{(p-1)l_1}a_{12}, -a_{12}^{p-1}) .
\]

Finally we compute \( E(u) : A \). Note that for \( n = 3 \) we have \( E_i \text{Id} + T_iU^iA = E_iT_iU^iA \) for all \( i \), but this is already false for \( n = 4 \), because of the failure of multiplicativity of Teichmüller representatives of polynomials. Thus

\[
E(u) : A = \begin{pmatrix}
  u^{e-l_1} & u^e a_{12} + u^{l_1} E_1 & u^e a_{13} + a_{12} E_1 + S_1(u^e a_{12}, u^{l_1} E_1) + u^{l_1} E_2 \\
  0 & u^{e-l_2} & u^e a_{23} + u^{l_2} E_1 \\
  0 & 0 & u^e a_{13} + a_{12} E_1 + S_1(u^e a_{12}, u^{l_1} E_1) + u^{l_1} E_2
\end{pmatrix} .
\]

and

\[
E(u) : A/\varphi(A) = \begin{pmatrix}
  u^{e-(p-1)l_1} & u^e a_{12} + u^{e-(p-1)l_1} a_{12}^{p} & q_{13} \\
  0 & u^{e-(p-1)l_2} & u^e a_{23} + u^{e-(p-1)l_2} a_{23}^{p} \\
  0 & 0 & u^{e-(p-1)l_3}
\end{pmatrix}
\]

where

\[
q_{13} = \frac{u^e a_{12} + a_{12} E_1 + S_1(u^e a_{12}, u^{l_1} E_1) + u^{l_1} E_2 - u^{e-(p-1)l_1} a_{12}^{p}}{u^{p l_3}}.
\]
6.2 Translation of the conditions of the theorem

- Condition 1) yields
  \[ \deg_u(a_{12}) \leq l_2 - 1, \quad \deg_u(a_{13}) \leq l_3 - 1 \quad \text{and} \quad \deg_u(a_{23}) \leq l_3 - 1. \]

- Condition 2) yields
  \[ l_1 \geq l_2 \geq l_3 \quad \text{and} \quad a_{12} - u^{l_1 - l_2}a_{23} \equiv 0 \mod u^{l_3}. \]

- 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
  \[ a_{13}^p - u^{(p-1)l_1}a_{13} = \frac{a_{12}^p - u^{(p-1)l_1}a_{12}}{u^{l_2}} a_{23} - S_1(u^{(p-1)l_1}a_{12}, -a_{12}^p) \equiv 0 \mod u^{l_3}. \]

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

\[ a_{12}^p \equiv 0 \mod u^{l_2} \quad \text{and} \quad a_{23}^p \equiv 0 \mod u^{l_3}. \]

Concerning the third, observe that since \((p-1)l_1 \geq l_3\) the term \(u^{(p-1)l_1}a_{13}\) can be neglected. Also since the valuation of \(S_1(x, y)\) is at least the maximum of \(\val_u(x)\) and \(\val_u(y)\), we see that the \(S_1\) term can be neglected. Finally the term \(u^{(p-1)l_1 - l_2}a_{12}a_{23}\) can also be neglected, indeed, \(pl_1 \geq 2l_1 \geq l_2 + l_3\) implies that its valuation is at least

\[ ((p-1)l_1 - l_2) + \frac{l_2}{p} + \frac{l_3}{p} = \frac{1}{p}((p-1)(pl_1 - l_2) + l_3) \geq \frac{1}{p}((p-1)l_3 + l_3) = l_3. \]

So the third condition is equivalent to

\[ a_{13}^p - u^{-l_2}a_{12}^p a_{23} \equiv 0 \mod u^{l_3}. \]

- Condition 4) yields
  \[ u^e a_{12} + u^{l_1}E_1 - u^{e-(p-1)l_1}a_{12}^p \equiv 0 \mod u^{pl_2}, \]
  \[ u^e a_{23} + u^{l_2}E_1 - u^{e-(p-1)l_2}a_{23}^p \equiv 0 \mod u^{pl_3} \]

and

\[ u^e a_{13} + a_{12}E_1 + S_1(u^e a_{12}, u^{l_1}E_1) + u^{l_1}E_2 - u^{e-(p-1)l_1}a_{13}^p \]

\[ - \frac{u^e a_{12} + u^{l_1}E_1 - u^{e-(p-1)l_1}a_{12}^p}{u^{pl_2}} a_{23}^p - S_1(u^{e-(p-1)l_1}a_{12}^p, -u^e a_{12} - u^{l_1}E_1) \equiv 0 \mod u^{pl_3}. \]
With the formula $S_1(x, y) = S_1(x, y - x)$ we have
\[
S_1(u^{e-(p-1)l_1}a_{12}^p, -u^{e}a_{12} - u^{l_1}E_1) = S_1(u^{e-(p-1)l_1}a_{12}^p, u^{e}a_{12} + u^{l_1}E_1 - u^{e-(p-1)l_1}a_{12}^p)
\]
which in view of a previous boxed congruence is 0 modulo $u^{pl_2}$ hence also modulo $u^{pl_3}$. Finally we obtain
\[
\begin{align*}
&u^{e}a_{13} + a_{12}E_1 + S_1(u^{e}a_{12}, u^{l_1}E_1) + u^{l_1}E_2 - u^{e-(p-1)l_1}a_{12}^p
\end{align*}
\]
\[
- \frac{u^{e}a_{12} + u^{l_1}E_1 - u^{e-(p-1)l_1}a_{12}^p}{u^{pl_2}}a_{23}^p \equiv 0 \mod u^{pl_3}. 
\]

6.2.1 Corollary. The models of $\mu_p^3$ over $\mathcal{O}_K$ are parametrized by three integers $0 \leq l_3 \leq l_2 \leq l_1 \leq e/(p - 1)$ and three polynomials $a_{12}, a_{13}, a_{23} \in k[u]$ satisfying
i. $\deg_u a_{12} \leq l_2 - 1$, $\deg_u a_{13} \leq l_3 - 1$, $\deg_u a_{23} \leq l_3 - 1$,
ii. $a_{12} - u^{l_1-2}a_{23} \equiv 0 \mod u^{l_1}$, $a_{12}^p \equiv 0 \mod u^{l_1-2}$, $a_{23}^p \equiv 0 \mod u^{l_1}$,
iii. $a_{13}^p - u^{-l_2}a_{12}^p a_{23} \equiv 0 \mod u^{l_1}$
iv. $u^{e}a_{12} + u^{l_1}E_1 - u^{e-(p-1)l_1}a_{12}^p \equiv 0 \mod u^{pl_2}$, $u^{e}a_{12} + u^{l_1}E_1 - u^{e-(p-1)l_1}a_{12}^p \equiv 0 \mod u^{pl_3}$
\[
u. \frac{-u^{e}a_{12} + a_{12}E_1 - u^{e-(p-1)l_1}a_{12}^p}{u^{pl_2}}a_{23}^p \equiv 0 \mod u^{pl_3}. 
\]

6.3 The tamely ramified case

In the tamely ramified case $(e, p) = 1$, some of these congruences can be strengthened.

