UNIVERSITÉ DE LIMOGES
ECOLE DOCTORALE Science - Technologie - Santé
Faculté des Sciences et Techniques
Département de Mathématiques, Laboratoire Xlim

Année 2008

Thèse
pour obtenir le grade de
DOCTEUR DE L'UNIVERSITÉ DE LIMOGES
Discipline : Mathématiques et ses applications
soutenue et présentée par

Sandrine JEAN
le 9 juillet 2008.

Classification à conjugaison près des séries de p-torsion.

Thèse codirigée par **François LAUBIE** et **Alain SALINIER**

Jury

Président	
Abbas MOVAHHEDI	Professeur à l'université de Limoges.
Rapporteurs	
Bruno ANGLÈS	Professeur à l'université de Caen.
Ivan FESENKO	Professeur à l'université de Nottingham.
Examinateurs	
Denis BENOÎS	Professeur à l'université de Bordeaux 1.
François LAUBIE	Professeur à l'université de Limoges.
Abbas MOVAHHEDI	Professeur à l'université de Limoges.
Alain SALINIER	Maître de conférence HDR à l'université de Limoges.

Remerciements

Ces trois années de thèse ont été pour moi l'occasion de vivre une expérience formidable au sein de l'université de Limoges. Certes, il y a eu de moments de découragements et d'autres plus exaltants mais l'ensemble constitue une aventure merveilleuse dans l'apprentissage du métier de chercheur en mathématiques.

En premier lieu, je tiens à remercier mes directeurs de thèse François LAUBIE et Alain SALINIER sans qui rien n'aurait été possible. Je veux les remercier pour les conseils et les explications qu'ils ont su me donner pendant ces trois années.

Je suis également très reconnaissante envers Ivan FESENKO qui m'a permis d'étudier au sein de l'Université de Nottingham pendant trois mois et qui a ensuite été un des rapporteurs de cette thèse. Sa disponibilité et son intérêt pour mes travaux ont rendu mon séjour à Nottingham très agréable.

Je remercie chaleureusement Bruno ANGLÈS d'avoir accepter de rapporter ce travail de thèse.

Je suis très honorée par la présence lors de ma soutenance de thèse de Denis BENOIS et Chazad MOVAHHEDI au sein du jury.

J'ai aussi une pensée pour Eckhard PFLÜGEL qui m'a donnée de précieux conseils lors de la préparation de la soutenance de thèse.

Je remercie chaleureusement toutes les personnes rencontrées lors de ces trois années. Les sécrétaires Sylvie LAVAL, Patricia VAREILLE, Yolande VIECELI puis Aurélie DOUCET du département de mathématiques, Chantale SUBILEAU de l'administration et Gaëlle PEYRAT de l'école doctorale qui géraient mes soucis matériels toujours avec le sourire.

Je remercie la région Limousin pour le financement qu'elle m'a accordée pour faire cette thèse de doctorat et le laboratoire XLIM de m'avoir accueillie.

Mes remerciements s'adressent également aux autres thésards de Limoges qui sont devenus au fil des mois des amis. Je pense tout d'abord à ceux qui ont partagé le bureau du milieu avec moi : Samuel MAFFRE, Adrien POTEAUX, Romain VALIDIRE et Daouda Niang DIATTA puis aux autres thésards qui se sont succédés et qui m'ont apporté leur soutien et leur bonne humeur : Guilhem CASTAGNOS, Ahmed AÏT MOKTAR, Pierre-Louis CAYREL, Elsa BOUSQUET, Benjamin POUSSE, Ainhoa APARICIO MONFORTE, Nicolas LE ROUX, Julien ANGÉLI, Hassan SAOUD, Christophe CHABOT et Aurore BERNARD. Je n'oublie pas non plus Matthew MORROW, doctorant à l'université de Nottingham, qui résolvait mes problèmes de toutes sortes lors de mon séjour dans cette université.

Je veux faire un clin d'oeil à tous mes amis sportifs de l'université de Limoges. Le sport m'a permis de trouver un équilibre en dehors de la recherche mathématiques. Je voudrais donc remercier tous ceux que j'ai pu rencontré dans le gymnase, à la piscine ou sur le stade et plus paticulièrement les enseignants Geneviève MOUDELAUD et Bruno MARTIN.

Enfin, je remercie tout particulièrement Lara THOMAS qui m'a aidée dans mon travail de thèse en m'expliquant la théorie d'Artin-Schreier-Witt avec des mots simples et qui est devenue pour moi une véritable amie. Je la remercie pour son soutien indéfectible et ses conseils sur le metier de chercheur. Elle est pour moi un modèle.

Table des matières

Introduction

L'objet de cette thèse est l'étude des classes de conjugaison des séries formelles d'ordre fini pour la loi de composition en caractéristique positive p. Nous allons développer certains outils permettant de proposer une classification à conjugaison près des séries formelles d'ordre p^n.

B. Green et M. Matignon ont montré dans leurs articles [9] et [10] qu'une conjecture de F. Oort se réduisait à montrer qu'une série d'ordre p^n peut être relevée en une série de même ordre et dont les coefficients sont entiers dans une extension convenable du corps $\mathbb{Q}_p$ des nombres p-adique. Ce résultat est maintenant prouvé pour $n \leq 2$. Ce travail est motivé par cette conjecture. Ainsi pour montrer la conjecture de F. Oort, il suffirait de relever une série particulière de chaque classe de conjugaison.

Nous noterons dans la suite $K = k(\!(t)\!)$ le corps des séries formelles méromorphes à coefficients dans k. Muni de la valuation t-adique, K est un corps local, c'est-à-dire un corps valué complet. Les séries inversibles pour la loi de composition sont précisément les séries entières sans termes constant et dont la dérivée en 0 est non nulle. Ces séries, munies de la loi de composition, constituent un groupe noté dans la suite $\mathcal{G}_0(k)$:

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

Le groupe de Nottingham, que nous noterons $\mathcal{N}(k)$ est le sous-groupe de $\mathcal{G}_0(k)$ formé des séries dont la dérivée en 0 est 1 :

$$\mathcal{N}(k) = \Big\{ \sum_{\iota \geq 1} a_\iota t^\iota \text{ tel que } a_1 = 1 \Big\}.$$

Un théorème de C. Leedham-Green et A. Weiss dit que tout p-groupe fini est inclus dans $\mathcal{N}(k)$. Ce théorème a ensuite été généralisé par R. Camina à tout

pro-p-groupe à base dénombrable ([6], p.216). Dans ses articles, R. Camina note toutefois, la difficulté qu'il existe, à décrire les sous-groupe non-ouverts de $\mathcal{N}(k)$, et en particulier les sous-groupes finis. Lorsque le corps résiduel k de K est fini, les séries d'ordre p du groupe de Nottingham ont été étudiées par B. Klopsch lors de sa thèse de doctorat à Oxford (1999) puis dans ses articles [13] et [14]. Il parvient à donner une forme explicite à un représentant de chaque classe de conjugaison du groupe de Nottingham. En effet, toute série d'ordre p de $\mathcal{N}(k)$ est conjuguée à une série de la forme :

$$F(m,\gamma) = t(1 - m\gamma t^m)^{-1/m}$$

où m est un entier premier à p et γ un élément inversible de k.

Dans le cas plus général des séries d'ordre p^n, nous allons suivre un procédé différent. Nous nous appuierons principalement sur la théorie d'Artin-Schreier-Witt qui décrit les extensions cycliques de degré p^n grâce aux vecteurs de Witt de longueur n. Lorsque le corps résiduel est fini, K. Kanesaka et K. Sekiguchi [12] ont caractérisé la ramification de telles extensions en introduisant un certain sous-module $\mathcal{B}_n$ de vecteurs de Witt de longueur n. En généralisant cette idée au cas où k est la clôture algébrique de $\mathbb{F}_p$, nous sommes en mesure de paramétrer un ensemble $\mathcal{X}_n$ de couples (L,σ) où L est une extension cyclique totalement ramifiées de degré p^n de K et σ un générateur de son groupe de Galois par un élément de $\mathcal{A}_n$ (Théorème 5.1.2) où $\mathcal{A}_n$ désigne un certain sous-ensemble de $\mathcal{B}_n$. Par cette correspondance, nous pourrons calculer les sauts de ramification d'une extension cyclique L/K grâce aux termes du vecteur de Witt dans $\mathcal{A}_n$ correspondant. Cette méthode donne des calculs plus explicites des sauts de ramification que celle décrite dans l'article de J.L. Brylinski [4]. Dans un second temps, nous pourrons mettre en bijection les classes de conjugaison des séries d'ordre p^n et les orbites de $\mathcal{A}_n$ sous une certaine action de $\mathcal{G}_0(k)$ (Théorème 6.2.7). Il est important de remarquer que dans cette bijection, la ramification de l'extension L/K est contrôlée.

Nous commencerons, dans un premier chapitre par rappeler les définitions et les propriétés les plus importantes sur les corps locaux. En particulier, nous décrirons le corps local K des séries formelles munies de la valuation t-adique. Nous rappellerons également les notions de ramification et de groupes de ramification et leurs principales caractéristiques.

Dans le deuxième chapitre, nous nous attacherons à rappeler plus précisément les définitions des groupes $\mathcal{G}_0(k)$ et $\mathcal{N}(k)$. Nous rappellerons alors les principaux théorèmes de la théorie d'Artin-Schreier qui nous permetteront de généraliser les résultats de B. Klopsch dans le cas où le corps résiduel n'est plus fini mais algébriquement clos de caractéristique positive p.

Le troisième chapitre sera consacré à l'anneau des vecteurs de Witt. Nous commencerons par le vecteurs de Witt de longueur infinie puis par les vecteurs de Witt de longueur finie dans un cadre très général. Enfin, nous étudierons plus précisément les vecteurs de Witt de longueur finie à coefficients dans le corps local K étudié dans le premier chapitre.

Le quatrième chapitre sera dédié à la théorie d'Artin-Schreier-Witt qui généralise la théorie d'Artin-Schreier aux extensions de degré p^n grâce aux vecteurs de Witt de longueur n. Puis, nous nous placerons dans le cadre où K est un corps local de corps résiduel algébriquement clos. Nous définirons deux ensembles $\mathcal{B}_n$ et $\mathcal{A}_n$ qui nous seront très utiles dans les chapitres suivant.

Dans le cinquième chapitre, nous chercherons à établir une bijection entre les extensions cycliques totalement ramifiées de degré p^n et les éléments de $\mathcal{A}_n$. Nous verrons alors que les sauts de ramification des extensions cycliques totalement ramifiées de K peuvent être lu par un calcul sur l'élément de $\mathcal{A}_n$ qui correspond à cette extension.

Nous terminerons finalement notre étude des séries d'ordre p^n dans le sixième chapitre. Dans celui-ci, nous décrirons les classes de conjugaison des séries d'ordre p^n grâce aux orbites de $\mathcal{A}_n$ sous une certaine action. Nous verrons alors que la ramification sera conservée sous cette action.

Enfin, le dernier chapitre donnera deux moyens de calculer explicitement une série d'ordre 4. La première méthode utilise la théorie de Lubin-Tate sur le groupe formel additif. La seconde est basée sur la théorie d'Artin-Schreier-Witt.

Notations

Dans toute la suite, p désigne un nombre premier et $n \geq 1$ un entier. Nous regroupons ici les principales notations utilisées dans ce travail.

Notations du chapitre 1 :

Ce chapitre permet d'introduire les objets que nous allons étudier. Nous commençons par les définir dans un cadre très général puis dans une situation de plus en plus précise.

Notations de la section 1.1 :

Cette section concerne les corps locaux dans un cadre très général.

. K Corps local quelconque.
. v_K Valuation discrète de K.
. U_K Groupe des unités de K.
. $\mathcal{O}_K$ Anneau de valuation ou anneau des entiers de K.
. $\mathfrak{p}_K$ Idéal maximal de $\mathcal{O}_K$.
. U_n Filtration du groupe des unités de K i.e. $U_n = 1 + \mathfrak{p}_K^n$.

Notations de la section 1.2 :

Dans cette section, K est un corps local dont la caractéristique est p.

. k Corps résiduel de K.
. t Uniformisante de K.
. v_K Valuation t-adique de K.
. $\mathcal{O}_K$ Anneau de valuation de K i.e. $\mathcal{O}_K = k[\![t]\!]$.
. $\mathfrak{p}_K$ Idéal maximal de $\mathcal{O}_K$ i.e. $\mathfrak{p}_K = tk[\![t]\!]$.
. F Application de Frobenius sur K.
. $\wp$ Homomorphisme de groupes $\wp = F - Id$ dans K.

Notations de la section 1.3 :

Dans cette section, nous nous restreignons maintenant au cas où le corps résiduel k de K est parfait et de caractéristique p.

- L Extension finie de K.
- $e_{L/K}$ Indice de ramification de l'extension L/K.
- $f_{L/K}$ Degré résiduel de l'extension L/K.
- L_0 Sous-corps d'inertie de l'extension L/K.
- $N_{L/K}$ Norme de l'extension L/K.
- $Tr_{L/K}$ Trace de l'extension L/K.

Notations de la section 1.4 :

Dans cette section, l'extension L/K est supposée galoisienne et finie.

- G_u Groupes de ramification en numérotation inférieure.
- G^v Groupes de ramification en numérotation supérieure.
- $\psi_{L/K}$ Fonction de Herbrand.
- $\varphi_{L/K}$ Réciproque de la fonction de Herbrand.
- G_0 Groupe d'inertie de l'extension L/K.

Notations du chapitre 2 :

Dans ce chapitre, nous introduirons les notations concernant les deux groupes de séries formelles étudiés dans la suite.

Notations de la section 2.1 :

Le corps résiduel k est maintenant égale à la clôture algébrique de $\mathbb{F}_p$. C'est donc un corps infini, parfait de caractéristique p.

- $\mathcal{G}_0(k)$ Groupe des séries de $tk[\![t]\!]$ de dérivée en 0 non nulle.
- $\mathcal{N}(k)$ Groupe de Nottingham.
- $i(\sigma)$ Nombre de ramification de la série σ.
- $\mathcal{G}_j(k)$ Filtration de $\mathcal{G}_0(k)$.

Notations du chapitre 3 :

Le chapitre 3 concerne l'anneau des vecteurs de Witt, d'abord dans un cadre très général puis sur l'anneau des séries formelles méromorphes introduit dans les chapitres précédents.

Notations de la section 3.1 :

Soit R un anneau commutatif unitaire de caractéristique p.

- $W(R)$ Anneau des vecteurs de Witt de longueur infinie.
- W_n $n^{\text{ième}}$ polynôme de Witt.
- x^* Suite des composantes fantômes du vecteur x.
- $H(R)$ Anneau des suites d'éléments de R.
- g_R Application $x \in W(R) \mapsto x^* \in H(R)$.
- W Foncteur de Witt.
- $\{x\}$ Vecteur de Witt $(x, 0, 0, ...)$.
- F Application de Frobenius sur $W(R)$
- $\wp$ Homomorphisme de groupes $\wp = F - Id$ dans $W(R)$.
- V Application de décalage ou "Shift" ou "Vershiebung".
- $\mathbf{p}$ Multiplication par p dans $W(R)$.

Notations de la section 3.2 :

Nous fixons un entier $n \geq 1$.

- I_n Idéal de $W(R)$ donné par $V^n(W(R))$.
- $W_n(R)$ Anneau des vecteurs de Witt de longueur $n : W_n(R) = W(R)/I_n$.
- T^j Applications de troncation.
- F Application de Frobenius sur $W_n(R)$.
- $\wp$ Homomorphisme de groupes $\wp = F - Id$ dans $W_n(R)$.

Notations de la section 3.3 :

Reprenons $K = k(\!(t)\!)$ où k est la clôture algébrique de $\mathbb{F}_p$.

- m_n Application $x \mapsto \min\{p^{n-1-\iota} v_K(x_\iota)$ avec $\iota = 0, ..., n-1\}$.
- d_n Distance $d_n(x, y) = p^{-m_n(x-y)}$.
- $W_n(\mathfrak{p}_K)$ Ensemble des vecteurs de Witt de composantes dans $\mathfrak{p}_K$.

Notations du chapitre 4 :

Nous donnons ici les notations utilisées dans la suite pour décrire les bijections obtenues dans ce travail.

Notations de la section 4.1 :

Nous reprenons ici $K = k(\!(t)\!)$ avec k un corps de caractéristique p.

- $[.,.\rangle$ Symbole d'Artin lié à l'accouplement d'Artin-Schreier-Witt.
- $\overline{a}$ Classe de a modulo $\wp(W_n(K))$.
- G_i Groupe de Galois de l'extension $K(\wp^{-1}(x_0, ..., x_i))/K$.

Notations de la section 4.2 :

Maintenant, nous supposons de plus que le corps résiduel k est la clôture algébrique de $\mathbb{F}_p$. Soit $x = \sum_{\iota>1} \alpha_\iota t^\iota$ une série de K.

- $\mathbb{N}_p$ Ensemble des entiers positifs premiers à p.
- $\mathcal{B}_n$ Sous-module engendré par les vecteurs $\{t^{-\iota}\}$ avec $\iota \in \mathbb{N}_p$.
- $I(x)$ Ensemble $\{\iota \in \mathbb{Z}$ tel que $\alpha_\iota \neq 0\}$.
- $\nu(x)$ Application : $x \mapsto \min\{v_p(\iota)$ tel que $\iota \in I(x)\}$.
- ord Ordre additif du vecteur a dans le groupe $W_n(k)$.
- ρ_n Application telle que $\rho_n(a) = \max\{\iota p^{-1}\text{ord}(a_\iota)$ pour $a \in \mathcal{B}_n\}$.
- $\mathcal{A}_n$ Ensemble des éléments de $\mathcal{B}_n$ inversibles dans $W_n(K)$.

Notations du chapitre 5 :

Ce chapitre présente la première bijection obtenue. Il reprend donc les notations utilisées précédemment.

Notations de la section 5.1 :

Dans la suite L designera une extension cyclique totalement ramifiée de K.

- $\mathcal{X}_n$ Ensemble des couples (L, σ) tel que $\langle\sigma\rangle = \text{Gal}(L/K)$.
- $\overline{a}$ Classe de a modulo $\wp(W_n(K))$.

Notations du chapitre 6 :

Ce chapitre donne la seconde bijection décrite dans ce travail. Nous introduirons pour cela une certaine action de groupe.

Notations de la section 6.1 :

Nous décrirons dans un premier temps l'action utilisée pour construire cette bijection.

. β_n Action de $\mathcal{G}_0(k)$ sur le groupe $\mathcal{B}_n$.

Notations de la section 6.2 :

Enfin, nous définirons la seconde bijection décrite par l'application λ_n.

. $\mathcal{Y}_n$ Ensemble des classes de conjugaison de $\mathcal{G}_0(k)$ des séries d'ordre p^n.
. λ_n Application de $\mathcal{X}_n$ dans $\mathcal{Y}_n$.

Notations du chapitre 7 :

Le chapitre 7 donne deux méthodes de calculs permettant de trouver des séries d'ordre 4.

Notations de la section 7.1 :

Nous avons besoin dans cette section des groupes formels et notamment de groupe formel additif.

. $F(X,Y)$ Groupe formel.
. $\mathbb{G}_a$ Groupe formel additif.

Chapitre 1

Corps locaux

Dans ce chapitre, nous nous attachons à rappeler, de la façon la plus précise possible, les notions principales et à mettre en place les notations utilisées dans la suite de ce travail. Nous donnerons les définitions essentielles sur les corps locaux, d'abord dans un cadre très général puis sur un corps de caractéristique strictement positive.
Ensuite, nous rappelerons, dans ce cas précis, les différents types de ramification possibles des extensions galoisiennes de corps locaux. Nous irons alors un peu plus loin dans cette caractérisation en redonnant les propriétés principales des groupes et des sauts de ramification en numérotation inférieure puis supérieure.
Ce chapitre permet donc de présenter le corps local K qui sera notre corps de référence dans la suite de ce travail.

1.1 Les corps locaux.

Ce paragraphe regroupe les définitions essentielles sur les corps locaux dans un cadre très général. Soit K un corps, on appelle valuation discrète sur K une application vérifiant les trois conditions suivantes :

1. $v_K(x)$ est un nombre rationnel pour tout x non nul et $v_K(0) = +\infty$.
2. Pour tout x et y de K, $\min(v_K(x), v_K(y)) \leq v_K(x+y)$.
3. Pour tout x et y de K, $v_K(x) + v_K(y) = v_K(xy)$.

L'élément $x \in K$ appartient au groupe des unités U_K de K si et seulement si $v_K(x) = 0$. C'est à dire :

$$U_K = \ker(v_K) = \{x \in K \text{ tel que } v_K(x) = 0\}.$$

Un élément π_K de K est une uniformisante si :

$$v_K(\pi_K) = \min\{v_K(x) > 0 \text{ avec } x \in K^*\}.$$

La valuation v_K est dite normalisée si $v_K(K^*) = \mathbb{Z}$. Dans ce cas, les uniformisantes de K sont les éléments de valuation 1.

On définit l'anneau de valuation et on note $\mathcal{O}_K$, l'anneau des éléments de K dont la valuation est positive ou nulle :

$$\mathcal{O}_K = \{x \in K \text{ tel que } v_K(x) \geq 0\}.$$

C'est un anneau de valuation discrète, i.e. principal et n'ayant qu'un seul idéal maximal noté $\mathfrak{p}_K$:

$$\mathfrak{p}_K = \{x \in K \text{ tel que } v_K(x) > 0\}.$$

Le quotient $\mathcal{O}_K/\mathfrak{p}_K$ est un corps appelé corps résiduel de K noté k.

Nous obtenons deux situations :

1. Le corps K est de caractéristique nulle, par exemple, lorsque K est une extension finie de $\mathbb{Q}_p$ avec k un corps fini.
2. Le corps K est de caractéristique $p > 0$ alors (voir, par exemple Serre [20]) $K = k(\!(t)\!)$ où t est une uniformisante. C'est le cas qui nous intéressera par la suite.

1.2 Corps locaux de caractéristique p.

Soit p un nombre premier, d'après le paragraphe précédent, si K est un corps local de caractéristique p alors $K = k(\!(t)\!)$ avec t une uniformisante de K ([20], Chap 2, §4, Prop 5). Nous allons donner une description des notions introduites précédemment dans ce cas précis.

1.2.1 Description du corps local $K = k(\!(t)\!)$.

L'anneau de valuation ou anneau des entiers de K sera l'anneau des séries formelles dont la valuation t-adique est positive ou nulle :

$$\mathcal{O}_K = k[\![t]\!] = \Big\{ \sum_{\iota \geq 0} a_\iota t^\iota \text{ avec } a_\iota \in k \text{ pour tout } \iota \geq 0 \Big\}.$$

et l' idéal maximal du corps local K est l'idéal formé de l'ensemble des séries formelles dont la valuation t-adique est strictement positive :

$$\mathfrak{p}_K = tk[\![t]\!] = \Big\{ \sum_{\iota > 0} a_\iota t^\iota \text{ avec } a_\iota \in k \text{ pour tout } \iota > 0 \Big\}.$$

Le corps résiduel est dans ce cas égal au corps k.

Nous considérons une filtration particulière sur le corps K en définissant une suite de sous-groupes de K^* de cette façon :

$$U_0 = U = \Big\{ x \in K \text{ tel que } x = \sum_{\iota \geq 0} a_\iota t^\iota \text{ et } a_0 \neq 0 \Big\}$$

et pour tout $n \geq 1$:

$$U_n = 1 + \mathfrak{p}_K^n = \Big\{ x \in K \text{ tel que } x = 1 + \sum_{\iota \geq n} a_\iota t^\iota \Big\}.$$

On obtient ainsi la suite d'inclusions :

$$\{1\} \subset ... \subset U_n \subset ... \subset U_1 \subset U_0 = U \subset K^*$$

telle que

$$U_0/U_1 \xrightarrow{\sim} \mathfrak{p}_K^\times \text{ et } U_n/U_{n+1} \xrightarrow{\sim} \mathfrak{p}_K^+ \text{ pour tout } n \geq 1.$$

1.2.2 Premières propriétés de $k(\!(t)\!)$.

Lemme 1.2.1 *:*
Soit L un corps contenant k et inclus dans $k(\!(t)\!)$, si l'extension L/k est algébrique, alors l'extension L/k est triviale (autrement dit k est algébriquement fermé dans $k(\!(t)\!)$).

Démonstration :
Soit σ un élément de $k(\!(t)\!)$ algébrique sur k, alors il existe un polynôme à coefficients dans k tel que :

$$(*) \quad A_n\sigma^n + A_{n-1}\sigma^{n-1} + ... + A_1\sigma + A_0 = 0,$$

avec A_nA_0 non nul. Montrons d'abord que $v_K(\sigma)$ est nul.

En effet, si $v_K(\sigma) > 0$ alors $\sigma(t) = t\tau(t)$ avec τ une série entière à coefficients dans k, donc la relation $(*)$ donne :

$$A_n(t\tau(t))^n + A_{n-1}(t\tau(t))^{n-1} + ... + A_1(t\tau(t)) + A_0 = 0.$$

Donc t divise A_0 dans l'anneau $k[\![t]\!]$, ce qui entraîne une contradiction.

Si $v_K(\sigma) < 0$ alors en divisant la relation $(*)$ par σ^n, on obtient :

$$A_n + A_{n-1}\sigma^{-1} + ... + A_1(\sigma^{-1})^{n-1} + A_0(\sigma^{-1})^n = 0$$

avec $v_K(\sigma^{-1}) = -v_K(\sigma) > 0$ ce qui nous ramène au cas précédent et nous donne aussi une contradiction.

Donc $\sigma = c + t\tau(t)$ où c est un élément non nul de k et $\tau(t)$ une série entière à coefficients dans k. On suppose que la série $\tau(t)$ est non nulle et on va en déduire une contradiction. Nous avons :

$$A_n(c + t\tau(t))^n + A_{n-1}(c + t\tau(t))^{n-1} + ... + A_1(c + t\tau(t)) + A_0 = 0.$$

Ce qui nous donne :

$$\sum_{i=0}^{n} A_i \sum_{k=0}^{i} \binom{i}{k} c^{i-k} (t\tau(t))^k = 0.$$

Donc

$$\sum_{k=0}^{n} \Big(\sum_{i=k}^{n} A_i \binom{i}{k} c^{i-k} \Big) (t\tau(t))^k = 0.$$

Puisque $v_K(t\tau(t)) > 0$, d'après ce qui précède, il ne peut être algébrique sur k. Donc pour tout $k \in \{0, ..., n\}$;

$$\sum_{i=k}^{n} A_i \binom{i}{k} c^{i-k} = 0.$$

En prenant $k = n$ on obtient $A_n = 0$ ce qui donne une contradiction. □

1.2.3 Le Frobenius F et l'homomorphisme $\wp$.

Soit K un corps de caractérsitique p.
On définit l'application de Frobenius dans K :

$$\begin{array}{rccc} F: & K & \to & K \\ & x & \mapsto & x^p. \end{array}$$

On définit également l'application de K dans K appelée isogénie :

$$\begin{array}{rccc} \wp: & K & \to & K \\ & x & \mapsto & x^p - x. \end{array}$$

L'application $\wp = F - id$ est un endomorphisme additif du $\mathbb{F}_p$-espace vectoriel $K = k(\!(t)\!)$.

