JOURNAL
de Théorie des Nombres
de BORDEAUX
anciennement Séminaire de Théorie des Nombres de Bordeaux

Sandrine JEAN

Conjugacy classes of series in positive characteristic and Witt vectors.

Tome 21, n° 2 (2009), p. 263-284.

<http://jtnb.cedram.org/item?id=JTNB_2009__21_2_263_0>

Journal de Théorie des Nombres
de Bordeaux **21** (2009), 263-284

Conjugacy classes of series in positive characteristic and Witt vectors.

par Sandrine JEAN

Résumé. Soit k la clôture algébrique de $\mathbb{F}_p$ et K le corps local des séries formelles à coefficients dans k. Le but de cet article est de décrire l'ensemble $\mathcal{Y}_n$ des classes de conjugaison des séries d'ordre p^n pour la loi de composition. Ce travail concerne les séries formelles réversibles à coefficients dans un corps de caractéristique p qui sont d'ordre p^n pour la loi de composition. Dans le but d'explorer la conjecture de Oort, je donne une description des classes de conjugaison des séries au moyens de vecteurs de Witt de longueur finie. Nous developpons certains outils permettant de constuire une bijection entre un ensemble $\mathcal{A}_n$ de vecteurs de Witt et un ensemble $\mathcal{X}_n$ de couples constitués d'une extension L/K cyclique totalement ramifiée de degré p^n et d'un générateur du groupe de Galois. Nous pouvons définir pour chaque élément de $\mathcal{A}_n$ une suite de sauts de ramification. Nous pouvons également décrire une seconde bijection entre $\mathcal{Y}_n$ et les orbites $\mathcal{A}_n$ sous une certaine action de groupe. Les sauts de ramification d'une série appartenant à $\mathcal{Y}_n$ peuvent être retrouvés grâce aux composantes du vecteur de Witt correspondant dans $\mathcal{A}_n$.

Abstract. Let k be the algebraic closure of $\mathbb{F}_p$ and K be the local field of formal power series with coefficients in k. The aim of this paper is the description of the set $\mathcal{Y}_n$ of conjugacy classes of series of order p^n for the composition law. This work is concerned with the formal power series with coefficients in a field of characteristic p which are invertible and of finite order p^n for the composition law. In order to investigate Oort's conjecture, I give a description of conjugacy classes of series by means of Witt vectors of finite length. We develop some tools which permit us to construct a bijection between a set $\mathcal{A}_n$ of Witt vectors and a set $\mathcal{X}_n$ of pairs constituted by a cyclic totally ramified extension L/K of degree p^n and a generator of its Galois group. We are able to define for any element of $\mathcal{A}_n$ a sequence of ramification breaks. We also describe another bijection between $\mathcal{Y}_n$ and the orbits of $\mathcal{A}_n$ under a certain group action. Ramification breaks of a series belonging to $\mathcal{Y}_n$ can be recovered from the components of a corresponding vector in $\mathcal{A}_n$.

1. Introduction

Let p be a prime number, k the algebraic closure of $\mathbb{F}_p$ and $K = k(\!(t)\!)$ the field of meromorphic series with coefficients in k. The main aim of this paper is to develop some tools in order to classify, up to conjugacy, power series which are invertible for the composition law. According to a conjecture of Frans Oort, such a series could be lifted to a series of same order for the composition law whose coefficients are integer in an extension of a p-adic number field. This result is known just for $n = 1$ and $n = 2$. If a series can be lifted by a series of the same order then each series in the conjugacy class can be lifted. Invertible series are precisely formal power series without constant term such that their derivative at 0 is not zero. They form a group with regard to the composition law denoted by $\mathcal{G}_0(k)$:

$$\mathcal{G}_0(k) = \Big\{ \sum_{\iota \geq 1} a_\iota t^\iota \text{ such that } a_1 \in k^* \Big\}.$$

When the residue field is finite, the case of series of order p was studied by B. Klopsch. His results prove that two series of order p are conjugate in $\mathcal{G}_0(k)$ if and only if they have the same ramification number [7], ramification number of a series σ, or depth, being the t-adic valuation of $\frac{\sigma(t)}{t} - 1$.

For the case of series of order p^n, we will lean on Artin-Schreier-Witt theory which describes cyclic extensions of order p^n with the aid of Witt vectors of length n. In the case of a finite residue field, K. Kanesaka and K. Sekiguchi [6] have described the ramification of such extensions by introducing a certain set $\mathcal{B}_n$ of Witt vectors of length n. Extending this idea to the case where k is the algebraic closure of $\mathbb{F}_p$, we are able to parametrize the set of pairs (L, σ) where L is a cyclic totally ramified extension of order p^n of K and σ a generator of its Galois group by a subset $\mathcal{A}_n$ in $\mathcal{B}_n$ (Theorem 3.8). Thanks to this correspondence, we can compute ramification breaks of the extension L/K in term of Witt vectors of $\mathcal{A}_n$, always following K. Kanesaka and K. Sekiguchi's paper.

Any pair (L, σ) will correspond to a conjugacy class of series of order p^n. Then we will be able to put in bijection conjugacy classes of series of order p^n and elements of $\mathcal{A}_n$ under a certain action of $\mathcal{G}_0(k)$ (Theorem 5.6).

I am grateful to Ivan B. Fesenko for having supported me during my stay at the University of Nottingham in 2007. I would like to thank also my supervisors F. Laubie and A. Salinier who help me for this work.

2. The ring of Witt vectors.

Witt vectors are useful in the description of extensions of degree p^n thanks to Artin-Schreier-Witt theory.

2.1. Properties of Witt vectors.

Let R be a commutative ring with a unit element, and p be a prime number.

We denote by $W(R)$ the ring of Witt vectors of infinite length.

For all Witt vectors $x = (x_j)_{j\geq 1}$ in $W(R)$, the sequence $x^* = (x^{(h)})_h$ of ghost components is defined by $x^{(h)} = x_0^{p^h} + px_1^{p^{h-1}} + ... + p^h x_h$.

Let $H(R) = R^{\mathbb{N}}$ be the ring of sequences of elements in R provided with componentwise addition and multiplication laws. Let g_R be the map from $W(R)$ to $H(R)$ defined by $g_R(x) = x^*$. Then g_R is a ring homomorphism.

Let R and S be two commutative rings, φ a homomorphism from R to S, let $W(\varphi) : W(R) \to W(S)$ by $W(\varphi)(r_n) = \varphi(r_n)$ so $W(\varphi)$ is a homomorphism.

The Witt functor W is the unique functor from the category of commutative rings into itself satisfying the following property: the transformation which associates to a commutative ring R the map g_R is a functorial homomorphism of W to the functor H.

2.2. The additive law in $W(R)$.

In this paragraph, we give a technical lemma about the n^{th} component of Witt vectors. This Lemma will be used in several ways in the next chapters. We need firstly to define the weight of a monomial to state this lemma.

Definition 2.1. *In the $2j$-indeterminate-polynomial ring $R[x_0, ..., x_{j-1}, y_0, ..., y_{j-1}]$, the weight of a monomial $x_0^{\eta_0}...x_{j-1}^{\eta_{j-1}} y_0^{\mu_0}...y_{j-1}^{\mu_{j-1}}$ in R is defined by:*

$$\sum_{h=0}^{j-1} p^h(\eta_h + \mu_h).$$

A polynomial is said to be homogeneous if it is a linear combination of same weight monomials.

Let us notice that the weight depends on the prime p.

Lemma 2.2.

1) *Let $x = (x_0, x_1, ...) \in W(R)$, the j^{th} component of $-x$ is $-x_{j-1} + \Omega_{j-1}$ with Ω_{j-1} a homogeneous polynomial of weight p^{j-1} in $\mathbb{Z}[x_0, ..., x_{j-2}]$.*
2) *Let $x = (x_0, x_1, ...)$ and $y = (y_0, y_1, ...)$ be two Witt vectors, the j^{th} component of $x + y$ is $x_{j-1} + y_{j-1} + \Sigma_{j-1}$ where Σ_{j-1} is a homogeneous polynomial of weight p^{j-1} in $\mathbb{Z}[x_0, ..., x_{j-2}, y_0, ..., y_{j-2}]$.*

Proof.

1) Consider firstly the case of the ring $R_{\mathbb{Z}} = \mathbb{Z}[X_0, X_1, ..., X_j, ...]$ of polynomials in countably infinite indeterminates with integer coefficients. We put

$X = (X_0, X_1, ..., X_j, ...)$. Let $Y = (Y_0, Y_1, ..., Y_j, ...)$ such that $Y = -X$ in $W(R_{\mathbb{Z}})$. The j^{th} ghost components of X and Y are respectively:

$$X^{(j-1)} = X_0^{p^{j-1}} + pX_1^{p^{j-2}} + ... + p^{j-2}X_{j-2}^p + p^{j-1}X_{j-1}$$

$$Y^{(j-1)} = Y_0^{p^{j-1}} + pY_1^{p^{j-2}} + ... + p^{j-2}Y_{j-2}^p + p^{j-1}Y_{j-1}.$$

Since $g_{R_{\mathbb{Z}}}$ is a ring homomorphism, in $H(R_{\mathbb{Z}})$ we get: $X^{(j-1)} + Y^{(j-1)} = 0$.

Define the ring $R_{\mathbb{Q}} = \mathbb{Q}[X_0, X_1, ..., X_j, ...]$ of polynomials in countably infinite indeterminates with rational coefficients. Hence, in the ring $H(R_{\mathbb{Q}})$

$$Y_{j-1} = -X_{j-1} - \frac{1}{p^{j-1}}(X_0^{p^{j-1}} + Y_0^{p^{j-1}} + ... + p^{j-2}(X_{j-2}^p + Y_{j-2}^p)).$$

So $Y_{j-1} = -X_{j-1} + \Omega_{j-1}$ where Ω_{j-1} is, by induction on j, a polynomial of $X_0, X_1, ..., X_{j-2}$, necessarily with integer coefficients as Y_{j-1} is in $R_{\mathbb{Z}}$. Furthermore Ω_{j-1} is a homogeneous polynomial of weight p^{j-1}.

2) The proof of the second part is similar to the first one. □

2.3. Witt vectors of length n.

Let $n \geq 1$ be an integer and define the ring of Witt vectors of length n.

We define the shift map on $W(R)$ by $V : W(R) \to W(R)$ such that for any vector $x = (x_0, x_1, ...)$, we have $V(x_0, x_1, ...) = (0, x_0, x_1, ...)$. We note that for all x and y in $W(R)$, we get $V(x + y) = V(x) + V(y)$ ([12], ch II, §6).