To begin with, let us prove that
\[
[l_1 \geq pl_2] \quad \text{and} \quad [l_2 \geq pl_3].
\]

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
\[
\text{val}_u(u^{e}a_{12}) \geq e + l_2/p > e \geq (p - 1)l_1 \geq l_1.
\]

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

It follows that the condition given by the congruence $a_{12} - u^{l_1-2}a_{23} \equiv 0 \mod u^{l_3}$ 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
\[
u^{e-(p-1)l_1}a_{12}^p \equiv 0 \mod u^{pl_2}, \quad u^{e-(p-1)l_1}a_{12}^p \equiv 0 \mod u^{pl_3}
\]
and
\[
a_{12}E_1 - u^{e-(p-1)l_1}a_{13}^p - \frac{u^{e}a_{12} + u^{l_1}E_1 - u^{e-(p-1)l_1}a_{12}^p}{u^{pl_2}}a_{23}^p \equiv 0 \mod u^{pl_3}. 
\]
6.3.1 Corollary. In the tamely ramified case $(e, p) = 1$, the models of $\mu_{p^3}$ over $\mathcal{O}_K$ are parametrized by three integers $0 \leq p^2 l_3 \leq pl_2 \leq l_1 \leq e/(p-1)$ and three polynomials $a_{12}, a_{13}, a_{23} \in k[u]$ satisfying

i. $\deg_u a_{12} \leq l_2 - 1, \deg_u a_{13} \leq l_3 - 1, \deg_u a_{23} \leq l_3 - 1,$

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

7 Sekiguchi-Suwa theory

7.1 Some definitions about Witt vectors

7.1.1 Definition. For any ring $A$, let $W_n(A)$ be the ring of Witt vectors of length $n$ and $W(A)$ the ring of infinite Witt vectors. We define

$$
\hat{W}(A) = \left\{ (a_0, \ldots, a_n, \ldots) \in W(A) : \begin{array}{c} a_i \text{ is nilpotent for any } i \text{ and } \\
a_i = 0 \text{ for all but a finite number of } i \end{array} \right\}.
$$

We recall the definition of the so-called Witt-polynomial: for any $r \geq 0$ it is

$$
\Phi_r(T_0, \ldots, T_r) = T_0^{p^r} + p T_1^{p^r-1} + \cdots + p^r T_r.
$$

Then the following maps are defined:

- **Verschiebung**

  $$
  V : W(A) \longrightarrow W(A) \\
  (a_0, \ldots, a_n, \ldots) \longmapsto (0, a_0, \ldots, a_n, \ldots)
  $$

- **Frobenius**

  $$
  F : W(A) \longrightarrow W(A) \\
  (a_0, \ldots, a_n, \ldots) \longmapsto (F_0(T), F_1(T), \ldots, F_n(T), \ldots),
  $$

where the polynomials $F_r(T) = F_r(T_0, \ldots, T_r) \in \mathbb{Q}[T_0, \ldots, T_{r+1}]$ are defined inductively by

$$
\Phi_r(F_0(T), F_1(T), \ldots, F_r(T)) = \Phi_{r+1}(T_0, \ldots, T_{r+1}).
$$

If $p = 0 \in A$ then $F$ is the usual Frobenius. The ideal $\hat{W}(A)$ is stable with respect to these maps.

For any morphism $G : \hat{W}(A) \longrightarrow \hat{W}(A)$ we will set $\hat{W}(A)^G := \ker G$. And for any $a \in A$ we denote the element $(a, 0, 0, \ldots, 0, \ldots) \in W(A)$ by $[a]$. It is called the Teichmüller representant of $a$.

Moreover we recall the definition of the following operator

7.1.2 Definition. Let $A$ be a ring and $a = (a_0, \ldots, a_n, \ldots)$ an element of $W(A)$. Then we define the operator

$$
T_a : W(A) \longrightarrow W(A)
$$

by

$$
\Phi_n(T_a x) = \sum_{i=0}^{n} p^ia_i^{n-i} \Phi_{n-i}(x)
$$
We define a formal power series $E$ in fact it is an element of $T$. Let us suppose that $T_a$ is a morphism of groups. For instance if $a = [a_0]$ then $T_a$ is nothing else that the left multiplication by $[a_0]$. While if $x = [x_0]$ then

$$T_a x = (a_0 x_0, a_1 x_0, \ldots, a_n x_0, \ldots).$$

**7.1.3 Lemma.** Let $A$ be a ring then, for any $a = (a_0, \ldots, a_n, \ldots) \in W(A)$ with $a_0$ not a divisor of the zero then the morphism $T_a$ is injective.

**Proof:** Let us suppose that $T_a x = 0$ with $x = (x_0, \ldots, x_n, \ldots) \in W(A)$. We prove, by induction, that $x_n = 0$ for any $n$. Since $T_0 T_a x = a_0 x_0 = 0$ and since $a_0$ is not a divisor of the zero then $b_0 = 0$. We now suppose that $x_i = 0$ for $i \leq n$. Since

$$
\Phi_{n+1}(T_a x) = \sum_{i=0}^{n+1} p^i a^{p^{n+1-i}} \Phi_{n+1-i}(x) = a_0^{p^{n+1}} \Phi_{n+1}(x) a_0^{p^{n+1}} x_{n+1} = 0.
$$

Since $a_0$ is not a divisor of the zero then $x_{n+1} = 0$. □

**7.1.4 Lemma.** For any $x = (x_0, \ldots, x_n, \ldots) \in W(A)$ with $x_0$ not a divisor of the zero we have that $T_a x = T_b x$ implies $a = b$.