Ces deux appplications jouent un rôle crucial dans la théorie d'Artin-Schreier developpée dans le chapitre suivant.

1.2.4 Stabilité de $\mathcal{O}_K$ par l'endomorphisme de groupes $\wp$.

Ce lemme nous sera également utile dans la démonstration d'un théorème de B. Klopsch étudiée dans le chapitre suivant. Il sera, de plus, généralisé à tous vecteurs de Witt par la proposition 3.3.8.

Lemme 1.2.2 *:*
Supposons que k soit un corps algébriquement clos. L'anneau de valuation $\mathcal{O}_K = k[\![t]\!]$ est inclus dans l'image de $k[\![t]\!]$ par $\wp$ c'est à dire $k[\![t]\!] = \wp(k[\![t]\!])$ ou encore $\mathcal{O}_K = \wp(\mathcal{O}_K)$.

Démonstration :
Soit ξ une série appartenant à $k[\![t]\!]$ et montrons que ξ appartient à $\wp(k[\![t]\!])$. Supposons dans un premier temps que ξ est de valuation strictement positive. Le corps $k(\!(t)\!)$ est complet pour la valuation t-adique v_K, or $v_K(\xi^{p^i})$ est égal à $p^i v_K(\xi)$ donc $v_K(\xi^{p^i})$ tend vers $+\infty$ lorsque i tend vers $+\infty$. Donc la série

$$-\sum_{i=0}^{+\infty} \xi^{p^i}$$

est convergente dans $k(\!(t)\!)$. Comme $\wp$ est continue et additive alors on a :

$$\wp(-\sum_{i=0}^{+\infty} \xi^{p^i}) = -\sum_{i=0}^{+\infty} \wp(\xi^{p^i}) = \xi.$$

Donc ξ appartient à $\wp(k[\![t]\!])$.

Maintenant, si ξ est un élément quelconque de $k[\![t]\!]$ alors ξ est la somme de deux éléments η et ζ tels que η soit dans k et ζ appartienne à $tk[\![t]\!]$.

Puisque le corps k est algébriquement clos alors η appartient à $\wp(k)$ donc à $\wp(k[\![t]\!])$. On a également vu dans la première partie de la démonstration que $\zeta \in \wp(k[\![t]\!])$.
Comme $\wp$ est un morphisme additif alors ξ appartient à $\wp(k[\![t]\!])$ □

1.3 Ramification.

Soit k un corps parfait de caractéristique p. Nous allons rappeler dans ce paragraphe quelques notions sur la ramification des extensions de corps locaux. La ramification nous donne une première idée sur les différents types d'extensions.

1.3.1 Extensions résiduelles.

Soit $K = k(\!(t)\!)$ un corps local de caractéristique p et de corps résiduel k supposé parfait. Soit L une extension finie de K de corps résiduel l, l'extension résiduelle l/k est donc séparable.

De plus, si l'extension L/K est galoisienne alors l'extension résiduelle l/k est également galoisienne et son groupe de Galois $\mathrm{Gal}(l/k)$ est un quotient du groupe de Galois $\mathrm{Gal}(L/K)$.

1.3.2 Indice de ramification et degré résiduel.

Soit L/K une extension finie telle que (L, v_L) et (K, v_K) sont deux corps locaux. La valuation v_K est alors la restriction de v_L au corps K.

L'indice de ramification de l'extension L/K est le nombre $e_{L/K}$ tel que :

$$e_{L/K} = [v_L(L^*) : v_K(K^*)].$$

Soient l et k respectivement les corps résiduels de L et K.
Le degré résiduel de l'extension L/K est le nombre $f_{L/K}$ tel que :

$$f_{L/K} = [l : k]$$

Remarque :
L'indice de ramification et le degré résiduel jouissent des propriétés importantes suivantes (voir Serre [20]) :

1. L'indice de ramification, comme le degré résiduel, est un entier ≥ 1.
2. Si l'extension L/K est finie de degré n, on a la relation :

$$n = e_{L/K} f_{L/K}.$$

3. Si M est une sous-extension de L/K alors on a les relations :

$$e_{L/K} = e_{L/M} e_{M/K} \quad \text{et} \quad f_{L/K} = f_{L/M} f_{M/K}.$$

1.3.3 Extensions totalement ramifiées et extensions non ramifiées.

Soit K un corps local et L une extension de K de degré n.

L'extension L/K est dite totalement ramifiée si son indice de ramification

$e_{L/K}$ est égal à n et son degré résiduel égal à 1 tandis qu'elle est dite non ramifiée si son indice de ramification $e_{L/K}$ est égal à 1 et son degré résiduel égal à n et si l'extension résiduelle est séparable.

Une extension L/K est dite sauvagement ramifiée si p divise son indice de ramification $e_{L/K}$.

Si L/K est une extension totalement ramifiée alors l'extension résiduelle l/k est triviale.

Soit L/K une extension de degré n, alors il existe une sous-extension L_0 de L/K telle que L_0/K soit une extension non ramifiée de degré $f_{L/K}$ et L/L_0 une extension totalement ramifiée de degré $e_{L/K}$. Le corps L_0 est appelé sous-corps d'inertie de l'extension L/K.
Nous obtenons le schéma suivant :

$$\begin{array}{c} L \\ {\scriptstyle e_{L/K}}\big| \\ L_0 \\ {\scriptstyle f_{L/K}}\big| \\ K \end{array} \Bigg)^{n}$$

Si le corps résiduel k de K est algébriquement clos, toutes les extensions de K sont totalement ramifiées.
Dans la suite, nous étudierons plus particulièrement les extensions cycliques totalement ramifiées de degré p^n du corps local $K = k(\!(t)\!)$ ayant pour corps résiduel $k = \mathbb{F}_p^{alg}$ la clôture algébrique de $\mathbb{F}_p$.

1.3.4 Norme et trace.

Soient L/K une extension finie séparable de degré n et $\sigma_1, \sigma_2, ..., \sigma_n$ les n plongements de L dans une clôture algébrique de K.

Nous rappelons que la norme et la trace de α dans l'extension L/K sont respectivement définies par :

$$N_{L/K}(\alpha) = \prod_{\iota=1}^{n} \sigma_\iota(\alpha) \quad \text{et} \quad Tr_{L/K}(\alpha) = \sum_{\iota=1}^{n} \sigma_\iota(\alpha).$$

Il est bien connu que ces deux applications sont transitives : en effet si M est

une sous-extension de L/K alors :

$$N_{L/K} = N_{M/K} \circ N_{L/M} \quad \text{et} \quad Tr_{L/K} = Tr_{M/K} \circ Tr_{L/M}.$$

La norme $N_{L/K}$ est un homomorphisme multiplicatif de L^* dans K^* alors que la trace est un homomorphisme additif de L dans K.

Soit (K, v_K) un corps local et L une extension finie de K. Alors il existe une seule application v_L qui prolonge la valuation v_K et telle que (§2.5, [8]) :

$$v_L = \frac{1}{f_{L/K}} v_K \circ N_{L/K}.$$

En particulier :

1. Si l'extension L/K est non ramifiée et si π_K est une uniformisante de K alors elle est aussi une uniformisante de L.
2. Si l'extension L/K est totalement ramifiée et si π_K est une uniformisante de K alors $N_{L/K}(\pi_K)$ est une uniformisante de L.

1.4 Groupes de ramification.

Soit L/K une extension galoisienne finie et soit $G = \mathrm{Gal}(L/K)$ son groupe de Galois. Les groupes de ramification vont nous permettre de caractériser plus précisément encore les types d'extensions.
Il existe deux numérotations différentes pour définir les groupes de ramification. L'une est adaptée aux sous-groupes tandis que l'autre est adaptée au quotient. Cependant, les deux numérotations sont liées par la fonction de Herbrand et sa fonction réciproque.

1.4.1 Groupes de ramification en numérotation inférieure.

Comme dans "Corps Locaux" de J.P. Serre [20], nous commençons par définir les groupes de ramification en numérotation inférieure.

Définition 1.4.1 *:*
Pour tout $u \geq -1$, on appelle sous-groupe de ramification en numérotation inférieure d'indice u, le groupe :

$$G_u = \{s \in G \text{ tel que } v_L(s(a) - a) \geq u + 1 \text{ pour tout } a \in \mathcal{O}_L\}.$$

La numérotation inférieure s'adapte aux sous-groupes. C'est à dire si H est un sous-groupe de G alors

$$H_u = G_u \cap H.$$

Cependant, elle est mal adaptée aux passages aux quotients.

Remarques :

1. Les groupes de ramification G_u forment une suite décroissante de sous-groupes distingués de G.
2. On a $G_{-1} = G$ et $G_u = \{1\}$ pour u assez grand.
3. Les groupes de ramification G_u définissent une filtration du groupe de Galois G. Il existe un plus petit entier m tel que $G_m = 1$.

On dit que le nombre $u \in \mathbb{R}$ est un saut de ramification de l'extension L/K en numérotation inférieure si pour tout $\epsilon > 0$, on a $G_u \neq G_{u+\epsilon}$. Ce sont des entiers congrus entre eux modulo p.

1.4.2 Groupes de ramification en numérotation supérieure.

Toujours en suivant "Corps locaux" de J.P. Serre [20], nous définissons une seconde numérotation des groupes de ramification adaptée au passage au quotient qui permet par la suite de définir des groupes de ramification pour une extension galoisienne infinie.

Définition 1.4.2 *:*
Soit $\varphi_{L/K}$ la fonction définie sur $[-1, +\infty[$ de la façon suivante :

$$\begin{aligned} \varphi_{L/K}(u) &= \int_0^u \frac{dt}{(G_0 : G_t)} && si\ u \geq 0 \\ &= u && si\ -1 \leq u \leq 0. \end{aligned}$$

Cette fonction est continue, linéaire par morceaux, croissante et concave. De plus, on a $\varphi_{L/K}(0) = 0$. C'est un homéomorphisme de $[-1, +\infty[$ sur $[-1, +\infty[$.

On appelle $\psi_{L/K}$ la bijection réciproque de $\varphi_{L/K}$. La fonction $\psi_{L/K}$ est donc continue, linéaire par morceaux, croissante et convexe. On a également $\psi_{L/K}(0) = 0$. Nous allons maintenant définir les groupes de ramification en numérotation supérieure :

Définition 1.4.3 *:*
Pour tout $v \geq -1$, on appelle sous-groupe de ramification en numérotation supérieure d'indice v, le groupe : $G^v = G_{\psi(v)}$.
Réciproquement, on a $G^{\varphi(u)} = G_u$.

On peut également écrire l'application ψ sous la forme :

$$\begin{aligned} \psi_{L/K}(v) &= \int_0^v (G^0 : G^w)dw \quad \text{si } v \geq 0 \\ &= v \qquad\qquad\qquad\quad \text{si } -1 \leq v \leq 0. \end{aligned}$$

La numérotation supérieure s'adapte bien au quotient, en effet si H est un sous-groupe distingué de G alors on a pour tout v :

$$(G/H)^v = G^v H/H.$$

Les nombres réels t tels que $G^t \neq G^{t+\epsilon}$ pour tout $\epsilon > 0$ sont appelés les sauts de ramification de l'extension L/K en numérotation supérieure.

Soit K un corps local de corps résiduel k fini et L/K une extension galoisienne totalement ramifiée de groupe de Galois G. Soit c le plus grand entier tel que $G_c \neq \{1\}$ et soit $f = \varphi(c) + 1$, l'idéal $\mathfrak{p}_K^f$ s'appelle le conducteur de l'extension L/K. Ceci nous servira dans le chapitre 5 où nous généraliserons le conducteur lorsque le corps résiduel k de K n'est plus fini.

Théorème 1.4.4 *:(Hasse-Arf)*
Si G est un groupe abélien, les sauts de ramification en numérotation supérieure sont des entiers ([20] ch.IV. §3).

Remarque :
Si L est une extension infinie d'un corps local K on a

$$G^v = \varprojlim \mathrm{Gal}(M/K)^v$$

où M décrit l'ensemble des sous-extensions galoisiennes finies de L/K.

1.4.3 Le groupe d'inertie.

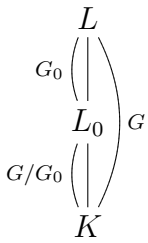
Le sous-groupe G_0 est appelé groupe d'inertie de L/K, G/G_0 désigne le groupe de Galois de la sous-extension maximale non ramifiée de L/K.

On obtient la suite exacte :

$$1 \to G_0 \to G \to \mathrm{Gal}(l/k) \to 1$$

où l et k désignent respectivement les corps résiduels de L et K.

On retrouve le schéma :



En particulier, l'extension L/K est non ramifiée si et seulement si $G_0 = 1$ et est totalement ramifiée si et seulement si $G_0 = G$.

Chapitre 2

Groupe des séries réversibles et groupe de Nottingham

Dans ce chapitre, nous présenterons deux groupes de séries formelles méromorphes $\mathcal{G}_0(k)$ et $\mathcal{N}(k)$. Le groupe $\mathcal{N}(k)$ fût étudié simultanément en théorie de groupes où il est appelé "groupe de Nottingham" et en théorie des nombres où il est appelé "groupe des automorphismes sauvages". Les séries appartenant à $\mathcal{N}(k)$ s'identifient naturellement à des automorphismes d'extensions de corps sauvagement ramifiées.
Ce chapitre nous permet de donner une première approche de ces deux groupes, puis nous rappelons les principaux résultats de la théorie d'Artin-Schreier. Enfin, nous rappelons le résultat de B. Klopsch, paru en 2002, décrivant une famille de représentants des classes de conjugaison des séries d'ordre p. Nous donnerons ensuite une autre démonstration de ce théorème utilisant la théorie d'Artin-Schreier.
Ce chapitre permet donc d'avoir une formule permettant de donner une classification des séries d'ordre p. Nous nous intéresserons dans les chapitres suivants aux séries d'ordre p^n avec $n > 1$.

Nous nous placerons sur un corps local K de caractéristique $p > 0$ et de corps résiduel k supposé parfait. En particulier, on identifie K au corps des séries formelles $K = k(\!(t)\!)$ pour une certaine uniformisante $t \in K$.

2.1 Les groupes $\mathcal{G}_0(k)$ et $\mathcal{N}(k)$.

Nous donnons dans ce paragraphe les principales définitions et propriétés de ces deux groupes de séries formelles à coefficients dans la corps k où k désigne la clôture algébrique de $\mathbb{F}_p$.

2.1.1 Définitions.

Soit k la clôture algébrique de $\mathbb{F}_p$ et $K = k(\!(t)\!)$ le corps des séries formelles à coefficients dans k. Nous allons étudier les séries formelles sans terme constant telles que leur dérivée en 0 est non nulle. Muni de la loi de composition des séries, cet ensemble forme un groupe que nous noterons $\mathcal{G}_0(k)$:

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

Le groupe de Nottingham $\mathcal{N}(k)$ est l'ensemble des séries appartenant à $t + t^2 k[\![t]\!]$ muni de la loi de composition des séries. C'est un sous-groupe de $\mathcal{G}_0(k)$:

$$\mathcal{N}(k) = \Big\{ \sum_{\iota \geq 1} a_\iota t^\iota \text{ tel que } a_1 = 1 \Big\}.$$

Un théorème de C. Leedham-Green et A. Weiss nous dit que tout p-groupe fini peut être inclus dans $\mathcal{N}(k)$. Ce théorème a ensuite pu être généralisé par R. Camina à tout pro-p-groupe à base dénombrable ([6], p.216). En effet, dans son article paru en 1997, R. Camina prouve que tout pro-p-groupe à base dénombrable se plonge, comme sous-groupe fermé, dans le groupe de Nottingham.

Nous avons l'isomorphisme suivant :

$$\mathcal{G}_0(k) \simeq k^* \ltimes \mathcal{N}(k).$$

2.1.2 Nombre de ramification d'une série.

Soit $K = k(\!(t)\!)$ le corps des séries formelles à coefficients dans k.

Définition 2.1.1 *:*
Le nombre de ramification d'une série $\sigma \in K$ est définie par la formule :

$$i(\sigma) = v_K\Big(\frac{\sigma(t)}{t} - 1\Big).$$

Dans le cas où σ est une série appartenant au groupe de Nottingham, Rachel Camina ([6], p.208) nomme profondeur "Depth", le nombre de ramification.

On dit aussi qu'une série σ est sauvagement ramifiée si $i(\sigma) \geq 1$. L'ensemble des séries sauvagement ramifiées muni de la loi de composition des séries correspond donc au groupe de Nottingham.

La fonction $i(\sigma)$ nous permet alors de définir une filtration du groupe $\mathcal{G}_0(k)$, pour tout $j \geq 0$, on pose :

$$\mathcal{G}_j(k) = \Big\{\sigma \in \mathcal{G}_0 \text{ tel que } i(\sigma) \geq j\Big\}.$$

Le premier sous-groupe de cette filtration $\mathcal{G}_1(k)$ est le groupe de Nottingham $\mathcal{N}(k)$.

2.2 Invariance du nombre de ramification par conjugaison dans $\mathcal{N}(k)$.

Par le lemme suivant, on prouve que le nombre de ramification i et le coefficient en t^{i+1} sont indépendants du représentant choisi dans une classe de conjugaison du groupe de Nottingham.

Lemme 2.2.1 *:*
Soit σ une série entière réversible de $k[\![t]\!]$, le nombre de ramification i et le coefficient en t^{i+1} de σ sont invariants par conjugaison dans $\mathcal{N}(k)$.

Démonstration :
Posons $\rho = \tau^{-1} \circ \sigma \circ \tau$ alors $\tau \circ \rho = \sigma \circ \tau$. Posons :

$$\tau(t) = t\Big(1 + \sum_{i=m}^{+\infty} \alpha_i t^i\Big), \text{ avec } i(\tau) = m \text{ si et seulement si } \alpha_m \neq 0,$$

$$\rho(t) = t\Big(1 + \sum_{j=n}^{+\infty} \beta_j t^j\Big), \text{ avec } i(\rho) = n \text{ si et seulement si } \beta_n \neq 0$$

et

$$\sigma(t) = t\Big(1 + \sum_{k=r}^{+\infty} \gamma_k t^k\Big), \text{ avec } i(\sigma) = r \text{ si et seulement si } \gamma_r \neq 0.$$

Par composition des séries nous obtenons :

$$(\tau \circ \rho)(t) = t\Big(1 + \sum_{j=n}^{m+n} \beta_j t^j + \sum_{i=m}^{m+n} \alpha_i t^i + (m+1)\alpha_m \beta_n t^{m+n} + t^{m+n+2}\varphi(t)\Big)$$

$$(\sigma \circ \tau)(t) = t\Big(1 + \sum_{i=m}^{m+r} \alpha_i t^i + \sum_{k=r}^{m+r} \gamma_k t^k + (r+1)\gamma_r \alpha_m t^{m+r} + t^{m+r+2}\psi(t)\Big)$$

où ici φ et ψ désignent des séries formelles entières en t.

On se place maintenant modulo t^{n+2}. Trois cas se présentent en fonction des valeurs de n et de m :

1er cas : Si n est inférieur à m.

$$(\tau \circ \rho)(t) \equiv t(1 + \beta_n t^n) \quad \text{modulo } t^{n+2}$$

et

$$(\sigma \circ \tau)(t) \equiv t\Big(1 + \sum_{k=r}^{m+r} \gamma_k t^k\Big) \quad \text{modulo } t^{n+2}$$

Donc $n = r$ et $\beta_n = \gamma_n$.

2eme cas : Si n est égal à m.

$$(\tau \circ \rho)(t) \equiv t(1 + \beta_n t^n + \alpha_n t^n) \quad \text{modulo } t^{n+2}$$

et

$$(\sigma \circ \tau)(t) \equiv t\Big(1 + \alpha_n t^n + \sum_{k=r}^{m+r} \gamma_k t^k\Big) \quad \text{modulo } t^{n+2}$$

Donc $n = r$ et $\beta_n = \gamma_n$.

3eme cas : Si n est supérieur à m.

$$(\tau \circ \rho)(t) \equiv t\Big(1 + \beta_n t^n + \sum_{i=m}^{n} \alpha_i t^i\Big) \quad \text{modulo } t^{n+2}$$

et

$$(\sigma \circ \tau)(t) \equiv t\Big(1 + \sum_{i=m}^{m+r} \alpha_i t^i + \sum_{k=r}^{m+r} \gamma_k t^k + (r+1)\gamma_r \alpha_m t^{m+r}\Big) \quad \text{modulo } t^{n+2}$$

Donc $n = r$ et $\beta_n = \gamma_n$.
Donc i et le coefficient en t^i sont invariants par conjugaison dans $\mathcal{N}(k)$. □

2.3 Rappels sur la théorie d'Artin-Schreier.

La théorie d'Artin-Schreier permet de caractériser les extensions cycliques de degré p du corps local K de caractéristique p. Cette théorie sera généralisée aux extensions cycliques de degré p^n dans le chapitre 4.

2.3.1 Théorème 90 de Hilbert et Théorème d'Artin-Schreier.

Commençons par le théorème 90 de Hilbert sous sa forme multiplicative :

Théorème 2.3.1 *:*
Soit L/K une extension cyclique de degré n, de groupe de Galois G et soit σ un générateur de G. Soit x un élément de L alors la norme $N_{L/K}(x)$ est égale à 1 si et seulement s'il existe un élément y de L^* tel que $x = y/\sigma(y)$.

Idée de la démonstration :
Comme G est cyclique, on peut prouver aisément que si un tel élément existe, alors sa norme vaut 1.
De plus, l'existence d'un tel élément est démontrée grâce au théorème d'indépendance des caractères d'Artin. □

Ce théorème a une forme additive utilisant la trace de l'extension L/K :

Théorème 2.3.2 *:*
Soit L/K une extension cyclique de degré n, de groupe de Galois G et soit σ un générateur de G. Soit $x \in L$ alors la trace $Tr_{L/K}(x)$ est égale à 0 si et seulement s'il existe un élément $y \in L$ tel que $x = y - \sigma(y)$.

La démonstration de ce théorème est fondée également sur le théorème d'indépendance des caractères d'Artin.

Par ces théorèmes, nous obtenons le théorème d'Artin-Schreier décrivant les extensions cycliques de degré p :

Théorème 2.3.3 *:*
Supposons que K est un corps de caractéristique p.

1. *Soit L une extension cyclique de K de degré p, alors il existe un élément x de L tel que $L = K(x)$ et x satisfaisant à une équation de la forme $\mathcal{P}(X) = X^p - X - a = 0$ où $a \in K$.*
2. *Soit $a \in K$, le polynôme $\mathcal{P}(X) = X^p - X - a$ est soit scindé sur K soit irréductible sur K. S'il est irréductible, alors l'extension $K(y)$ est cyclique de degré p où y désigne une racine de $\mathcal{P}(X) = X^p - X - a$ et son groupe de Galois est engendré par l'unique automorphisme qui envoie y sur $y + 1$.*

Démonstration :
Soit L/K une extension cyclique de degré p. Alors :

$$\mathrm{Tr}_{L/K}(-1) = (-1) + (-1) + ... + (-1) = 0.$$

Soit σ un élément engendrant $G = \mathrm{Gal}(L/K)$. Par la forme additive du théorème 90 de Hilbert (cf. th.2.3.2), il existe $y \in L$ tel que $\sigma(y) - y = 1$ et donc $\sigma(y) = y + 1$. Ainsi $\sigma^i(y) = y + i$ pour tout entier $i = 1, ..., p$ et y a p éléments conjugués. Donc $[K(y) : K] \geq p$. On obtient ainsi que $L = K(y)$.
On a de plus :

$$\sigma(y^p - y) = \sigma(y)^p - \sigma(y) = (y+1)^p - (y+1) = y^p - y.$$

Donc l'élément $y^p - y$ est fixe par σ, donc par toutes les puissances de α et ainsi par tous les éléments du groupe G. Il est donc dans le sous-corps K^G de K. On obtient la première assertion du théorème en posant $a = y^p - y$.

Réciproquement, soit $a \in K$. Si y est une racine du polynôme $\mathcal{P}(X) = X^p - X - a$ alors $y+i$ est également une racine du polynôme $\mathcal{P}$ pour $i = 1, ..., p$. Donc $\mathcal{P}$ a p racines distinctes.
Si une de ces racines appartient à K alors toutes les autres racines appartiennent aussi à K.

Supposons donc qu'aucune racine n'est dans K. On veut montrer que le polynôme est irréductible sur K. Posons $\mathcal{P}(X) = g(X)h(X)$ avec g et h deux polynômes de $K[X]$ et tels que $1 \leq \deg(g) < p$. Puisque

$$\mathcal{P}(X) = \prod_{i=1}^{p} (X - y - i)$$

on voit que $g(X)$ est un produit sur des entiers i. Posons $d = \deg(g)$. Le coefficient de X^{d-1} dans g est la somme des termes $-(y+i)$ prise sur les d entiers i. Aussi est-il égal à $-dy + j$ pour certains entiers j. Comme d est non nul dans K alors y appartient à K car nécessairement, les coefficients de g sont dans K. Ce qui nous donne une contradiction. Donc $\mathcal{P}$ est irréductible.

Toutes les racines sont dans $K(y)$. Comme $\mathcal{P}(X)$ n'a pas de racine multiple, alors l'extension $K(y)/K$ est galoisienne. Il existe de cette façon un automorphisme σ de $K(y)$ sur K tel que $\sigma(y) = y + 1$. Les puissances σ^i de σ donnent $\sigma^i(y) = y + i$ pour tout $i = 1, ..., p$.
Le groupe de Galois est donc constitué de toutes les puissances de σ.
C'est donc un groupe cyclique d'ordre p. □

2.3.2 Caractérisation de l'extension L/K par la valuation du coefficient a du polynôme d'Artin-Schreier.

Soit K un corps local de caractéristique $p > 0$ et de corps résiduel k parfait. Si L désigne le corps de décomposition du polynôme d'Artin-Schreier

$\mathcal{P}(X) = X^p - X - a$, la valuation de l'élément a nous permet de caractériser la nature de cette extension.

Proposition 2.3.4 *:*
Soit L le corps de décomposition du polynôme $\mathcal{P}(X) = X^p - X - a$ avec $a \in K$ et soit G le groupe de Galois de l'extension L/K. Alors on a :

1. *Si $v_K(a) > 0$ ou si $v_K(a) = 0$ avec $a \in \wp(K)$ alors l'extension L/K est triviale.*
2. *Si $v_K(a) = 0$ avec $a \notin \wp(K)$ alors l'extension L/K est cyclique de degré p et non ramifiée.*
3. *Si $v_K(a) = -m < 0$ avec $m \in \mathbb{N}^*$ et $pgcd(m, p) = 1$ alors l'extension L/K est cyclique de degré p et totalement ramifiée. De plus, les groupes de ramification en numérotation supérieure sont $G = G^1 = ... = G^m$ et $G^{m+1} = \{1\}$.*

Le saut de ramification de l'extension L/K est donc m.