Definition 2.3. *Let $I_n = V^n(W(R)) = \{(0, ..., 0, x_n, x_{n+1}, ...)\}$ be the set of Witt vectors where the n first components are zero.*

The set I_n is a subgroup and an ideal of $W(R)$. Let $W_n(R) = W(R)/I_n$. Elements of $W_n(R)$ are identified with the vectors $(x_0, ..., x_{n-1}) \in R^n$. These vectors are called Witt vectors of length n. The addition in $W_n(R)$ is given by the same formulae as the addition in $W(R)$.

2.4. Witt vectors on a field of formal power series.

Let k be a field of characteristic p and $K = k(\!(t)\!)$ provided with the t-adic valuation v_K be the local field of formal power series. Denote by $\mathcal{O}_K$ its valuation ring and $\mathfrak{p}_K$ its maximal ideal. We have $\mathcal{O}_K = k[\![t]\!]$ and $\mathfrak{p}_K = tk[\![t]\!]$.

Let F be the Frobenius map from $W(K)$ to itself such that for any vector $x = (x_0, x_1, ...)$ we get $Fx = (x_0^p, x_1^p, ...)$, the map F is a ring homomorphism. Let $\wp = F - id$ be the abelian group homomorphism from $W(K)$ to itself whose kernel is $W(\mathbb{F}_p)$ [12]. The same notations F and $\wp$ will be used in $W_n(K)$. We also define the truncation map T which is the ring epimorphism from $W_n(K)$ to $W_{n-1}(K)$ such that $T(x_0, ..., x_{n-2}, x_{n-1}) = (x_0, ..., x_{n-2})$.

Define on $W_n(K)$ the map introduced firstly in the PhD thesis of V. Shabat:

Definition 2.4. *Let $x = (x_0, x_1, ..., x_{n-1})$ be a Witt vector of length n, and put:*

$$m_n(x) = \min\{p^{n-1-\iota} v_K(x_\iota) \text{ for } \iota = 0, 1, ..., n-1\}.$$

We also have for any $x \in W_n(K)$, $m_n(x) = \max\{pm_{n-1}(T(x)), v_K(x_{n-1})\}$. By Proposition 4.2 of [13], m_n is an ultrametric function.

Definition 2.5. *Let d_n be the metric on $W_n(K)$ given by $d_n(x, y) = p^{-m_n(x-y)}$.*

This metric is compatible with the additive law. The topology defined on $W_n(K)$ by the metric d_n coincides with the product topology on the set K^n.

Lemma 2.6. *The additive group $W_n(K)$ provided with the metric d_n is a complete ultrametric group.*

Proof. We prove by induction on n that $W_n(K)$ is complete.

If $n = 1$ then $W_1(K) = K$ and the property is obvious.

Assume now that $W_{n'}(K)$ is complete up to $n' \leq n-1$. Let $x^{(h)}$ be a Cauchy sequence in $(W_n(K), d_n)$ then $m_n(x^{(h+1)} - x^{(h)})$ tends to $+\infty$. As $m_{n-1}(T(x^{(h+1)}) - T(x^{(h)})) \geq \frac{1}{p} m_n(x^{(h+1)} - x^{(h)})$ so $m_{n-1}(T(x^{(h+1)}) - T(x^{(h)}))$ tends to $+\infty$ and $T(x^{(h)})$ is a Cauchy sequence in $(W_{n-1}(K), d_{n-1})$. By induction hypothesis, $T(x^{(h)})$ tends to $T(l)$ with $l \in W_n(K)$. For any h, we can write $x^{(h)} = l + y^{(h)}$ for a vector $y^{(h)} = (y_0^{(h)}, ..., y_{n-1}^{(h)})$ of length n. So $T(y^{(h)})$ tends to the zero vector of $W_{n-1}(K)$. On other hand, $y^{(h)}$ is a Cauchy sequence in $(W_n(K), d_n)$ as it is a translated sequence of a Cauchy sequence. Let $y^{(h)} = (T(y^{(h)}), \beta_{n-1}^{(h)})$ with $\beta_{n-1}^{(h)} \in K$ and $T(y^{(h)})$ being the $n-1$ first components of $y^{(h)}$. There is $\Delta_{n-1} \in K$ such that:

$$y^{(h+1)} - y^{(h)} = (T(y^{(h+1)}) - T(y^{(h)}), \beta_{n-1}^{(h+1)} - \beta_{n-1}^{(h)} + \Delta_{n-1}).$$

By Lemma 2.2, Δ_{n-1} is a homogeneous polynomial in $y_0^{(h+1)}, ..., y_{n-2}^{(h+1)}$, $y_0^{(h)}, ..., y_{n-2}^{(h)}$ so it converges to 0 as for all i, $y_i^{(h)}$ and $y_i^{(h+1)}$ tend to 0. Hence $(\beta_{n-1}^{(h+1)} - \beta_{n-1}^{(h)})_h$ tends to 0. Thus $\beta_{n-1}^{(h)}$ is a Cauchy sequence and therefore it converges to β_{n-1} in K. We deduce that $y^{(h)}$ converges to $(0, ..., 0, \beta_{n-1})$. So $x^{(h)}$ converges to $l + (0, ..., 0, \beta_{n-1})$ and $W_n(k)$ is a complete group. □

In the following, the notation $W_n(\mathfrak{p}_K)$ design the set of Witt vectors of length n with components in the maximal ideal $\mathfrak{p}_K$.

Lemma 2.7. *Let $x \in W_n(\mathcal{O}_K)$ then $x = y + z$ with $y \in W_n(k)$ and $z \in W_n(\mathfrak{p}_K)$.*

Proof. By induction on n. If $n = 1$, the property is obvious.

Assume now that the property is satisfied for all Witt vectors of length less than or equal to $n-1$. Let $x = (x_0, ..., x_{n-2}, x_{n-1}) \in W_n(\mathcal{O}_K)$ and $x' = (x_0, ..., x_{n-2})$ its truncation in $W_{n-1}(\mathcal{O}_K)$. By induction hypothesis, there are $y' \in W_{n-1}(k)$ and $z' \in W_{n-1}(\mathfrak{p}_K)$ such that $x' = y' + z'$.

We have to prove that there exist $y_{n-1} \in k$ and $z_{n-1} \in \mathfrak{p}_K$ such that $x = y + z$ with y and z some Witt vectors of length n for which the $n-1$ first components are respectively the components of y' and z'. By Lemma 2.2, $x_{n-1} - \Sigma_{n-1} = y_{n-1} + z_{n-1}$ where Σ_{n-1} is a homogeneous polynomial in $y_0, ..., y_{n-2}, z_0, ..., z_{n-2}$. Substitute the values of y' and z' into Σ_{n-1} so $v_K(\Sigma_{n-1})$ is non negative. Since $v_K(x_{n-1})$ is non negative, then $x_{n-1} - \Sigma_{n-1}$ belongs to $\mathcal{O}_K$. We then find y_{n-1} in k and z_{n-1} in $\mathfrak{p}_K$. □

2.5. The case of an algebraically closed residue field.

From now, let k be a finite algebraically closed field. In this paragraph, we give some results about Witt vectors in $W_n(k)$.

Lemma 2.8. *If k is an algebraically closed field then $W_n(k) = \wp(W_n(k))$.*

Proof. It is obvious that $\wp(W_n(k)) \subset W_n(k)$.

Now the inclusion $W_n(k) \subset \wp(W_n(k))$ is obvious for $n = 1$. We assume the property $W_n(k) \subset \wp(W_n(k))$ is satisfied up to n.

Let $x = (x_0, ..., x_n) \in W_{n+1}(k)$. We have $x_0 \in k$ so there exists a in k such that $x_0 = \wp(a)$. Let $\{a\}$ be the Witt vector of length $n+1$: $(a, 0, ..., 0)$. So

$$x - \wp(\{a\}) = (0, x'_1, ..., x'_n) = V(x'_1, ..., x'_n).$$

By induction hypothesis, for any $(x'_1, ..., x'_n) \in W_n(k)$ there exists $(y_1, ..., y_n)$ in $W_n(k)$ such that $(x'_1, ..., x'_n) = \wp(y_1, ..., y_n)$. So

$$x - \wp(\{a\}) = V(x'_1, ..., x'_n) = V(\wp(y_1, ..., y_n)) = \wp(V(y_1, ..., y_n)).$$

Hence $x = \wp(\{a\}) + \wp(V(y_1, ..., y_n)) = \wp(\{a\} + V(y_1, ..., y_n))$. □

Proposition 2.9. *A Witt vector in $W_n(\mathcal{O}_K)$ belongs to $\wp(W_n(\mathcal{O}_K))$.*

Proof. Firstly, if $x = (x_0, ..., x_{n-1}) \in W_n(\mathfrak{p}_K)$.

We have $F^h x = (x_0^{p^h}, x_1^{p^h}, ..., x_{n-1}^{p^h})$.

$$m_n(F^h x) = \min(p^{n-1-\iota} v_K(x_\iota^{p^h})) = p^h \min(p^{n-1-\iota} v_K(x_\iota)) = p^h m_n(x).$$

Hence $m_n(F^h x) \geq p^h$ as $m_n(x) \geq 1$, so $m_n(F^h x)$ tends to $+\infty$.

Let $y = -\sum_{h \geq 0} F^h x$, by Lemma 2.6, the series y converges. Since the Frobenius map F is continuous, we get:

$$\wp(y) = (F - Id)(y) = -\sum_{h \geq 0} F^{h+1} x + \sum_{h \geq 0} F^h x = x.$$

So $x \in \wp(W_n(\mathcal{O}_K))$.

If one or more components are series of valuation zero. By Lemma 2.7, $x = y + z$ with $y \in W_n(k)$ and $z \in W_n(\mathfrak{p}_K)$. Since k is algebraically closed, then $W_n(k) \subset \wp(W_n(k))$. As $W_n(\mathfrak{p}_K) \subset \wp(W_n(\mathcal{O}_K))$ then x is the sum of two elements in $\wp(W_n(\mathcal{O}_K))$ and so $x \in \wp(W_n(\mathcal{O}_K))$. □

We deduce from this the following reduction of Witt vectors :

Proposition 2.10. *Every Witt vector $x \in W_n(K)$ is congruent modulo $\wp(W_n(K))$ to a vector $(y_0, y_1, ..., y_{n-1})$ where for all $\iota = 0, ..., n-1$, the component y_ι is a polynomial in t^{-1} with coefficients in k without constant term.*

Proof. By Proposition 2.9, it suffices to show that every Witt vector can be written as the sum of two vectors $(y_0, ..., y_{n-1})$ and $(z_0, ..., z_{n-1})$, where for every $\iota = 0, 1, ..., n-1$, $y_\iota \in t^{-1}k[t^{-1}]$ and $z_\iota \in \mathcal{O}_K$.