**Proof:** Let $a = (a_0, \ldots, a_n, \ldots)$ and $b = (b_0, \ldots, b_n, \ldots)$ as above. We will prove by induction that $a_n = b_n$ for any $n$. If $T_a x = T_b x$ in particular $a_0 x_0 = b_0 x_0$. Since $x_0$ is not a divisor of the zero them $a_0 = b_0$. Now let us suppose that $a_i = b_i$ for $i \leq n$. We prove $a_n = b_n$. By hypothesis we have that

$$T_a x - T_b x = T_a x = \sum_{k=0}^{\infty} V^k((a_k) - (b_k)) x = \sum_{k=n+1}^{\infty} V^k((a_k) - (b_k)) x = 0$$

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 divisor of the zero.

□

**7.2 Deformation of Artin-Hasse exponential**

The so called Artin-Hasse exponential series is given by

$$E_p(X) := \exp(X + \frac{X^p}{p} + \cdots + \frac{X^{p^n}}{p^n} + \cdots) \in \mathbb{Z}_p[[X]].$$

We define a formal power series $E_p(U, \Lambda, X)$ in $\mathbb{Q}[U, \Lambda][[X]]$ by

$$E_p(U, \Lambda; X) := (1 + \lambda X)^{\frac{X^p}{p^0} \prod_{k=1}^{\infty} (1 + \Lambda X \lambda^{p^k} X^{p^k})^{\frac{1}{p^k}} (X^{p^k})^{p^k}}$$

In fact it is an element of $\mathbb{Z}_{(p)}[U, \Lambda][[X]]$ (see [SS, Lemma 4.8]) One can easily check that $E_p(U, 0; X) = E_p(U X)$. Now let $A$ be a $\mathbb{Z}_{(p)}$-algebra, $\lambda \in A$ and $a = (a_0, \ldots, a_n, \ldots) \in W(A)$. We define a formal power series $E_p(a, \lambda; X)$ in $A[[X]]$ by

$$\prod_{k=0}^{\infty} E_p(a_k, \lambda^{p^k}; X^{p^k}) = (1 + \lambda X) \prod_{k=1}^{\infty} (1 + \lambda X \lambda^{p^k} X^{p^k})^{\frac{1}{p^k}} (\Phi_{k-1}(\lambda^{F(k)}(\mathbb{A})))$$
7.3 Main theorem of Sekiguchi-Suwa Theory

7.3.1 Definition. Let $\lambda_1, \ldots, \lambda_n \in R$ and let $\mathcal{E}$ be a flat $R$ group scheme. If there exist exact sequences of flat $R$-group schemes

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

for $i = 1, \ldots, n$, with $\exists G^{(\lambda_i)} \subseteq \text{Spec}[T, 1/(\lambda_i T + 1)]$, $\mathcal{E}_0 = 0$ and $\mathcal{E}_n = \mathcal{E}$, we call the sequence of flat $R$-group schemes $\mathcal{E}_1 = G^{(\lambda_1)}, \mathcal{E}_2, \ldots, \mathcal{E}_n = \mathcal{E}$

or, sometimes, simply $\mathcal{E}$ a filtered $R$-group scheme of type $(\lambda_1, \ldots, \lambda_n)$.

We now define, by induction, an operator $U^j : \hat{\mathcal{W}}(R/\pi^j R)^j \to \mathcal{W}(R/\pi^j R)^j$. For a vector $a \in \mathcal{W}(R/\pi^j R)$ we denote by $\overline{a} = (\overline{a_0}, \overline{a_i}, \ldots) \in \mathcal{W}(R)$ one of its representative. If $a \in \hat{\mathcal{W}}(R/\pi^j R)$ we suppose that $\overline{a}_i = 0$ for almost all $i$. Let us define $U^1$ as $F(1) = F - [\pi^1]$. Now we choose $a^j = (a^j_i) \in \ker U^{j-1} : \hat{\mathcal{W}}(R/\pi^j R)^j = \mathcal{W}(R/\pi^j R)^j$ for $2 \leq j \leq n - 1$ and we define

$$U^n = \left( \begin{array}{cccc}
F(b_1^n) & -T_{b_1^n} & & \\
0 & F(b_2^n) & -T_{b_2^n} & \\
\vdots & \ddots & \ddots & \ddots \\
0 & 0 & \ddots & -T_{b_n^{n-1}} \\
0 & 0 & \ldots & 0 \\
\end{array} \right)$$

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

$$b^j_i := \frac{1}{\pi^m} (\overline{a}^j_i - \sum_{t=2}^{n-1} T_{b_t^j} a^j_i) = \frac{U^{n-1} \overline{a}^{n-1}}{\pi^m}$$

7.3.2 Theorem. For a filtered $R$-group scheme $\{\mathcal{E}_1, \ldots, \mathcal{E}_n = \mathcal{E}\}$ of type $\{\pi^1, \ldots, \pi^n\}$ there exists homomorphisms

$$D_i : i^*\mathcal{E}_i \to i_*\mathcal{G}_{m,R/\pi^i R}$$

for each $1 \leq i \leq n - 1$ and each $\mathcal{E}_i$ is given by

$$\mathcal{E}_i \simeq \text{Spec}[R[X_1, \ldots, X_i, 1/1 + \lambda_1 X_1, \ldots, D_{i-1}(X_1, X_2, \ldots, 1)]].$$

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

$$\alpha^{(i)} : \mathcal{E}_i \to (\mathcal{G}_{m,R})^i$$

$$(X_1, \ldots, X_i) \mapsto (1 + \pi^i X_1, D_1(X_1) + \pi^i X_2, \ldots, D_{i-1}(X_1, \ldots, X_{i-1}) + \pi^i X_i)$$

a group-scheme homomorphism. Moreover, for $j = 2, \ldots, n$, there exists

$$a^j = (a^j_i)_{2 \leq i \leq j} \in \ker(\hat{\mathcal{W}}(R/\pi^j R)^j \xrightarrow{U^{j-1}} \hat{\mathcal{W}}(R/\pi^j R)^j)$$

with

$$D_i(X_1, \ldots, X_i) = E_p(\overline{a}^{i+1}, (\pi^i)_{1 \leq s \leq i}, X_1, \ldots, X_i)$$

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

$$\ker(\hat{\mathcal{W}}(R/\pi^l R)^n) \xrightarrow{U^n} \hat{\mathcal{W}}(R/\pi^l R)^n \to \text{hom}_{R/\pi^l - m}(i^*\mathcal{E}, i_*\mathcal{G}_{m,R/\pi^l R})$$

given by

$$c^n \mapsto E_p(c^n, (\pi^i)_{1 \leq s \leq i}, X_1, \ldots, X_n)$$

21
Proof: See [SS, 5.2](4).

In the next section we will give a computable interpretation of this result.