Tous les cas sont représentés. En effet, si a est un élément de valuation négative et divisible par p alors a est congru, modulo $\wp(W_n(K))$, à un vecteur b tel que $v_K(b) > v_K(a)$ car le corps résiduel est parfait. L'extension L de K est alors définie par le polynôme $X^p - X - b$ et par itération, on peut se ramener à l'un des cas précédents.

Démonstration : Nous allons nous appuyer sur la démonstration donnée par L. Thomas [21] dans sa thèse.

1. Si a appartient à l'idéal $\mathfrak{p}_K$ alors par réduction modulo $\mathfrak{p}_K$, l'équation $\mathcal{P}(X) = 0$ devient $\overline{X}^p - \overline{X} = 0$ sur le corps résiduel k. Comme k est un corps de caractéristique p alors par le lemme de Hensel ([20], Chap.II, §4, Prop.7), le polynôme $\mathcal{P}$ est scindé sur K, donc l'extension L/K est triviale.

2. Par le théorème d'Artin-Schreier, l'extension L/K est cyclique de degré p. Son extension résiduel l/k est donc soit de degré p soit triviale. Or, par hypothèse, $v_K(a) = 0$ donc le corps l contient le corps de décomposition du polynôme réduit $\mathcal{P}$ modulo $\mathfrak{p}_L$. En utilisant à nouveau, le théorème d'Artin-Schreier, l'extension l/k est donc cyclique de degré p et l'extension L/K est non ramifiée de degré p.
De plus, $L = K(\alpha)$ où α est une racine du polynôme $\mathcal{P}$. On a donc $\alpha^p - \alpha = a$ ce qui entraîne : $v_L(\alpha^p - \alpha) = v_L(a)$. Or cette égalité est vraie seulement si $v_L(\alpha)$ est nulle. On obtient donc le résultat voulu.

3. On va d'abord montrer que l'extension L/K est cyclique de degré p. Par le théorème d'Artin-Schreier, soit le polynôme $\mathcal{P}$ est irréductible soit il est scindé sur K. On peut montrer par le polygone de Newton que le polynôme $\mathcal{P}$ admet p racines distinctes, toutes de valuation $-m/p$. Comme $pgcd(m,p) = 1$, alors $-m/p$ n'est pas un entier. Le polynôme $\mathcal{P}$ n'a donc pas de racine dans K et l'extension L/K est ainsi cyclique de degré p.

On montre ensuite que l'extension L/K est totalement ramifiée. Soit α une racine du polynôme $\mathcal{P}$ telle que $L = K(\alpha)$. On obtient donc sa valuation sur L :

$$v_L(\alpha) = \frac{-m}{p} e_{L/K},$$

où $e_{L/K}$ désigne l'indice de ramification de l'extension L/K. Comme α appartient à L et comme m et p sont premier entre eux alors sa valuation est entière. L'indice de ramification $e_{L/K}$ est donc divisible par p. Donc $e = p$ et l'extension est totalement ramifiée.

On doit maintenant calculer le saut de ramification de l'extension L/K. On sait que celui-ci est strictement positif. D'après ce qui précède, on peut donc écrire :

$$G = G^{-1} = G^0 = ... = G^t \quad \text{et} \quad G^{t+1} = \{id\}.$$

Soit π_K une uniformisante de K. Puisque m est premier à p, il existe deux entiers a et b avec $a \in \{0, 1, ..., p-1\}$ tels que : $-am + bp = 1$. Comme $v_L(\alpha) = -m$ et $v_L(\pi_K) = p$ alors $v_L(\alpha^a \pi_K^b) = 1$ et donc l'élément défini par $\pi_L = \alpha^a \pi_K^b$ est une uniformisante du corps local L. En outre, les conjugués de α étant les $\alpha + i$ avec $i \in \{0, 1, ..., p-1\}$, ceux de π_L sont donnés par :

$$\pi_L^{(i)} = (\alpha + i)^a \pi_K^b$$

pour tout $i \in \{0, 1, ..., p-1\}$.

Il faut maintenant calculer chaque $v_L(\pi_L - \pi_L^{(i)})$ afin de déterminer le saut de la filtration de l'extension L/K.

$$\begin{aligned} v_L(\pi_L - \pi_L^{(i)}) &= v_L(\pi_K^b(\alpha^a - (\alpha + i)^a)) \\ &= v_L(\pi_K^b) + v_L(\alpha^{a-1} i) \\ &= bp + v_L(\alpha^{a-1} i) \\ &= bp + (a-1)(-m) \\ &= m + 1. \end{aligned}$$

On montre ainsi que le saut de ramification en numérotation inférieure est m. Le groupe G étant d'ordre p, l'entier m est également le saut de ramification de l'extension L/K en numérotation supérieure. □

2.4 Classes de conjugaison des séries d'ordre p.

Dans ce paragraphe, nous rappelons le résultat de B. Klopsch puis nous en donnons une autre démonstration qui généralise ce résultat lorsque le corps résiduel n'est plus fini mais parfait. Nous prendrons par exemple le corps $\mathbb{F}_p^{alg}$ comme corps résiduel. De plus cette démonstration est valable pour tous les nombres premiers p.

2.4.1 Résultats de B. Klopsch.

Dans son article "Automorphisms of the Nottingham group" [13] paru en 1998, B. Klopsch donne l'ensemble des classes de conjugaison des séries d'ordre p appartenant au groupe de Nottingham. Soit k un corps fini de caractéristique $p > 5$, notons $k[\![t]\!]$ l'anneau des séries formelles entières à coefficients dans k et $K = k(\!(t)\!)$ le corps des fractions de $k[\![t]\!]$, B. Klopsch a prouvé que toute série d'ordre p dans $\mathcal{N}(k)$ est conjuguée à une série de $\mathcal{N}(k)$ de la forme :

$$F(m,\gamma) = \frac{t}{(1-m\gamma t^m)^{1/m}},$$

où m est un entier premier à p et γ est un élément de k^* ([13], Proposition 1.2).

Dans le cas $p = 2, 3$, la démonstration est donnée implicitement dans l'appendice de l'article [13].

Soient $f = t + \sum_{k=1}^{+\infty} f_k t^{k+1}$ et $g = t + \sum_{k=1}^{+\infty} g_k t^{k+1}$ deux séries d'ordre p de $\mathcal{N}(k)$. B. Klopsch montre aussi qu'elles sont conjuguées dans $\mathcal{N}(k)$ si et seulement si leur nombre de ramification et leur premier terme sont égaux (i.e. $i(f) = i(g)$ et $f_{i(f)} = g_{i(g)}$). Elles sont conjuguées dans $\mathcal{G}_0(k)$ si et seulement si leur nombre de ramification sont égaux (i.e. $i(f) = i(g)$) et si $\frac{f_{i(f)}}{g_{i(g)}} \in K^d$ ([13], Proposition 3.3).

2.4.2 Démonstration via la théorie d'Artin-Schreier.

Soit k un corps parfait de caractéristique p. Soit σ un automorphisme d'ordre p dans le groupe des k-automorphismes du corps K. On note G le groupe engendré par σ et on désigne par K^G le sous corps des séries fixées par G.

Nous voulons démontrer le théorème de B. Klopsch par une étude des extensions de degré p du corps K^G. On utilise pour cela la théorie d'Artin-Schreier, puis on montre que l'on peut choisir θ, racine d'un polynôme d'Artin-Schreier $\mathcal{P}(X) = X^p - X - a$ tel que K soit égal à $K^G(\theta)$ et de sorte que $v_K(a)$ soit un entier strictement négatif non divisible par p. Enfin par un changement d'uniformisante adéquat, on obtient la forme désirée. Cette démonstration illustre le lien entre séries et endomorphismes.

Commençons par énoncer le lemme suivant :

Lemme 2.4.1 *:*
Pour toute série entière $1 + t\psi(t)$ avec ψ appartenant à $k[\![t]\!]$, il existe une unique série entière $1 + t\psi'(t)$ avec ψ' dans $k[\![t]\!]$ telle que $(1 + t\psi'(t))^m$ soit égal à $1 + t\psi(t)$.

En d'autre termes, pour tout x appartenant au groupe des unités U_K du corps local K, il existe un unique élément y dans U_K tel que $y^m = x$.

Démonstration :
Posons dans $\mathbb{Q}[\![T]\!]$:

$$\omega(T) = \sum_{n=1}^{+\infty} \binom{1/m}{n} T^n$$

avec

$$\binom{1/m}{n} = \frac{\frac{1}{m} \times (\frac{1}{m} - 1) \times ... \times (\frac{1}{m} - n + 1)}{n!}.$$

On veut montrer que $(1 + \omega(T))^m = 1 + T$.
On part de la formule du binôme. Pour tout réel x tel que $|x| < 1$ et pour tout réel α, on a :

$$e^{\alpha ln(1+x)} = (1 + x)^\alpha = \sum_{n=0}^{+\infty} a_n x^n$$

avec pour tout n :

$$a_n = \frac{\alpha(\alpha - 1)...(\alpha - n - 1)}{n!}.$$

On prend $\alpha = 1/m$, donc $e^{\frac{1}{m} ln(1+x)} = 1 + \omega(x)$.
D'où $e^{ln(1+x)} = 1 + x = (1 + \omega(x))^m$. Donc par le principe d'unicité, on obtient : $1 + T = (1 + \omega(T))^m$.

Si p ne divise pas m alors $\binom{1/m}{n}$ est un entier p-adique. En effet si x_k est un entier relatif alors $\binom{x_k}{n}$ est un entier relatif et si x appartient à $\mathbb{Z}$ alors x est la limite d'une suite $(x_k)_k$ d'entiers relatifs, donc grâce à la continuité en x_k

de la fonction qui à x_k associe $\binom{x_k}{n}$, on obtient $\binom{x}{n}$ appartient à $\mathbb{Z}_p$.
Donc $\omega(T)$ appartient à $T\mathbb{Z}_p[\![T]\!]$, on peut réduire ω à $\overline{\omega}$ dans $\mathbb{F}_p[\![T]\!]$ vérifiant $(1+\overline{\omega}(T))^m = 1+T$.
En posant : $t\psi'(t) = \overline{\omega}(t\psi(t))$, on obtient l'existence de la série désirée ψ'.

Supposons maintenant qu'il existe deux séries ψ' et ψ'' telles que $(1+t\psi'(t))^m$ soit égal à $(1+t\psi''(t))^m$. Alors, comme $(1+t\psi''(t))^m$ est inversible dans $k[\![t]\!]$, on a :

$$\frac{(1+t\psi'(t))^m}{(1+t\psi''(t))^m} = 1.$$

Donc :

$$\frac{1+t\psi'(t)}{1+t\psi''(t)} = \zeta$$

où ζ est une racine $m^{\text{ème}}$ de l'unité. Or, en prenant $t=0$, on obtient $\zeta = 1$ d'où l'unicité de ψ'. □

Théorème 2.4.2 *:*
Soit p un nombre premier et k la clôture algébrique de $\mathbb{F}_p$. Toute série d'ordre p pour la composition est conjuguée dans $\mathcal{N}(k)$ à une unique série de la forme :

$$F(m,\gamma) = \frac{t}{(1+\gamma t^m)^{1/m}}$$

avec m un entier premier à p et γ un élément de k^*.

Démonstration du théorème :
Démonstration de l'existence d'une série $F(m,\gamma)$ conjuguée à σ.
On note K^G le corps composé des éléments $x \in K$ tels que $x^\sigma = x$ pour tous $\sigma \in G$. Par le théorème d'Artin ([15],p.264), puisque G est un groupe cyclique d'ordre p, l'extension K/K^G est cyclique d'ordre p.
De plus, par le théorème d'Artin-Schreier ([15], p.290), il existe un élément primitif θ de l'extension K/K^G tel que θ soit une racine d'un polynôme $\mathcal{P}(X) = X^p - X - a$ pour un certain a appartenant à K^G.
Par un théorème de P. Samuel [18], on a : $K^G = k(\!(t)\!)^G = k(\!(\nu)\!)$ où ν est la norme de t dans l'extension K/K^G.

On remarque que l'extension $k(\!(t)\!)/k(\!(\nu)\!)$ est totalement ramifiée, en effet, l'indice de ramification divisant le degré de l'extension ([11],p.15) et p étant un nombre premier alors l'indice de ramification e est égal à 1 ou à p.
L'image de $k(\!(t)\!)$ par l'application v_K est $\mathbb{Z} \cup \{+\infty\}$ et $v_K(\nu) = p$ d'où

$$v_K\Big(\sum_{i=i_0}^{+\infty} a_i \nu^i\Big) = p.v_{K^G}\Big(\sum_{i=i_0}^{+\infty} a_i \nu^i\Big)$$

ce qui appartient à $p\mathbb{Z}$. Donc $e = [\mathbb{Z} : p\mathbb{Z}] = p$.

On peut maintenant prouver que l'on peut choisir l'élément primitif θ de l'extension K/K^G de sorte que $v_{K^G}(a)$ soit un entier strictement négatif non divisible par p grâce à la proposition 2.3.4.

On a donc, par un choix judicieux de l'élément primitif θ, $v_{K^G}(a) = -m$ où m est un entier strictement positif, non divisible par p.
Comme $v_K(\theta)$ est strictement négatif alors $v_K(\theta)^p$ est strictement inférieur à $v_K(\theta)$.
Donc $v_K(\theta^p - \theta) = v_K(\theta^p) = pv_K(\theta)$ et $pv_K(\theta) = -mv_K(\nu) = -mp$.
D'où $v_K(\theta) = -m$.

On a donc $\theta(t) = \mu t^{-m}(1 + t\psi(t))$ avec ψ appartenant à $k[\![t]\!]$ et μ dans k^*.
En utilisant le lemme 2.4.1, on obtient :

$$\theta(t) = \mu t^{-m}(1 + t\psi'(t))^m = \mu t^{-m}(\varphi(t))^m.$$

Posons $\pi = \frac{t}{\varphi(t)}$. La série π est une uniformisante de $k(\!(t)\!)$ car $v_K(\varphi) = 0$ et π appartient à $\mathcal{N}(k)$ car $v_K(\frac{\pi}{t} - 1)$ est supérieur ou égal à 1. Donc $\theta(t) = \mu\pi^{-m}$.
On a d'une part $\sigma(\theta) = \theta + c = \mu\pi^{-m} + c$ avec c un élément de $\mathbb{F}_p^*$ et d'autre part $\sigma(\theta) = \mu(\pi^\sigma)^{-m} = \mu(\sigma(\pi))^{-m}$. Donc :

$$\frac{\mu(\pi^\sigma)^{-m}}{\mu\pi^{-m} + c} = 1.$$

Ainsi

$$(\pi^\sigma)^m = \frac{\mu}{\mu\pi^{-m} + c} = \frac{\pi^m}{1 + c\mu^{-1}\pi^m}.$$

Donc

$$(\pi^\sigma) = \frac{\xi\pi}{(1 + c\mu^{-1}\pi^m)^{1/m}}$$

où ξ est une racine $m^{\text{ème}}$ de l'unité.
Or σ est une série appartenant à $\mathcal{N}(k)$ donc le coefficient en t de $\pi^\sigma(t)$ est 1, le coefficient en t du numérateur $\xi\pi$ est ξ et le coefficient en t du dénominateur $(1 + c\mu^{-1}\pi^m)^{1/m}$ est 1, donc ξ est égal à 1.
Ceci conclut la démonstration de l'existence d'une série $F(m, \gamma)$ conjuguée dans $\mathcal{N}(k)$ à $\sigma(t)$ avec $\gamma = c\mu^{-1}$.

Démonstration de l'unicité de $F(m, \gamma)$.
Par le lemme 2.2.1, on sait que le nombre de ramification i et le coefficient en t^{i+1} sont invariants par conjugaison dans $\mathcal{N}(k)$. Supposons que σ soit

conjuguée dans $\mathcal{N}(k)$ à $F(m,\gamma)$ et à $F(n,\delta)$, alors le nombre de ramification de $F(m,\gamma)$ est égal au nombre de ramification de $F(n,\delta)$ par transitivité de la conjugaison. Donc

$$v_K\Big(\frac{F(m,\gamma)}{t}-1\Big)=v_K\Big(\frac{F(n,\delta)}{t}-1\Big).$$

D'où

$$v_K\Big(\frac{1}{(1+\gamma t^m)^{1/m}}-1\Big)=v_K\Big(\frac{1}{(1+\delta t^n)^{1/n}}-1\Big).$$

Donc m est égal à n. Comme de plus, le coefficient en t^m est invariant par conjugaison dans $\mathcal{N}(k)$ alors on obtient γ égal à δ. Ce qui prouve l'unicité de la série $F(m,\gamma)$ conjuguée dans $\mathcal{N}(k)$ à σ et de la forme :

$$F(m,\gamma)=\frac{T}{(1+\gamma T^m)^{1/m}}.$$

□

Ce résultat généralise celui de B. Klopsch lorsque le corps résiduel n'est plus fini mais un corps parfait, par exemple, lorsque k est la clôture algébrique de $\mathbb{F}_p$. De plus, nous n'avons pas à distingué les cas $p=2$ et $p=3$ des autres nombres premiers.

Chapitre 3

Anneaux des vecteurs de Witt

Soit p un nombre premier et R un anneau commutatif unitaire de caractéristique strictement positive p. L'ensemble des vecteurs de Witt $W(R)$ étudié dans ce chapitre permet de généraliser la théorie d'Artin-Schreier aux extensions de degré p^n. La manipulation de tels vecteurs n'est pas aisée et pourtant d'une utilité cruciale dans la suite de ce travail. C'est pourquoi, nous essayerons de définir de façon précise les lois sur ces vecteurs faisant de $W(R)$ un anneau commutatif puis les méthodes de calculs sur cet anneau et ses propriétés.
Après avoir rappeler les définitions essentielles sur l'anneau des vecteurs de Witt de longueur infinie $W(R)$ puis de longueur finie $W_n(R)$, nous étudierons les vecteurs de Witt à coefficients dans le corps local des séries formelles $K = k(\!(t)\!)$.

3.1 Premières définitions sur les vecteurs de Witt.

Soit R un anneau commutatif quelconque.

Soient p un nombre premier et $(X_0, ..., X_n, ...)$ une suite d'indéterminées, on appelle "polynômes de Witt" les polynômes définis par la formule :

$$W_n = \sum_{l=0}^{n} X_l^{p^{n-l}} = X_0^{p^n} + pX_1^{p^{n-1}} + ... + p^n X_n.$$

Ces polynômes nous permettent de définir les composantes fantômes des vecteurs de Witt.

Définition 3.1.1 *:*
Pour tout vecteur de Witt $x = (x_j)_{j\geq 1}$ *de* $W(R)$*, la suite* $x^* = (x^{(h)})_h$ *des composantes fantômes est définie par :*

$$x^{(h)} = x_0^{p^h} + px_1^{p^{h-1}} + ... + p^h x_h.$$

Soit $H(R) = R^{\mathbb{N}}$ l'anneau des suites d'éléments de R muni des lois additive et multiplicative termes à termes. Soit g_R l'application de $W(R)$ dans l'anneau $H(R)$ définie par $g_R(x) = x^*$. L'application g_R est un homomorphisme.

3.1.1 Foncteur de Witt.

Soient R et S deux anneaux commutatifs et soit φ un homomorphisme d'anneaux de R dans S, on définit

$$W(\varphi) : W(R) \to W(S)$$

par $W(\varphi)(r_n) = (\varphi(r_n))$ et $W(\varphi)$ est un homomorphisme d'anneaux.

Le foncteur de Witt W est l'unique foncteur satisfaisant aux conditions :

1. Le foncteur W est un foncteur de la catégorie des anneaux commutatifs dans elle-même.
2. La transformation qui associe à un anneau commutatif R l'application g_R est un homomorphisme fonctoriel de W vers le foncteur H.

3.1.2 Addition et multiplication sur cet anneau.

On peut définir sur $W(R)$ deux lois de composition "$+$" et "$\times$" de sorte que $W(R)$ muni de ces deux lois soit un anneau commutatif.

Définition 3.1.2 *:*
Soit R *un anneau commutatif, pour tous* x *et* y *dans l'ensemble* $W(R)$*, on a*

$$g_R(x + y) = g_R(x) + g_R(y) \text{ et } g_R(x \times y) = g_R(x) \times g_R(y).$$

Lorsque l'anneau R contient le corps des rationnels $\mathbb{Q}$, l'application g_R est bijective. On peut donc calculer la somme et le produit de deux vecteurs de Witt appartenant à $W(R)$.

3.1.3 La $n^{\text{ième}}$ composante dans $W(R)$.

Dans ce paragraphe, on donne un lemme technique sur la $n^{\text{ème}}$ composante de l'opposé d'un vecteur de Witt et de la somme de deux vecteurs de Witt. Ce lemme nous servira de façon cruciale à différents moments dans les chapitres suivants.

Nous définissons dans un premier temps le poids d'un monôme afin d'établir ce lemme.

Dans l'anneau des polynômes à $2j$ indeterminées $R[x_0, ..., x_{j-1}, y_0, ..., y_{j-1}]$, le poids d'un monôme $x_0^{\eta_0}...x_{j-1}^{\eta_{j-1}}y_0^{\mu_0}...y_{j-1}^{\mu_{j-1}}$ est donné par la formule :

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

Un polynôme est dit homogène en poids s'il est combinaison linéaire de monômes de poids identiques.

Notons que le poids dépend de l'entier premier p.

Lemme 3.1.3 *:*

1. *Soit $x = (x_0, x_1, ...) \in W(R)$, la $j^{ème}$ composante de $-x$ est $-x_{j-1} + \Omega_{j-1}$ où $\Omega_{j-1} = \Omega_{j-1}(x_0, ..., x_{j-2})$ est un polynôme homogène de poids p^{j-1} à coefficients dans $\mathbb{Z}$.*
2. *Soient $x = (x_0, x_1, ...)$ et $y = (y_0, y_1, ...)$ deux vecteurs de Witt, la $j^{ème}$ composante de la somme $x + y$ est $x_{j-1} + y_{j-1} + \Sigma_{j-1}$ où $\Sigma_{j-1} = \Sigma_{j-1}(x_0, ..., x_{j-2}, y_0, ..., y_{j-2})$ est un polynôme homogène de poids p^{j-1} à coefficients dans $\mathbb{Z}$.*

Démonstration :
1. On considère dans un premier temps l'anneau $R_{\mathbb{Z}} = \mathbb{Z}[X_0, X_1, ..., X_j, ...]$ des polynômes en une infinité d'indéterminées à coefficients entiers.
Posons $X = (X_0, X_1, ..., X_j, ...)$ et soit $Y = (Y_0, Y_1, ..., Y_j, ...)$ le vecteur opposé au vecteur X dans $W(R_{\mathbb{Z}})$. Les $j^{\text{èmes}}$ composantes fantômes de X et Y sont respectivement données par les formules :

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

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

Puisque $g_{R_\mathbb{Z}}$ est un homomorphisme d'anneaux, on a dans l'anneau $H(R_\mathbb{Z})$:

$$X^{(j-1)} + Y^{(j-1)} = 0.$$

Soit $R_\mathbb{Q}$ l'anneau $R_\mathbb{Q} = \mathbb{Q}[X_0, X_1, ..., X_j, ...]$ des polynômes en une infinité dénombrable d'indéterminées à coefficients rationnels. Dans l'anneau $H(R_\mathbb{Q})$, on obtient :

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

et ainsi

$$Y_{j-1} = -X_{j-1} + \Omega_{j-1}$$

où Ω_{j-1} est par récurrence sur j un polynôme en $X_0, X_1, ..., X_{j-2}$ à coefficients nécessairement entiers car Y_{j-1} appartient à $R_\mathbb{Z}$. De plus Ω_{j-1} est par récurrence un polynôme homogène en poids de poids p^{j-1}.

Maintenant, pour tout anneau quelconque R, il existe un homomorphisme φ de $R_\mathbb{Z}$ dans R tel que $W(\varphi)(X) = x$. Posons $Y = -X$.
Comme $Y_{j-1} = -X_{j-1} + \Omega_{j-1}(X_0, X_1, ..., X_{j-2})$ où $\Omega_{j-1} \in \mathbb{Z}[X_0, X_1, ..., X_{j-1}]$, on peut en déduire que

$$\varphi(Y_{j-1}) = -\varphi(X_{j-1}) + \Omega_{j-1}(\varphi(X_0), \varphi(X_1), ..., \varphi(X_{j-2}))$$

car φ est un homomorphisme d'anneaux.

2. Soit $S_\mathbb{Z} = \mathbb{Z}[X_0, X_1, ..., X_j, ...Y_0, Y_1, ..., Y_j, ...]$ l'anneau des polynômes en une infinité dénombrable d'indéterminées à coefficients entiers. Soient $X = (X_0, X_1, ..., X_j, ...)$ et $Y = (Y_0, Y_1, ..., Y_j, ...)$ deux vecteurs de Witt dans $W(S_\mathbb{Z})$. Les $j^{\text{èmes}}$ composantes fantômes de X et Y sont :

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

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

Soit $Z = (Z_0, Z_1, ..., Z_j, ...) \in W(S_\mathbb{Z})$ le vecteur de Witt $Z = X + Y$. La $j^{\text{ème}}$ composante fantôme peut s'écrire sous la forme :

$$Z^{(j-1)} = Z_0^{p^{j-1}} + pZ_1^{p^{j-2}} + ... + p^{j-2}Z_{j-2}^p + p^{j-1}Z_{j-1}.$$

Comme $g_{S_\mathbb{Z}}$ est un homomorphisme d'anneaux et par définition de l'addition dans $H(S_\mathbb{Z})$, on obtient : $X^{(j-1)} + Y^{(j-1)} = Z^{(j-1)}$ et ainsi

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

Soit $S_{\mathbb{Q}}$ l'anneau $\mathbb{Q}[X_0, X_1, ..., X_j, ..., Y_0, Y_1, ..., Y_j, ...]$. La $j^{\text{ème}}$ composante de Z dans $S_{\mathbb{Q}}$ est donc :

$$Z_{j-1} = X_{j-1} + Y_{j-1} + \Sigma_{j-1}$$

avec Σ_{j-1} un polynôme à coefficients entiers. De plus Σ_{j-1} est par récurrence un polynôme homogène de poids p^{j-1}.