If $n = 1$, we have $W_1(K) = K$, so the property is satisfied.

Assume that the property is satisfied up to $n-1$. Let $x \in W_n(K)$ and x' its truncation in $W_{n-1}(K)$. Let y' and z' be two Witt vectors of length $n-1$ such that $y' = T(y)$, $z' = T(z)$ and $x' = y' + z'$ by induction hypothesis. Assume that for any $0 \leq \iota \leq n-2$, $y'_\iota \in t^{-1}k[t^{-1}]$ and $z' \in W_{n-1}(k[\![t]\!])$. There is $\Sigma_{n-1} \in \mathbb{Z}[y_0, ..., y_{n-2}, z_0, ..., z_{n-2}]$ such that $(y+z)_{n-1} = y_{n-1} + z_{n-1} + \Sigma_{n-1}$.

Then $x_{n-1} - \Sigma_{n-1}$ can be written into the form $x_{n-1} - \Sigma_{n-1} = y_{n-1} + z_{n-1}$ with $y_{n-1} \in t^{-1}k[t^{-1}]$ and $z_{n-1} \in k[\![t]\!]$. We verify that $y + z = x$. □

2.6. The filtered $W_n(k)$-submodule $\mathcal{B}_n$.

Denote by $\mathbb{N}_p$ the set of positive integers coprime to p and for each $x \in K$, let $\{x\}$ be the Witt vector of length n given by $(x, 0, ..., 0)$.

Definition 2.11. *Let $\mathcal{B}_n$ be the $W_n(k)$-module generated by vectors $\{t^{-\iota}\}$ with $\iota \in \mathbb{N}_p$.*

Elements of $\mathcal{B}_n$ are vectors in $W_n(K)$ of the form $a = \sum_{\iota \in \mathbb{N}_p} a_\iota \{t^{-\iota}\}$ with $a_\iota \in W_n(k)$ and $a_\iota = 0$ for ι sufficiently large. This form is unique:

Lemma 2.12. *The elements $\{t^{-\iota}\}$ with $\iota \in \mathbb{N}_p$ are linearly independent over $W_n(k)$.*

Proof. Let $a_\iota = (a_{\iota,0}, ..., a_{\iota,n-1}) \in W_n(k)$. By Proposition 1.10, [14], we have:

$$\begin{aligned} a_\iota\{t^{-\iota}\} &= (a_{\iota,0}, ..., a_{\iota,h}, ..., a_{\iota,n-1})\{t^{-\iota}\} \\ &= (a_{\iota,0}t^{-\iota}, ..., a_{\iota,h}t^{-\iota p^h}, ..., a_{\iota,n-1}t^{-\iota p^{n-1}}). \end{aligned}$$

So each component of $a_\iota\{t^{-\iota}\}$ is a monomial in $t^{-\iota p^h}$ with coefficient $a_{\iota,h}$ where $0 \leq h \leq n-1$ and $\iota \in \mathbb{N}_p$. Hence by Lemma 2.2:

$$\sum_{\iota\in\mathbb{N}_p} a_\iota\{t^{-\iota}\} = \Big(\sum_{\iota\in\mathbb{N}_p} a_{\iota,0}t^{-\iota}, ..., \sum_{\iota\in\mathbb{N}_p} a_{\iota,h}t^{-\iota p^h} + \Sigma_h, ..., \sum_{\iota\in\mathbb{N}_p} a_{\iota,n-1}t^{-\iota p^{n-1}} + \Sigma_{n-1}\Big).$$

The h^{th} component of $\sum_{\iota\in\mathbb{N}_p} a_\iota\{t^{-\iota}\}$ is $\sum_{\iota\in\mathbb{N}_p} a_{\iota,h}t^{-\iota p^h} + \Sigma_h$ with Σ_h a homogeneous polynomial in $a_{\iota,h'}t^{-\iota p^{h'}}$ with $h' < h$. Thus Σ_h are without constant term. Now, by induction on the rank of the components, if $\sum_{\iota\in\mathbb{N}_p} a_\iota\{t^{-\iota}\} = 0$ then every Σ_h is zero and then each $a_{\iota,h}$ is 0. □

Remark. The truncation T will send $\mathcal{B}_n$ to $\mathcal{B}_{n-1}$. Moreover $T(\mathcal{B}_n) = \mathcal{B}_{n-1}$.

The exponent of the group $W_n(k)$ is p^n and let $\text{ord}(a)$ be the order of a in $W_n(k)$ [12]. We have also $\text{ord}(a+b) \leq \max\{\text{ord}(a), \text{ord}(b)\}$.

Definition 2.13. *For any $a = \sum_{\iota\in\mathbb{N}_p} a_\iota\{t^{-\iota}\} \in \mathcal{B}_n$, we put:*

$$\begin{array}{ll} \rho_n(a) = \max(\iota\frac{ord(a_\iota)}{p}) & \text{for all } a_\iota \neq 0 \\ \rho_n(0) = 0 & \text{otherwise.} \end{array}$$

Lemma 2.14. *For any a and b in $\mathcal{B}_n$, we have:*

$$\rho_n(a+b) \leq \max\{\rho_n(a), \rho_n(b)\}.$$

The proof is obvious. By this lemma, we get an increasing filtration on $\mathcal{B}_n$.

Definition 2.15. *Let $\mathcal{A}_n$ be the set of elements $a = \sum_{\iota\in\mathbb{N}_p} a_\iota\{t^{-\iota}\} \in \mathcal{B}_n$ with at least one element $a_\iota \in W_n(k)^*$.*

Lemma 2.16. *Let $a = \sum_{\iota\in\mathbb{N}_p} a_\iota\{t^{-\iota}\} \in \mathcal{B}_n$. Then the following assertions are equivalent:*
(1) $a \in \mathcal{A}_n$.
(2) $\max\{ord(a_\iota)$ such that $a_\iota \neq 0\} = p^n$.
(3) $a \notin \boldsymbol{p}(\mathcal{B}_n)$. where $\boldsymbol{p}$ is the multiplication by p in $W_n(K)$.

Proof. (1) ⇔ (2) : Assume that $a \in \mathcal{A}_n$ so there is $\iota_0 \in \mathbb{N}_p$ such that $a_{\iota_0} \in W_n(k)^*$. Since $a \in W_n(k)$ has order p^n if and only if it is invertible, so ord $a_{\iota_0} = p^n$ and $\max\{\text{ord } (a_\iota)$ such that $a_\iota \neq 0\} = p^n$ is equivalent to a belongs to $\mathcal{A}_n$.

(1) ⇒ (3): A Witt vector is invertible if and only if its first component is invertible. Let $b = (b_0, ..., b_{n-1})$ be a vector in $\mathcal{B}_n$. Since $\mathbf{p} = VF$ [12], so $\mathbf{p}(b) = VF(b_0, ..., b_{n-1}) = (0, b_0^p, ..., b_{n-2}^p)$. So $\mathbf{p}(b)$ cannot be invertible.

(3) $\Rightarrow$ (2): If the vector a is such that $\max\{\mathrm{ord}(a_\iota) \text{ such that } a_\iota \neq 0\} \leq p^n$ then there exists a vector b such that $a = \mathbf{p}(b)$. □

2.7. The direct sum $W_n(K) = \wp(W_n(K)) \oplus \mathcal{B}_n$.

The main result of this paragraph is the direct sum of abelian groups: $W_n(K) = \wp(W_n(K)) \oplus \mathcal{B}_n$. It will be very useful in the following to get a way to describe an action of $\mathcal{G}_0(k)$ on $\mathcal{B}_n$. We firstly prove some lemmas:

Lemma 2.17. *Let $x = \sum_{\iota \geq 1} \alpha_\iota t^\iota$ in $K \setminus k$. Let $\nu(x)$ be the minimum integer such that there exists $\iota \geq 1$ with $v_p(\iota) = \nu(x)$ and $\alpha_\iota \neq 0$. Then we have $\nu(\wp(x)) = \nu(x)$.*

Proof. For any x, let $I(x) = \{\iota \in \mathbb{Z}, \alpha_\iota \neq 0\}$ so $\nu(x) = \min\{v_p(\iota) \text{ with } \iota \in I(x)\}$.

We have $x^p = \sum_{\iota \geq 1} \alpha_\iota^p t^{-\iota p}$ so $I(x^p) = \mathbf{p}(I(x))$ and $I(x^p - x) \subset \mathbf{p}(I(x)) \cup I(x)$.

By definition $v_p(\iota) \geq \nu(x)$ for all $\iota \in I(x)$ so $v_p(\iota) \geq \nu(x)$ for all $\iota \in \mathbf{p}(I(x))$.

Therefore $v_p(\iota) \geq \nu(x)$ for all $\iota \in \mathbf{p}(I(x)) \cup I(x)$. Hence $\nu(x^p - x) \geq \nu(x)$.

Conversely, let $\iota_0 \in \mathbb{N}$ such that $v_p(\iota_0) = \nu(x)$. We have $\iota_0 \in I(x) \setminus \mathbf{p}(I(x))$ and so $\iota_0 \in I(x^p - x)$. Hence, we have $\nu(x^p - x) \leq v_p(\iota_0) = \nu(x)$. □

Lemma 2.18. *If $x \in K$ and $m \in \mathbb{N}^*$ then there exists $y \in K$ and $\alpha_\iota \in k$ for all $\iota \in \mathbb{N}_p$ such that $\alpha_\iota = 0$ for $\iota >> 0$ and $x = \sum_{\iota \in \mathbb{N}_p} \alpha_\iota t^{-\iota p^{m-1}} + y^p - y$.*

Proof. If $m = 1$, let $x = \sum \alpha_\iota t^{-\iota}$. Using Proposition 2.10 we obtain $x = x' + y^p - y$ where $y \in K$ and x' a polynomial in t^{-1} without constant term.

So it suffices to show that each term $\alpha_\iota t^{-\iota}$ belongs to $\mathcal{B}_1 + \wp K$. We will proceed by induction on $\iota \in \mathbb{N}$. We consider two cases:

If $\gcd(\iota, p) = 1$, then $\sum \alpha_\iota t^{-\iota} \in \mathcal{B}_1$.

If $\gcd(\iota, p) \neq 1$, so $\iota = \iota' p$ then $\alpha'_\iota t^{-\iota} = \alpha'_\iota t^{-\iota' p}$.