7.4 T-multiplication

7.4.1 Definition. Let $M = (m_i^j), N \in M_n(W(A))$. We will define the $T$-multiplication by

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

where $T_M$ is the operator $T_{m_i^j}$.

We will now consider the ring $V_n(A) \subseteq M_n(W(A))$ of matrices of upper triangular matrices of the form

$$
\begin{pmatrix}
    a_1^1 & a_2^1 & a_3^1 & \ldots & a_n^1 \\
    0 & a_1^2 & a_3^2 & \ldots & a_2^2 \\
    \vdots & \vdots & \vdots & \ddots & \vdots \\
    0 & a_{n-1}^n & a_n^n & \ldots & a_n^n \\
    0 & 0 & a_{n-1}^n & \ldots & a_n^n
\end{pmatrix}
$$

with $a_i^j = (a_{i,0}^j, \ldots, a_{i,n}^j, \ldots)$ and $a_{i,0}^j$ not divisor of the zero.

7.4.2 Lemma. For the operation $\ast_T$ in $V_n$ the cancellation properties holds, i.e. if $M \ast_T N = M' \ast_T N$ then $M = M'$ and if $M \ast_T N = M \ast_T N'$ then $N = N'$.

Proof: We prove them by induction on $n$. For $n = 1$ they are obvious. Let us suppose that the first is true for $V_n$ and we prove it for $V_{n+1}$. We observe that for any $M, N \in V_{n+1}$.

$$U(M \ast_T N) = U(M) \ast_T U(N)$$

and

$$L(M \ast_T N) = L(M) \ast_T L(N).$$

Therefore if $M \ast_T N = M' \ast_T N$ we have, by induction, that $U(M) = U(M')$ and $L(M) = L(M')$. And also if $M \ast_T N = M \ast_T N'$ we have that $U(N) = U(N')$ and $L(N) = L(N')$. It remains to prove that $m_{i+1}^n = m'_{i+1}^n$ and $n_{i+1}^n = n'_{i+1}^n$. We begin with the first. From

$$(M \ast_T N)_{i+1}^{n+1} = (M' \ast_T N)_{i+1}^{n+1}$$

it follows that

$$\sum_{j=1}^{n+1} T_{m_i^j} n_j^{n+1} = \sum_{j=1}^{n+1} T_{m'_i^j} n_j^{n+1}.$$ 

Since $m_i^j = m'_{i+1}^j$ for $j = 1, \ldots, n$ it follows that

$$T_{m_i^{n+1}} n_{i+1}^{n+1} = T_{m'_i^{n+1}} n_{i+1}^{n+1}$$

which implies $m_i^{n+1} = m'_{i+1}^{n+1}$ by Lemma 7.1.3.

Now from

$$(M \ast_T N)_{i+1}^{n+1} = (M \ast_T N')_{i+1}^{n+1}$$

4The definition of $U_n$ depends on the choice of the liftings so I guess that the result is not correct as it is stated. I am however pretty sure that it is correct if $l_1 \geqslant l_2 \geqslant \ldots \geqslant l_n$, which is the situation we are interested. I already wrote to Suwa. I am waiting for an answer.
it follows that
\[ \sum_{j=1}^{n+1} T_{m_j} n_j^{n+1} = \sum_{j=1}^{m+1} T_{m_j} n_j^{m+1}. \]

Since \( n_j^2 = n_j'^2 \) for \( j = 1, \ldots, n \) it follows that
\[ T_{a_1} n_1^{n+1} = T_{a_1} n_1^{m+1} \]
which implies \( n_1^{n+1} = n_1^{m+1} \) by Lemma 7.1.4.

7.4.3 Lemma. Let \( a_j^i \in \hat{W}(R/\pi^i R) \). Then they satisfy the conditions of Theorem 7.3.2 if and only if, for any matrix

\[
A = \begin{pmatrix}
[\pi^{l_1}] & \tilde{a}_1^2 & \tilde{a}_1^3 & \cdots & \tilde{a}_1^n \\
0 & [\pi^{l_2}] & \tilde{a}_2^3 & \cdots & \tilde{a}_2^n \\
\vdots & & & & \\
0 & [\pi^{l_{n-1}}] & \tilde{a}_{n-1}^n & \cdots & \tilde{a}_{n-1}^n \\
0 & [\pi^{l_n}] & \tilde{a}_n^n & \cdots & \tilde{a}_n^n
\end{pmatrix}
\]

with \( \tilde{a}_j^i \in W(R) \) lifting of \( a_j^i \), there exists (uniquely by Lemma 7.4.2) \( B \in W(R) \) such that

\[ B \star_T A = F(A) \]

where \( F(A) \) is obtained by \( A \) applying the Frobenius to any entry.

Proof: Let suppose that \( a_j^i \) satisfy the conditions of the theorem. Then one easily verifies that

\[ B \star_T A = F(A) \]

with

\[
B = \begin{pmatrix}
[\pi^{(p-1)l_1}] & b_1^2 & b_1^3 & \cdots & b_1^n \\
0 & [\pi^{(p-1)l_2}] & b_2^3 & \cdots & b_2^n \\
\vdots & & & & \\
0 & [\pi^{(p-1)l_{n-1}}] & b_{n-1}^n & \cdots & b_{n-1}^n \\
0 & [\pi^{(p-1)l_n}] & b_n^n & \cdots & b_n^n
\end{pmatrix}
\]

Conversely if there exists such \( B \), it easy to check that it should be as above. And the fact that \( B \) has the coefficients in \( R \) implies that \( a_j^i \) satisfy the conditions of the theorem.

7.4.4 Remark. We observe that in fact the matrix \( B \) always exists in \( V_n(K) \) and it satisfies \( B \star_T A = F(A) \) in \( V_n(K) \). So in practice the existence of \( B \) as in the Lemma is equivalent to require \( b_j^i \equiv 0 \mod \pi^j \) for \( j \geq i + 1 \).
8 The conditions for a filtered group scheme to contain a model of $\mu_{p^n}$

Let $E_n$ be a filtered group scheme of dimension $n$. It has a canonical morphism $\alpha^{(n)}$ to $(\mathbb{G}_m)^n$, and the closure of $\ker(\alpha^{(n)}_K) \simeq \mu_{p^n \cdot K}$ inside $E_n$ is a quasi-finite flat subgroup $G_n$.