Maintenant pour tout anneau quelconque R, il y a un homomorphisme φ de $S_{\mathbb{Z}}$ dans R tel que :

$$W(\varphi)(X) = x \quad \text{et} \quad W(\varphi)(Y) = y.$$

Sachant que $Z_{j-1} = X_{j-1} + Y_{j-1} + \Sigma_{j-1}$ avec

$$\Sigma_{j-1} \in \mathbb{Z}[X_0, X_1, ..., X_{j-1}, Y_0, Y_1, ..., Y_{j-2}],$$

on peut en déduire que comme φ est un homomorphisme d'anneaux, on a :

$$\varphi(Z_{j-1}) = \varphi(X_{j-1}) + \varphi(Y_{j-1}) + P_{j-1}(\varphi(X_0), ..., \varphi(X_{j-2}), \varphi(Y_0), ..., \varphi(Y_{j-2}))$$

ce qui nous donne le résultat. □

Corollaire 3.1.4 *:*
La $j^{ème}$ composante du vecteur $x - y$ est $x_{j-1} - y_{j-1} + \Delta_{j-1}$ où $\Delta_{j-1} = \Delta_{j-1}(x_0, ..., x_{j-2}, y_0, ..., y_{j-2})$ est un polynôme homogène de poids p^{j-1} à coefficients dans $\mathbb{Z}$.

3.1.4 Les unités de $W(R)$ et la notation $\{x\}$.

Les unités de l'anneau des vecteurs de Witt sont les vecteurs dont la première composante est non nulle. C'est à dire, le vecteur de Witt $x = (x_0, x_1, ...)$ est une unité de $W(R)$ si et seulement si $x_0 \in R^*$.

Dans la suite, nous utiliserons régulièrement la notation $\{x\}$. Celle-ci désignera un vecteur de Witt dont toutes les composantes sont nulles hormis la première.
On note $\{x\}$ le vecteur de Witt donné par $(x, 0, ...)$.

Lemme 3.1.5 *:*
Pour tout vecteur de Witt $y = (y_0, y_1, ..., y_l, ...) \in W(R)$ et pour tout élément x de R, on a la relation :

$$\{x\}y = (xy_0, x^p y_1, ..., x^{p^l} y_l, ...).$$

Démonstration :
Pour montrer ce résultat, on va montrer que les composantes fantômes des vecteurs $\{x\}y$ et de $(xy_0, x^p y_1, ..., x^{p^l} y_l, ...)$ sont égales.

Pour tout $k \geq 1$, la $k^{\text{ème}}$ composante fantôme de $\{x\}$ est x^{p^k} donc la $k^{\text{ème}}$ composante fantôme du produit $\{x\}y$ est :

$$(\{x\}y)^{(k)} = x^{p^k}(y_0^{p^k} + py_1^{p^{k-1}} + p^2 y_2^{p^{k-2}} + ... + p^k y_k).$$

En calculant la $k^{\text{ème}}$ composante fantôme de $(xy_0, x^p y_1, ..., x^{p^l} y_l, ...)$, on obtient :

$$(xy_0)^{p^k} + p(x^p y_1)^{p^{k-1}} + p^2 (x^{p^2} y_2)^{p^{k-2}} + ... + p^k (x^{p^k} y_k).$$

On retrouve le résultat précédent d'où

$$(\{x\}y)^{(k)} = (xy_0, x^p y_1, ..., x^{p^l} y_l, ...)^{(k)}.$$

Pour tout $k \geq 1$, les composantes fantômes des vecteurs de Witt $\{x\}y$ et $(xy_0, x^p y_1, ..., x^{p^l} y_l, ...)$ sont donc égales.

Si l'anneau R contient $\mathbb{Q}$, l'application g_R qui associe au vecteur de Witt la suite de ses composantes fantômes est un isomorphisme d'anneaux, on obtient alors le résultat. Puis si R est un anneau quelconque, alors il existe un homomorphisme φ de $\mathbb{Z}$ dans R tel que $W(\varphi)(X) = x$, on obtient, de la même façon que dans la démonstration précédente, le résultat pour tout anneau R. □

3.1.5 L'application de Frobenius F, l'homomorphisme de groupe additif $\wp$ et le "Shift" V.

Soit R un anneau de caractéristique p. Nous généralisons aux vecteurs de Witt les applications F et $\wp$ du chapitre 1.

Définition 3.1.6 *:*
Soit F l'endomorphisme de Frobenius de $W(R)$ qui à tout vecteur de Witt $x = (x_0, x_1, ..., x_l, ...)$ associe le vecteur de Witt $Fx = (x_0^p, x_1^p, ..., x_{l-1}^p, ...)$.

Cette application est continue. Si R est un anneau parfait alors l'application F est un isomorphisme d'anneaux.

Grâce à l'application du Frobenius, on peut définir l'isogénie, notée $\wp$. C'est l'homomorphisme additif du groupe abélien $W(R)$:

$$\begin{array}{rccc} \wp : & W(R) & \to & W(R) \\ & (x_0, x_1, ..., x_l, ...) & \mapsto & (x_0^p, x_1^p, ..., x_l^p, ...) - (x_0, x_1, ...x_l, ...) \end{array}$$

Les applications F et $\wp$ généralisent les applications que l'on avait déjà notées F et $\wp$ dans le chapitre précedent à tous les vecteurs de Witt.

Définition 3.1.7 *:*
L'application de décalage "shift" de $W(R)$ est définie par $V : W(R) \to W(R)$ telle que pour tout vecteur $x = (x_0, x_1, ...)$, on a $V(x_0, x_1, ...) = (0, x_0, x_1, ...)$.

Notons que pour tout x et y dans $W(R)$, on obtient ([20], ch II, §6) :

$$V(x + y) = V(x) + V(y).$$

On remarque que pour tout anneau commutatif R de caractéristique p, on a sur l'anneau de Witt $W(R)$:

$$\mathbf{p} = FV = VF$$

où $\mathbf{p}$ désigne la multiplication par p.

3.2 Anneaux des vecteurs de Witt de longueur finie.

Dans la suite, nous fixons un entier $n \geq 1$ et nous définissons l'anneau des vecteurs de Witt de longueur n à coefficients dans un anneau commutatif R quelconque.

3.2.1 L'idéal I_n et définition de $W_n(R)$.

Définition 3.2.1 *:*
Soit $I_n = V^n(W(R)) = \{(0, ..., 0, x_n, x_{n+1}, ...)\}$ l'ensemble des vecteurs de Witt pour lesquels les n premières composantes sont nulles.

Cet ensemble I_n est un sous-groupe additif de $W(R)$ et un idéal de $W(R)$. La notation $W_n(R)$ désigne le quotient $W(R)/I_n$. Les éléments de $W_n(R)$ sont identifiés aux vecteurs $(x_0, ..., x_{n-1}) \in R^n$. Ces vecteurs sont appelés vecteurs de Witt de longueur n. L'addition et la multiplication dans $W_n(R)$ sont données par les mêmes formules que dans $W(R)$.

Remarque.
Dans le cas $n = 1$, $W_1(R)$ est identifié à R.

3.2.2 Applications de Troncation.

Définition 3.2.2 *:*
Pour tout $0 < j \leq n$, on définit l'application de troncation T^{n-j} de $W_n(R)$ dans $W_j(R)$ par :

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

L'anneau des vecteurs de Witt $W(R)$ peut ainsi être vu comme étant la limite projective des anneaux $W_n(R)$ pour les applications de troncation.

3.2.3 Les applications F et $\wp$ sur $W_n(R)$.

L'endomorphisme F défini sur $W(R)$ induit par passage au quotient un endomorphisme sur l'anneau $W_n(R)$ que nous noterons à nouveau F. C'est à dire, pour tout vecteur $x = (x_0, x_1, ..., x_{n-1})$ de $W_n(R)$, on a :

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

De la même façon, on définit par passage au quotient l'endomorphisme de $W_n(R)$ tel que pour tout vecteur de Witt de longueur n :

$$\wp(x_0, x_1, ..., x_{n-1}) = (x_0^p, x_1^p, ..., x_{n-1}^p) - (x_0, x_1, ..., x_{n-1}).$$

Cette application est un homomorphisme additif de $W_n(R)$.

3.3 Anneau des vecteurs de Witt de longueur finie à coefficients dans $K = k(\!(t)\!)$.

On se restreint maintenant à l'étude des vecteurs de Witt de longueur n à coefficients dans le corps $K = k(\!(t)\!)$ avec k la clôture algébrique de $\mathbb{F}_p$.

3.3.1 Surjectivité et noyau de $\wp$.

Soit k un corps de caractéristique p.

Lemme 3.3.1 *:*
Si k est un corps algébriquement clos alors $W_n(k) = \wp(W_n(k))$.

Démonstration :
Il est évident que $\wp(W_n(k)) \subset W_n(k)$.
L'inclusion $W_n(k) \subset \wp(W_n(k))$ est aussi évidente dans le cas $n = 1$. Nous supposons donc maintenant que la propriété $W_n(k) \subset \wp(W_n(k))$ est vérifiée jusqu'au rang n.
Soit $x = (x_0, ..., x_n) \in W_{n+1}(k)$. Nous avons $x_0 \in k$ donc il existe un élément a de k tel que $x_0 = \wp(a)$. Soit $\{a\}$ le vecteur de Witt de longueur $n+1$: $(a, 0, ..., 0)$. On a

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

Par hypothèse de récurrence, pour tout $(x'_1, ..., x'_n) \in W_n(k)$ il existe un vecteur $(y_1, ..., y_n) \in W_n(k)$ tel que $(x'_1, ..., x'_n) = \wp(y_1, ..., y_n)$. D'où

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

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

Proposition 3.3.2 *:*
Dans l'anneau $W(K)$ où $K = k(\!(t)\!) = \mathbb{F}_p^{alg}(\!(t)\!)$, le noyau de $\wp$ est $W(\mathbb{F}_p)$.

Démonstration :
Comme F fixe tous les éléments x de $\mathbb{F}_p$ alors $\wp(x) = 0$ donc $W_n(\mathbb{F}_p)$ est inclus dans le noyau de $\wp$.

On montre la seconde inclusion par récurrence sur n.
Si $n = 1$, l'anneau $W_1(K)$ est le corps K de caractéristique p donc ξ appartient à $\mathbb{F}_p$ si et seulement si $\xi^p - \xi = 0$. Le noyau de $\wp$ sur K est donc $\mathbb{F}_p$.

Supposons que la propriété est vérifiée jusqu'au rang n et montrons-là au rang $n+1$. Soit $\xi = (\xi_0, ..., \xi_n) \in W_{n+1}(K)$ un élément du noyau de $\wp$. On a deux cas :

Si $\xi_0 = 0$, on peut montrer, comme dans la démonstration de la prop 3.3.1, que $\wp(\xi_1, ..., \xi_n) = 0$. Ainsi, par hypothèse de récurrence, tous les coefficents du vecteur $(\xi_0, ..., \xi_n)$ sont dans $\mathbb{F}_p$ et donc $\xi \in W_{n+1}(\mathbb{F}_p)$.

Si $\xi_0 \neq 0$ alors $\wp(\xi_0) = \xi_0^p - \xi_0 = 0$ donc $\xi_0 \in \mathbb{F}_p$. Comme

$$(\xi_0, \xi_1, ..., \xi_n) = (\xi_0, 0, ..., 0) + (0, \xi_1, ..., \xi_n)$$

alors par additivité de $\wp$:

$$\wp(\xi_0, \xi_1, ..., \xi_n) = \wp(\xi_0, 0, ..., 0) + \wp(0, \xi_1, ..., \xi_n)$$

On a donc $\wp((0,\xi_1,...,\xi_n)=0$ car $\wp(\xi_0,0,...,0)$ est un vecteur de $W_{n+1}(\mathbb{F}_p)$ donc en se ramenant au cas précédent, ξ est un vecteur appartenant à $W_{n+1}(\mathbb{F}_p)$.
On obtient ainsi le résultat recherché. □

3.3.2 Le groupe complet $W_n(K)$.

On définit sur $W_n(K)$ l'application suivante ([22], Prop 4.2) introduite dans la thèse de V. Shabat en 2001 :

Définition 3.3.3 *:*
Soit $x=(x_0,x_1,...,x_{n-1})$ un vecteur de Witt de longueur n, posons :

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

Lemme 3.3.4 *:*
Par la troisième propriété de la Proposition 4.2 de [21], l'application m_n vérifie l'inégalité :

$$m_n(x+y)\geq\min\{m_n(x),m_n(y)\} \text{ pour tout } x \text{ et } y \text{ dans } W_n(K).$$

Démonstration :
Posons $m=\min\{m_n(x),m_n(y)\}$ et montrons que $m\leq m_n(x+y)$.
Par le lemme 3.1.3, on sait que la $\iota^{\text{ème}}$ composante du vecteur $x+y$ est $x_\iota+y_\iota+\Sigma_\iota$ où Σ_ι désigne un polynôme homogène de poids p^ι dont les indéterminées sont les composantes $x_0,x_1,...,x_{\iota-1},y_0,y_1,...,y_{\iota-1}$.
Donc $v_K((x+y)_\iota)=v_K(x_\iota+y_\iota+\Sigma_\iota)$, d'où pour tout indice $\iota=0,1,...,n-1$:

$$v_K((x+y)_\iota)\geq\min(v_K(x_\iota),v_K(y_\iota),v_K(\Sigma_\iota))\geq\frac{m}{p^{n-1-\iota}}.$$

Ainsi $p^{n-1-\iota}v_K((x+y)_\iota)\geq m$ pour tout ι, d'où le résultat. □

Remarque :
On note également que pour tout $x\in W_n(K)$,

$$m_n(x)=\min\{pm_{n-1}(T(x)),v_K(x_{n-1})\}.$$

A la fonction m_n, on peut lui associer une distance d_n faisant de $W_n(K)$ un espace métrique.

Définition 3.3.5 *:*
Soit d_n la distance sur $W_n(K)$ définie par $d_n(x,y)=p^{-m_n(x-y)}$.

Remarques :

1. Cette distance est compatible avec l'addition, c'est à dire, l'application :

$$\begin{array}{ll} W_n(K) \times W_n(K) & \to W_n(K) \\ (x, y) & \mapsto x + y \end{array}$$

est continue.

2. La topologie définie sur $W_n(K)$ par la distance d_n coïncide avec la topologie produit de l'ensemble K^n.

Lemme 3.3.6 *:*
Le groupe additif $W_n(K)$ muni de la distance d_n est un groupe complet.

Démonstration :
On va prouver par récurrence sur n que $W_n(K)$ est un espace complet.
Si $n = 1$ alors pour tout $x \in W_1(K) = K$, on a :

$$m_1(x) = v_K(x).$$

On sait que K est complet pour la valuation v_K, donc si $x^{(h)}$ est une suite de Cauchy, alors elle converge dans $W_1(K) = K$ pour la distance d_1.

Supposons maintenant que $W_n(K)$ est complet jusqu'au rang $n-1$ et prouvons ce résultat au rang n.
Soit $x^{(h)}$ une suite de Cauchy appartenant à $(W_n(K), d_n)$ alors $m_n(x^{(h+1)} - x^{(h)})$ tend vers $+\infty$. Comme $m_{n-1}(T(x^{(h+1)}) - T(x^{(h)})) \geq \frac{1}{p} m_n(x^{(h+1)} - x^{(h)})$ alors $m_{n-1}(T(x^{(h+1)}) - T(x^{(h)}))$ tend vers $+\infty$ et ainsi $T(x^{(h)})$ est une suite de Cauchy de $(W_{n-1}(K), d_{n-1})$.
Par hypothèse de récurrence, la suite $T(x^{(h)})$ tend vers $T(l)$ où l est un vecteur de Witt de $W_n(K)$. Pour chaque h, on peut écrire $x^{(h)} = l + y^{(h)}$ avec un certain vecteur de Witt $y^{(h)} = (y_0^{(h)}, ..., y_{n-1}^{(h)})$ de longueur n. Donc $T(y^{(h)})$ tend vers le vecteur nul de $W_{n-1}(K)$.
D'autre part, la suite $y^{(h)}$ est une suite de Cauchy de $(W_n(K), d_n)$ car translatée d'une suite de Cauchy. En écrivant $y^{(h)} = (T(y^{(h)}), \beta_{n-1}^{(h)})$ avec $\beta_{n-1}^{(h)} \in K$ et $T(y^{(h)})$ représentant les $n-1$ premières composantes de $y^{(h)}$. Il existe $\Delta_{n-1} \in K$ tel que :

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

Par le lemme 3.1.3, l'élément Δ_{n-1} est un polynôme homogène en les variables $y_0^{(h+1)}, ..., y_{n-2}^{(h+1)}, y_0^{(h)}, ..., y_{n-2}^{(h)}$, donc il converge vers 0 car toutes les

composantes $b_i^{(h)}$ et $b_i^{(h+1)}$ tendent vers 0.
Ainsi la suite $(\beta_{n-1}^{(h+1)} - \beta_{n-1}^{(h)})_h$ tend vers 0. La suite $\beta_{n-1}^{(h)}$ est donc une suite de Cauchy dans K, et elle converge vers une limite β_{n-1} dans K.
On peut en déduire que $y^{(h)}$ converge vers un vecteur de Witt $(0, ..., 0, \beta_{n-1})$.
Donc $x^{(h)}$ converge vers $l + (0, ..., 0, \beta_{n-1})$ et ainsi $W_n(k)$ est un groupe complet. □

3.3.3 Une réduction des vecteurs de Witt.

Dans la suite, la notation $W_n(\mathfrak{p}_K)$ désignera l'ensemble des vecteurs de Witt de longueur n dont les composantes sont toutes dans l'idéal maximal $\mathfrak{p}_K$. Comme $\mathfrak{p}_K$ n'est pas un anneau, l'ensemble $W_n(\mathfrak{p}_K)$ n'a pas de structure d'anneau.

Lemme 3.3.7 *:*
Soit $x \in W_n(\mathcal{O}_K)$ alors x peut s'écrire comme somme de deux vecteurs de Witt : $x = y + z$ avec $y \in W_n(k)$ et $z \in W_n(\mathfrak{p}_K)$.

Démonstration :
Par récurrence sur n.
Si $n = 1$, la propriété est évidente.
Supposons maintenant que la propriété est vérifiée pour tous les vecteurs de Witt de longueur inférieure ou égale à $n - 1$.
Soit $x = (x_0, ..., x_{n-2}, x_{n-1}) \in W_n(\mathcal{O}_K)$ et $x' = (x_0, ..., x_{n-2})$ sa troncation dans $W_{n-1}(\mathcal{O}_K)$.
Par hypothèse de récurrence, il existe $y' \in W_{n-1}(k)$ et $z' \in W_{n-1}(\mathfrak{p}_K)$ tels que $x' = y' + z'$.
Il faut donc prouver l'existence de $y_{n-1} \in k$ et de $z_{n-1} \in \mathfrak{p}_K$ tels que $x = y + z$ avec y et z des vecteurs de Witt de longueur n pour lesquels les $n-1$ premières composantes sont respectivement les composantes de y' et z'. Par le lemme 3.1.3, on sait que $x_{n-1} - \Sigma_{n-1} = y_{n-1} + z_{n-1}$ où Σ_{n-1} est un polynôme homogène en poids en les indeterminées $y_0, ..., y_{n-2}, z_0, ..., z_{n-2}$.
En substituant les valeurs de y' et z' dans le polynôme Σ_{n-1}, la valuation de Σ_{n-1} est positive. Comme la valuation de x_{n-1} est également positive, alors $x_{n-1} - \Sigma_{n-1}$ est une série formelle dans $\mathcal{O}_K$. On peut ainsi trouver y_{n-1} dans k et z_{n-1} dans $\mathfrak{p}_K$. □

3.3.4 Une propriété de $W_n(\mathcal{O}_K)$.

La proposition suivante généralise aux vecteurs de Witt le lemme 1.2.2 du paragraphe 1.2.4.

Proposition 3.3.8 *:*
Un vecteur de Witt dont toutes les composantes sont dans $\mathcal{O}_K$ appartient à $\wp(W_n(\mathcal{O}_K))$, i.e. $W_n(\mathcal{O}_K) = \wp(W_n(\mathcal{O}_K))$.

Démonstration :
Supposons dans un premier temps que toutes les composantes sont des séries de valuation strictement positives.
Soit $x = (x_0, ..., x_1) \in W_n(\mathfrak{p}_K)$. On a $F^h x = (x_0^{p^h}, x_1^{p^h}, ..., x_{n-1}^{p^h})$.
Soit $y = -\sum_{h\geq 0} F^h x$ donc :

$$\begin{aligned} m_n(F^h x) &= \min(p^{n-1-\iota} \mathrm{v}_K(x_\iota^{p^h})) \\ &= p^h \min(p^{n-1-\iota} \mathrm{v}_K(x_\iota)) \\ &= p^h m_n(x). \end{aligned}$$

D'où $m_n(F^h x) \geq p^h$ car $m_n(x) \geq 1$, donc $m_n(F^h x)$ tend vers $+\infty$. Grâce au lemme 3.3.6 prouvant que $W_n(K)$ est un espace complet, la série y converge. De plus, comme l'application du Frobenius F est un endomorphisme continu de $W_n(K)$, on a :

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

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

Maintenant supposons qu'une ou plusieurs composantes sont des séries de valuation nulle. Si $x \in W_n(\mathcal{O}_K)$ alors, par le lemme 3.3.7, x est la somme d'un élément de $W_n(k)$ et d'un élément de $W_n(\mathfrak{p}_K)$. Comme le corps k est algebriquement clos, alors $W_n(k) \subset \wp(W_n(k))$. De plus, comme $W_n(\mathfrak{p}_K) \subset \wp(W_n(\mathcal{O}_K))$ alors x est la somme de deux vecteurs de $\wp(W_n(\mathcal{O}_K))$ et donc $x \in \wp(W_n(\mathcal{O}_K))$. □

Chapitre 4

Vecteurs de Witt sur un corps local de caractéristique p et de corps résiduel algébriquement clos

Soit $K = k(\!(t)\!)$ et soit n un entier. Nous montrons, dans ce chapitre, plusieurs propriétés de l'anneau de Witt $W_n(K)$ lorsque le corps résiduel k de K est algébriquement clos. Nous rappelons dans le premier paragraphe la théorie d'Artin-Schreier-Witt qui généralise aux extensions cycliques de degré p^n la théorie d'Artin-Schreier. Nous nous placerons alors dans le cas où k est la clôture algébrique du corps à p éléments, i.e. $k = \mathbb{F}^{alg}$.
Nous introduirons alors un sous-module $\mathcal{B}_n$ de $W_n(K)$ et un certain sous-ensemble $\mathcal{A}_n$ de $\mathcal{B}_n$ qui jouerons un rôle crucial dans la suite de ce travail. En effet ceux-ci nous serviront dans la construction d'une bijection permettant de caractériser les extensions cycliques d'ordre p^n totalement ramifiées par un ensemble de vecteurs de Witt.

4.1 Rappels sur la théorie d'Artin-Schreier-Witt.

On commence ce chapitre par quelques rappels sur la théorie d'Artin-Schreier-Witt qui généralise le théorème d'Artin-Schreier aux extensions cycliques de degré p^n sur un corps de caractéristique p.

4.1.1 Accouplement d'Artin-Schreier-Witt.

L'accouplement suivant nous sera très utile dans la suite.

Par la théorie d'Artin-Schreier-Witt, si L/K est une extension cyclique de

degré p^n, alors il existe un accouplement non dégénéré ([3], chap IX) :

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

où $\wp(\alpha) = a$ et $\overline{a}$ est la classe de a modulo $\wp(W_n(K))$.
De plus, on sait que cet accouplement met en dualité le groupe de Galois $\mathrm{Gal}(L/K)$ et $(\wp(W_n(L)) \cap W_n(K))/\wp(W_n(K))$.

4.1.2 Théorème 90 de Hilbert sur $W_n(K)$.

Soient K un corps de caractéristique p et L une extension finie galoisienne de K de groupe de Galois G dont σ est un des générateurs. On définit la trace de tout vecteur de Witt grâce à la formule suivante :

$$\mathrm{Tr}_{L/K}(x) = \sum_{\sigma \in G} \sigma(x) = \sum_{\sigma \in G} (\sigma(x_0), \sigma(x_1), ..., \sigma(x_{n-1})).$$

Le théorème suivant généralise le théorème 90 de Hilbert à tout vecteur de Witt de longueur n. Nous retranscrirons la démonstration donnée par L. Thomas dans sa thèse [21].

Théorème 4.1.1 *:*
Soient K un corps de caractéristique p et L une extension finie galoisienne de K de groupe de Galois G et σ un générateurs de $G = Gal(L/K)$. Alors, pour tout entier $n \geq 1$, le premier groupe de cohomologie correspondant aux vecteurs de Witt est trivial, i.e. :

$$H^1(G, W_n(L)) = 0$$

Démonstration :
Soit f un cocycle de G c'est à dire une application de G dans $W_n(L)$ telle que pour tous σ, τ dans G, on a la relation : $f(\sigma.\tau) = \sigma f(\tau) + f(\sigma)$.
On veut montrer que f est un cobord c'est à dire qu'il existe un vecteur x dans $W_n(L)$ tel que pour tout σ de G, on a $f(\sigma) = x - \sigma(x)$.
Soit $y = (y_0, y_1, ..., y_{n-1})$ un vecteur de Witt de $W_n(L)$ tel que $\mathrm{Tr}_{L/K}(y_0) \neq 0$. L'existence d'un tel élément peut être prouvé par le théorème d'indépendance des caractères d'Artin. Comme $Tr_{L/K}(y_0)$ est la première composante de $\mathrm{Tr}_{L/K}(y)$, alors $\mathrm{Tr}_{L/K}(y)$ est une unité de $W_n(L)$.
Posons dans l'anneau de Witt $W_n(K)$:

$$x = \frac{1}{\mathrm{Tr}_{L/K}(y)} \sum_{\tau \in G} f(\tau)\tau(y).$$

pour tout élément σ dans G, nous obtenons :

$$\begin{aligned}
\sigma(x) &= \frac{1}{\sigma(\mathrm{Tr}_{L/K}(y))}\sum_{\tau\in G}\sigma(f(\tau))\sigma(\tau(y)) \\
&= \frac{1}{\mathrm{Tr}_{L/K}(y)}\sum_{\tau\in G}(f(\sigma\tau)-f(\sigma))\sigma\tau(y) \\
&= \frac{1}{\mathrm{Tr}_{L/K}(y)}\sum_{\tau\in G}f(\sigma\tau)\sigma\tau(y) - \frac{1}{\mathrm{Tr}_{L/K}(y)}\sum_{\tau\in G}f(\sigma)\sigma\tau(y) \\
&= \frac{1}{\mathrm{Tr}_{L/K}(y)}\sum_{\psi\in G}f(\psi)\psi(y) - \frac{f(\sigma)}{\mathrm{Tr}_{L/K}(y)}\sum_{\psi\in G}\psi(y) \\
&= x - f(\sigma).
\end{aligned}$$

Ce qui donne le résultat désiré. □

Remarque :
Ce théorème généralise le théorème 90 de Hilbert (cf. théorème 2.3.2 du chapitre 2) à tout vecteur de Witt de longueur n et est équivalent à l'énoncé suivant : "La trace d'un élément x de $W_n(L)$ est nulle si et seulement s'il existe un élément y dans $W_n(L)$ tel que $x = y - \sigma(y)$". En effet, l'isomorphisme

$$H^1(G, W_n(L)) \simeq Ker(Tr_{L/K})/(1-\sigma)W_n(L)$$

donne la suite exacte :

$$H^1(G, W_n(L)) \hookrightarrow Ker(Tr_{L/K}) \to Ker(Tr_{L/K})/(1-\sigma)W_n(L).$$

Par cette suite exacte, on peut ensuite prouver que tout cocycle est un cobord.