Since $k = \mathbb{F}_p^{alg}$, $\alpha'_\iota t^{-\iota' p} = \alpha''^p_\iota t^{-\iota' p} = (\alpha''_\iota t^{-\iota'})^p - \alpha''_\iota t^{-\iota'} + \alpha''_\iota t^{-\iota'}$ and $(\alpha''_\iota t^{-\iota'})^p - \alpha''_\iota t^{-\iota'} \in \wp K$ and $\alpha''_\iota t^{-\iota'} \in \mathcal{B}_1 + \wp K$ by induction hypothesis.

Now, if we have $x = \sum_{\iota \in \mathbb{N}_p} (-\alpha'_\iota) t^{-\iota p^{m-2}} + y^p - y$ with $y \in K$, we put $y = y' + \sum_{\iota \in \mathbb{N}_p} \alpha'_\iota t^{-\iota p^{m-2}}$ so that $y^p = y'^p + \sum_{\iota \in \mathbb{N}_p} \alpha'^p_\iota t^{-\iota p^{m-1}}$. Thus

$$\begin{aligned} y^p - y &= y'^p - y' + \sum_{\iota \in \mathbb{N}_p} \alpha'^p_\iota t^{-\iota p^{m-1}} - \sum_{\iota \in \mathbb{N}_p} \alpha'_\iota t^{-\iota p^{m-2}} \\ &= x + \sum_{\iota \in \mathbb{N}_p} \alpha'^p_\iota t^{-\iota p^{m-1}}. \end{aligned}$$

So x satisfies the conditions. □

Proposition 2.19. *We have the direct sum of abelian groups:*

$$W_n(K) = \wp(W_n(K)) \oplus \mathcal{B}_n.$$

Proof. 1) We want, $\mathcal{B}_n \cap \wp(W_n(K)) = \{0\}$.

If $n = 1$, then we have to show that $\wp(K) \cap \mathcal{B}_1 = \{0\}$. We use the 7^{th} property of Proposition 4.2 [13]. If $x \in \mathcal{B}_1$ and $x \neq 0$ then $v_K(x)$ is negative coprime to p and if $x \in \wp(K)$ then $v_K(x)$ is either positive or negative but in this latter case, $v_K(x)$ is a multiple of p. So $\wp(W_n(K)) \cap \mathcal{B}_n = \{0\}$.

Now, we want to prove that for every n, $\wp(W_n(K)) \cap \mathcal{B}_n = \{0\}$.

Let $a = \sum_{\iota \in \mathbb{N}_p} a_\iota \{t^{-\iota}\} \in \mathcal{B}_n \cap \wp(W_n(K))$. So $a = \wp(x_0, ..., x_{n-2}, x_{n-1})$ with $x_\iota \in K$. Assume that $(x_0, ..., x_{n-1}) \neq 0$. Denote by a' (resp a'_ι, resp $\{t^{-\iota}\}_{n-1}$) the truncation in W_{n-1} of the Witt vector a (resp a_ι, resp $\{t^{-\iota}\}$). By induction hypothesis, if $a' = \sum_{i \in \mathbb{N}_p} a'_\iota \{t^{-\iota}\}_{n-1} = \wp(x_0, ..., x_{n-2}) = 0$ then every $a'_\iota = 0$ by Lemma 2.12.

So $a_\iota = (0, ..., 0, a_{\iota,n-1})$ with $a_{\iota,n-1} \in k$ and $x_\iota \in \mathbb{F}_p$ for $0 \leq \iota \leq n-2$. Thus:

$$\begin{aligned} a &= (0, ..., 0, \sum_{\iota \in \mathbb{N}_p} a_{\iota,n-1} t^{-\iota p^{n-1}}) \\ &= (x_0^p, ..., x_{n-2}^p, x_{n-1}^p) - (x_0, ..., x_{n-2}, x_{n-1}). \end{aligned}$$

Hence $\sum_{\iota \in \mathbb{N}_p} a_{\iota,n-1} t^{-\iota p^{n-1}} = x_{n-1}^p - x_{n-1} + \Sigma_{n-1}$ with Σ_{n-1}, by Lemma 2.2, a homogeneous polynomial in $x_0, ..., x_{n-2}$ and since $x_\iota \in \mathbb{F}_p$ for $0 \leq \iota \leq n-2$ then $v_K(x_\iota) = 0$ and so $\Sigma_{n-1} \in \mathbb{F}_p$. So there is Σ'_{n-1} such that $\Sigma_{n-1} = \Sigma'^p_{n-1} - \Sigma'_{n-1}$. We now write $x'_{n-1} = x_{n-1} + \Sigma'_{n-1}$. We have:

$$x'^p_{n-1} - x'_{n-1} = \sum_{\iota \in \mathbb{N}_p} a_{\iota,n-1} t^{-\iota p^{n-1}}$$

We suppose there exists $\iota_0 \in \mathbb{N}_p$ such that $a_{\iota_0,n-1} \neq 0$, so

$$\nu\Big(\sum_{\iota \in \mathbb{N}_p} a_{\iota_0,n-1} t^{-\iota_0 p^{n-1}} \Big) = n - 1.$$

In other hand, by Lemma 2.17, we have:

$$\nu\Big(\sum_{\iota \in \mathbb{N}_p} a_{\iota_0,n-1} t^{-\iota_0 p^{n-1}} \Big) = \nu(x'^p_{n-1} - x'_{n-1}) = \nu(x'_{n-1}).$$

Hence $\nu(x'_{n-1}) = n-1$ so $v_K(x'_{n-1})$ is a multiple of p^{n-1}. Since $v_K(x'_{n-1}) < 0$ then $v_K(x'^p_{n-1} - x'_{n-1}) = p v_K(x'_{n-1})$. So $v_K(\sum_{\iota \in \mathbb{N}_p} a_{\iota_0,n-1} t^{-\iota_0 p^{n-1}})$ is a multiple of p^n.

We get a contradiction with the fact that $v_K(\sum_{\iota \in \mathbb{N}_p} a_{\iota_0,n-1} t^{-\iota_0 p^{n-1}})$ is of the form $\iota_0 p^{n-1}$ with $\iota_0 \in \mathbb{N}_p$. Hence $x = 0$ and we get the result $\mathcal{B}_n \cap \wp(W_n(K)) = \{0\}$ for all n.

2) Secondly, we have to prove that for any n, $W_n(K) = \wp(W_n(K)) + \mathcal{B}_n$.

If $n = 1$, we have already show it in the case $m = 1$ in Lemma 2.18.

Let $x \in W_n(K)$. By induction hypothesis, we have $T(x) \in \wp(W_{n-1}(K)) + \mathcal{B}_{n-1}$. Since the map T is an epimorphism, we can find $y \in W_n(K)$ and

$b \in \mathcal{B}_n$ such that: $T(x) = \wp(T(y)) + T(b) = T(\wp(y)) + T(b) = T(\wp(y) + b)$. So $x = \wp(y) + b + (0, ..., 0, \chi)$ with $\chi \in K$.

We can write by Lemma 2.18: $\chi = \sum_\iota \chi_\iota t^{-\iota p^{n-1}} + z^p - z$.

$$\begin{aligned}(0, ..., 0, \chi) &= (0, ..., 0, \sum_\iota \chi_\iota t^{-\iota p^{n-1}} + z^p - z) \\ &= (0, ..., 0, \sum_\iota \chi_\iota t^{-\iota p^{n-1}}) + (0, ..., 0, z^p) - (0, ..., 0, z) \\ &= \sum_\iota (0, ..., 0, \chi_\iota)\{t^{-\iota}\} + \wp(0, ..., 0, z)\end{aligned}$$

So $\sum_\iota (0, ..., 0, \chi_\iota)\{t^{-\iota}\}$ belongs to $\mathcal{B}_n$ and $\wp(0, ..., 0, z)$ belongs to $\wp(W_n(K))$. Hence we have for any n, $W_n(K) = \wp(W_n(K)) + \mathcal{B}_n$. □

3. Applications to cyclic extensions of degree p^n.

Let L/K be a field extension, if $x = (x_0, ..., x_{n-1})$ is a Witt vector in $W_n(L)$, the notation $K(x)$ will denote the extension $K(x_0, ..., x_{n-1})$ of K.

We will describe a way to characterize cyclic totally ramified extensions of degree p^n by a unique element of $\mathcal{A}_n$. We also determine the ramification breaks of these extensions in terms of coefficients of this element of $\mathcal{A}_n$.

We recall that k designs the algebraic closure of $\mathbb{F}_p$.

3.1. The conductor of a cyclic extension.

Let k' be a field of characteristic p and $K' = k'((t))$. Let L'/K' be a cyclic totally ramified extension of degree p^n. Let U be the unit group of K'. The conductor of the extension L'/K' is defined by $(t)^{r(L'/K')}$ where :

$$r(L'/K') = \min\{l \in \mathbb{N} \text{ such that } U^{(l)} \subset N_{L'/K'}(L'^*)\}.$$

with $U^{(l)} = \{u \in U \text{ such that } v_{K'}(u-1) \geq l\} = 1 + t^l k'[\![t]\!]$ the l^{th} term in the natural filtration of U.

Let $s(L/K)$ be the greatest ramification break of L/K, that is the greatest integer such that $\mathrm{Gal}(L/K)_{s(L/K)} \neq \{1\}$. The integer $r(L/K)$ is equal to $\varphi(s(L/K)) + 1$ where φ is the reciprocity map of the Herbrand function [11]. So a link between the conductor and the greatest ramification break holds.

Lemma 3.1. *Let L/K be a cyclic extension of degree p^n and K' be a closed subfield of K such that $L = KL'$ with L'/K' of degree p^n. Assume that K/K' is unramified. The two extensions L'/K' and L/K have the same ramification breaks. In particular the conductor of L/K is the same as the conductor of L'/K'.*

Proof. Since K/K' is unramified, the extension L/L' is also unramified. The map $\sigma \mapsto \sigma_{|L'}$ is an isomorphism between $\mathrm{Gal}(L/K)$ and $\mathrm{Gal}(L'/K')$.

We have:

$$\mathrm{Gal}(L/K)_\omega = \Big\{\sigma \in \mathrm{Gal}(L/K) \text{ such that } v_L\Big(\frac{\sigma(\pi_L)}{\pi_L} - 1\Big) \geq \omega\Big\}$$

where π_L is a prime element of L. Let π be a prime element of L', since the extension L/L' is unramified then π is also a prime element of L. Hence $\sigma \in \mathrm{Gal}(L/K)_\omega$ if and only if $\sigma_{|L'} \in \mathrm{Gal}(L'/K')_\omega$. So the ramification breaks in lower numbering are the same. We get, with the Herbrand functions, the same ramification in upper numbering.