If $G_n$ is finite, then the quotient $F_n$ is a filtered group scheme and the quotient map $\Psi_n : E_n \to F_n$ is an isogeny. For each $\mu$ we have a pullback map

$$\Psi_n^* : \text{Hom}_{A/\mu-Sch}(F_n, \mathbb{G}_m) \to \text{Hom}_{A/\mu-Sch}(E_n, G_m).$$

But we have:

8.0.5 Theorem. The canonical map given by the deformed Artin-Hasse exponential

$$(W \times A^1)^n \to \text{Hom}_{Ptd-Sch}(E, \mathbb{G}_m)$$

is an isomorphism and the preimage of $\text{Hom}_{\text{Gr}}(E, \mathbb{G}_m)$ is $\ker(F - \Lambda)$.

Needs to be rewritten: indeed the source is not $W^n$ but a twisted Witt vector thing, giving a $W$ for fixed parameters $\lambda_i$.

Moreover, if we restrict to the subfunctor $\hat{A}^1$, i.e. if on the points we restrict to nilpotents, then this gives isomorphisms

$$(\hat{W} \times \hat{A}^1)^n \to \text{Hom}_{Ptd-Sch}(E, \mathbb{G}_m)$$

and $\ker((F - \Lambda)|_{\hat{W} \times \hat{A}^1}) \to \text{Hom}_{\text{Gr}}(E, \mathbb{G}_m)$.

So we can identify $\Psi_n^*$ with an endomorphism of $\hat{W}(A)^n$ i.e. with a matrix which we call $\Upsilon$.

8.0.6 Theorem. ([SS], def. 9.1 and thm. 9.4) Let $E_{n+1}$ be a filtered group scheme and let $G_{n+1}$ be a filtered $\mu_{p^{n+1} \cdot K}$ inside $E_{n+1} \cdot K$. Assume that the closure of $G_n$ inside $E$ is finite flat. Then, the following are equivalent:

- the closure of $G_{n+1}$ inside $E_{n+1}$ is finite flat,
- there exists vectors $u^n$ and $v^n$ such that

$$pa^n - c^{n-1} - \Upsilon^n u^n = \tau_{\lambda^n} (v^n)$$

where $\tau_{\lambda^n} : W_{\lambda^n} \to W$ is the map from the twisted Witt vectors.

In this case, the filtered group scheme $\mathcal{F}_{n+1} = E_{n+1} / G_{n+1}$ is given by the matrix

$$\Upsilon_{n+1} = \begin{pmatrix}
\Upsilon_n & T_{v^n} \\
0 & \ldots & 0 & T_{p\lambda_{n+1}/\lambda_{n+1}^p}
\end{pmatrix}$$
9 Computation of Sekiguchi-Suwa’s models for $n = 3$

We assume throughout that $p \geq 3$.

9.1 Preliminary computations

9.1.1 Lemma. ([To], lemma 2.4) Let $R$ be a discrete valuation ring with residue characteristic $p$ and let $l \geq 1$ be an integer. Then the following hold.

(1) For all $a, b \in \hat{W}(R/\pi^l R)$ such that $v(a_i) \geq l/p$ and $v(b_i) \geq l/p$ for all $i \geq 0$, we have $a + b = (a_0 + b_0, a_1 + b_1, \ldots)$.

(2) Assume moreover that $p \geq (p - 1)l$ if $R$ has characteristic 0. Then for any $a \in \hat{W}(R/\pi^1 R)^F$ we have $v(a_i) \geq l/p$ for all $i \geq 0$.

We have the obvious lemma:

9.1.2 Lemma. i. $S_n(\mathbf{X}, \mathbf{Y}) \in \mathbb{Z}[\mathbf{X}, \mathbf{Y}]$ is an homogeneous polynomial of total degree $p^n$ for the weighted variables $X_i, Y_i$ of weight $p^i, i \in \mathbb{N}$.
ii. $S_0(\mathbf{X}, \mathbf{Y}) = X_0 + Y_0$,

$$S_1(\mathbf{X}, \mathbf{Y}) = S_0(X_1, Y_1) + s_1(X_0, Y_0), \text{ with } s_1(X_0, Y_0) = \frac{X_0^p + Y_0^p - (X_0 + Y_0)^p}{p}$$

$$S_2(\mathbf{X}, \mathbf{Y}) = S_0(X_2, Y_2) + s_1(X_1, Y_1) + s_1(X_1 + Y_1, s_1(X_0, Y_0)) + s_2(X_0, Y_0),$$

with

$$s_2(X_0, Y_0) = \frac{X_0^p + Y_0^p - (X_0 + Y_0)^p - p s_1(X_0, Y - 0)^p}{p^2} \in \mathbb{Z}[X_0, Y_0]$$

homogeneous of total degree $p^2$.

iii. $\text{val}(s_i(a, b)) \geq \min \left( (p^i - 1) \text{val}(a) + \text{val}(b), (p^i - 1) \text{val}(b) + \text{val}(a) \right), i = 1, 2$.

9.2 Computations for $n = 2$

Shift of indices: we write the vectors $a^i$ in [SS] rather $a^{i+1}$ in order to have a correspondance with the notations for the Breuil-Kisin matrices.

The group scheme $E_2$ is described by a Witt vector $a^2_1$ lying in the kernel of the operator $U^1 = F^{(\lambda_1)}$. Dajano proved that one can choose $a_1^2 = [a_1^2]$ Teichmüller. Is this a problem later on for $n = 3$ ?? In dimension one less, the canonical quasi-finite subgroup $G_1$ is finite and we have a $(1, 1)$ matrix

$$\Upsilon^1 = (T_{p[u^1]/u^2}).$$

The theorem refresult3 of Sekiguchi-Suwa gives, for $n = 2$:

9.2.1 Fact. The canonical quasi-finite subgroup $G_2$ is finite if and only if there exists a vector $u^2 \in \hat{W}(A/\lambda_2^0)$ in the kernel of $\ker(F^{(\pi^2)})$ such that $p[a_1^2] - [\lambda_1] = \Upsilon^1(u^2) \mod \lambda_2^0$. 