4.1.3 Théorème d'Artin-Schreier-Witt.

On énonce le théorème sur les extensions cycliques de degré p^n suivant :

Théorème 4.1.2 *:*

1. *Pour tout vecteur de Witt $x = (x_0, x_1, ..., x_{n-1}) \in W_n(K)$, soit l'équation $\wp(y) = x$ n'admet aucune solution dans $W_n(K)$, soit elle en admet p^n.*
2. *Si l'équation $\wp(y) = x$ n'admet aucune solution dans $W_n(K)$ alors l'extension $K(\wp^{-1}(x))$ est cyclique sur le corps K de degré divisant p^n. Le degré est égal à p^n si et seulement si x_0 n'appartient pas à $\wp(K)$.*
3. *Réciproquement, si l'extension L/K est cyclique de degré p^n alors il existe un vecteur de Witt $x \in W_n(K)$ tel que $L = K(\wp^{-1}(x))$ et $x_0 \notin \wp(K)$.*

Démonstration :
Nous nous baserons sur la démonstration donnée dans [21].

1. Comme le noyau de $\wp$ sur $W_n(K)$ est $W_n(\mathbb{F}_p)$ et comme $\mathbb{F}_p$ s'injecte dans le corps K, si l'équation $\wp(\xi) = x$ admet une solution dans $W_n(K)$ alors toutes ses solutions sont dans $W_n(K)$ et il y a p^n telles solutions. Elles diffèrent entre elles par un élément de $W_n(\mathbb{F}_p)$.

2. Supposons que l'équation n'admette aucune solution dans $W_n(K)$.
Soit ξ un vecteur de Witt de longueur n tel que $\wp(\xi) = x$. Soit le K-isomorphisme de corps $\varphi : K(\wp^{-1}(x)) \to K^{alg}$ où K^{alg} désigne la clôture algébrique de K. Ce morphisme définit fonctoriellement un homomorphisme d'anneaux :

$$W_n(\varphi) : W_n(K(\wp^{-1}(x))) \to W_n(K^{alg})$$

en posant $W_n(\varphi)(\xi_0, \xi_1, ..., \xi_{n-1}) = (\varphi(\xi_0), \varphi(\xi_1), ..., \varphi(\xi_{n-1}))$.
La restriction de $W_n(\varphi)$ à $W_n(K)$ est donc l'identité sur $W_n(K)$. On a donc :

$$\wp(W_n(\varphi)(\xi)) = F(W_n(\varphi)(\xi)) - W_n(\varphi)(\xi) = W_n(\varphi)F(\xi) - W_n(\varphi)(\xi).$$

Donc

$$\wp(W_n(\varphi)(\xi)) = W_n(\varphi)(F(\xi) - \xi) = W_n(\varphi)(x) = x$$

car x est un vecteur dans $W_n(K)$. Ainsi comme le noyau de $\wp$ sur $W_n(K)$ est $W_n(\mathbb{F}_p)$, on obtient que $W_n(\varphi)(\xi)$ appartient à $W_n(K(\wp^{-1}(x)))$ et donc l'application φ fixe globalement $K(\wp^{-1}(x))$ ce qui prouve que l'extension est normale. Elle est donc séparable sur K et donc galoisienne.

Etudions maintenant son groupe de Galois.
Il existe un vecteur ξ dans $W_n(K^{alg})$ tel que $\wp(\xi) = x$.
En posant $\xi = (\xi_0, \xi_1, ..., \xi_{n-1})$, on a $x_0 = \varphi(\xi_0)$.

Soit G_1 le groupe de Galois : $G_1 = \mathrm{Gal}(K(\wp^{-1}(x_0))/K) = \mathrm{Gal}(K(\xi_0))/K)$.
Comme G_1 agit sur les racines du polynôme $\wp(X) - x_0 = X^p - X - x_0$ alors nous obtenons pour tout $\sigma \in G_1$: $\sigma(\xi_0) - \xi_0 \in W_1(\mathbb{F}_p)$ avec $W_1(\mathbb{F}_p) = \mathbb{F}_p$.
On définit l'application suivante :

$$\begin{array}{rccc} \varphi_1 : & G_1 & \to & W_1(\mathbb{F}_p) \\ & \sigma & \mapsto & \sigma(\xi_0) - \xi_0 \end{array}$$

On peut vérifier que φ_1 est un homomorphisme de groupes injectif. De la même façon, on définit pour tout n, l'application suivante :

$$\begin{array}{rccc} \varphi_n : & G_n & \to & W_n(\mathbb{F}_p) \\ & \sigma & \mapsto & \sigma(\xi) - \xi \end{array}$$

On peut également vérifier que pour tout n, φ_n est un homomorphisme de groupes injectif. D'où le diagramme suivant :

$$\begin{array}{ccc} G_n & \xrightarrow{\varphi_n} & W_n(\mathbb{F}_p) \\ \downarrow{\scriptstyle r_n} & & \downarrow{\scriptstyle T^{n-1}} \\ G_1 & \xrightarrow{\varphi_1} & W_1(\mathbb{F}_p) \end{array}$$

où r_n désigne l'application de restriction de G_n sur G_1 et T^{n-1} la troncation de $W_n(\mathbb{F}_p)$ dans $\mathbb{F}_p$ et qui au vecteur $x = (x_0, x_1, ..., x_{n-1})$ associe x_0.

Ce diagramme est commutatif car :

$$T^{-1}n \circ \varphi_n(\sigma) = T^{n-1}(\sigma(\xi) - \xi) = T^{n-1}(\sigma(\xi_0) - \xi_0, *, ...) = \sigma(\xi_0) - \xi_0$$

et

$$\varphi_1 \circ r_n(\sigma) = \sigma(\xi_0) - \xi_0.$$

On obtient alors deux cas :

• Si x_0 n'appartient pas à $\wp(K)$, c'est à dire si l'extension $K(\xi_0)/K$ est de degré p, alors G_1 agit transitivement sur les racines du polynôme $\wp(X) - x_0$ et donc on a $\varphi_1(G_1) = W_1(\mathbb{F}_p) = \mathbb{F}_p$. Par commutativité du diagramme précédent, le monomorphisme de groupes φ_n est surjectif donc c'est un isomorphisme. On a donc : $G_n \simeq W_n(\mathbb{F}_p)$.

• Si x_0 appartient à $\wp(K)$, alors $G_1 = \{Id\}$ et l'homomorphisme φ_1 est trivial. Le monomorphisme φ_n ne peut donc pas être surjectif et G_n est donc un sous-groupe strict du groupe cyclique $\mathbb{Z}/p^n\mathbb{Z}$.

3. Soit L/K une extension cyclique de degré p^n. Notons G_n son groupe de Galois. On veut montrer que :

$$[\wp(W_n(L)) \cap W_n(K) : \wp(W_n(K))] = p^n.$$

Prenons la suite exacte :

$$0 \to W_n(\mathbb{F}_p) \hookrightarrow W_n(L) \xrightarrow{\wp} \wp(W_n(L)) \to 0.$$

Par le théorème 90 de Hilbert (th. 4.1.1), la suite exacte de cohomologie est :

$$0 \to W_n(\mathbb{F}_p) \hookrightarrow W_n(K) \xrightarrow{\wp} \wp(W_n(L)) \cap W_n(K) \xrightarrow{\varphi} H^1(G, W_n(\mathbb{F}_p)) \to 0.$$

où φ envoie x sur $\{\sigma \mapsto \sigma(\xi) - \xi\}$ et où ξ est un vecteur de $W_n(L)$ tel que $\wp(\xi) = x$.

Comme le groupe G agit trivialement sur $W_n(\mathbb{F}_p)$, on a l'égalité :

$$H^1(G, W_n(\mathbb{F}_p)) = \mathrm{Hom}(G, W_n(\mathbb{F}_p)).$$

or les groupes G et $W_n(\mathbb{F}_p)$ sont tous les deux cycliques de degré p^n donc $H^1(G, W_n(\mathbb{F}_p))$ est également cyclique.

Le quotient $(\wp(W_n(L)) \cap W_n(K))/\wp(W_n(K))$ est donc cyclique d'ordre p^n et son dual est isomorphe à $\mathrm{Hom}(\wp(W_n(L)) \cap W_n(K)/\wp(W_n(K)), W_n(\mathbb{F}_p))$.

Soit x un vecteur appartenant à $\wp(W_n(L)) \cap W_n(K)/\wp(W_n(K)), W_n(\mathbb{F}_p)$ tel que $x + \wp(W_n(K))$ engendre ce quotient. Nécessairement $x_0 \notin \wp(K)$.
On veut maintenant montrer que $L = K(\wp^{-1}(x))$. Comme chaque racine ξ de $\wp(\xi) = x$ est dans l'anneau $W_n(L)$ alors $K(\wp^{-1}(x)) \subset L$.
Pour montrer l'autre inclusion, prenons l'accouplement suivant :

$$\wp(W_n(L)) \cap W_n(K)/\wp(W_n(K)) \times G \longrightarrow W_n(\mathbb{F}_p)$$

donné par $(x + \wp(W_n(K)), \sigma) \mapsto \sigma(\xi) - \xi$ avec $\xi \in W_n(L)$ tel que $\wp(\xi) = x$.

Par le théorème de dualité, comme les noyaux sont triviaux et comme le groupe G est fini, on a un isomorphisme de groupes δ :

$$\begin{array}{rccc} \delta : & G & \xrightarrow{\sim} & \mathrm{Hom}(\wp(W_n(L)) \cap W_n(K)/\wp(W_n(K)), W_n(\mathbb{F}_p)) \\ & \sigma & \mapsto & (x + \wp(W_n(K)) \mapsto \sigma(\xi) - \xi). \end{array}$$

Si σ est un élément de G tel que sa restriction à $K(\wp^{-1}(x))$ soit l'identité alors $\delta(\sigma) = id$ car δ est un isomorphisme. Donc $\mathrm{Gal}(L/K(\wp^{-1}(x)))$ est réduit à l'identité, c'est à dire $L = K(\wp^{-1}(x))$. □

4.1.4 Nature de l'extension L/K en fonction de a.

Cette proposition découle de la proposition 2.3.4 de la section 2.3.2. Soit K un corps local de caractéristique $p > 0$ et de corps résiduel k parfait.

Corollaire 4.1.3 *:*
Soit L le corps de décomposition du polynôme $X^p - X - a = 0$ avec $a \in W_n(K)$. Si les n composantes du vecteur de Witt $a = (a_0, ..., a_{n-1})$ sont dans l'anneau de valuation $\mathcal{O}_K$ alors l'extension L/K est non ramifiée.

Démonstration :
Soit $\alpha = (\alpha_0, \alpha_1, ..., \alpha_{n-1})$ un vecteur de Witt tel que $\wp(\alpha) = a$. Pour tout $i = 1, ..., n$, notons $K_i = K(\alpha_0, \alpha_1, ..., \alpha_{i-1})$. Par itération, chaque extension K_i/K_{i-1} est cyclique de degré p et est donnée par une équation $P_i = X^p - X$ où P_i désigne un polynôme en $\alpha_0, \alpha_1, ..., \alpha_{i-2}, a_0, a_1, ..., a_{i-2}$.
Grâce à la proposition 2.3.4, les extensions K_i/K_{i-1} sont toutes non-ramifiées et donc l'extension L/K est aussi non-ramifiée. □

4.2 Lorsque le corps résiduel est algébriquement clos.

Nous nous plaçons maintenant sur le corps local $K = \mathbb{F}_p^{alg}((t))$. Nous allons introduire dans un premier temps un sous-module $\mathcal{B}_n$ de $W_n(K)$. Ce sous-module nous donnera ensuite une somme exacte qui sera déterminante dans la construction d'une bijection entre un certain ensemble $\mathcal{A}_n$ de vecteurs de Witt et $\mathcal{X}_n$ formé des couples (L, σ) où L est une extension totalement ramifiée de degré p^n de K et σ un générateur du groupe de Galois de L/K.

4.2.1 Congruence modulo $\wp(W_n(K))$.

Dans ce paragraphe, nous donnons une congruence des vecteurs de Witt de $W_n(k)$ modulo $\wp(W_n(K))$. Le quotient $W_n(K)/\wp(W_n(K))$ nous sera très utile dans la description d'une bijection entre certains vecteurs de Witt de longueur n et les extensions cycliques totalement ramifiées de degré p^n.

Proposition 4.2.1 *:*
Tout vecteur de Witt $x \in W_n(K)$ est congru modulo $\wp(W_n(K))$ à un vecteur $(y_0, y_1, ..., y_{n-1})$ où pour tout $\iota = 0, ..., n-1$, la composante y_ι est un polynôme en t^{-1} à coefficients dans k sans terme constant.

Démonstration :
Par la proposition 3.3.8, il suffit de montrer que tout vecteur de Witt peut s'écrire comme somme de deux vecteurs $(y_0, ..., y_{n-1})$ et $(z_0, ..., z_{n-1})$, où pour chaque $\iota = 0, 1, ..., n-1$, $y_\iota \in t^{-1}k[t^{-1}]$ et $z_\iota \in \mathcal{O}_K$. On va prouver ceci par récurrence sur n.
Si $n = 1$, l'anneau des vecteurs de Witt sur K de longueur 1 peut s'identifier à K, donc la propriété est vérifiée.

Supposons maintenant que la propriété est vérifiée jusqu'au rang $n-1$.
Soit $x \in W_n(K)$. Nous recherchons deux vecteurs de Witt y et z dans $W_n(K)$

tels que $x = y + z$ et satisfaisant aux conditions $y_\iota \in t^{-1}k[t^{-1}]$ pour tout $0 \leq \iota \leq n-1$ et $z \in W_n(\mathcal{O}_K)$.
Soient $x \in W_n(K)$ et x' sa troncation dans $W_{n-1}(K)$. Soient y' et z' deux vecteurs de Witt de longueur $n-1$ tels que $x' = y' + z'$. Supposons que pour tout $0 \leq \iota \leq n-2$, $y'_\iota \in t^{-1}k[t^{-1}]$ et $z' \in W_{n-1}(k[\![t]\!])$.
Il existe un polynôme $\Sigma_{n-1} \in \mathbb{Z}[y_0, y_1, ..., y_{n-2}, z_0, z_1, ..., z_{n-2}]$ tel que $(y' + z')_{n-1} = y'_{n-1} + z'_{n-1} + \Sigma_{n-1}$. Alors $x_{n-1} - \Sigma_{n-1}$ peut être décomposé sous la forme $x_{n-1} - \Sigma_{n-1} = y_{n-1} + z_{n-1}$ avec y_{n-1} un polynôme en $t^{-1}k[t^{-1}]$ et z_{n-1} une série formelle de $k[\![t]\!]$. On vérifie par le lemme 3.3.7 que l'on obtient bien $y + z = x$. □

4.2.2 Le $W_n(k)$-sous-module $\mathcal{B}_n$.

Notons $\mathbb{N}_p$ l'ensemble des entiers positifs premiers à p et pour $x \in K$, on note par $\{x\}$ le vecteur de Witt de longueur n donné par $(x, 0, ..., 0)$. On va définir un sous-module $\mathcal{B}_n$ dans $W_n(K)$ et une filtration sur ce sous-module.

Définition 4.2.2 *:*
Soit $\mathcal{B}_n$ le $W_n(k)$-module engendré par les vecteurs $\{t^{-\iota}\}$ avec $\iota \in \mathbb{N}_p$.

Les éléments de $\mathcal{B}_n$ sont les vecteurs de $W_n(K)$ de la forme :

$$a = \sum_{\iota \in \mathbb{N}_p} a_\iota \{t^{-\iota}\}$$

avec $a_\iota \in W_n(k)$ et $a_\iota = 0$ pour ι suffisamment grand. Le lemme suivant nous donne l'unicité de l'écriture de $a \in \mathcal{B}_n$ comme somme : $\sum_{\iota \in \mathbb{N}_p} a_\iota \{t^{-\iota}\}$.

Lemme 4.2.3 *:*
Pour tout entier ι premier à p, les éléments $\{t^{-\iota}\}$ sont linéairement indépendants sur $W_n(k)$.

Démonstration :
Notons par $(a_{\iota,0}, ..., a_{\iota,n-1})$ les composantes du vecteur $a_\iota \in W_n(k)$. Donc par le lemme 3.1.5, on a :

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

Donc chaque composante de $a_\iota\{t^{-\iota}\}$ est un monôme en $t^{-\iota p^h}$ ayant pour coefficients $a_{\iota,h}$ avec $0 \leq h \leq n-1$ et $\iota \in \mathbb{N}_p$. Ainsi par le lemme 3.1.3 :

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

C'est à dire, la $h^{\text{ème}}$ composante de $\sum_{\iota\in\mathbb{N}_p} a_\iota\{t^{-\iota}\}$ est un polynôme de la forme $\sum_{\iota\in\mathbb{N}_p} a_{\iota,h}t^{-\iota p^h} + \Sigma_h$ où Σ_h est un polynôme homogène en $a_{\iota,h'}t^{-\iota p^{h'}}$ avec $h' < h$.
Donc les polynômes Σ_h sont sans terme constant. Par récurence sur le rang des composantes, si $\sum_{\iota\in\mathbb{N}_p} a_\iota\{t^{-\iota}\} = 0$ on peut montrer que chaque polynôme Σ_h est nul ainsi que chaque coefficient $a_{\iota,h}$. □

L'application de troncation T envoie $\mathcal{B}_n$ sur $\mathcal{B}_{n-1}$. De plus $T(\mathcal{B}_n) = \mathcal{B}_{n-1}$.

4.2.3 La somme directe $W_n(K) = \wp(W_n(K)) \oplus \mathcal{B}_n$.

Le résultat principal de ce paragraphe est la somme directe de groupes abéliens : $W_n(K) = \wp(W_n(K)) \oplus \mathcal{B}_n$. Ce résultat nous sera très utile dans la suite surtout afin de construire une action de $\mathcal{G}_0(k)$ sur le sous-module $\mathcal{B}_n$. On prouve dans un premier temps quelques lemmes :

Lemme 4.2.4 *:*
Soit $x \in K \setminus k$ et notons $x = \sum_{\iota\geq 1}\alpha_\iota t^\iota$. Soit $\nu(x)$ le plus petit entier tel qu'il existe $\iota \geq 1$ avec $v_p(\iota) = \nu(x)$ et $\alpha_\iota \neq 0$. Alors on a $\nu(\wp(x)) = \nu(x)$.

Démonstration :
Pour tout x, on appelle $I(x)$ l'ensemble $\{\iota \in \mathbb{Z}, \alpha_\iota \neq 0\}$.
Alors $\nu(x) = \min\{v_p(\iota)/\iota \in I(x)\}$.
On obtient $x^p = \sum_{\iota\geq 1}\alpha_\iota^p t^{-\iota p}$ d'où $I(x^p) = pI(x)$ et $I(x^p - x) \subset pI(x) \cup I(x)$.
Par définition $v_p(\iota) \geq \nu(x)$ pout tout $\iota \in I(x)$ donc $v_p(\iota) \geq \nu(x)$ pour tout $\iota \in pI(x)$.
De plus $v_p(\iota) \geq \nu(x)$ pour tout $\iota \in pI(x) \cup I(x)$.
Donc $\nu(x^p - x) \geq \nu(x)$.

Réciproquement, soit ι_0 un entier tel que $v_p(\iota_0) = \nu(x)$.
On obtient $\iota_0 \in I(x) \setminus pI(x)$ et donc $\iota_0 \in I(x^p - x)$.
Ainsi obtenons-nous $\nu(x^p - x) \leq v_p(\iota_0) = \nu(x)$ □

Lemme 4.2.5 *:*
Si $x \in K$ et $m \in \mathbb{N}^*$ alors il existe $y \in K$ et $\alpha_\iota \in k$ pour tout $\iota \in \mathbb{N}_p$ tel que $\alpha_\iota = 0$ pour $\iota >> 0$ et $x = \sum_{\iota\in\mathbb{N}_p}\alpha_\iota t^{-\iota p^{m-1}} + y^p - y$.

Démonstration :
Par récurrence sur n.
Si $m = 1$, soit $x = \sum_{\iota \in \mathbb{N}_p} \alpha_\iota t^{-\iota}$.
En appliquant la proposition 4.2.1 on obtient $x = x' + y^p - y$ où y est un élément de K et x' un polynôme en t^{-1} sans terme constant c'est à dire

$$x' = \sum_{\iota \geq 1}^{\iota_0} \alpha'_\iota t^{-\iota}.$$

Il suffit donc de montrer que chaque terme $\alpha_\iota t^{-\iota}$ appartient à $\mathcal{B}_1 + \wp K$. On va procéder par récurrence sur $\iota \in \mathbb{N}$. Considérons deux cas :
Si $\text{pgcd}(\iota, p) = 1$, alors $\sum \alpha_\iota t^{-\iota} \in \mathcal{B}_1$.
Si $\text{pgcd}(\iota, p) \neq 1$, donc $\iota = \iota' p$ alors $\alpha'_\iota t^{-\iota} = \alpha'_\iota t^{-\iota' p}$.
Comme k est un corps algébriquement clos, alors on a :

$$\alpha'_\iota t^{-\iota' p} = \alpha''^p_\iota t^{-\iota' p} = (\alpha''_\iota t^{-\iota'})^p - \alpha''_\iota t^{-\iota'} + \alpha''_\iota t^{-\iota'}$$

et donc $(\alpha''_\iota t^{-\iota'})^p - \alpha''_\iota t^{-\iota'} \in \wp K$ et $\alpha''_\iota t^{-\iota'} \in \mathcal{B}_1 + \wp K$ par hypothèse de récurrence.

Maintenant, si on a $x = \sum_{\iota \in \mathbb{N}_p} (-\alpha'_\iota) t^{-\iota p^{m-2}} + y^p - y$ avec $y \in K$.
Posons $y = y' + \sum_{\iota \in \mathbb{N}_p} \alpha'_\iota t^{-\iota p^{m-2}}$ pour avoir $y^p = y'^p + \sum_{\iota \in \mathbb{N}_p} \alpha'^p_\iota t^{-\iota p^{m-1}}$. Donc

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

Ainsi x satisfait aux conditions. □

Proposition 4.2.6 *:*
On obtient la somme directe de groupes abéliens :

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

Démonstration :
1) Nous voulons que pour tout n, $\mathcal{B}_n \cap \wp(W_n(K)) = \{0\}$. Nous allons montrer ce résultat par récurrence sur n.

Si $n = 1$, alors nous devons montrer que $\wp(K) \cap \mathcal{B}_1 = \{0\}$.

Nous utilisons pour cela la $7^{\text{ème}}$ propriété de la proposition 4.2 [21]. Si $x \in \mathcal{B}_1$ et $x \neq 0$ alors sa valuation t-adique est strictement négative première à p et si $x \in \wp(K)$ alors sa valuation t-adique est soit positive soit négative mais dans ce dernier cas, sa valuation est alors un multiple de p.
Donc $\wp(W_1(K)) \cap \mathcal{B}_1 = \{0\}$.

Maintenant, nous devons prouver que pour tout n, $\wp(W_n(K)) \cap \mathcal{B}_n = \{0\}$.
Soit $a = \sum_{\iota \in \mathbb{N}_p} a_\iota \{t^{-\iota}\} \in \mathcal{B}_n \cap \wp(W_n(K))$.
Donc $a = \wp(x_0, ..., x_{n-2}, x_{n-1})$ avec $x_\iota \in K$.
Supposons que $(x_0, ..., x_{n-1}) \neq 0$. Notons par a' (resp a'_ι, resp $\{t^{-\iota}\}_{n-1}$) la troncation dans $W_{n-1}(K)$ du vecteur de Witt a (resp a_ι, resp $\{t^{-\iota}\}$).
Par hypothèse de récurrence, on sait que si

$$a' = \sum_{i \in \mathbb{N}_p} a'_\iota \{t^{-\iota}\}_{n-1} = \wp(x_0, ..., x_{n-2}) = 0$$

alors chaque $a'_\iota = 0$ par le lemme 4.2.3. Donc on obtient $a_\iota = (0, ..., 0, a_{\iota,n-1})$ avec $a_{\iota,n-1} \in k$ et $x_\iota \in \mathbb{F}_p$ pour $0 \leq \iota \leq n-2$. Ainsi :

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

Donc $\sum_{\iota \in \mathbb{N}_p} a_{\iota,n-1} t^{-\iota p^{n-1}} = x_{n-1}^p - x_{n-1} + \Sigma_{n-1}$ où Σ_{n-1} est, par le lemme 3.1.3, un polynôme homogène en $x_0, ..., x_{n-2}$.

Comme $x_\iota \in \mathbb{F}_p$ pour $0 \leq \iota \leq n-2$ alors $v_K(x_\iota) = 0$ et $\Sigma_{n-1} \in \mathbb{F}_p$. Donc il existe Σ'_{n-1} tel que $\Sigma_{n-1} = \Sigma'^p_{n-1} - \Sigma'_{n-1}$. Changeons x_{n-1} par $x'_{n-1} + \Sigma'_{n-1}$. Nous avons :

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

Supposons qu'il existe $\iota_0 \in \mathbb{N}_p$ tel que $a_{\iota_0,n-1} \neq 0$, alors

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

D'un autre coté, par le lemme 4.2.4, on obtient :

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

Donc $\nu(x'_{n-1}) = n-1$, d'où $v_K(x'_{n-1})$ est un multiple de p^{n-1}.
De plus $v_K(x'^p_{n-1} - x'_{n-1}) = pv_K(x'_{n-1})$ car la valuation de x'_{n-1} est strictement négative.

D'où $v_K(\sum_{\iota \in \mathbb{N}_p} a_{\iota_0,n-1} t^{-\iota_0 p^{n-1}})$ est un multiple de p^n, ce n'est donc pas de la forme $\iota_0 p^{n-1}$ avec $\iota_0 \in \mathbb{N}_p$.
Ainsi $x = 0$ et obtenons-nous le résultat $\mathcal{B}_n \cap \wp(W_n(K)) = \{0\}$ pour tout n.

2) Nous devons en outre prouver que pour tout n, $W_n(K) = \wp(W_n(K)) + \mathcal{B}_n$.
Nous allons à nouveau faire une récurrence sur n.

Si $n = 1$, nous avons déjà prouver ce résultat dans le cas $m = 1$ du lemme 4.2.5.