By [11], Proposition 9, we know that the conductor is equal to $(t)^{r(L/K)}$ where $r(L/K)$ is the greatest ramification break in upper numbering plus one, so the conductor of the extension L/K is preserved. □

The map from $G(L/K)$ to $G(L'/K')$ which associates to σ, the element $\sigma_{|L'}$ is an isomorphism of filtrered groups by the filtrations of ramification.

3.2. Parametrization of cyclic extensions.

We describe in this paragraph, a way to characterize cyclic totally ramified extensions of degree p^n from an element of $\mathcal{A}_n$.

Remark. By Artin-Schreier-Witt theory, if L/K is a cyclic extension of degree p^n, then there exists a non degenerate pairing ([2], chap IX):

$$\begin{array}{rcl} (\wp W_n(L) \cap W_n(K))/\wp W_n(K) \times \mathrm{Gal}(L/K) & \to & W_n(\mathbb{F}_p) \\ (\overline{a}, \sigma) & \mapsto & [\overline{a}, \sigma\rangle = \sigma\alpha - \alpha. \end{array}$$

where $\wp(\alpha) = a$ and $\overline{a}$ denotes the class of a modulo $\wp(W_n(K))$. Moreover this pairing puts $\mathrm{Gal}(L/K)$ and $(\wp W_n(L) \cap W_n(K))/\wp W_n(K)$ in duality.

Proposition 3.2. *Let L/K be a cyclic totally ramified extension of degree p^n and σ a Galois group generator of L/K. There is a unique element $a \in \mathcal{A}_n$ such that:*
1) $L = K(\wp^{-1}(a))$
2) $[\overline{a}, \sigma\rangle = 1 = (1, 0, ..., 0)$ where $\overline{a}$ denotes the class of a modulo $\wp(W_n(K))$.

Proof. Prove firstly the uniqueness of the element a. By Proposition 2.19, we have: $\wp(W_n(K)) \cap \mathcal{B}_n = \{0\}$. If $L = K(\wp^{-1}(a)) = K(\wp^{-1}(a'))$ and $[a, \sigma\rangle = [a', \sigma\rangle$. Then by additivity on the right of Artin's symbol, we have:

$$[\overline{a}, \sigma\rangle - [\overline{a'}, \sigma\rangle = [\overline{a - a'}, \sigma\rangle = 0.$$

Since the pairing is non-degenerate then $a - a' \in \wp(W_n(K))$. As a and a' belong to $\mathcal{B}_n$ and since $\mathcal{B}_n \cap \wp(W_n(K)) = \{0\}$ then necessarily $a = a'$.

Prove now the existence of such an element a. By the previous remark:

$$\mathrm{Hom}(\mathrm{Gal}(L/K), W_n(\mathbb{F}_p)) \simeq (\wp(W_n(L)) \cap W_n(K))/\wp(W_n(K)),$$

where the groups $\mathrm{Gal}(L/K)$ and $W_n(\mathbb{F}_p)$ are cyclic of order p^n. Then there is a homomorphism φ which associates to σ the element 1 in $W_n(\mathbb{F}_p)$. So φ corresponds in the above isomorphism to $\overline{a} \in \wp(W_n(L)) \cap W_n(K)/\wp(W_n(K))$ generating the group. Let a be a lift of $\overline{a}$ in $\wp(W_n(L)) \cap W_n(K)$.

Since, $a \in \wp(W_n(L))$ then $K(\wp^{-1}(a)) \subset L$.

Conversely, we want to prove that $H = \mathrm{Gal}(L/K(\wp^{-1}(a))) = \{id\}$. Let $\tau \in H$, so for any integer λ, we have,

$$[\lambda\overline{a}, \tau\rangle = \lambda[\overline{a}, \tau\rangle = \lambda(\tau\alpha - \alpha)$$

with $\wp(\alpha) = a$. Thus α belongs to $K(\wp^{-1}(a))$ so $\tau\alpha = \alpha$ therefore $[\overline{a}, \tau\rangle = 0$. So τ is trivial as it is orthogonal to each element of $\wp(W_n(L)) \cap W_n(K)$.

The element a belongs to $\mathcal{A}_n$ since the extension L/K has degree p^n. □

3.3. An explicit formula for ramification breaks.

We describe in this paragraph a result on ramification breaks of the Galois groups of a tower of extensions. For that, we firstly generalize a result due to K. Kanesaka and K. Sekiguchi [6] to any cyclic ramified extensions.

We recall that we denote by $\mathrm{ord}(a)$ the order of a in the additive group $W_n(k)$. This order divides p^n [12].

Lemma 3.3. *Let $a = \sum_{\iota \in \mathbb{N}_p} a_\iota \{t^{-\iota}\} \in \mathcal{A}_n$. Let $L = K(\wp^{-1}(a))$ be a cyclic extension of degree p^n, the conductor is $(t)^{r(L/K)}$ with $r(L/K)$ defined by:*

$$r(L/K) = \max_{\iota \in \mathbb{N}_p} \Big\{ \frac{\iota}{p} ord(a_\iota) + 1 \text{ for } a_\iota \neq 0 \Big\}.$$

Proof. To prove this result, we use Lemma 3.1 and a paper due to K. Kanesaka and K.Sekiguchi [6]. Let $L = K(\wp^{-1}(a))$ be a cyclic extension of K of degree p^n with $a \in \mathcal{A}_n$. Let $a = \sum_{\iota \in \mathbb{N}_p} a_\iota \{t^{-\iota}\}$ with $a_\iota \in W_n(k)$.

Let k' be the subfield of k generated by the components of the vectors a_ι. As $a_\iota = 0$ for all but a finite number of $\iota \in \mathbb{N}_p$, k' is a finite field. Put $K' = k'(\!(t)\!)$ and now let $L' = K'(\wp^{-1}(a))$. Thanks to Lemma 3.1, we know that the ramification breaks of L'/K' are preserved in the extension L/K. So $r(L/K) = r(L'/K')$. By Kanesaka and Sekiguchi's theorem, ([6], p.367):

$$r(L'/K') = \max\{\iota p^{l_\iota - 1} + 1 \text{ such that } \iota \in \mathbb{N}_p \text{ and } a_\iota \neq 0, l_\iota \geq 1\}$$

with $l_\iota = n - s_\iota$ and s_ι defined by :

$$\begin{aligned} s_\iota &= \max\{\nu \text{ such that } p^\nu \mid a_\iota\} && \text{if } a_\iota \neq 0 \\ s_\iota &= n && \text{if } a_\iota = 0. \end{aligned}$$

We have to prove $\mathrm{ord}(a_\iota) = p^{l_\iota}$. This is clear if $a_\iota = 0$ so we assume $a_\iota \neq 0$. By definition there is an invertible vector α_ι such that $a_\iota = p^{s_\iota}\alpha_\iota$ with α_ι in $W_n(k) \setminus \mathbf{p}(W_n(k))$. So $\mathrm{ord}(\alpha_\iota) = p^n$ since $W_n(k)$ has characteristic p^n. Hence

$$\mathrm{ord}(a_\iota) = \mathrm{ord}(p^{s_\iota}\alpha_\iota) = \frac{\mathrm{ord}(\alpha_\iota)}{\gcd(\mathrm{ord}(\alpha_\iota), p^{s_\iota})} = p^{n-s_\iota} = p^{l_\iota}$$

which concludes the proof. □

Definition 3.4. *For any $0 < j \leq n$, we define the maps T^{n-j} such that:*

$$\begin{array}{rccc} T^{n-j}: & W_n(K) & \to & W_j(K) \\ & (x_0,...,x_{n-1}) & \mapsto & (x_0,...,x_{j-1}). \end{array}$$

Lemma 3.5. *Let L/K be a cyclic totally ramified extension of degree p^n such that $L = K(\wp^{-1}(a))$ with $a \in W_n(K)$. Let K_j be the subextension of L/K such that $K_j = K(\wp^{-1}(T^{n-j}(a)))$. Then K_j/K is an extension of degree p^j.*

Proof. We obviously have $K_j \subset K_{j+1} \subset L$.

Let $L = K(\wp^{-1}(a))$ with $a \in W_n(K)$. It suffices to show that for every integer j between 1 and n and every $a \in W_j(K)$, we have:

$$[K(\wp^{-1}(a)) : K(\wp^{-1}(T(a)))] = p.$$

Let $x = (x_0, ...x_{n-1})$ be an element of $W_n(K)$ such that $\wp(x) = a$. Since $\wp$ commutes with the truncation map T, we have:

$$\wp(x_0,...,x_{j-1}) = a \Rightarrow \wp(x_0,...,x_{j-2}) = T(a).$$

We have $K(x_0,...,x_{j-1}) = K(x_0,...,x_{j-2})(x_{j-1})$. By Lemma 2.2, the j^{th} component of $\wp(x_0,..,x_{j-1})$ is $x_{j-1}^p - x_{j-1} + \Delta_{j-1}(x_0,..,x_{j-2})$ where Δ_{j-1} is a polynomial with integer coefficients. So $\wp(x_{j-1}) = x_{j-1}^p - x_{j-1} \in K(x_0,...x_{j-2})$.