25
We wish to translate this condition. First, recall:

Since \( \text{val}(a_{12}) \geq l_2/p, S_1(a_{12}, [a_{12}]) = 0 \in A/\pi^{l_2p}, i \geq 2 \) and by induction

\[ p[a_{12}] = (pa_{12}, [a_{12}]^p(1 - p^{p-1}), 0, \ldots) \in \hat{W}(A/\pi^{l_2p}) \]

Since \( p \geq 3, \text{val}(p^{p-1}) = (p - 1)e \geq l_2p \). Hence

\[ p[a_{12}] = (pa_{12}, a_{12}^p, 0, \ldots) \in \hat{W}(A/\pi^{l_2p}) \]

Using Lemma [?] and \( \text{val}(pa_{12}) \geq e, \text{val}(a_{12})^p \geq l_2, \text{val} \pi^k = l_1 \geq l_2 \), we obtain \( \text{val} S_i(p[a_{12}], -[\pi^k]) \geq l_2p, i \geq 2 \) and

\[ p[a_{12}] - [\pi^k] = (pa_{12} - \pi^k, (a_{12})^p, 0, \ldots) \in \hat{W}(A/\pi^{l_2p}). \]

In the same way, we obtain

\[ p^{[\pi^k]} = \left( \frac{p}{\pi^{(p-1)k}}, 1, 0, \ldots \right) \in \hat{W}(A/\pi^{l_2p}) \]

Let \( u^2 = (u_0, u_1, u_2, \ldots) \) be a vector like in 9.2.1 above. Set \( \omega = \frac{p}{\pi^{(p-1)k}} \). It follows that \( T_{p^{[\pi^k]}/\pi^{l_2}} u^2 = [\omega]u^2 + V u^2 \) in \( \hat{W}(A/\pi^{l_2p}) \). Now note that in \( \hat{W}(A/\pi^{l_2p}) \) we have \( \ker(F^{[\pi^k]}) = \ker(F) \). It follows from lemma 9.1.1 that

\[ u^2 \equiv 0 \mod \pi^{l_2}, \]

hence also

\[ [\omega]u^2 \equiv Vu^2 \equiv 0 \mod \pi^{l_2}, \]

and their sum in \( \hat{W}(A/\pi^{l_2p}) \) is computed componentwise:

\[ T_{p^{[\pi^k]}/\pi^{l_2}} u^2 = (\omega u_0, \omega^p u_1 + u_0, \omega^{p^2} u_2 + u_1, \omega^{p^3} u_3 + u_2, \ldots). \]

Let us call \( u_k \) the last nonzero coefficient of \( u^2 \). It follows from the above that

\[ (pa_{12} - \pi^k, (a_{12})^p, 0, \ldots) = (\omega u_0, \omega^p u_1 + u_0, \omega^{p^2} u_2 + u_1, \ldots \omega^{p^3} u_k + u_{k-1}, u_k \ldots) \]

This is possible only if \( k = 0 \), hence \( u^2 = (u_0, 0, \ldots) = [u_0] \) in \( \hat{W}(A/\pi^{l_2p}) \). Now we identify

\[ T_{p^{[\pi^k]}/\pi^{l_2}} u^2 = (\omega u_0, u_0, \ldots). \]

and obtain \( u_0 \equiv (a_{12})^p \mod \pi^{l_2p} \) and

\[ pa_{12} - \pi^k - \frac{p}{\pi^{(p-1)k}}(a_{12})^p \equiv 0 \mod \pi^{l_2p} \]

We then recover Tossici and Caruso results ??

9.2.2 Corollary. The models of \( \mu_{p^2} \) over are given by the following equations
9.3 Computations for $n = 3$

We want to express the condition of theorem 8.0.6 that there exists $u_{13}$ such that

$$
\gamma_{13} = \frac{1}{\pi^{pl_3}} \left( p[a_{13}] - [a_{12}] - T_{p[\pi^{l_1}] / \pi^{pl_3}} U_{13} - T_{\gamma_{12}} [(a_{23})^p] \right)
$$

is an integer. In other words, we need to compute the term in the bracket modulo $\pi^{pl_3}$.

First we explicit the integrality condition of $\gamma_{12}$ and $T_{\gamma_{12}} [(a_{23})^p]$.

9.3.1 Lemma. The integrality of the element

$$
\gamma_{12} = \frac{1}{\pi^{pl_2}} \left( \left(p[a_{12}] - [\pi^{l_1}] - T_{p[\pi^{l_1}] / \pi^{pl_2}} [(\pi^{l_1})^p] \right) \right).
$$

gives the congruence

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

Proof: We have:

$$
\gamma_{12} = \frac{1}{\pi^{pl_2}} \left( \left(p[a_{12}] - [\pi^{l_1}] - T_{p[\pi^{l_1}] / \pi^{pl_2}} [(\pi^{l_1})^p] \right) \right).
$$

Thus we will compute the term in the bracket modulo $\pi^{p(l_2+ls)}$. We come to the first term in $\gamma_{12}$:

Since $\text{val}(a_{12}) \geq l_2/p$, $\text{val}(S_1([a_{12}],[a_{12}])) \geq l_2p^{-1}$, $i \in \mathbb{N}$. For $i \geq 3$, $l_2p^{i-1} \geq l_2p^2 \geq pl_2 + pl_3$, hence

$$
p[a_{12}] = \left( pa_{12}, (1 - p^{p-1})(a_{12})^p, *p^{p-1}(a_{12})^p, \ldots \right) \in \tilde{W}(A / \pi^{pl_2})
$$

with $\text{val} * \geq 0$.

Note that

$$\text{val}(p^{p-1}(a_{12})^p) \geq e(p-1) + pl_2 \geq l_3(p-1)^2 + pl_2 \geq pl_2 + pl_3$$

so finally

$$
p[a_{12}] = \left( pa_{12}, (1 - p^{p-1})(a_{12})^p, 0, \ldots \right) \in \tilde{W}(A / \pi^{pl_2})
$$

We now compute:

$$
p[a_{12}] - [\pi^{l_1}] = \left( \left(pa_{12} - \pi^{l_1}, (1 - p^{p-1})(a_{12})^p + s_1(pa_{12}, -\pi^{l_1}), S_2(p[a_{12}], -[\pi^{l_1}], \ldots) \right) \right).
$$