Soit $x \in W_n(K)$. Par hypothèse, nous savons que $T(x) \in \wp(W_{n-1}(K)) + \mathcal{B}_{n-1}$.
Comme l'application de troncation T est un homomorphisme surjectif, on peut trouver un élément $y \in W_n(K)$ et un élément $b \in \mathcal{B}_n$ tels que :

$$T(x) = \wp(T(y)) + T(b) = T(\wp(y)) + T(b) = T(\wp(y) + b).$$

Donc $x = \wp(y) + b + (0, ..., 0, \chi)$ avec $\chi \in K$.
On peut écrire grâce au lemme 4.2.5 : $\chi = \sum_{\iota \in \mathbb{N}_p} \chi_\iota t^{-\iota p^{n-1}} + z^p - z$.

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

Donc $\sum_{\iota \in \mathbb{N}_p} (0, ..., 0, \chi_\iota)\{t^{-\iota}\}$ appartient à $\mathcal{B}_n$ et $\wp(0, ..., 0, z)$ à $\wp(W_n(K))$.
Ainsi pour tout n, $W_n(K) = \wp(W_n(K)) + \mathcal{B}_n$. □

Remarque :
Si $n = 1$ alors $\mathcal{B}_1$ est l'ensemble des polynômes à coefficients dans k et dont les puissances de t sont toutes premières à p. Dans ce cas, la proposition 4.2.6 nous dit que toute série peut s'écrire comme somme de deux éléments. L'un de ces éléments appartient à $\wp(K)$ tandis que l'autre est dans $\mathcal{B}_1$.

4.2.4 L'ordre additif d'un vecteur de Witt et la fonction ρ_n.

L'exposant du groupe additif $W_n(k)$ est p^n et soit $\mathrm{ord}(a)$ l'ordre de l'élément a dans le groupe $W_n(k)$. Cet ordre divise p^n [20]. On a aussi

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

Nous appellons ρ_n l'application suivante de $\mathcal{B}_n$ dans $\mathbb{N}$:

Définition 4.2.7 *:*
Pour tout $a = \sum_{\iota \in \mathbb{N}_p} a_\iota \{t^{-\iota}\} \in \mathcal{B}_n$*, posons :*

$$\begin{array}{ll} \rho_n(a) = \max\left(\iota \frac{ord_{(a_\iota)}}{p}\right) & \text{pour tout } a_\iota \neq 0 \\ \rho_n(0) = 0. & \text{si } a = 0 \end{array}$$

Le lemme suivant montre que ρ_n définit une filtration croissante sur $\mathcal{B}_n$.

Lemme 4.2.8 *:*
Pour tout a *et* b *dans* $\mathcal{B}_n$*, on a :* $\rho_n(a+b) \leq \max\{\rho_n(a), \rho_n(b).\}$

Démonstration :
On a :

$$\begin{aligned} \rho_n(a+b) &= \max(\iota \mathrm{ord} \tfrac{(a+b)_\iota}{p}) \\ &\leq \max(\iota \tfrac{(\max(\mathrm{ord}_{(a_\iota)}, \mathrm{ord}_{(b_\iota)})}{p} \\ &\leq \max(\iota \frac{\mathrm{ord}_{(a_\iota)}}{p}, \iota \frac{\mathrm{ord}_{(b_\iota)}}{p}) \\ &\leq \max(\rho_n(a), \rho_n(b)) \end{aligned}$$

□

4.2.5 Définition de l'ensemble $\mathcal{A}_n$.

Afin de décrire des extensions totalement ramifiées, nous avons besoin de définir un sous-ensemble $\mathcal{A}_n$ de $\mathcal{B}_n$.

Définition 4.2.9 *:*
On appelle $\mathcal{A}_n$ *le sous-ensemble de* $\mathcal{B}_n$ *composé des vecteurs* $a = \sum_{\iota \in \mathbb{N}_p} a_\iota \{t^{-\iota}\}$ *ayant au minimum un élément* a_ι *inversible dans* $W_n(k)$*.*

Lemme 4.2.10 *:*
On a $\mathcal{A}_n = \mathcal{B}_n \cap W_n(K)^*$*.*

Démonstration :
Soit $a \in \mathcal{A}_n$ alors

$$a = \sum_{\iota \in \mathbb{N}_p} a_\iota \{t^{-\iota}\} = \sum_{\iota \in \mathbb{N}_p} (a_{\iota,0}, a_{\iota,1}, ..., a_{\iota,n-1})\{t^{-\iota}\}$$

tel qu'il existe a_ι inversible dans $W_n(k)$, c'est-à-dire, qu'il existe un élément $a_{\iota,0}$ non nul. Puisque les $\{t^{-\iota}\}$ sont linéairement indépendants alors la première composante $\sum_{\iota \in \mathbb{N}_p} a_{\iota,0} t^{-\iota}$ est non nul. Donc a appartient à $W_n(K)^*$.
D'où $\mathcal{A}_n \subset \mathcal{B}_n \cap W_n(K)^*$

Soit $a \in \mathcal{B}_n \cap W_n(K)^*$ alors

$$a = \sum_{\iota \in \mathbb{N}_p} a_\iota \{t^{-\iota}\} = \sum_{\iota \in \mathbb{N}_p} (a_{\iota,0}, a_{\iota,1}, ..., a_{\iota,n-1})\{t^{-\iota}\}$$

La première composante $\sum_{\iota \in \mathbb{N}_p} a_{\iota,0} t^{-\iota}$ est non nul car $a \in W_n(K)^*$. Donc il existe $a_{\iota,0}$ non nul. D'où l'existence d'un vecteur a_ι inversible.
Donc a appartient à $\mathcal{A}_n$. D'où $\mathcal{B}_n \cap W_n(K)^* \subset \mathcal{A}_n$ □

Lemme 4.2.11 *:*
Soit $a = \sum_{\iota \in \mathbb{N}_p} a_\iota \{t^{-\iota}\}$ *un élément de* $\mathcal{B}_n$.
Les assertions suivantes sont équivalentes :
(1) $a \in \mathcal{A}_n$.
(2) $\max\{ord(a_\iota)$ *tel que* $a_\iota \neq 0\} = p^n$.
(3) $a \notin \boldsymbol{p}(\mathcal{B}_n)$.

Démonstration :
(1) $\Leftrightarrow$ (2) :
Supposons que $a \in \mathcal{A}_n$ alors il existe $\iota_0 \in \mathbb{N}_p$ tel que a_{ι_0} est inversible dans $W_n(k)$. Comme un élément du groupe $W_n(k)$ a pour ordre p^n si et seulement s'il est inversible. Donc $\text{ord}(a_{\iota_0}) = p^n$ si et seulement si a_{ι_0} est inversible. Et de plus, $\max\{\text{ord } (a_\iota)$ tel que $a_\iota \neq 0\} = p^n$ est équivalent à dire que a appartient à $\mathcal{A}_n$.

(1) $\Rightarrow$ (3) :
Un vecteur de Witt est inversible si et seulement si sa première composante est inversible. Soit $b = (b_0, ..., b_1)$ un vecteur de $\mathcal{B}_n$, comme la multiplication $\mathbf{p}$ par p est égale à VF, où V est l'application "shift" et F l'application du Frobenius [20], donc $\mathbf{p}(b) = VF(b_0, ..., b_1) = (0, b_0^p, ..., b_{n-2}^p)$. Donc $\mathbf{p}(b)$ ne

peut pas être inversible.

(3) $\Rightarrow$ (2) : Si a est un vecteur tel que $\max\{\text{ord}(a_\iota) \text{ tel que } a_\iota \neq 0\} \leq p^n$ alors il existe un vecteur b tel que $a = \mathbf{p}(b)$. $\square$

4.2.6 Sauts de ramification des éléments de $\mathcal{A}_n$.

On va définir dans l'ensemble $\mathcal{A}_n$ la filtration suivante.

Définition 4.2.12 *:*
On appelle sauts de ramification d'un élément a de $\mathcal{A}_n$, les n entiers définis par $\rho_{n-j}(T^j(a))$ pour chaque $0 \leq j \leq n-1$.

Chapitre 5

Séries d'ordre p^n

Dans ce chapitre, nous explicitons une première bijection permettant de décrire les séries d'ordre p^n. Pour cela, nous allons introduire l'ensemble $\mathcal{X}_n$ formé des couples (L, σ) où L désigne une extension cyclique totalement ramifiée de K de degré p^n et σ un générateur du groupe de Galois de cette extension L/K.

Nous établirons d'abord une correspondance entre les vecteurs de Witt appartenant à $\mathcal{A}_n$ et les couples (L, σ) de $\mathcal{X}_n$. Puis, nous vérifierons que les sauts de ramification des extensions L cycliques totalement ramifiées de degré p^n de K peuvent être lus sur le vecteur $a \in \mathcal{A}_n$ correspondant à cette extension. Nous obtiendrons alors une bijection respectant les sauts de ramification entre $\mathcal{X}_n$ et $\mathcal{A}_n$.

5.1 Paramétrisation des extensions cycliques totalement ramifiées.

Soit $K = k(\!(t)\!)$, notons $\mathcal{X}_n$ l'ensemble des couples (L, σ) tel que L est une extension cyclique totalement ramifiée de degré p^n de K et σ un générateur du groupe de Galois $\mathrm{Gal}(L/K)$.
On décrit dans ce paragraphe un moyen de caractériser les extensions cycliques totalement ramifiés à partir d'un élément de $\mathcal{B}_n$. Afin d'obtenir des extensions totalement ramifiées de degré p^n, nous allons voir que l'on doit se restreindre aux éléments a appartenant à $\mathcal{A}_n$.

Grâce au théorème de K. Kanesaka et K. Sekiguchi ([12], th.5), qui permet d'obtenir l'indice de ramification de l'extension cyclique L/K où $L = K(\wp^{-1}(a))$ à partir des coefficients a_ι de l'élément $a \in \mathcal{B}_n$ nous devons nous

restreindre à l'étude des éléments de $\mathcal{A}_n$ pour obtenir des extensions totalement ramifiées de degré p^n.

Proposition 5.1.1 *:*
Soit $a = (a_0, a_1, ..., a_j, ..., a_{n-1}) \in \mathcal{B}_n$, l'extension $L = K(\wp^{-1}(a))$ de K est une extension cyclique totalement ramifiée de degré p^{n-j} où j est le plus petit entier compris entre 0 et $n-1$ tel que $a_j \neq 0$.

Démonstration :
Soit a un vecteur de Witt dans $\mathcal{B}_n$, on construit la tour d'extensions ci-dessous :

$$\begin{array}{c} L = K_n = K(\wp^{-1}(a_0, a_1, ..., a_{n-1})) = K(\wp^{-1}(a)) \\ \vdots \\ K_{n-1} = K(\wp^{-1}(a_0, a_1, ..., a_{n-2})) \\ \vdots \\ K_j = K(\wp^{-1}(a_0, a_1, ..., a_{j-1})) \\ \vdots \\ K_1 = K(\wp^{-1}(a_0)) \\ \vdots \\ K_0 = K \end{array}$$

Les extensions sont toutes totalement ramifiées car le corps résiduel k de K est algébriquement clos.

Si $a_0 = 0$ c'est à dire si $a \in \mathcal{B}_n \setminus \mathcal{A}_n$, alors $\wp^{-1}(a_0) = 0$ et l'extension K_1/K est triviale. Puis par récurrence sur les composantes du vecteur a, si $a_0 = a_1 = ... = a_{j-1} = 0$ alors les extensions $K_1, K_2, ..., K_j$ sont triviales. $\square$

Remarque :
L'extension L/K est donc de degré p^n si et seulement si $a_0 \neq 0$, c'est à dire si et seulement si $a \in \mathcal{A}_n$.

Nous rappelons de plus que par la théorie d'Artin-Schreier-Witt, si L/K est une extension cyclique de degré p^n, alors il existe un accouplement non dégénéré ([3], chap IX) :

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

où $\wp(\alpha) = a$ et $\overline{a}$ est la classe de a modulo $\wp(W_n(K))$.
Nous avions déjà croisé le quotient $(\wp(W_n(L)) \cap W_n(K))/\wp(W_n(K))$ dans la démonstration du théorème d'Artin-Schreier-Witt (th. 4.1.2).
De plus, on sait que cet accouplement met en dualité le groupe de Galois $\mathrm{Gal}(L/K)$ et $(\wp(W_n(L)) \cap W_n(K))/\wp(W_n(K))$.

Le théorème suivant donne une bijection entre l'ensemble des vecteurs de Witt appartenant à $\mathcal{A}_n$ et les couples (L, σ) de $\mathcal{X}_n$.

Théorème 5.1.2 *:*
Soit L/K une extension cyclique totalement ramifiée de degré p^n et σ un générateur du groupe de Galois de l'extension L/K. Il existe un unique élément $a \in \mathcal{A}_n$ tel que :

1. $L = K(\wp^{-1}(a))$
2. $[\overline{a}, \sigma\rangle = 1 = (1, 0, ..., 0)$ *où $\overline{a}$ est la classe de a modulo $\wp(W_n(K))$.*

Démonstration :
Prouvons dans un premier temps l'unicité d'un tel élément a.
Rappelons que $\wp(W_n(K)) \cap \mathcal{B}_n = \{0\}$ par la proposition 4.2.6. Supposons que $L = K(\wp^{-1}(a)) = K(\wp^{-1}(a'))$ et $[a, \sigma\rangle = [a', \sigma\rangle$. Par additivité à droite du symbole d'Artin, on a :

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

Comme l'accouplement est non dégénéré alors $a - a' \in \wp(W_n(K))$. Comme a et a' appartiennent à $\mathcal{B}_n$ et comme $\mathcal{B}_n \cap \wp(W_n(K)) = \{0\}$ alors nécessairement $a = a'$.

Prouvons maintenant l'existence d'un tel élément a. Par le rappel précédent, on a l'isomorphisme de groupes suivant :

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

où les groupes $\mathrm{Gal}(L/K)$ et $W_n(\mathbb{F}_p)$ sont tous les deux cycliques d'ordre p^n. Ainsi existe-t-il un homomorphisme φ qui associe à σ l'élément 1 de $W_n(\mathbb{F}_p)$. Cet homomorphisme φ correspond dans l'isomorphisme précédent à $\overline{a} \in \wp(W_n(L)) \cap W_n(K)/\wp(W_n(K))$ engendrant le groupe. Soit a un représentant de $\overline{a}$ dans $\wp(W_n(L)) \cap W_n(K)$.

Comme $a \in \wp(W_n(L))$ alors $K(\wp^{-1}(a)) \subset L$.
Réciproquement, soit H le groupe de Galois $\mathrm{Gal}(L/K(\wp^{-1}(a)))$, on veut montrer que $H = \{id\}$.

Soit $\tau \in H$, alors pour tout entier λ, on a,

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

avec $\wp(\alpha) = a$.
Ainsi α appartient à $K(p^{-1}(a))$ donc $\tau\alpha = \alpha$, et ainsi $[\overline{a}, \tau\rangle = 0$. Donc τ est trivial car il est orthogonal à tout élément de $\wp(W_n(L)) \cap W_n(K)$. □

5.2 Calcul des sauts de ramification.

Le conducteur d'Artin permet de construire un lien entre les sauts de ramification de $\mathcal{A}_n$ et les sauts de ramification des extensions L/K définies par les éléments de $\mathcal{X}_n$. Nous commençons par généraliser le conducteur sur des extensions cycliques de corps résiduel infini.

5.2.1 Définition du conducteur.

Nous définissons dans un premier temps, de manière précise, le conducteur d'une extension cyclique totalement ramifiée de corps local à corps résiduel fini. C'est la définition utilisée par K. Kanesaka et K. Sekiguchi dans leur article [12].

Définition 5.2.1 *:*
Soit k' un corps fini de caractéristique p et $K' = k'(\!(t)\!)$. Soit L'/K' une extension cyclique totalement ramifiée de degré p^n. Soit U le groupe des unités principales de K'. Le conducteur $(t)^{r(L'/K')}$ de l'extension L'/K' est l'idéal défini par :

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

où $U^{(l)} = \{u \in U/v(u-1) \geq l\} = 1 + t^l k[\![t]\!]$ est le $l^{ème}$ terme dans la filtration naturelle de U.

Soit $s(L/K)$ le plus grand saut de ramification de L/K, c'est à dire le plus grand entier tel que $\mathrm{Gal}(L/K)_{s(L/K)} \neq \{1\}$. L'entier $r(L/K)$ est égal à $\varphi(s(L/K)) + 1$ où φ est la fonction réciproque de la fonction de Herbrand ([20], chap XV, corollaire 2). Ainsi, avons-nous un lien entre le conducteur et le plus grand saut de ramification.

Nous avons la définition du conducteur dans le cas d'un corps local ayant un corps résiduel fini. Nous cherchons à généraliser ce résultat à tout corps local.

5.2.2 Descente d'extensions cycliques.

Le lemme suivant nous permet de généraliser certaines propriétés à toute extension cyclique.

Lemme 5.2.2 *:*
Toute extension cyclique L/K de degré p^n est la composée de k avec une extension cyclique L'/K' de degré p^n où $K' = k'(\!(t)\!)$ avec k' un corps fini.

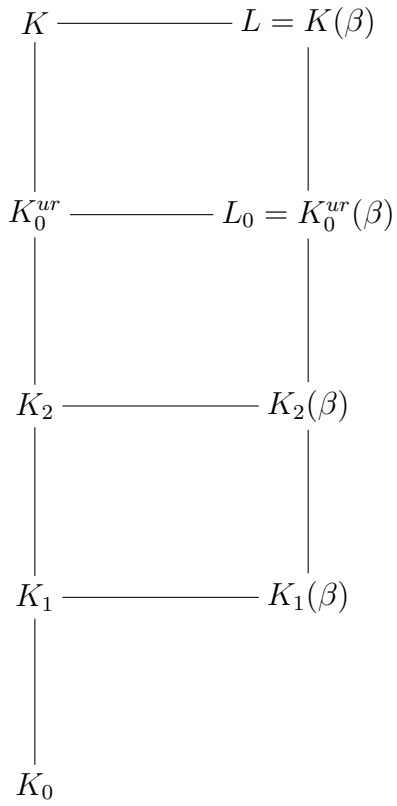
Démonstration :
Nous avons $K = k(\!(t)\!) = \mathbb{F}_p^{alg}(\!(t)\!)$ donc K est la completion de l'extension maximale non-ramifiée K_0^{ur} de $K_0 = \mathbb{F}_p(\!(t)\!)$. L'extension L/K est séparable alors par le théorème de l'élément primitif [15], nous obtenons $L = K(\alpha)$ où α est un élément algébrique de L. Soit f un polynôme irréductible en α sur K, on le note $f = \mathrm{Irr}(\alpha/K)$. Ce polynôme f est de degré p^n.
Comme K_0^{ur} est dense sur K, il existe un polynôme unitaire $g \in K[X]$ de degré p^n tel que les coefficients de g peuvent être arbitrairement proches des coefficients de f grâce au lemme de Krasner [2], il existe donc une racine β du polynôme g proche de α tel que $L = K(\alpha) = K(\beta)$.

Soit $L_0 = K_0(\beta)$. Puisque L/K est une extension galoisienne, les conjugués de β dans K_0^{ur} engendrent sur K_0^{ur} une extension finie M de L_0 incluse dans le complété de L.
On montre facilement que $M = L_0$ (l'extension résiduelle de M/L_0 est triviale et toute uniformisante de L_0 est également une uniformisante de M). Donc L_0/K_0^{ur} est une extension galoisienne.

Soit K_1 le sous-corps de K_0^{ur} engendré par les coefficients du polynôme $g(X)$. C'est une extension finie de K_0 et $K_1(\beta)/K_1$ est de degré p^n. Les extensions K/K_1 et $K_1(\beta)/K_1$ sont linéairement disjointes et $L = K.K_1(\beta)$.

Les conjugués de β dans K_0^{ur} peuvent s'écrire sous la forme de somme finie : $\sum b_{i,j}\beta^i$ avec $b_{i,j} \in K_0^{ur}$.
Soit K_2 le sous-corps de K_0^{ur} engendré sur K_1 par $b_{i,j}$. C'est une extension

finie de K_1 et $K_2(\beta)/K_2$ est une extension galoisienne.



De plus $K_2(\beta)/K_2$ et K/K_2 sont linéairement disjointes, donc la restriction à $K_2(\beta)$ des K-automorphismes de L est un isomorphisme de $\mathrm{Gal}(L/K)$ sur $\mathrm{Gal}(K_2(\beta)/K_2)$. □

5.2.3 Généralisation du conducteur aux extensions cycliques.

On rappelle la définition du conducteur d'une extension abélienne de corps locaux. Soit k' un corps de caractéristique p et $K' = k'(\!(t)\!)$. Soit L'/K' une extension cyclique totalement ramifiée de degré p^n. Soit U le groupe des unités principales de K'. Le conducteur $(t)^{r(L'/K')}$ de l'extension L'/K' est défini par :

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

avec $U_l = \{u \in U/v(u-1) \geq l\} = 1 + t^l k[\![t]\!]$ le $l^{\text{ème}}$ terme de la filtration naturelle de U.

Lemme 5.2.3 *:*
Soit K' un sous-corps fermé de K et L/K une extension finie. Supposons que K/K' est non-ramifiée. Les deux extensions L'/K' et L/K de corps locaux ont les mêmes sauts de ramification. En particulier, le conducteur de L/K est le même que celui de L'/K'.

Démonstration :
Comme K/K' est non-ramifiée, l'extension L/L' est également non-ramifiée. L'application $\sigma \mapsto \sigma_{/L'}$ est un isomorphisme entre $\mathrm{Gal}(L/K)$ et $\mathrm{Gal}(L'/K')$. Nous obtenons, en numérotation inférieure :

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

où π_L est une uniformisante de L.
Soit π une uniformisante de L', comme l'extension L/L' est non-ramifiée alors π est aussi une uniformisante L. Donc

$$\sigma \in \mathrm{Gal}(L/K)_\omega \Leftrightarrow \sigma_{/L'} \in \mathrm{Gal}(L'/K')_\omega.$$

Ainsi les sauts de ramification en numérotation inférieure sont les mêmes. Nous obtenons, grâce aux fonctions de Herbrand, les mêmes sauts en numérotation supérieure.

Par [19], proposition 9, on sait que le conducteur est égal à $(t)^{r(L/K)}$ où $r(L/K)$ est le plus grand saut de ramification en numérotation supérieure plus 1, donc le conducteur de l'extension L/K est conservé. □

5.2.4 Calcul du conducteur via l'ordre de l'élément engendrant l'extension.

On rappelle que $\mathrm{ord}(a)$ désigne l'ordre de a dans le groupe additif $W_n(k)$. Cet ordre divise p^n [20].

Lemme 5.2.4 *:*
Soit $K = k(\!(t)\!)$ et $a = \sum_{\iota \in \mathbb{N}_p} a_\iota \{t^{-\iota}\} \in \mathcal{B}_n$.
Soit $L = K(\wp^{-1}(a))$ une extension cyclique totalement ramifiée de degré p^n, alors le conducteur de cette extension est $(t)^{r(L/K)}$ où $r(L/K)$ est défini par :

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

Démonstration :
Nous utiliserons pour montrer ce résultat le lemme 5.2.3 et un article dû à K. Kanesaka et K. Sekiguchi [12]. Soit $L = K(\wp^{-1}(a))$ une extension cyclique totalement ramifiée de K de degré p^n avec $a \in \mathcal{A}_n$. Donc a peut s'écrire sous la forme :

$$a = \sum_{\iota \in \mathbb{N}_p} a_\iota \{t^{-\iota}\}$$

avec $a_\iota \in W_n(k)$.

Notons k' le sous-corps de k engendré par les composantes des vecteurs de Witt a_ι. Comme $a_\iota = 0$ sauf pour un nombre fini de $\iota \in \mathbb{N}_p$ alors k' est un corps fini. Posons $K' = k'(\!(t)\!)$ et soit $L' = K'(\wp^{-1}(a))$. Grâce au lemme 5.2.3, nous savons que les sauts de ramification de $L'K'$ sont les mêmes que ceux de l'extension L/K. Donc $r(L/K) = r(L'/K')$. Grâce au théorème de K. Kanesaka et K. Sekiguchi, ([12], p.367), nous savons que :

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

avec $l_\iota = n - s_\iota$ et s_ι défini par :

$$\begin{array}{ll} s_\iota = \max\{\nu \text{ tel que } p^\nu / a_\iota\} & \text{si } a_\iota \neq 0 \\ s_\iota = n & \text{si } a_\iota = 0. \end{array}$$

On veut maintenant montrer que $\mathrm{ord}(a_\iota) = p^{l_\iota}$.
Ceci est clair lorsque $a_\iota = 0$, on suppose donc que $a_\iota \neq 0$.
Par définition, il existe un vecteur de Witt inversible α_ι tel que $a_\iota = p^{s_\iota}\alpha_\iota$ avec α_ι dans $W_n(k) \setminus \mathbf{p}(W_n(k))$. Donc $\mathrm{ord}(\alpha_\iota) = p^n$ puisque l'anneau $W_n(k)$ est de caractéristique p^n. Donc

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

ce qui conclut la démonstration. □

5.2.5 Lecture des sauts de ramification de l'extension L/K sur les éléments de $\mathcal{A}_n$.

La proposition suivante permet de calculer de manière effective les sauts de ramification de l'extension L/K avec $L = K(\wp^{-1}(a))$ à partir des coefficients du vecteur $a \in \mathcal{A}_n$.

Lemme 5.2.5 *:*
Soit L/K une extension cyclique totalement ramifiée de degré p^n tel que $L = K(\wp^{-1}(a))$ avec a un vecteur de Witt de $W_n(K)$. Notons K_j la sous-extension de L/K tel que $K_j = K(\wp^{-1}(T^{n-j}(a)))$. Alors l'extension K_j/K est une extension de degré p^j.