By Artin-Schreier-Witt theory, $K(x_0,...,x_{j-1})/K(x_0,...,x_{j-2})$ is an extension of degree 1 or p. Since L/K has degree p^n, then the extension $K(x_0,...,x_{n-1})/K(x_0,...,x_{n-2})$ and each $K(\wp^{-1}(T^j(a)))/K(\wp^{-1}(T^{j+1}(a)))$ has degree p and then the extension $K(\wp^{-1}(T^j(a)))/K$ has degree p^j. □

Proposition 3.6. *Let $a \in \mathcal{A}_n$. The ramification breaks in upper numbering of the Galois group Gal$(K(\wp^{-1}(a))/K)$ are $\rho_{n-j}(T^j(a))$ for $0 \leq j \leq n-1$.*

Proof. Let a be an element of $\mathcal{A}_n$ and $L = K(\wp^{-1}(a))$. Since the truncation map is a ring homomorphism which commutes with the additive law, we obtain:

$$T^j(a) = T^j(\sum_{\iota \in \mathbb{N}_p} a_\iota \{t^{-\iota}\}) = \sum_{\iota \in \mathbb{N}_p} T^j(a_\iota \{t^{-\iota}\}) = \sum_{\iota \in \mathbb{N}_p} T^j(a_\iota) T^j(\{t^{-\iota}\}).$$

So we have:

$$\rho_{n-j}(T^j(a)) = \max_{\iota \in \mathbb{N}_p} \Big(\frac{\iota}{p} \text{ord}(T^j(a_\iota)) \Big).$$

Therefore, following Lemma 3.3, we obtain that the conductor of each subextension K_j/K is $(t)^{r(K_j/K)}$ with:

$$r(K_j/K) = \max_{\iota \in \mathbb{N}_p} \Big\{ \frac{\iota}{p} \text{ord}(T^j(a_\iota)) + 1 \Big\}.$$

For any subextension K_j/K of L/K, we put for $\delta = 0, .., j-1$,

$$i_\delta(K_j/K) = \max\{\epsilon \text{ such that } \mathrm{Gal}(K_j/K_\delta) \subset \mathrm{Gal}(K_j/K)_\epsilon\}.$$

Let $\psi_{L/K}$ be the Herbrand function for the extension L/K and $\varphi_{L/K}$ its inverse map. By the property of the function $\varphi_{L/K}$ [12], we have:

$$\mathrm{Gal}(K_j/K)_\epsilon = \mathrm{Gal}(K_j/K)^{\varphi_{L/K}(\epsilon)}.$$

In the filtration of the Galois group $\mathrm{Gal}(K_j/K)$ in lower numbering:

$$\mathrm{Gal}(K_j/K)_\epsilon = \Big\{\sigma \in \mathrm{Gal}(K_j/K) \text{ such that } \mathrm{ord}\Big(\frac{\sigma(\pi_{K_j})}{\pi_{K_j}} - 1\Big) \geq \epsilon\Big\}$$

where $\mathrm{Gal}(K_j/K) \simeq K^*/N_{K_j/K}K_j^*$. Since:

$$(K^*/N_{K_j/K}K_j^*)^u = \{1\} \Leftrightarrow U^u \subset N_{K_j/K}K_j^* \Leftrightarrow \mathrm{Gal}(K_j/K)^u = \{1\}.$$

So $r(K_j/K) = \min\{u \in \mathbb{N} \text{ such that } \mathrm{Gal}(K_j/K)^u = \{1\}\}$.

$$\begin{aligned}
\epsilon \leq i_{j-1}(K_j/K) &\Leftrightarrow \mathrm{Gal}(K_j/K_{j-1}) \subset \mathrm{Gal}(K_j/K)^{\varphi_{L/K}(\epsilon)} \\
&\Leftrightarrow \mathrm{Gal}(K_j/K)^{\varphi_{L/K}(\epsilon)} \neq \{1\} \\
&\Leftrightarrow \varphi_{L/K}(\epsilon) < r(K_j/K) \\
&\Leftrightarrow \varphi_{L/K}(\epsilon) \leq r(K_j/K) - 1 \\
&\Leftrightarrow \epsilon \leq \psi_{L/K}(r(K_j/K) - 1).
\end{aligned}$$

So $i_{j-1}(K_j/K) = \psi_{L/K}(r(K_j/K) - 1)$. Hence, in upper numbering, the ramification breaks of K_j/K is $r(K_j/K) - 1$ that is $\rho_{n-j}(T^j(a))$. □

Definition 3.7. *We call ramification breaks of $a \in \mathcal{A}_n$ the n integers defined by $\rho_{n-j}(T^j(a))$.*

By Proposition 3.2 and Proposition 3.6 we obtain the following theorem:

Theorem 3.8. *Let L/K be a cyclic totally ramified extension of degree p^n and σ a Galois group generator of L/K. There is a unique element $a \in \mathcal{A}_n$ such that:*
1) $L = K(\wp^{-1}(a))$
2) $[\overline{a}, \sigma\rangle = 1 = (1, 0, ..., 0)$ where $\overline{a}$ denotes the class of a modulo $\wp(W_n(K))$. Moreover this bijection preserves ramification breaks between $\mathcal{A}_n$ and $\mathcal{X}_n$.

4. Action of $\mathcal{G}_0(k)$ on the group $\mathcal{B}_n$.

In the following, we use an action β_n of $\mathcal{G}_0(k)$ on $\mathcal{B}_n$. The isomorphism between $\mathcal{B}_n$ and $W_n(K)/\wp(W_n(K))$ is necessary to define this action.

4.1. Definition of the action of $\mathcal{G}_0(k)$ on the ring $W_n(K)$.

Let $\gamma \in \mathcal{G}_0(k)$ and $\hat{\gamma}$ be the automorphism of K fixing k associated with γ such that $\hat{\gamma}(f) = f \circ \gamma^{-1}$ for all $f \in K$. By the Witt functor W, we can deduce an automorphism $W(\hat{\gamma})$ of $W(K)$ such that:

$$W(\hat{\gamma})(a_0, a_1, ..., a_n, ...) = (a_0 \circ \gamma^{-1}, a_1 \circ \gamma^{-1}, ..., a_n \circ \gamma^{-1}, ...).$$

We recall that I_n is the additive subgroup of $W(K)$ such that the n first components of Witt vectors are 0. We have defined $W_n(K)$ to be $W(K)/I_n$. Since $W(\hat{\gamma})(I_n)$ is I_n, we can define an automorphism $W_n(\hat{\gamma})$ in $W_n(K)$ such that $W(\hat{\gamma})(a_0, a_1, ..., a_{n-1}) = (a_0 \circ \gamma^{-1}, a_1 \circ \gamma^{-1}, ..., a_{n-1} \circ \gamma^{-1})$. Moreover $W_n(k) \subset W_n(K)^{W_n(\hat{\gamma})}$ so the automorphism $W_n(\hat{\gamma})$ is $W_n(k)$-linear.

Definition 4.1. *We define in this way an action $\hat{W}_n$ of $\mathcal{G}_0(k)$ on the ring $W_n(K)$ such that $\mathcal{G}_0(k)$ acts on every component of $W_n(K)$ i.e.:*

$$\begin{array}{rccc} \hat{W}_n : & \mathcal{G}_0(k) \times W_n(K) & \to & W_n(K) \\ & (\gamma, (a_0, a_1, ..., a_{n-1})) & \mapsto & (a_0 \circ \gamma^{-1}, a_1 \circ \gamma^{-1}, ..., a_{n-1} \circ \gamma^{-1}). \end{array}$$

That is $\hat{W}_n(\gamma) = W_n(\hat{\gamma})$.

Remarks.

- For $n = 1$, the action $\hat{W}_1$ is simply $\gamma \mapsto \hat{\gamma}$.
- The action $\hat{W}_n$ is $W_n(k)$-linear.
- The action $\hat{W}_n$ of $\mathcal{G}_0(k)$ commutes with the map $\wp$.
- The actions $\hat{W}_n$ and $\hat{W}_{n-1}$ of $\mathcal{G}_0(k)$ respectively on the rings $W_n(K)$ and $W_{n-1}(K)$ commute with the map T of $W_n(K)$ to $W_{n-1}(K)$.

4.2. Definition of the action of $\mathcal{G}_0(k)$ on the group $\mathcal{B}_n$.

The map $\wp$ commutes with $\hat{W}_n$ on $W_n(K)$. So the $W_n(\mathbb{F}_p)$-module $\wp(W_n(K))$ is globally invariant under this action and we obtain an action of $\mathcal{G}_0(k)$ on $W_n(K)/\wp(W_n(K))$. As $\mathcal{B}_n$ and $W_n(K)/\wp(W_n(K))$ are naturally isomorphic (Proposition 2.19), a linear $W_n(\mathbb{F}_p)$-automorphism $\beta_n(\gamma)$ of $\mathcal{B}_n$ holds. Finally $\beta_n : \mathcal{G}_0(k) \to \mathrm{Aut}_{W_n(\mathbb{F}_p)}(\mathcal{B}_n)$ is an action of the group $\mathcal{G}_0(k)$ on the $W_n(\mathbb{F}_p)$-module $\mathcal{B}_n$. The map $\overline{W_n}(\hat{\gamma})$ is a linear automorphism of $W_n(K)/\wp(W_n(K))$ hence $\beta_n(\gamma)$ is also a $W_n(\mathbb{F}_p)$-linear automorphism of $\mathcal{B}_n$.

Definition 4.2. *We get the action of $\mathcal{G}_0(k)$ on $\mathcal{B}_n$ for any $\gamma \in \mathcal{G}_0(k)$ and any $a \in \mathcal{B}_n$:*

$$\begin{array}{rccc} \beta_n : & \mathcal{G}_0(k) \times \mathcal{B}_n & \to & \mathcal{B}_n \\ & (\gamma, a) & \mapsto & a' \end{array}$$

where a' is the vector in the submodule $\mathcal{B}_n$ which is congruent to the vector $(a_0 \circ \gamma^{-1}, a_1 \circ \gamma^{-1}, ..., a_{n-1} \circ \gamma^{-1})$ modulo $\wp(W_n(K))$.

Lemma 4.3. *The set $\mathcal{A}_n$ is globally invariant under the action β_n.*

Proof. Let $a \in \mathcal{A}_n$ and $\gamma \in \mathcal{G}_0(k)$, we want to show that $\beta_n(\gamma)(a) \in \mathcal{A}_n$. Lemma 2.16 claims that $\mathcal{A}_n = \mathcal{B}_n \setminus \mathbf{p}(\mathcal{B}_n)$ so we must prove that if $\beta_n(\gamma)(a) \in \mathbf{p}(\mathcal{B}_n)$ then $a \in \mathbf{p}(\mathcal{B}_n)$. Let $\beta_n(\gamma)(a) = \mathbf{p}(a')$ with $a' \in \mathcal{B}_n$. Hence

$$a = \beta_n(\gamma^{-1})(\beta_n(\gamma)(a)) = \beta_n(\gamma^{-1})(\mathbf{p}(a')) = \mathbf{p}(\beta_n(\gamma^{-1})(a'))$$

so a lies in $\mathbf{p}(\mathcal{B}_n)$. Hence $\mathcal{A}_n$ is globally invariant under the action β_n. □

4.3. Link between the action β_n and the map of truncation.

We recall that the truncation map T satisfies $T(\mathcal{B}_n) = \mathcal{B}_{n-1}$.