Since $\text{val} pa_{12} \geq e$, $\text{val}(1 - p^{p-1})(a_{12})^p \geq l_2$, $\text{val} \pi^{l_1} = l_1$, $S_i(p[a_{12}], -[\pi^{l_1}]) = 0 \in A / \pi^{pl_2}$ and

$$\text{val}(s_2(pa_{12}, -\pi^{l_1})) \geq (p^2 - 1)l_1 + e \geq (p^2 - 1)p^2 - 1)l_1 + (p-1)l_1 = pl_1 + (p^2 - 2)l_1 \geq pl_2 + pl_3$$

so finally

$$
p[a_{12}] - [\pi^{l_1}] = \left( \left(pa_{12} - \pi^{l_1}, (1 - p^{p-1})(a_{12})^p + s_1(pa_{12}, -\pi^{l_1}), 0, \ldots) \right) \right).
$$

The last term contributing to $\gamma_{12}$ is

$$
T_{p[\pi^{l_1}] / \pi^{pl_2}} [(a_{23})^p] = \left( \left( \pi^{\pi^{l_1}}(a_{12})^p, (1 - p^{p-1})(a_{12})^p, 0, \ldots \right) \right) \in \tilde{W}(A / \pi^{pl_2})
$$

We add up and we obtain the lemma. \(\square\)
9.3.2 Lemma. We have the following integrality condition

\[ T_{\pi^{12}}[(a_{23})^p] = \left( \frac{(a_{23})^p}{\pi^{pl_2}} \left( pa_{12} - \pi^{l_1} - \frac{p}{\pi^{(p-1)}l_1} (a_{12})^p \right), \frac{(a_{23})^p}{\pi^{pl_2}} s_1 \left( pa_{12} - \pi^{l_1} \right), 0, \ldots \right). \]

Proof: Now we can compute, in \( \tilde{W}(A/\pi^{pl_1}) \) this time:

\[ T_{\pi^{12}}[(a_{23})^p] = \left( \frac{(a_{23})^p}{\pi^{pl_2}} \left( pa_{12} - \pi^{l_1} - \frac{p}{\pi^{(p-1)}l_1} (a_{12})^p \right), \frac{(a_{23})^p}{\pi^{pl_2}} s_1 \left( pa_{12} - \pi^{l_1} \right) + \frac{(a_{23})^p}{\pi^{pl_2}} s_1 \left( pa_{12} - \pi^{l_1}, \frac{p}{\pi^{(p-1)}l_1} (a_{12})^p \right), 0, \ldots \right). \]

We simplify a little bit. Using the identity \( s_1(x, y) = s_1(x, -y - x) \), we get

\[ s_1 \left( pa_{12} - \pi^{l_1}, \frac{p}{\pi^{(p-1)}l_1} (a_{12})^p \right) = s_1 \left( pa_{12} - \pi^{l_1}, -\frac{p}{\pi^{(p-1)}l_1} (a_{12})^p + \pi^{l_1} - pa_{12} \right). \]

After lemma [?]:

\[ \text{val}(s_1(a, b)) \geq \min \left( (p-1) \text{val}(a) + \text{val}(b), (p-1) \text{val}(b) + \text{val}(a) \right). \]

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

\[ \text{val} \left( \frac{(a_{23})^p}{\pi^{pl_2}} s_1(a, b) \right) \geq l_3 - pl_2 + min((p-1)l_1 + pl_2, l_1 + (p-1)pl_2) \geq pl_3 \]

so this term vanishes. Finally we obtain the lemma. \( \Box \)

9.3.3 Lemma.

\[ p[a_{13}] - [a_{12}] - T_{\pi^{12}}[(a_{23})^p] \]

\[ = (pa_{13} - a_{12}, (a_{13})^p + s_1(pa_{13}, -a_{12}), 0, \ldots) \]

\[ = \left( \frac{(a_{23})^p}{\pi^{pl_2}} \left( pa_{12} - \pi^{l_1} - \frac{p}{\pi^{(p-1)}l_1} (a_{12})^p \right), \frac{(a_{23})^p}{\pi^{pl_2}} s_1 \left( pa_{12} - \pi^{l_1} \right), 0, \ldots \right) \]

\[ = (c_0, c_1, c_2, \ldots) \]

with

\[ c_0 = pa_{13} - a_{12} - \frac{(a_{23})^p}{\pi^{pl_2}} \left( pa_{12} - \pi^{l_1} - \frac{p}{\pi^{(p-1)}l_1} (a_{12})^p \right) \]

\[ c_1 = (a_{13})^p + s_1(pa_{13}, -a_{12}) - \frac{(a_{23})^p}{\pi^{pl_2}} s_1 \left( pa_{12} - \pi^{l_1} \right) + s_1 \left( pa_{13} - a_{12}, -\frac{(a_{23})^p}{\pi^{pl_2}} \left( pa_{12} - \pi^{l_1} - \frac{p}{\pi^{(p-1)}l_1} (a_{12})^p \right) \right) \]

and \( c_i = 0, i \geq 2 \).

Proof:

We have

\[ p[a_{13}] - [a_{12}] = (pa_{13}, (a_{13})^p, 0, \ldots) - (a_{12}, 0, \ldots) \]

\[ = (pa_{13} - a_{12}, (a_{13})^p + s_1(pa_{13}, -a_{12}), s_2(pa_{13}, -a_{12}), \ldots) \in \tilde{W}(A/\pi^{pl_1}). \]
Note the easy lemma, same as above:

$$\text{val}(s_2(a, b)) \geq \min \left( (p^2 - 1) \text{val}(a) + \text{val}(b), (p^2 - 1) \text{val}(b) + \text{val}(a) \right).$$

Using this we see immediately that $s_2(pa_{13}, -a_{12}) \equiv 0 \mod \pi^{p l_3}$ so that

$$p[a_{13}] - [a_{12}] = (pa_{13} - a_{12}, (a_{13})^p + s_1(pa_{13}, -a_{12}), 0, \ldots) \in \hat{W}(A/\pi^{p^{l_3}}).$$

\[\square\]

9.3.4 Lemma. If $l_1 \geq p l_3$ then $c_1 = a_{13}^p \in A/\pi^{l_3 p}$.

Proof: Remind

$$c_1 = (a_{13})^p + s_1(pa_{13}, -a_{12}) - \frac{(a_{23})^p}{\pi^{p l_3}} s_1(pa_{12}, -\pi^{l_1}) + s_1 \left( pa_{13} - a_{12}, -\frac{(a_{23})^p}{\pi^{p l_3}} \left( pa_{12} - \pi^{l_1} - \frac{p}{\pi^{l_1 - 1}} a_{12}^p \right) \right)$$