Démonstration :
La relation $K_j \subset K_{j+1} \subset L$ est évidente.
Soit $L = K(\wp^{-1}(a))$ avec $a \in W_n(K)$, il suffit de montrer que pour tout entier j entre 1 et n et pour tout $a \in W_j(K)$, on a :

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

Soit $x = (x_0, ...x_{n-1})$ un élément de $W_n(K)$ tel que $\wp(x) = a$. Comme $\wp$ commute avec l'application de troncation T, nous obtenons :

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

Nous avons $K(x_0, ..., x_{j-1}) = K(x_0, ..., x_{j-2})(x_{j-1})$. Par le lemme 3.1.3, on sait que la $j^{\text{ème}}$ composante de $\wp(x_0, .., x_{j-1})$ est égale à $x_{j-1}^p - x_{j-1} + \Delta(x_0, .., x_{j-2})$ où Δ est un polynôme à coefficients entiers. Donc nous avons $\wp(x_{j-1}) = x_{j-1}^p - x_{j-1} \in K(x_0, ...x_{j-2})$. Par la théorie d'Artin-Schreier-Witt, l'extension $K(x_0, ..., x_{j-1})/K(x_0, ..., x_{j-2})$ est de degré 1 ou p.
Comme l'extension L/K est de degré p^n, alors $K(x_0, ..., x_{n-1})/K(x_0, ..., x_{n-2})$ et chaque extension $K(\wp^{-1}(T^j(a)))/K(\wp^{-1}(T^{j+1}(a)))$ est de degré p et ainsi $K(\wp^{-1}(T^j(a)))/K$ est une extension de degré p^j. □

On a la situation suivante :

$$\begin{array}{c} L = K_n = K(\wp^{-1}(a)) \\ {\scriptstyle p}\Big| \\ K_{n-1} = K(\wp^{-1}(T(a))) \\ \vdots \\ K_j = K(\wp^{-1}(T^{n-j}(a))) \\ \vdots \\ K_1 = K(\wp^{-1}(T^{n-1}(a))) = K(\wp^{-1}(a_0)) \\ {\scriptstyle p}\Big| \\ K_0 = K \end{array}$$

Proposition 5.2.6 *:*
Soit $a \in \mathcal{A}_n$ les sauts de ramification en numérotation supérieure du groupe de Galois $Gal(K(\wp^{-1}(a))/K)$ sont $\rho_{n-j}(T^j(a))$ pour $0 \leq j \leq n-1$.

Démonstration :
Soit a un élément de $\mathcal{A}_n$ et $L = K(\wp^{-1}(a))$.
Comme l'application de troncation est un homomorphisme d'anneaux qui commute avec l'addition, on a :

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

Donc on obtient :

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

Ainsi, selon le lemme 5.2.4, nous obtenons que le conducteur de chaque sous-extension K_j/K est $(t)^{r(K_j/K)}$ avec :

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

Pour chaque sous-extension K_j/K de L/K, on pose pour $\delta = 0, .., j-1$,

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

Soit $\psi_{L/K}$ le fonction de Herbrand pour l'extension L/K et $\varphi_{L/K}$ son application réciproque. Par les propriétés de $\varphi_{L/K}$ [20], on a :

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

Dans la filtration du groupe de Galois $\mathrm{Gal}(K_j/K)$ en numérotation inférieure :

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

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

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

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

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

D'où $i_{j-1}(K_j/K) = \psi_{L/K}(r(K_j/K) - 1)$.
Ainsi, en numérotation supérieure, le saut de ramification de l'extension K_j/K est $r(K_j/K) - 1$ c'est à dire $\rho_{n-j}(T^j(a))$. □

Corollaire 5.2.7 *:*
L'application de $\mathcal{X}_n$ dans $\mathcal{A}_n$ et qui associe à tout couple (L, σ) de $\mathcal{X}_n$ un vecteur $a \in \mathcal{X}_n$ tel que $[a, \sigma\rangle = 1$ et $L = K(\wp^{-1}(a))$ est une bijection respectant les sauts de ramification entre $\mathcal{X}_n$ et $\mathcal{A}_n$.

Chapitre 6

Classes de conjugaison des séries d'ordre p^n

Enfin, dans ce chapitre, nous chercherons à classer les séries d'ordre p^n à conjugaison près. Nous allons introduire une action β_n de $\mathcal{G}_0(k)$ sur le groupe $\mathcal{B}_n$ grâce à la somme directe vue dans le chapitre précédent :

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

Nous chercherons ensuite à décrire les classes de conjugaison des séries d'ordre p^n grâce à une application λ_n allant de $\mathcal{X}_n$ vers $\mathcal{Y}_n$ où $\mathcal{Y}_n$ désigne l'ensemble des classes de conjugaison des séries d'ordre p^n. Enfin, nous établirons une seconde bijection respectant également les sauts de ramification entre les orbites de $\mathcal{A}_n$ sous l'action β_n et l'ensemble $\mathcal{Y}_n$ des classes de conjugaison des séries d'ordre p^n.

6.1 Définition d'une action de $\mathcal{G}_0(k)$ sur $\mathcal{B}_n$.

Dans la suite, nous allons utiliser une action β_n de $\mathcal{G}_0(k)$ sur le groupe $\mathcal{B}_n$. Afin de définir cette action, nous devons utiliser l'isomorphisme entre $\mathcal{B}_n$ et le quotient $W_n(K)/\wp(W_n(K))$ vu à la proposition 4.2.6.

6.1.1 Définition d'une action de $\mathcal{G}_0(k)$ sur $W_n(K)$.

Soit $\gamma \in \mathcal{G}_0(k)$ et $\hat{\gamma}$ un automorphisme de K fixant k associé à γ tel que $\hat{\gamma}(f) = f \circ \gamma^{-1}$ pour tout $f \in K$. Par le foncteur de Witt W, on peut en déduire un automorphisme $W(\hat{\gamma})$ de $W(K)$ tel que :

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

On rappelle que I_n désigne l'ensemble des vecteurs de Witt dont les n premières composantes sont nulles. Cet ensemble I_n est un sous-groupe additif de $W(K)$ et un idéal de $W(K)$. Nous avons défini $W_n(K)$ comme étant le quotient $W(K)/I_n$.
Comme $W(\hat{\gamma})(I_n)$ est égal à I_n, on peut définir un automorphisme $W_n(\hat{\gamma})$ sur l'anneau des vecteurs de Witt de longueur n tel que :

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

Ainsi obtenons-nous le diagramme commutatif suivant :

$$\begin{array}{ccc} W(K) & \xrightarrow{W(\hat{\gamma})} & W(K) \\ \downarrow & & \downarrow \\ W_n(K) & \xrightarrow{W_n(\hat{\gamma})} & W_n(K) \end{array}$$

De plus $W_n(k)$ est inclus dans $W_n(K)^{W_n(\hat{\gamma})}$ donc l'automorphisme $W_n(\hat{\gamma})$ est $W_n(k)$-linéaire.

Définition 6.1.1 *:*
On définit une action $\hat{W}_n$ de $\mathcal{G}_0(k)$ sur l'anneau $W_n(K)$ tel que $\mathcal{G}_0(k)$ agit sur chaque composante de $W_n(K)$ i.e. :

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

C'est à dire $\hat{W}_n(\gamma) = W_n(\hat{\gamma})$.

Remarques :

1. Pour $n = 1$, l'action $\hat{W}_1$ est simplement $\gamma \mapsto \hat{\gamma}$.
2. L'action $\hat{W}_n$ est $W_n(k)$-linéaire.
3. L'action $\hat{W}_n$ de $\mathcal{G}_0(k)$ commute avec l'application d'isogenie $\wp$.
4. Pour tout entier $0 \leq j \leq n$, les actions $\hat{W}_n$ et $\hat{W}_{n-j}$ de $\mathcal{G}_0(k)$ respectivement sur les anneaux $W_n(K)$ et $W_{n-j}(K)$ commutent avec les applications de troncation T^j de $W_n(K)$ sur $W_{n-j}(K)$. Autrement dit, nous obtenons le diagramme commutatif suivant :

$$\begin{array}{ccc} W_n(K) & \xrightarrow{T^j} & W_{n-j}(K) \\ \downarrow{\scriptstyle \hat{W}_n} & & \downarrow{\scriptstyle \hat{W}_{n-j}} \\ W_n(K) & \xrightarrow{T^j} & W_{n-j}(K) \end{array}$$

6.1.2 Définition de l'action de $\mathcal{G}_0(k)$ sur le groupe $\mathcal{B}_n$.

L'application $\wp$ commute avec l'action $\hat{W}_n$ sur $W_n(K)$. Donc le $W_n(\mathbb{F}_p)$-module $\wp(W_n(K))$ est globalement invariant sous cette action, donc nous obtenons une action de $\mathcal{G}_0(k)$ sur le quotient $W_n(K)/\wp(W_n(K))$ comme sur le diagramme suivant. Comme le $W_n(\mathbb{F}_p)$-module $\mathcal{B}_n$ et $W_n(K)/\wp(W_n(K))$ sont naturellement isomorphique (Proposition 4.2.6), on peut trouver un $W_n(\mathbb{F}_p)$-automorphisme linéaire $\beta_n(\gamma)$ de $\mathcal{B}_n$.
Finalement $\beta_n : \mathcal{G}_0(k) \to \mathrm{Aut}_{W_n(\mathbb{F}_p)}(\mathcal{B}_n)$ est une action du groupe $\mathcal{G}_0(k)$ sur le $W_n(\mathbb{F}_p)$-module $\mathcal{B}_n$.

$$\begin{array}{ccc}
W_n(K) & \xrightarrow{W_n(\hat{\gamma})} & W_n(K) \\
\downarrow & & \downarrow \\
W_n(K)/\wp(W_n(K)) & \xrightarrow{\overline{W_n}(\hat{\gamma})} & W_n(K)/\wp(W_n(K)) \\
\wr\uparrow & & \wr\uparrow \\
\mathcal{B}_n & \xrightarrow{\beta_n(\gamma)} & \mathcal{B}_n
\end{array}$$

L'application $\overline{W_n}(\hat{\gamma})$ est un automorphisme linéaire de $W_n(K)/\wp(W_n(K))$ donc $\beta_n(\gamma)$ est également un $W_n(\mathbb{F}_p)$-linéaire automorphisme de $\mathcal{B}_n$.

Définition 6.1.2 *:*
Nous obtenons l'action suivante de $\mathcal{G}_0(k)$ sur $\mathcal{B}_n$: pour tout $\gamma \in \mathcal{G}_0(k)$ et tout $a \in \mathcal{B}_n$, on pose

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

où a' est un vecteur du sous-module $\mathcal{B}_n$ congru au vecteur $(a_0 \circ \gamma^{-1}, a_1 \circ \gamma^{-1}, ..., a_{n-1} \circ \gamma^{-1})$ modulo $\wp(W_n(K))$.

Lemme 6.1.3 *:*
L'ensemble $\mathcal{A}_n$ est globalement invariant sous l'action β_n.

Démonstration :
Soit $a \in \mathcal{A}_n$ et $\gamma \in \mathcal{G}_0(k)$, on veut montrer que $\beta_n(\gamma)(a)$ appartient à $\mathcal{A}_n$. Le lemme 4.2.11 prouve que $\mathcal{A}_n = \mathcal{B}_n \setminus \mathbf{p}(\mathcal{B}_n)$ donc nous pouvons en déduire

que si $\beta_n(\gamma)(a)$ appartient à $\mathbf{p}(\mathcal{B}_n)$ alors a est dans $\mathbf{p}(\mathcal{B}_n)$.
Soit $\beta_n(\gamma)(a) = \mathbf{p}(a')$ avec $a' \in \mathcal{B}_n$. Donc

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

donc a appartient à $\mathbf{p}(\mathcal{B}_n)$.
D'où $\mathcal{A}_n$ est globalement invariant sous l'action β_n. □

6.1.3 Lien entre l'action β_n et l'application de troncation.

On rappelle que l'application de T vérifie $T(\mathcal{B}_n) = \mathcal{B}_{n-1}$.

Proposition 6.1.4 *:*
Les actions $\beta_n(\gamma)$ et $\beta_{n-1}(\gamma)$ de $\mathcal{G}_0(k)$ respectivement sur les groupes $\mathcal{B}_n$ et $\mathcal{B}_{n-1}$ commutent avec l'application de troncation T de $W_n(K)$ sur $W_{n-1}(K)$.

Démonstration :
Puisque T envoie $\wp(W_n(K))$ dans $\wp(W_{n-1}(K))$ on peut définir un homomorphisme induit $\overline{T}$ de $W_n(K)/\wp(W_n(K))$ vers $W_{n-1}(K)/\wp(W_{n-1}(K))$. On obtient le diagramme commutatif suivant :

$$\begin{array}{ccc} \mathcal{B}_n & \longrightarrow & W_n(K)/\wp(W_n(K)) \\ \Big\downarrow{\scriptstyle T} & & \Big\downarrow{\scriptstyle \overline{T}} \\ \mathcal{B}_{n-1} & \longrightarrow & W_{n-1}(K)/\wp(W_{n-1}(K)) \end{array}$$

Grâce aux remarques situées après la définition 6.1.1 on a

$$T \circ W_n(\hat{\gamma}) = W_{n-1}(\hat{\gamma}) \circ T$$

d'où $\overline{T} \circ \overline{W_n}(\hat{\gamma}) = \overline{W_{n-1}}(\hat{\gamma}) \circ \overline{T}$, et par identification de $\mathcal{B}_n$ et $\mathcal{B}_{n-1}$ avec respectivement $W_n(K)/\wp(W_n(K))$ et $W_{n-1}(K)/\wp(W_{n-1}(K))$, l'application $T \circ \beta_n(\gamma)$ correspond à $\overline{T} \circ \overline{W_n}(\hat{\gamma})$ et l'application $\beta_{n-1}(\gamma) \circ T$ correspond à $\overline{W_{n-1}}(\hat{\gamma}) \circ \overline{T}$.
Donc $T \circ \beta_n(\gamma) = \beta_{n-1}(\gamma) \circ T$. □

6.2 Description des classes de conjugaison des séries d'ordre p^n.

On rappelle que $\mathcal{X}_n$ désigne l'ensemble des couples (L, σ) où L/K est une extension cyclique totalement ramifiée de degré p^n et σ un générateur du

groupe de Galois de l'extension L/K. On désigne aussi par $\mathcal{Y}_n$ l'ensemble des classes de conjugaison dans $\mathcal{G}_0(k)$ des séries de $\mathcal{G}_0(k)$ d'ordre p^n. Pour tout $\sigma \in \mathcal{G}_0(k)$, on désigne par $[\sigma]$ la classe de conjugaison de σ dans le groupe $\mathcal{G}_0(k)$.

6.2.1 Rappel de la filtration sur $\mathcal{G}_0(k)$.

Par identification de $\mathcal{G}_0(k)$ avec le groupe des automorphismes continus $\mathrm{Autcont}_k(K)$, nous définissons une filtration de $\mathcal{G}_0(k)$ correspondante à la ramification de la filtration de $\mathrm{Autcont}_k(K)$ en numérotation inférieure ([20], p.69). On rappelle que si σ est un automorphisme de K fixant k, on pose

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

où π est une uniformisante de K, par exemple t. La fonction i est centrale, i.e. elle ne dépend pas du choix de l'uniformisante.

La fonction i est de plus une fonction d'ordre de groupe filtré sur $\mathrm{Autcont}_k(K)$ que l'on appellera filtration de ramification en numérotation inférieure. Ainsi on peut définir sur $\mathcal{G}_0(k)$ la filtration suivante :

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

Pour tout j, l'ensemble $\mathcal{G}_j(k)$ est un groupe de séries appartenant à $\mathcal{G}_0(k)$ dont le nombre de ramification est supérieur ou égal à j. On obtient les isomorphismes : $\mathcal{G}_0(k)/\mathcal{G}_1(k) \simeq k^*$ et pour tout $j \geq 1$, $\mathcal{G}_j(k)/\mathcal{G}_{j+1}(k) \simeq k$.

6.2.2 Définition de l'application λ_n.

Nous allons définir, dans ce paragraphe, une application entre $\mathcal{X}_n$ et $\mathcal{Y}_n$.

Définition 6.2.1 *:*
Définissons l'application $\lambda_n : \mathcal{X}_n \to \mathcal{Y}_n$ de cette façon : si $(L, \sigma) \in \mathcal{X}_n$ on choisit une uniformisante $\pi \in L$ et nous définissons $\lambda_n(L, \sigma)$ comme classe de conjugaison de la série $\sigma(\pi) \in L = k(\!(\pi)\!)$.

Dans un premier temps, nous allons vérifier que l'application λ_n est bien définie, i.e. elle ne dépend pas du choix de l'uniformisante π.
Soient π et π' deux uniformisantes du corps L. Nous avons alors deux fonctions f et f' telles que $f(\pi) = \pi^\sigma$ et $f'(\pi') = \pi'^\sigma$. Nous pouvons donc écrire π' comme série en π, et il existe de cette manière une série φ de $\mathcal{G}_0(k)$ telle que $\pi' = \varphi(\pi)$ où $k(\!(\pi')\!) = k(\!(\pi)\!)$. Nous obtenons d'une part, $f'(\pi') = f'(\varphi(\pi))$ et

d'autre part, $f'(\pi') = \pi'^{\sigma} = \varphi(\pi)^{\sigma} = \varphi(\pi^{\sigma}) = \varphi(f(\pi))$, car les applications φ et σ commutent par continuité de σ. Donc $f' \circ \varphi = \varphi \circ f$, et ceci montre que λ_n est bien indépendant du choix de l'uniformisante.

6.2.3 Propriétés de l'application λ_n sur la ramification.

Nous voulons montrer dans ce paragraphe que l'application λ_n vérifie quelques propriétés sur les ramifications entre $\mathcal{X}_n$ et $\mathcal{Y}_n$.

Proposition 6.2.2 *:*
L'application λ_n est surjective et respecte la ramification, en d'autres termes, nous avons : $i(\sigma) = i(\lambda_n(L, \sigma))$.

Démonstration :
L'appplication λ_n est surjective. En effet, soit f un élément de $\mathcal{G}_0(k)$ d'ordre p^n et posons $G = \{h \mapsto h \circ f^{\circ i} / 1 \leq i \leq p^n\}$ le groupe des automorphismes de K d'ordre p^n et $K^G = \{h / h \mapsto h \circ f^{\circ i} = h\}$ le corps des éléments de K fixés par G. Par le théorème d'Artin ([15], th 1.8, p.264), K est une extension galoisienne de K^G d'ordre p^n et de groupe de Galois G donc c'est une extension cyclique. Par un théorème dû à P. Samuel [18], on obtient $K^G = k(\!(s)\!)$ avec $s = \prod_{i=1}^{p^n} f^{\circ i}(t) = N_G(t)$ où N_G est la norme de l'extension L/K. Donc $K^G \simeq K$ par un isomorphisme fixant tous les éléments de k et envoyant s sur t.

Soit P le polynôme irréductible de K sur $K^G = k(\!(s)\!)$ de façon à avoir $K \simeq K^G[X]/(P)$ et posons $L = K[X]/(\chi P(X))$. L'isomorphisme χ prolonge un isomorphisme $\widetilde{\chi}$ de K sur L.
Donc $\mathrm{Aut}_K(L) = \widetilde{\chi}\mathrm{Gal}(K/K^G)\widetilde{\chi}^{-1}$ d'où L/K est une extension cyclique de degré p^n. Comme χ, et chaque élément de G, fixe les éléments de k, alors l'extension L/K est totalement ramifiée.
Posons $\sigma = \widetilde{\chi}\hat{f}\widetilde{\chi}^{-1}$ alors $\lambda_n(L, \sigma) = [f]$ et donc $i(\sigma) = i(\lambda_n(L, \sigma))$. □

Pour tout entier $j \in \{0, 1, ...n\}$, la sous-extension de L/K de degré p^j est notée K_j. L'extension L/K_j est évidemment de degré p^{n-j}. L'ensemble des extensions $(K_j)_j$ forme une tour croissante dans L/K, on peut donc utiliser la filtration des groupes Galois :

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

Posons, en numérotation inférieure :

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

Sur $\mathcal{Y}_n$, on pose :

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

où $[\sigma]$ désigne la classe de conjugaisons de la série σ dans $\mathcal{G}_0(k)$.

Nous obtenons alors $i_j([\sigma]) = i(\sigma^{\circ p^j}) = i(\lambda(L, \sigma^{\circ p^j}))$ par la proposition précédente.
Soit $(L, \sigma) \in \mathcal{X}_n$ et $[\sigma]$ l'image par λ_n de (L, σ). Nous pouvons donc en déduire le corollaire suivant :

Corollaire 6.2.3 *:*
L'application surjective λ_n de $\mathcal{X}_n$ sur $\mathcal{Y}_n$ préserve également les sauts de ramification des extensions, c'est à dire pour tout entier $j \in 0, 1, ..., n-1$, on a $i_j(L, \sigma) = i_j([\sigma])$.

6.2.4 Définition des k-isomorphismes.

Dans ce paragraphe, nous donnons une caractérisation pour que deux couples (L_1, σ_1) et (L_2, σ_2) soient dans la même image par λ_n.

Définition 6.2.4 *:*
Deux couples (L_1, σ_1) et (L_2, σ_2) sont dits k-isomorphes s'il existe un isomorphisme bi-continu θ de L_1 sur L_2 tel que $\theta(K) = K$ et $\theta \circ \sigma_1 = \sigma_2 \circ \theta$.

Proposition 6.2.5 *:*
Deux couples (L_1, σ_1) et (L_2, σ_2) ont la même image par λ_n si et seulement s'ils sont k-isomorphes.

Démonstration :
Choisissons deux uniformisantes π_1 de L_1 et π_2 de L_2 telles que $L_1 = k(\!(\pi_1)\!)$ et $L_2 = k(\!(\pi_2)\!)$ ainsi $t = f_1(\pi_1) = f_2(\pi_2)$ où f_1 et f_2 sont deux séries. Comme σ_1 est une série dans π_1 et σ_2 une série dans π_2 alors il existe une série s_1 de $\mathcal{G}_0(k)$ telle que $g^{\sigma_1} = g \circ s_1$ pour tout g appartenant à L_1 et de la même manière, il existe s_2 telle que $g^{\sigma_2} = g \circ s_2$ pour tout g dans L_2.

Supposons tout d'abord que (L_1, σ_1) et (L_2, σ_2) sont k-isomorphes et prouvons qu'ils ont la même image par λ_n. Soit φ une série de $\mathcal{G}_0(k)$ telle que $\pi_1^\theta = \pi_2^\varphi$. Nous obtenons d'un coté :

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

et d'un autre coté :

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

Par hypothèse, nous avons $\theta \circ \sigma_1 = \sigma_2 \circ \theta$ donc $s_1(\pi_2^\varphi) = s_2(\pi_2)^\varphi$ et $s_1 \circ \varphi = \varphi \circ s_2$.

Supposons maintenant que (L_1, σ_1) et (L_2, σ_2) ont la même image par λ_n et prouvons qu'ils sont k-isomorphes. Notons respectivement par G_1 et G_2 les groupes de Galois de L_1/K et L_2/K. Soit π_1 (resp π_2) une uniformisante de L_1 (resp de L_2) et soit $S \in \mathcal{G}_0(k)$ une série telle que pour tout automorphisme σ_1 de G_1, la série $\sigma_2 = S^{-1} \circ \sigma_1 \circ S$ est un élément de G_2. Soit θ le k-isomorphisme de L_1 sur L_2 défini par $\pi_1^\theta = S(\pi_2)$. On montre que θ est un k-isomorphisme entre les couples (L_1, σ_1) et (L_2, σ_2), c'est à dire $\theta(K) = K$. Pour $x \in K$, il existe une unique série f_1 dans K tel que $x = f_1(\pi_1)$. Nous avons $x^\theta = f_1(\pi_1)^\theta = f_1 \circ S(\pi_2)$. Comme $x^{\sigma_1} = x$, et puisque $x \in K$, alors $f_1 \circ \sigma_1(\pi_1) = f_1(\pi_1)$ et donc $f_1 \circ \sigma_1 = f_1$. D'où :

$$\begin{aligned}(x^\theta)^{\sigma_2} &= f_1 \circ S(\pi_2)^{\sigma_2} \\ &= f_1 \circ S \circ \sigma_2(\pi_2) \\ &= f_1 \circ \sigma_1 \circ S(\pi_2) \\ &= f_1 \circ S(\pi_2) \\ &= x^\theta.\end{aligned}$$

□

6.2.5 Détermination des classes de conjugaison par les orbites de $\mathcal{A}_n$.

On termine ce chapitre en décrivant une bijection entre $\mathcal{Y}_n$ et les orbites de $\mathcal{A}_n$.

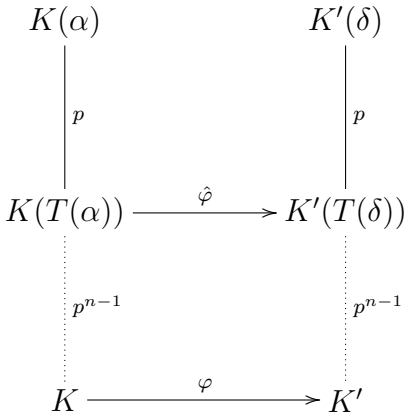
Rappel : Extension des homomorphismes.
Si φ est un homomorphisme de corps de K vers K', nous pouvons étendre celui-ci à un homomorphisme d'anneaux de $K[X]$ vers $K'[X]$. Soit β un nombre algébrique sur K, P son polynôme minimal sur K et β' une racine de $\varphi(P)$ alors il existe un unique homomorphisme $\widetilde{\varphi}$ de $K(\beta)$ sur $K'(\beta')$ tel que $\widetilde{\varphi}$ prolonge φ et $\widetilde{\varphi}(\beta) = \beta'$.

Lemme 6.2.6 *:*
Soit α un vecteur de Witt de $W_n(K)$ et supposons que $L = K(\alpha)$ est une extension de K de degré p^n. Soit $a = \wp(\alpha)$ et φ un homomorphisme de corps

de K sur un autre corps K'. Soit δ un vecteur de Witt tel que $\wp(\delta) = \varphi(a)$ alors φ peut être prolongé en un unique homomorphisme $\widetilde{\varphi}$ de L sur $L' = K'(\delta)$ tel que $\widetilde{\varphi}(\alpha) = \delta$.

Démonstration :
Par récurrence sur n.
Si $n = 1$, soit a un élément de K et α tel que $\wp(\alpha) = \alpha^p - \alpha = a$. Soit P un polynôme $X^p - X - a$ dans $K[X]$. Comme le degré de α sur K est p alors P est le polynôme minimal de α donc il est irréductible. On peut donc utiliser le précédent rappel. Soit δ une des racines du polynôme $X^p - X - \varphi(\alpha)$. Donc $\wp(\delta) = \varphi(a)$ et nous obtenons le résultat désiré.

Maintenant, supposons que l'assertion est vérifiée pour tous les vecteurs de Witt de longueur inférieure à n. Notons par $T(\alpha)$ et $T(\delta)$ la troncation de α et δ de longueur $n-1$. Il existe $\widehat{\varphi}$ tel que $\widehat{\varphi}(T(\alpha)) = T(\delta)$.



Nous avons $K(\alpha) = K(T(\alpha))(\alpha_{n-1})$ où α_{n-1} est la $n^{\text{ème}}$ composante du vecteur de Witt α. Comme, par le lemme 3.1.3, $a_{n-1} = \alpha_{n-1}^p - \alpha_{n-1} + \Delta(\alpha_0, ..., \alpha_{n-2})$ où Δ est un polynôme à coefficients entiers et puisque $\varphi(a) = \wp(\delta)$, nous obtenons $\varphi(a_{n-1}) = \delta_{n-1}^p - \delta_{n-1} + \Delta(\delta_0, ..., \delta_{n-2})$. Puisque pour chaque indice $j \leq n-2$ on a $\widehat{\varphi}(\alpha_j) = \delta_j$, on peut de nouveau utiliser le rappel précédent afin d'obtenir le résultat. □

Théorème 6.2.7 *:*
Il existe une bijection déterminée par λ_n entre $\mathcal{Y}_n$, i.e. l'ensemble des classes de conjugaison de $\mathcal{G}_0(k)$ des séries d'ordre p^n, et les orbites de $\mathcal{A}_n$ sous l'action β_n de $\mathcal{G}_0(k)$ sur $\mathcal{A}_n$.