Proposition 4.4. *The actions $\beta_n(\gamma)$ and $\beta_{n-1}(\gamma)$ of $\mathcal{G}_0(k)$ respectively on the groups $\mathcal{B}_n$ and $\mathcal{B}_{n-1}$ commute with the map of truncation T from $W_n(K)$ to $W_{n-1}(K)$.*

Proof. As T sends $\wp(W_n(K))$ in $\wp(W_{n-1}(K))$ we have an induced homomorphism $\overline{T}$ from $W_n(K)/\wp(W_n(K))$ to $W_{n-1}(K)/\wp(W_{n-1}(K))$. By the remarks after Definition 4.1 we have $T \circ W_n(\hat{\gamma}) = W_{n-1}(\hat{\gamma}) \circ T$ hence $\overline{T} \circ \overline{W_n}(\hat{\gamma}) = \overline{W_{n-1}}(\hat{\gamma}) \circ \overline{T}$, and by the identification of $\mathcal{B}_n$ and $\mathcal{B}_{n-1}$ with respectively $W_n(K)/\wp(W_n(K))$ and $W_{n-1}(K)/\wp(W_{n-1}(K))$, the map $T \circ \beta_n(\gamma)$ corresponds to $\overline{T} \circ \overline{W_n}(\hat{\gamma})$ and the map $\beta_{n-1}(\gamma) \circ T$ corresponds to $\overline{W_{n-1}}(\hat{\gamma}) \circ \overline{T}$. Therefore $T \circ \beta_n(\gamma) = \beta_{n-1}(\gamma) \circ T$. □

5. Application to the conjugacy classes of series of order p^n.

We are looking for a way to characterize conjugacy classes of series of order p^n for any n. We recall that $\mathcal{X}_n$ is the set of pairs (L, σ) where L/K is a cyclic totally ramified extension of degree p^n and σ a generator of $\mathrm{Gal}(L/K)$. We denote by $\mathcal{Y}_n$ the set of conjugacy classes in $\mathcal{G}_0(k)$ of series of $\mathcal{G}_0(k)$ of order p^n. For any $\sigma \in \mathcal{G}_0(k)$, $[\sigma]$ is the conjugacy class of σ in $\mathcal{G}_0(k)$.

5.1. Filtration over $\mathcal{G}_0(k)$.

For any $g \in \mathcal{G}_0(k)$, the ramification number $i(g)$ of g is $v_K(\frac{g(t)}{t} - 1)$. By convention, the ramification number of identity is ∞. By identification of $\mathcal{G}_0(k)$ with the group $\mathrm{Autcont}_k(K)$, we define a filtration on $\mathcal{G}_0(k)$ corresponding to the ramification filtration of $\mathrm{Autcont}_k(K)$ in lower numbering ([12], p.69). We recall that if σ is an automorphism of K fixing k, we put

$$i(\sigma) = v_K\Big(\frac{\pi^\sigma}{\pi} - 1\Big)$$

where π is a prime element of K, for example t. The map i is central, i.e. it doesn't depend of the choice of the prime element, and is an order function of a filtered group over $\mathrm{Autcont}_k(K)$ which is called the ramification

filtration in lower numbering. Then we can define on $\mathcal{G}_0(k)$ the following filtration:

$$\mathcal{G}_j(k) = \{\sigma \text{ such that } i(\sigma) \geq j\}.$$

For all j, the set $\mathcal{G}_j(k)$ is the group of series belonging to $\mathcal{G}_0(k)$ whose ramification number is greater than or equal to j. One gets the isomorphisms: $\mathcal{G}_0(k)/\mathcal{G}_1(k) \simeq k^*$ and for all $j \geq 1$, $\mathcal{G}_j(k)/\mathcal{G}_{j+1}(k) \simeq k$.

5.2. The map λ_n.

We define in this paragraph a map between $\mathcal{X}_n$ and $\mathcal{Y}_n$.

Definition 5.1. *We define the map $\lambda_n : \mathcal{X}_n \to \mathcal{Y}_n$ in this way: if $(L, \sigma) \in \mathcal{X}_n$ we choose a prime element $\pi \in L$ and we define $\lambda_n(L, \sigma)$ as the conjugacy class of the series $\sigma(\pi) \in L = k(\!(\pi)\!)$.*

Firstly, we will verify that λ_n is well-defined, i.e. it doesn't depend on the choice of the prime element π.

Let π and π' be two prime elements of the field L. Then we have two functions f and f' such that $f(\pi) = \pi^\sigma$ and $f'(\pi') = \pi'^\sigma$. We thus can write π' as a series in π, and there exists in this way φ in $\mathcal{G}_0(k)$ such that $\pi' = \varphi(\pi)$ where $k(\!(\pi')\!) = k(\!(\pi)\!)$. So we get on one hand $f'(\pi') = f'(\varphi(\pi))$ and on the other hand $f'(\pi') = \pi'^\sigma = \varphi(\pi)^\sigma = \varphi(\pi^\sigma) = \varphi(f(\pi))$, since the maps φ and σ commute by continuity of σ. So $f' \circ \varphi = \varphi \circ f$, and this shows that λ_n is independent of the choice of the prime element.

5.3. Some ramification properties of λ_n.

We will show in this paragraph that the map λ_n satisfies some properties about the ramification between $\mathcal{X}_n$ and $\mathcal{Y}_n$.

Proposition 5.2. *The map λ_n is surjective and respects the ramification, i.e. $i(\sigma) = i(\lambda_n(L, \sigma))$.*

Proof. The map λ_n is surjective. Indeed, let f be an element in $\mathcal{G}_0(k)$ of order p^n and define $G = \{h \mapsto h \circ f^{\circ i} \text{ such that } 1 \leq i \leq p^n\}$ the automorphism group of K of order p^n and $K^G = \{h \text{ such that } h \circ f^{\circ i} = h\}$ the invariant field of G. By Artin's theorem, K is a Galois extension of K^G of order p^n and of Galois group G so it is a cyclic extension. By a theorem due to Samuel [10], we obtain $K^G = k(\!(s)\!)$ with $s = \prod_{i=1}^{p^n} f^{\circ i}(t) = N_G(t)$ where N_G is the norm of the extension L/K. So $K^G \simeq K$ by an isomorphism χ fixing each element of k and sending s to t. Let P be the irreducible polynomial of K over $K^G = k(\!(s)\!)$ so that $K \simeq K^G[X]/(P)$ and put $L = K[X]/(\chi P(X))$. The isomorphism χ is extended by an isomorphism $\widetilde{\chi}$ from K to L. Hence $\mathrm{Aut}_K(L) = \widetilde{\chi}\mathrm{Gal}(K/K^G)\widetilde{\chi}^{-1}$ so L/K is a cyclic extension of degree p^n. As χ and each element of G fix the elements of k, then the extension L/K is totally ramified. Put $\sigma = \widetilde{\chi}\hat{f}\widetilde{\chi}^{-1}$ then $\lambda_n(L, \sigma) = [f]$ and so $i(\sigma) = i(\lambda_n(L, \sigma))$. □

For all integers $j \in \{0, 1, ...n\}$, let K_j be the subextension of L/K of degree p^j. The extension L/K_j has degree p^{n-j}. The set of extensions $(K_j)_j$ form an increasing extension tower in L/K, thus we get the Galois group filtration:

$$G(L/K) = G(L/K_0) \supset G(L/K_1) \supset ... \supset G(L/K_{n-1}) \supset G(L/K_n) = \{1\}.$$

Put, in lower numbering:

$$i_j(L, \sigma) = \max\{\nu \in \mathbb{N} \text{ such that } \mathrm{Gal}(K_{j+1}/K)_\nu \neq \{1\}\}.$$

Let $[\sigma]$ be the conjugacy class of the series σ in $\mathcal{G}_0(k)$. On $\mathcal{Y}_n$, we put:

$$i_j([\sigma]) = i(\sigma^{\circ p^j}) = v_K\Big(\frac{\sigma^{\circ p^j}(t)}{t} - 1\Big)$$

So we get, $i_j([\sigma]) = i(\sigma^{\circ p^j}) = i(\lambda_n(L, \sigma^{\circ p^j}))$ by the previous proposition.

Let $(L, \sigma) \in \mathcal{X}_n$ and $[\sigma]$ be the image by λ_n of (L, σ). We get by this way:

Corollary 5.3. *The surjective map λ_n of $\mathcal{X}_n$ on $\mathcal{Y}_n$ preserves the ramification breaks, that is for all integers $j \in 0, 1, ..., n-1$, we have $i_j(L, \sigma) = i_j([\sigma])$.*

5.4. *k*-isomorphism.

This paragraph gives a characterization for two pairs (L_1, σ_1) and (L_2, σ_2) to be in the same image under λ_n.

Two pairs (L_1, σ_1) and (L_2, σ_2) are k-isomorphic if there is a bi-continuous isomorphism θ from L_1 to L_2 such that $\theta(K) = K$ and $\theta \circ \sigma_1 = \sigma_2 \circ \theta$.

Proposition 5.4. *Two pairs (L_1, σ_1) and (L_2, σ_2) have the same image by λ_n if and only if they are k-isomorphic.*

Proof. Choose prime elements π_1 of L_1 and π_2 of L_2 so that $L_1 = k(\!(\pi_1)\!)$ and $L_2 = k(\!(\pi_2)\!)$ and thus $t = f_1(\pi_1) = f_2(\pi_2)$ where f_1 and f_2 are two series. Since σ_1 is a series in π_1 and σ_2 a series in π_2 then there is a series s_1 in $\mathcal{G}_0(k)$ such that $g^{\sigma_1} = g \circ s_1$ for all g in L_1 and in the same way, there exists s_2 such that $g^{\sigma_2} = g \circ s_2$ for all g in L_2.

Assume firstly that (L_1, σ_1) and (L_2, σ_2) are k-isomorphic and prove they have the same image by λ_n. Let φ be a series of $\mathcal{G}_0(k)$ such that $\pi_1^\theta = \pi_2^\varphi$. On one hand, we have:

$$\sigma_1(\pi_1^\theta) = (\sigma_1(\pi_1))^\theta = s_1^\theta = s_1(\pi_1^\theta) = s_1(\pi_2^\varphi),$$

and on the other hand:

$$\sigma_2(\pi_1^\theta) = \sigma_2(\pi_2^\varphi) = (\sigma_2(\pi_2))^\varphi = (s_2(\pi_2))^\varphi = s_2(\pi_2)^\varphi.$$

By hypothesis, $\theta \circ \sigma_1 = \sigma_2 \circ \theta$ so $s_1(\pi_2^\varphi) = s_2(\pi_2)^\varphi$ and $s_1 \circ \varphi = \varphi \circ s_2$.