We have $\text{val}(pa_{13}, -a_{12}) \geq e + (p - 1)l_2/p \geq (p - 1)l_1 \geq p l_3$,

\[\text{val} \left( \frac{(a_{23})^p}{\pi^{p l_3}} s_1(pa_{12}, -\pi^{l_1}) \right) \geq l_3 - p l_2 + l_1(p - 1) + e + l_2/p \geq p l_3\]

\[\text{val} \left( pa_{13} - a_{12}, -\frac{(a_{23})^p}{\pi^{p l_3}} \left( pa_{12} - \pi^{l_1} - \frac{p}{\pi^{l_1 - 1}} a_{12}^p \right) \right) \geq l_1/p + (p - 1)l_3 \geq p l_3.\]

\[\square\]

9.3.5 Lemma.

For $u_{13} = (u_0, u_1, \ldots)$, the condition

$$T_{p^{[\pi^{l_3}]/\pi^{p l_3}}} u_{13} = \left[ \frac{p}{\pi^{[p^{l_1} l_1]}} \right] u_{13} + V u_{13}$$

implies in $A/\pi^{p l_3}$,

$$c_0 = \frac{p}{\pi^{[p^{l_1} l_1]}} u_0$$

$$c_1 - u_0 = \left( \frac{p}{\pi^{[p^{l_1} l_1]}} \right)^p u_1$$

$$s_1(c_1, -u_0) - u_1 = 0.$$

Proof: $\frac{p^{[\pi^{l_3}]}_{\pi^{p^{l_3}}}}{\pi^{p l_3}} = \left( \frac{p}{\pi^{[p^{l_1} l_1]}} , 1, 0, \ldots \right)$ modulo $\pi^{p l_3}$. We deduce

$$\left[ \frac{p}{\pi^{[p^{l_1} l_1]}} \right] u_{13} = -V u_{13} + (c_0, c_1, 0, \ldots)$$

$$= -(0, u_0, u_1, \ldots) + (c_0, c_1, 0, \ldots)$$

Remark $\text{val}(c_0) \geq l_3$, $\text{val}(c_1) \geq l_3/p$. Note that $u_{13} \in \hat{W}(A/\pi^{l_3 p})^{F^2}$ so $\text{val}(u_i) \geq l_3/p$, $i \geq 0$.

By Lemma \text{Im ker F}

$$\left[ \frac{p}{\pi^{[p^{l_1} l_1]}} \right] u_{13} = (c_0, c_1 - u_0, s_1(c_1, -u_0) - u_1, -u_2, \ldots, -u_k, 0, \ldots) \in \hat{W}(A/\pi^{p l_3})$$

where $u_k$ is by definition the last nonzero term in $u_{13}$ and $-u_k$ occurs here at the $(k + 1)$-th place. On the other hand

$$\left[ \frac{p}{\pi^{[p^{l_1} l_1]}} \right] u_{13} = \left( \frac{p}{\pi^{[p^{l_1} l_1]}} u_0 \right)^p u_1, \left( \frac{p}{\pi^{[p^{l_1} l_1]}} \right)^{p^2} u_2, \ldots, \left( \frac{p}{\pi^{[p^{l_1} l_1]}} \right)^{p^k} u_k, 0, \ldots$$
where here the term involving $u_k$ occurs at the $k$-th place. This is not possible if $k \geq 2$. Hence $k \leq 1$ and

$u_{13} = (u_0, u_1, 0, \ldots) \in \widehat{W}(A/\pi^{pl_3})$.

Identifying, with Lemma 9.3.3, we obtain the expected formulas.

\[0\]

9.3.6 Lemma. Assume $l_1 \geq pl_3$ the integrality gives the congruences

\[
\left(\frac{p}{\pi(p-1)l_1}\right) a_{13}^p \equiv pa_{13} - a_{12} - \left(\frac{a_{23}}{\pi^{pl_2}}\right) \left(pa_{12} - \frac{p}{\pi(p-1)l_1}(a_{12})^p\right) \mod \pi^{pl_3}
\]

Proof: We have $u_0 = c_1 - \left(\frac{p}{\pi(p-1)l_1}\right)^p s_1(c_1, -u_0)$. Since $c_1$ divides $s_1(c_1, -u_0) \in A/\pi^{pl_3}$, $u - 0 = c_1u_0'$ with val $u_0' \geq 0$. Write $\beta = c_1\left(\frac{p}{\pi(p-1)l_1}\right)$ then

$\beta = \frac{p}{\pi(p-1)l_1} \beta s_1(1, u_0')$

and val $\beta \geq \text{val} c_1 \geq l_3/p$. We obtain

$\beta = c_0 + \left(\frac{p}{\pi(p-1)l_1}\right)^p s_1(1, u_0')c_0 + \left(\frac{p}{\pi(p-1)l_1}\right)^p s_1(1, u_0')c_0^p \in A/\pi^{pl_3}$

Recall $c_0 = pa_{13} - a_{12} - \left(\frac{a_{23}}{\pi^{pl_2}}\right) \left(pa_{12} - \frac{p}{\pi(p-1)l_1}(a_{12})^p\right)$ Hence $c_0^p = a_{12}^p \in A/\pi^{pl_3}$. Now we come back to the congruence

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

If $e + \text{val} a_{12} \leq e - l_1(p-1) + p \text{val} a_{12}$ then $\text{val} a_{12} \geq l_1$ and $a_{12}^p = 0 \in A/\pi^{pl_3}$.

If $e + \text{val} a_{12} > e - l_1(p-1) + p \text{val} a_{12}$, then $e - l_1(p-1) + p \text{val} a_{12} \geq \text{min}(pl_2, l_1)$ and $\left(\frac{p}{\pi(p-1)l_1}\right)a_{12}^p = 0 \in A/\pi^{pl_3}$. hence $\beta = c_0 \in A/\pi^{pl_3}$ Since $\beta = \left(\frac{p}{\pi(p-1)l_1}\right)c_1$, we obtain the lemma.

\[\Box\]

10 Conclusion

10.0.7 Theorem. Let $p \geq 3$ be a prime number. Let $0 \leq l_3 \leq l_2 \leq l_1 \leq e/(p-1)$ and $a_{12}, a_{13}, a_{23} \in k[u]$ be the parameters of the models of $\mu_{p^3}$ over $\mathcal{O}_K$. Assume moreover that $l_1 \geq pl_3$. Then the models of $\mu_{p^3}$ over $\mathcal{O}_K$ is given by

$G = \ker (\phi : \text{Spec } R[X_1, X_2, X_3]/(\))$

References


[Li] T. Liu