Démonstration :
Nous allons utiliser la surjectivité de l'application λ_n de $\mathcal{X}_n$ sur $\mathcal{Y}_n$ (Proposition 6.2.2).

Nous voulons prouver que a et a' sont deux éléments dans la même orbite de $\mathcal{A}_n$ sous l'action β_n si et seulement s'ils définissent deux couples (L,σ) et (L',σ') k-isomorphes avec $L = K(\wp^{-1}(a))$, $L' = K(\wp^{-1}(a'))$ et σ et σ' deux éléments engendrant respectivement $\mathrm{Gal}(L/K)$ et $\mathrm{Gal}(L'/K)$.

Soit γ une série dans le groupe $\mathcal{G}_0(k)$ telle que $\gamma a - a'$ appartient à $\wp(W_n(K))$. Par la théorie d'Artin-Schreier-Witt, a' définit la même extension que γa. Donc nous devons prouver l'existence d'un k-isomorphisme $\widetilde{\gamma}$ entre les extensions $L = K(\wp^{-1}(a))$ et $L' = K(\wp^{-1}(\gamma a))$. Soit α et α' deux vecteurs de Witt tels que $\wp(\alpha) = a$ et $\wp(\alpha') = \gamma a$. On sait que $[\overline{a},\sigma\rangle = \sigma(\alpha) - \alpha$ et $[\overline{\gamma a},\sigma'\rangle = \sigma(\alpha') - \alpha'$.
Par le lemme 6.2.6, il existe un homomorphisme $\widetilde{\gamma}$ de L sur L' tel que $(\sigma' \circ \widetilde{\gamma})(\alpha) = \sigma'(\alpha') = \alpha' + 1$ dans l'extension $K(\alpha')$ et nous obtenons de plus $(\widetilde{\gamma} \circ \sigma)(\alpha) = \widetilde{\gamma}(\alpha + 1) = \widetilde{\gamma}(\alpha) + \widetilde{\gamma}(1) = \alpha' + 1$.
Donc $\widetilde{\gamma}$ est un k-isomorphisme entre (L,σ)et (L',σ').

Réciproquement, soit a et a' deux éléments de $\mathcal{A}_n$ tels qu'il existe un k-isomoprhisme θ entre $(K(\wp^{-1}(a)),\sigma)$ et $(K(\wp^{-1}(a')),\sigma')$ c'est à dire :

$$\theta : K(\wp^{-1}(a)) \xrightarrow{\sim} K(\wp^{-1}(a')).$$

Soit γ la série $\gamma(t)$ dans K. On veut trouver un homomorphisme $\theta = \widetilde{\gamma}$ où γ est la restriction de θ dans le corps K.
Soit σ et σ' deux éléments engendrant respectivement $\mathrm{Gal}(K(\wp^{-1}(a))/K)$ et $\mathrm{Gal}(K(\wp^{-1}(a'))/K)$ tels que $[\overline{a},\sigma\rangle = 1$ et $[\overline{a'},\sigma'\rangle = 1$. Nous recherchons une série $\gamma \in \mathcal{G}_0(k)$ telle que $a' = \beta_n(\gamma)a$, c'est à dire $a' = \gamma a$ modulo $\wp(W_n(K))$. En posant $\gamma = \theta(t)$ nous avons alors à montrer que :

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

et ceci est vrai car $\wp(\theta(\alpha)) = \gamma a$ et $a = \wp(\alpha)$
donc $\wp(\theta(\alpha)) = \theta(a)$. □

Corollaire 6.2.8 *:*
Si deux éléments de $\mathcal{A}_n$ sont dans la même orbite de $\mathcal{A}_n$ par l'action β_n alors ils ont les mêmes sauts de ramification.

Démonstration :
Soient a et a' deux éléments de $\mathcal{A}_n$ dans la même orbite sous l'action β_n.

Soient $(u_n)_n$ et $(u'_n)_n$ les suites de sauts de ramification respectivement de a et a'.
Par le corollaire 5.2.7, la bijection entre $\mathcal{A}_n$ et $\mathcal{X}_n$ préserve les sauts de ramification donc $(u_n)_n$ et $(u'_n)_n$ sont les suites de sauts de ramification de (L, σ) et (L', σ'), où (L, σ) et (L', σ') sont respectivement les éléments de $\mathcal{X}_n$ correspondant à a et a'.
Les sauts de ramification sont également conservés par l'application λ_n grâce au corollaire 6.2.3, donc $(u_n)_n$ et $(u'_n)_n$ sont les suites de sauts de ramification de $[\sigma]$ et $[\sigma']$ où $[\sigma]$ et $[\sigma']$ sont les éléments de $\mathcal{Y}_n$ correspondant respectivement à (L, σ) et (L', σ').
Comme a et a' appartiennent à la même orbite, alors par le théorème 6.2.7, ils correspondent avec la même classe de conjugaison dans $\mathcal{Y}_n$.
Donc $[\sigma] = [\sigma']$ et les suites $(u_n)_n$ et $(u'_n)_n$ sont égales. □

Remarque :
Il pourrait être interessant de trouver une démonstration plus directe, c'est à dire sans utiliser l'application λ_n.

Chapitre 7

Séries d'ordre 4

Ce dernier chapitre aborde le calcul de séries d'ordre 4. Nous donnerons d'abord une méthode permettant de calculer une série d'ordre 4 grâce à la théorie de Lubin-Tate et aux groupes formels. Puis une seconde méthode permettant également de trouver une série d'ordre 4 grâce à la théorie d'Artin-Schrier-Witt sur des vecteurs de Witt de longueur 2 sera décrite. On obtiendra une expression explicite de cette série grâce à une formule de Belardinelli.

Les résultats ci-dessous ont été obtenus en collaboration avec Mr F. Laubie et Mr A. Salinier.

7.1 Par la théorie de Lubin-Tate.

Nous commençons par redonner quelques propriétés sur la théorie de Lubin-Tate et sur les groupes formels pour faire apparaître une série d'ordre 4.

7.1.1 Groupe formel. Théorie de Lubin-Tate.

On rappelle suivant [11] qu'une série $F(X,Y)$ est un groupe formel si elle satisfait aux trois conditions suivantes :

1. $F(Y,Y) \equiv X+Y \bmod \deg 2$.
2. $F(F(X,Y),Z) = F(X,F(Y,Z))$
3. $F(X,Y) = F(Y,X)$.

Posons $K = \mathbb{F}_2(\!(t)\!)$ et $\mathcal{O}_K = \mathbb{F}_2[\![t]\!]$ son anneau de valuation et considérons sur cet anneau le polynôme de Lubin-Tate $f(X) = X^2 + tX$.

Pour toute série $f(X)$ de $K[X]$ telle que :

$$f(X) \equiv tX \text{ modulo } X^2 \quad \text{et} \quad f(X) \equiv X^2 \text{ modulo } t,$$

il existe une unique loi de groupe formel $F(X,Y)$ dans $\mathcal{O}_K[\![X,Y]\!]$ telle que f soit un endomorphisme de groupe formel F [17]. Ici par unicité, nous avons $F = \mathbb{G}_a$ où $\mathbb{G}_a$ désigne le groupe formel additif. En effet :

$$f(X) + f(Y) = X^2 + tX + Y^2 + tY = (X+Y)^2 + t(X+Y) = f(X+Y).$$

Le polynôme f est donc l'endomorphisme de $\mathbb{G}_a$ associé à $[t]$ (avec $t = f'(0)$).

$$f(X) = [t] = X^2 + tX$$

Soit K^{alg} la clôture algébrique de K et $\mathcal{O}_{K^{alg}}$ l'anneau des entiers de K^{alg}.
Choisir un générateur du module de Tate du groupe formel $\mathbb{G}_a$ revient à choisir une suite $(\pi_n)_n$ telle que $f(\pi_1) = 0$ avec $\pi_1 \neq 0$ et par récurrence pour n supérieur ou égal à 2, π_n satisfaisant à l'équation $f(\pi_n) = \pi_{n-1}$.
On obtient de cette manière $K(\pi_1) = K$, $K(\pi_2)$ une extension de K de degré 2 et $K(\pi_3)$ une extension de $K(\pi_2)$ de degré 2. Donc $K(\pi_3)$ est une extension de K de degré 4.

$$\begin{array}{c} K(\pi_3) \\ {\scriptstyle 2}\left(\left| \right. \right. \\ K(\pi_2) \\ {\scriptstyle 2}\left(\left| \right. \right. \\ K = K(\pi_1) \end{array}$$

Posons $K_t = K((\pi_n)_{n\geq 1})$ et $U(K)$ le $\mathbb{Z}_2$-module des unités de K. On a :

$$U(K) = 1 + t\mathbb{F}_2[\![t]\!] \text{ et } U^{(3)}(K) = 1 + t^3\mathbb{F}_2[\![t]\!].$$

Soit le quotient $U(K)/U^{(3)}(K) = 1 + t^3\mathbb{F}_2[\![t]\!]$ et G le groupe ayant pour éléments les classes représentées par les séries : $\{1, 1+t, 1+t^2, 1+t+t^2\}$.
Le groupe G est engendré par la série $\sigma = 1 + t$.

Posons $K_G = K(\pi_3)$, grâce à la théorie de Lubin-Tate, on sait que G est isomorphe au groupe de Galois de l'extension K_G/K.
Le groupe $G \simeq U(K)/U^{(3)}(K)$ est cyclique d'ordre 4.
On a donc $\mathrm{Gal}(K_t/K_G) \simeq 1 + t^3\mathbb{F}_2[\![t]\!]$.

7.1.2 Calcul effectif d'une série.

En suivant cette méthode, on va trouver une série d'ordre 4.
Calculons d'abord les éléments π_1, π_2 et π_3 de la suite π_n. On obtient :

$$[t](\pi_1) = 0 \Leftrightarrow t\pi_1 + \pi_1^2 = 0 \Leftrightarrow t = \pi_1,$$

puis :

$$[t](\pi_2) = \pi_1 \Leftrightarrow t\pi_2 + \pi_2^2 = t \Leftrightarrow t = \frac{\pi_2^2}{1+\pi_2}.$$

Enfin $[t](\pi_3) = \pi_2$ nous donne $t\pi_3 + \pi_3^2 = \pi_2$, c'est à dire :

$$\frac{\pi_2^2}{1+\pi_2}\pi_3 + \pi_3^2 = \pi_2.$$

Nous obtenons : $\pi_2^2\pi_3 + \pi_3^2 + \pi_2\pi_3^2 + \pi_2 + \pi_2^2 = 0$.
Puis $(1+\pi_3)\pi_2^2 + (1+\pi_3)^2\pi_2 + \pi_3^2 = 0$.
D'où $(1+\pi_3)(\pi_2+\pi_3)^2 + (1+\pi_3)^2(\pi_2+\pi_3) + \pi_3 = 0$
En divisant par $(1+\pi_3)^3$, nous obtenons l'équation :

$$\frac{(\pi_3+\pi_2)^2}{(1+\pi_3)^2} - \frac{\pi_3+\pi_2}{1+\pi_3} = \frac{\pi_3}{(1+\pi_3)^3}.$$

C'est une équation d'Artin-Schreier de la forme $y^p - y = x$, on obtient donc :

$$\frac{\pi_3+\pi_2}{1+\pi_3} = \sum_{n=0}^{+\infty} \Big(\frac{\pi_3}{(1+\pi_3)^3}\Big)^{2^n}$$

car la série $\sum_{n=0}^{+\infty} \big(\frac{\pi_3}{(1+\pi_3)^3}\big)^{2^n}$ converge. D'où :

$$\pi_3 + \pi_2 = \sum_{n=0}^{+\infty} \frac{\pi_3^{2^n}}{(1+\pi_3)^{3.2^n-1}}.$$

Or $\sigma(\pi_3) = [1+t](\pi_3) = \pi_3 + \pi_2$.
D'où la série d'ordre 4 :

$$\sigma(\pi_3) = \sum_{n=0}^{+\infty} \frac{\pi_3^{2^n}}{(1+\pi_3)^{3.2^n-1}}.$$

7.2 Par la théorie d'Artin-Schreier-Witt.

Nous donnons maintenant une seconde méthode permettant également de trouver une série d'ordre 4 grâce à la théorie d'Artin-Schreier-Witt et utilisant la filtration du groupe de Galois $G = \mathrm{Gal}(L/K)$ où L/K est une extension de degré 4.

7.2.1 Filtration.

Soit $W_2(K)$ l'ensemble des vecteurs de Witt de longueur 2 sur K. Soit $\wp = F - id$ l'application qui au vecteur (y_0, y_1) de $W_2(K)$ associe le vecteur :

$$(x_0, x_1) = (y_0^2, y_1^2) - (y_0, y_1) = (y_0^2 - y_0, y_1^2 - y_1 - y_0^2 + y_0^3).$$

Posons $M = K(y_0) \simeq \mathbb{F}_2(\!(t)\!)$ et $L = K(y_0, y_1) \simeq \mathbb{F}_2(\!(u)\!)$.

$$\begin{array}{c} L = K(y_0, y_1) \\ {\scriptstyle 2}\Big| \\ M = K(y_0) \\ {\scriptstyle 2}\Big| \\ K \end{array}$$

Soit G le groupe de Galois de l'extension L/K : $G = \{1, 1+t, 1+t^2, 1+t+t^2\}$. Posons $\sigma = 1 + t$ un générateur de G. Le groupe G est isomorphe à $W_2(\mathbb{F}_2)$ en associant par exemple à σ le vecteur $(1, 0)$, les deux éléments d'ordre 4 de l'anneau $W_2(\mathbb{F}_2)$ étant les vecteurs $(1, 0)$ et $(1, 1)$.

Soit $H =< \sigma^2 >$ le sous-groupe de G d'indice 2, on obtient une filtration décroissante de G :

$$G \supset H \supset \{1\}.$$

On a l'isomorphisme d'Artin-Schreier-Witt :

$$A = \frac{\wp(W_2(L)) \bigcap W_2(K)}{\wp(W_2(K))} \simeq \mathrm{Hom}(G, W_2(\mathbb{F}_2))$$

tel que

$$a + \wp(W_2(K)) \mapsto (\sigma \mapsto \sigma(\alpha) - \alpha).$$

• C'est bien un morphisme car :
$(\sigma\tau)(\alpha) = \sigma(\tau(\alpha) - \alpha) + \sigma(\alpha) - \alpha = \tau(\alpha) - \alpha + \sigma(\alpha) - \alpha$
Si $a = \wp(\alpha)$ et $a' = \wp(\alpha')$ alors :
$a + a' = \wp(\alpha + \alpha')$ et $\sigma(\alpha + \alpha') - (\alpha + \alpha') = \sigma(\alpha) - \alpha + \sigma(\alpha') - \alpha'$.
• C'est injectif car si on a a tel que pour tout σ, $\sigma(\alpha) = \alpha$, avec $\alpha \in W_2(K)$ et $a = \wp(\alpha)$ alors a appartient à $\wp(W_2(K))$.
• C'est surjectif car si on a $(x_0, x_1) = \wp(y_0, y_1) \notin \wp(W_2(K))$ alors $(x_0, x_1) \in A$ et $(x_0, x_1) \neq 0$. De plus $(x_0, x_1) + (x_0, x_1) = (0, x_0^2)$ est également un élément de A non nul donc A comporte au moins 4 éléments.

Considérons l'accouplement suivant :

$$A \times G \longrightarrow W_2(\mathbb{F}_2)$$

tel que $(f + \wp(W_2(K)), \sigma) \longmapsto \sigma(\xi) - \xi$ où $\wp(\xi) = f$ avec $\xi \in W_2(L)$.
Soit $m_2 : W_2(L) \to \mathbb{Z} \bigcup \{+\infty\}$ la fonction vue dans le chapitre 4 :

$$m_2(x) = m_2((x_0, x_1)) = \min\{2v_L(x_0), v_L(x_1)\}.$$

Posons $W_2^{(u)}(L) = \{x \in W_2(L)/m_2(x) \geq u\}$, les $W_2^{(u)}(L)$ forment une filtration décroissante sur $\wp(W_2(L)) \bigcap W_2(K)$. En quotientant par $\wp(W_2(K))$, on obtient une filtration décroissante sur A.
Pour tout vecteur $a = (a_0, a_1)$ de $W_2(K)$, posons :

$$w_K((a_0, a_1) + \wp(W_2(K)) = \sup\{v_K(a + \wp(b))/b \in W_2(K)\},$$

w_K est indépendant du choix du vecteur a.
Posons maintenant

$$A^{(u)} = \{(a + \wp(W_2(K)) \in A/w_K(a + \wp(W_2(K)) \geq -u\}.$$

On obtient ainsi une filtration croissante du groupe A.
Le groupe A admet trois sous-groupes : $\{0\}$, $2A$ et A.

7.2.2 Sauts de ramification de cette filtration.

On va maintenant déterminer les sauts u_0 et u_1 de la filtration en fonction de (x_0, x_1). Sur G, posons $i(\sigma) = v_K(\frac{\sigma(\pi)}{\pi} - 1)$, ceci détermine une filtration sur G donc $H = \mathrm{Hom}(G, W_2(\mathbb{F}_2))$ est également un groupe filtré, la filtration croissante sur H correspond avec la filtration croissante sur A, donc les sauts u_0 et u_1 correspondent. On a :

$$H_n = \{h \in H/\forall \sigma \in G_n, h(\sigma) = 0\} \text{ où } G_n = \{\sigma \in G/i(\sigma) \geq n\}.$$

Le groupe G, engendré par σ, admet trois sous-groupes $\{id\}$, $\langle \sigma^2 \rangle$ et $\langle \sigma \rangle$. On a $G_{i_0(\sigma)} = G = \langle \sigma \rangle$ et $G_{i_1(\sigma)} = \langle \sigma^2 \rangle$. En passant aux groupes orthogonaux la filtration $\{id\} \subset \langle \sigma^2 \rangle \subset \langle \sigma \rangle$ de G donne la filtration $H \supset \langle \sigma^2 \rangle^{\perp} \supset \{0\}$ de H.

Déterminons maintenant les sauts u_0 et u_1 en numérotation supérieure de la ramification en utilisant les conducteurs des extensions L/K et M/K [12].
Prenons $\sigma(\xi) = \xi + (1, 0)$.
Ainsi $\sigma(y_0, y_1) = (y_0, y_1) + (1, 0) = (y_0 + 1, y_1 + y_0)$.
D'où $\sigma(y_0) = y_0 + 1$ et $\sigma(y_1) = y_1 + y_0$.

Quitte à rajouter à x_0 des éléments de $\wp(K)$, on peut obtenir une valuation impaire et négative de x_0. Choisissons x dans l'anneau $W_2(\mathbb{F}_2)$ tel que $x_0 = t^{-1} = \wp(y_0)$ et $x_1 = 0$, on a donc $v_K(x_0) = -1$ puis choisissons les uniformisantes u de L telle que $y_1 = u^{-3}$ et t de M telle que $y_0 = t^{-1}$.
On a $u^2 + tu = s$ et $s^2 + ts = t$.

On obtient l'équation dans $W_2(K)$: $(x_0, x_1) = \wp(y_0, y_1)$. Soit t_1 l'entier positif tel que $2^{t_1}/b(1)$ et $2^{t_1+1} \nmid b(1)$. On obtient $t_1 = 0$ et donc $l_1 = 2 - t_1 = 2$.
Le conducteur de l'extension L/K est l'idéal $(s)^{r_{L/K}}$ où $r_{L/K} = 1 + 2h_1$ avec dans notre cas $h_1 = 1$.
En numérotation supérieure de la filtration de ramification du groupe G on obtient ainsi $G^{(3)} = \{1\}$ et $G^{(2)} \neq \{1\}$.

Dans l'extension M/K on obtient $t_1 = 1$ et donc $l_1 = 2 - t_1 = 1$. Le conducteur de l'extension M/K est alors l'idéal $(s)^{r_{M/K}}$ où $r_{M/K} = 1 + 1h_1$ avec ici $h_1 = 1$. On obtient par passage au quotient dans la filtration, le saut $(G/H)^{(2)} = \{1\}$ et $(G/H)^{(1)} \neq \{1\}$. Par le théorème de Herbrand ([20] chap IV, §3), on a : $(G/H)^{(2)} = G^{(2)}/H \bigcap G^{(2)}$.
On a donc $G^{(2)} \subset H$ et $G^{(1)} \nsubseteq H$.
Soit ψ la fonction de Herbrand attachée à l'extension L/K liant les numérotations inférieure et supérieure de la filtration de ramification de G :

$$\psi(v) = \int_0^v (G^0 : G^w)dw.$$

et φ son application réciproque. L'application ψ est continue, linéaire par morceaux et convexe.
On a : $G^w = G_{\psi(w)} = \{s \in G/i(s) \geq \psi(w)\}$.
Si $w \leq 1$ alors $\psi(v) = v$ et $G^w = G$.
Si $1 < w \leq 2$ alors $\psi(v) = 2v - 1$ et $G^w = H$.
Si $2 < w \leq 3$ alors $\psi(v) = 4v - 5$ et $G^w = \{1\}$.
On a :
Si $u \leq 1$ alors $\varphi(u) = u$.
Si $1 \leq u \leq 3$ alors $\varphi(u) = \frac{u+1}{2}$.
Si $3 \leq u \leq 7$ alors $\varphi(u) = \frac{u+5}{4}$.

On passe maintenant à une filtration en numérotation inférieure :
On note pour tout i, $g_i = \text{Card}(G_i)$.
$\frac{1}{g_0}(g_0 + g_1) = \varphi(1) + 1 = 2$ d'où $g_1 = 4$ donc $G_1 = G$.
$\frac{1}{g_0}(g_0 + g_1 + g_2) = \varphi(2) + 1 = \frac{5}{2}$ d'où $g_2 = 2$ donc $G_2 = H$.
$\frac{1}{g_0}(g_0 + g_1 + g_2 + g_3) = \varphi(3) + 1 = 3$ d'où $g_3 = 2$ donc $G_3 = H$.
$\frac{1}{g_0}(g_0 + g_1 + g_2 + g_3 + g_4) = \varphi(4) + 1 = \frac{13}{4}$ d'où $g_4 = 1$ donc $G_4 = 1$.

Ainsi obtient-on la filtration en notation inférieure $G_i = \{s \in G / i(s) \geq i\}$ et les sauts de cette filtration ; $i_0 = 1$ et $i_1 = 3$.

7.2.3 Calcul effectif d'une série.

Si $x_1 = 0$ dans l'équation $x_1 + y_1^2 - y_1 - y_0^2 + y_0^3 = 0$ puis en développant t en fonction de u, on obtient l'équation :

$$\frac{1}{u^6} + \frac{1}{u^3} + \frac{1}{t^3} + \frac{1}{t^2} = 0.$$

C'est à dire : $(1+u^3)t^3 + tu^6 + u^6 = 0$. En divisant par t^3, on a :

$$\frac{u^6}{t^3} + \frac{u^6}{t^2} + (1+u^3) = 0.$$

puis en posant $\frac{u^2}{t} = (1+u^3)^{1/3}\rho$ et en divisant par $1+u^3$, on obtient l'équation de Belardinelli ([1], p.40). Dans le cercle $|\frac{u^4}{(1+u^3)^{\frac{2}{3}}}| < \frac{3}{\sqrt[3]{4}}$, on a :

$$\rho^3 + \frac{u^4}{(1+u^3)^{2/3}}\rho + 1 = 0.$$

puis par le théorème de prolongement analytique on obtient alors :

$$\rho = \frac{1}{3}\sum_{\alpha=0}^{+\infty} \frac{\Gamma(\frac{1-\alpha}{3})}{\Gamma(\alpha+1)\Gamma(\frac{1-2\alpha}{3})}\Big(\frac{u^4}{(1+u^3)^{2/3}}\Big)^{\alpha}.$$

D'où la série :

$$\rho = \frac{1}{3}\sum_{\alpha=0}^{+\infty} \frac{(-1)^{\alpha}}{\alpha!}\Big(\frac{1-2\alpha}{3} + \alpha - 1\Big)...\Big(\frac{1-2\alpha}{3} + 1\Big)\frac{u^{4\alpha}}{(1+u^3)^{2\alpha/3}}.$$

Bibliographie

[1] G. Belardinelli, *Fonction hypergéométriques de plusieurs variables et résolution analytique des équations algébriques générales* Memor. Sci. Math., **145**, Gautiers-Villars, Paris, (1960).

[2] S. Bosch, U. Güntzer and R. Remmert, *Non-archimedean analysis*, Springer-Verlag, Berlin, (1984).

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

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

[5] R. Camina, *Subgroups of the Nottingham group*, Journal of Algebra, **196** (1997), p. 101-113.

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

[7] I. Fesenko, *On just infinite pro-p-groups and arithmetically profinite extensions of local fields.* J.reine angew. Maths **517** (1999), p.61-80

[8] I. Fesenko and S. Vostokov, *Local Fields and their Extensions*, AMS Providence, 2nd edition.

[9] B. Green et M. Matignon, *Liftings of Galois covers of smooth curves*, Compositio Mathematica **113** (1998), p.237-272.

[10] B. Green et M. Matignon, *Errata : Liftings of Galois covers of smooth curves*, Compositio Mathematica **116** (1999), p.239.

[11] K. Iwasawa : Local Class Field Theory

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

[13] B. Klopsch, *Automorphisms of the Nottingham group*, Journal of Algebra, **223** (2000), p. 37-56.

[14] B. Klopsch, *Normal subgroups in substitution groups of formal power series*, Journal of Algebra, **228** (2000), p. 91-106.

[15] S. Lang, *Algebra.* Revised Third Edition, GTM, Springer, (2002).

[16] F. Laubie, A. Movahhedi et A. Salinier, *Systèmes dynamiques non archimédiens et corps des normes*, Compositio Mathematica **132** (2002), p.57-98.

[17] J. Neukirch, *Algebraic Number Theory.*(1992)

[18] P. Samuel, *Groupes finis d'automorphismes des anneaux de séries formelles*, Bull. Sc. math., **90** (1966), p.97-101.

[19] J.P. Serre, *Sur les corps locaux à corps résiduel algébriquement clos*, Bull. Soc. Math. France, **89**, 1961, p. 105-154.

[20] J.P. Serre, *Corps locaux* , Hermann, Paris, (1962).

[21] L. Thomas, *Arithmétique des extensions d'Artin-Schreier-Witt*, Thèse de doctorat, Toulouse, (2005).

[22] L. Thomas, *Ramification groups in Artin-Schreier-Witt extensions.* Journal de théorie des Nombres de Bordeaux **17** (2005) p.689-720.