Assume now that (L_1, σ_1) and (L_2, σ_2) have the same image by λ_n and prove they are k-isomorphic. Denote respectively by G_1 and G_2 the Galois

groups of L_1/K and L_2/K. Let π_1 (resp π_2) be a prime element of L_1 (resp of L_2) and let $S \in \mathcal{G}_0(k)$ be a series such that for any automorphism σ_1 of G_1, the series $\sigma_2 = S^{-1} \circ \sigma_1 \circ S$ is an element of G_2. Let θ be the k-isomorphism of L_1 to L_2 defined by $\pi_1^\theta = S(\pi_2)$. We show that θ makes the pairs (L_1, σ_1) and (L_2, σ_2) k-isomorphic, that is $\theta(K) = K$. For $x \in K$, there is a unique series f_1 in K such that $x = f_1(\pi_1)$. We have $x^\theta = f_1(\pi_1)^\theta = f_1 \circ S(\pi_2)$. As $x^{\sigma_1} = x$, since $x \in K$, then $f_1 \circ \sigma_1(\pi_1) = f_1(\pi_1)$ and so $f_1 \circ \sigma_1 = f_1$. Hence:

$$(x^\theta)^{\sigma_2} = f_1 \circ S(\pi_2)^{\sigma_2} = f_1 \circ S \circ \sigma_2(\pi_2) = f_1 \circ \sigma_1 \circ S(\pi_2) = f_1 \circ S(\pi_2) = x^\theta$$

and we get the result. □

5.5. Determination of conjugacy classes by the orbits of $\mathcal{A}_n$.

We finish now by describing a bijection between $\mathcal{Y}_n$ and the orbits of $\mathcal{A}_n$.

Lemma 5.5. *Let $\alpha \in W_n(K)$ and suppose that $L = K(\alpha)$ is an extension of K of degree p^n. Let $a = \wp(\alpha)$ and φ be a field homomorphism from K to another field K'. Let δ be a Witt vector such that $\wp(\delta) = \varphi(a)$ then φ may be extended to a unique homomorphism $\widetilde{\varphi}$ from L to $L' = K'(\delta)$ such that $\widetilde{\varphi}(\alpha) = \delta$.*

Proof. If $n = 1$, let $a \in K$ and α such that $\wp(\alpha) = a$. Let $P = X^p - X - a \in K[X]$. Since the degree of α on K is p then P is the minimum polynomial of α so it is irreducible. Let δ be a root of $X^p - X - \varphi(\alpha)$. Hence $\wp(\delta) = \varphi(a)$.

Now, if the assertion is true for vectors of length less than n. Let $T(\alpha)$ and $T(\delta)$ be the truncation of $\alpha = (\alpha_0, ..., \alpha_{n-1})$ and δ of length $n-1$. There is $\widehat{\varphi}$ such that $\widehat{\varphi}(T(\alpha)) = T(\delta)$. We have $K(\alpha) = K(T(\alpha))(\alpha_{n-1})$. By Lemma 2.2, $a_{n-1} = \alpha_{n-1}^p - \alpha_{n-1} + \Delta(\alpha_0, ..., \alpha_{n-2})$ with Δ a polynomial with integer coefficients. As $\varphi(a) = \wp(\delta)$ so $\varphi(a_{n-1}) = \delta_{n-1}^p - \delta_{n-1} + \Delta(\delta_0, ..., \delta_{n-2})$. For any $j \leq n-2$ we have $\widehat{\varphi}(\alpha_j) = \delta_j$, we obtain the result. □

Theorem 5.6. *There is a bijection determined by λ_n between $\mathcal{Y}_n$ and the orbits of $\mathcal{A}_n$ under the action β_n of $\mathcal{G}_0(k)$ on $\mathcal{A}_n$.*

Proof. We want to prove that a and a' are two elements in the same orbit of $\mathcal{A}_n$ under the action β_n if and only if they define two k-isomorphic pairs (L, σ) and (L', σ') with $L = K(\wp^{-1}(a))$, $L' = K(\wp^{-1}(a'))$ and σ and σ' two generators of respectively $\mathrm{Gal}(L/K)$ and $\mathrm{Gal}(L'/K)$.

Let $\gamma \in \mathcal{G}_0(k)$ such that $\gamma a - a' \in \wp(W_n(K))$. By Artin-Schreier-Witt theory, a' and γa define the same extension. So we have to prove the existence of a k-isomorphism $\widetilde{\gamma}$ between $L = K(\wp^{-1}(a))$ and $L' = K(\wp^{-1}(\gamma a))$. Let α and α' be the Witt vectors such that $\wp(\alpha) = a$ and $\wp(\alpha') = \gamma a$, so $[\overline{a}, \sigma\rangle = \sigma(\alpha) - \alpha$ and $[\overline{\gamma a}, \sigma'\rangle = \sigma(\alpha') - \alpha'$. By Lemma 5.5, there is a homomorphism $\widetilde{\gamma}$ from L to L' such that $(\sigma' \circ \widetilde{\gamma})(\alpha) = \sigma'(\alpha') = \alpha' + 1$ in $K(\alpha')$ and we obtain $(\widetilde{\gamma} \circ \sigma)(\alpha) = \widetilde{\gamma}(\alpha + 1) = \widetilde{\gamma}(\alpha) + \widetilde{\gamma}(1) = \alpha' + 1$. Hence $\widetilde{\gamma}$ is a k-isomorphism between (L, σ) and (L', σ').

Conversely, let a and a' be two elements of $\mathcal{A}_n$ such that there exists a k-isomorphism θ between $(K(\wp^{-1}(a)), \sigma)$ and $(K(\wp^{-1}(a')), \sigma')$.

Let γ be the series $\gamma(t) \in K$. We want to find the homomorphism $\theta = \widetilde{\gamma}$ where γ is the restriction of θ in the field K. Let σ and σ' be generators of $\mathrm{Gal}(K(\wp^{-1}(a))/K)$ and $\mathrm{Gal}(K(\wp^{-1}(a'))/K)$ such that $[\overline{a}, \sigma\rangle = [\overline{a'}, \sigma'\rangle = 1$.

We are looking for a series $\gamma \in \mathcal{G}_0(k)$ such that $a' = \beta_n(\gamma)a$, i.e. $a' = \gamma a$ modulo $\wp(W_n(K))$. If we put $\gamma = \theta(t)$ we have then to show that:

$$\begin{aligned}[\overline{a'} - \overline{\gamma a}, \sigma'\rangle = 0 &\Rightarrow [\overline{a'}, \sigma'\rangle - [\overline{\gamma a}, \sigma'\rangle = 0\\ &\Rightarrow 1 - [\overline{\gamma a}, \sigma'\rangle = 0\\ &\Rightarrow 1 - [\overline{\theta(a)}, \sigma'\rangle = 0\\ &\Rightarrow 1 - \sigma'(\theta(\alpha)) + \theta(\alpha) = 0.\end{aligned}$$

And this is true since $\wp(\theta(\alpha)) = \gamma a$ and $a = \wp(\alpha)$ so $\wp(\theta(\alpha)) = \theta(a)$. □

Corollary 5.7. *If two elements of $\mathcal{A}_n$ lie in the same orbit of $\mathcal{A}_n$ by the action β_n then they have the same ramification breaks.*

Proof. Let $a \in \mathcal{A}_n$ and $a' \in \mathcal{A}_n$ be in the same orbit under the action β_n. Let $(u_n)_n$ and $(u'_n)_n$ the sequences of ramification breaks of a and a'. By Theorem 3.8, the bijection between $\mathcal{A}_n$ and $\mathcal{X}_n$ preserves ramification breaks so $(u_n)_n$ and $(u'_n)_n$ are the sequences of ramification breaks of (L, σ) and (L', σ'), where (L, σ) and (L', σ') correspond respectively to a and a'. Ramification breaks are preserved by λ_n (Corollary 5.3), so $(u_n)_n$ and $(u'_n)_n$ are the sequences of ramification breaks of $[\sigma]$ and $[\sigma']$ where $[\sigma]$ and $[\sigma']$ are the elements of $\mathcal{Y}_n$ corresponding to (L, σ) and (L', σ'). Since a and a' are in the same orbit, by Theorem 5.6, they correspond with the same conjugacy class in $\mathcal{Y}_n$. So $[\sigma] = [\sigma']$ and the sequences $(u_n)_n$ and $(u'_n)_n$ are equal. □

Remark. It should be interesting to find a more direct proof, that is a proof which does not use the map λ_n.

References

[1] S. Bosch, U. Güntzer, R. Remmert, *Non-archimedean analysis*. Springer-Verlag, Berlin, 1984.

[2] N. Bourbaki, *Algèbre Commutative*. Eléments de mathématique, Chapitres 8 et 9, Masson, 1983.

[3] J.L. Brylinski, *Théorie du corps de classes de Kato et revêtement abéliens de surfaces*. Ann. Inst. Fourier, Grenoble, **33**, 3 (1983), 23–38.

[4] R. Camina, *The Nottingham group*. In: New horizons in pro-p groups, M. du Sautoy, Dan Segal and Aner Shalev. Ed., 2001, 205–221.

[5] I. Fesenko, S. Vostokov, *Local Fields and their Extensions*. American Mathematical Society, Providence, 2nd edition, 2002.

[6] K. Kanesaka, K. Sekiguchi, *Representation of Witt Vectors by formal power series and its applications*. Tokyo J. Math Vol **2** No 2. (1979), 349–370.

[7] B. Klopsch, *Automorphisms of the Nottingham group*. Journal of Algebra **223** (2000), 37–56.
[8] S. Lang, *Algebra*. Revised Third Edition, GTM, Springer, 2002.
[9] F. Laubie, A. Movahhedi, A. Salinier, *Systèmes dynamiques non archimédiens et corps des normes*. Compositio Mathematica **132** (2002), 57–98.
[10] P. Samuel, *Groupes finis d'automorphismes des anneaux de séries formelles*. Bull. Sc. math. **90** (1966), 97–101.
[11] J.P. Serre, *Sur les corps locaux à corps résiduel algébriquement clos*. Bull. Soc. Math. France **89** (1961), 105–154.
[12] J.P. Serre, *Corps locaux*. Hermann, Paris, 1962.
[13] L. Thomas, *Arithmétique des extensions d'Artin-Schreier-Witt*. Thèse de doctorat, Toulouse, 2005.
[14] L. Thomas, *Ramification groups in Artin-Schreier-Witt extensions*. Journal de théorie des Nombres de Bordeaux **17** (2005), 689–720.

Sandrine Jean
XLIM UMR 6172
Département de Mathématiques et Informatique
Université de Limoges
123 avenue Albert Thomas
87 060 Limoges Cedex, France
E-mail: sandrine.jean@xlim.fr