Thèse

présentée à

l'Université de Toulouse II le Mirail

pour l'obtention du

Doctorat de Mathématiques de l'Université

par

Lara Thomas

Arithmétique des extensions d'Artin-Schreier-Witt

Rapporteurs : B. Anglès, Professeur à l'Université de Caen.
Ph. Cassou-Noguès, Professeur à l'Université de Bordeaux I.

Thèse soutenue le vendredi 23 septembre 2005 devant la Commission d'Examen :

Président :	B. Anglès	Professeur à l'Université de Caen.
Directeur :	C. Maire	Professeur à l'Université de Toulouse II.
Examinateurs :	D. Benois	Professeur à l'Université de Franche-Comté.
	J.-M. Couveignes	Professeur à l'Université de Toulouse II.
	F. Hajir	Professeur-Assistant à l'Université du Massachusetts, USA.
	A. Mézard	Maître de Conférences à l'Université de Paris XI.
	M. Perret	Professeur à l'Université de Toulouse II.
	B. de Smit	Professeur à l'Université de Leiden, Pays-Bas.

Travaux de thèse co-encadrés par C. Maire et B. de Smit.

Remerciements

J'ai vécu mes trois années de thèse comme une aventure formidable, jalonnée bien sûr de passages difficiles. Ma plus belle chance a été de travailler à la fois avec Christian Maire et Bart de Smit. J'ai rencontré deux personnes qui sont pour moi bien plus que des directeurs de thèse.

Il m'est difficile de trouver les mots pour exprimer toute ma reconnaissance envers Christian. Je le remercie pour sa très grande disponibilité et pour ses encouragements qui n'ont jamais cessé. Christian guidait mes recherches mathématiques de façon juste, précise et rigoureuse, tout en m'expliquant chaque facette du métier. Il m'a initiée au monde des chercheurs et il a fait en sorte que je m'y sente bien. Je suis fière d'avoir été sa première étudiante en thèse.

Travailler avec Bart est une superbe expérience. Bart manipule les mathématiques de façon étonnante et élégante. Il porte toujours un regard imprévisible mais tellement enrichissant sur les moindres objets algébriques. Bart m'a aussi apporté un soutien très fort. A chaque fois, c'était une joie de prendre l'avion pour Leiden.

Christian et Bart m'ont tous deux prouvé qu'il est possible d'associer une vie familiale réussie à côté d'une vie professionnelle exaltante.

Je tiens à témoigner toute ma reconnaissance envers mes rapporteurs Bruno Anglès et Philippe Cassou Noguès. Ils ont écrit dans leurs rapports ce que j'avais envie qu'on me dise, cela m'a profondément touchée.

Je souhaite vivement remercier Ariane Mézard, Denis Benois et Farshid Hajir. Ils m'ont fait l'honneur d'accepter spontanément de participer à mon jury de soutenance. J'en suis très fière.

La thèse m'a permis de croiser des personnes fort sympathiques, à Toulouse et à Leiden, que je n'oublierai pas. Mon équipe de Toulouse : c'est du cent pour cent pure vie. En entrant dans les locaux, on rencontre d'abord Jean-Marc Couveignes, personne d'une rare compétence dans ce métier. Je tiens à le remercier tout particulièrement pour m'avoir introduite dans l'équipe et surtout pour m'avoir présentée à Christian.

Deux portes à gauche, c'est le bureau de Marc Perret. Marc m'a initiée à la théorie de Galois quand je fréquentais l'ENS de Lyon. On le voyait transpirer au tableau pour nous faire toucher ces groupes qui fusionnent avec des corps. C'était magique.

En face du bureau des étudiants, il y a Emmanuel Hallouin et Thierry Henocq. Ils ont été pour moi un soutien précieux, encore plus durant les dernières semaines. Je les apprécie énormément.

Au fond du couloir, on trouve du chocolat dans les tiroirs et surtout une note féminine avec les admirables Laurence et Nathalie. Elles se sont toujours montrées très disponibles et leur présence me rassurait. Elles me manquent déjà.

Avant de reprendre les escaliers pour quitter les lieux, je n'oublie pas d'aller embrasser Caroline, Claudie et la douce Sabine, elles le valent vraiment. Je croise Francis, grâce à qui mes TD de statistique étaient un vrai plaisir. Je fais également un petit coucou à Julien qui m'a souvent remotivée lors d'agréables soirées.

J'adorais aussi passer au bureau des secrétaires. Le motif était un fax, une photocopie ou une boîte de craies. Je repartais avec les sourires de Véronique et Michelle. J'y croisais également mes étudiants de Deug Mass que j'appréciais beaucoup.

Pour finir, un dernier tour à la Maison de la Recherche où Valérie Sanchou m'a toujours rassurée sur mes diverses questions administratives. Au quatrième étage, je laisse mon bureau. Dans le couloir, j'aimais discuter avec Racha, Jean-François, Majid et Abshin... pour m'envoler un moment. Il y a aussi Bertrand, notre correspondant à SLR, et Louis qui comprenait mon manque d'oxygène

parfois. La liste est longue mais je me rappellerai de chaque informaticien, de chaque statisticien et de chaque membre du séminaire de théorie des nombres du Mirail, en particulier Jacqueline Lacaze et Bin Zhang.

J'aurais besoin des mêmes mots pour décrire l'équipe de Leiden. Mais pour éviter les répétitions, je voudrais davantage insister sur l'accueil qui m'y était réservé à chacun de mes déplacements. J'ai été très flattée de pouvoir participer à des discussions mathématiques avec Hendrik Lenstra. Bas Edixhoven et Peter Stevenhagen m'ont aussi témoigné une très forte sympathie et j'étais honorée de côtoyer de si grands noms. J'ai également fait la connaissance d'autres doctorants que je considérais très vite comme ma famille hollandaise : Jeanine, Bas, Christiaan, Reinier, Willem et récemment Eleonora. J'adresse un remerciement tout particulier à Robert Carls et à Gabor Wiese.

Enfin, je tiens à remercier les secrétaires du centre international de Leiden, Maureen et Astrid, qui m'ont toujours réservé une chambre des plus confortables lors de mes multiples séjours à Leiden. Je m'y sentais chez moi et c'était tellement important.

Au début de cette histoire, il y a aussi Bruno Deschamps qui m'a fait découvrir la recherche, puis Martine Girard que j'ai rencontrée lors de mon premier séjour à Leiden. Viennent ensuite Emmanuel Riboulet et Nicolas Ros, mes deux frères aînés de l'Equipe Grimm. Je souhaite également adresser un remerciement sincère à Christophe Delaunay pour ses conseils judicieux et son soutien constant.

Mon apprentissage de la recherche n'aurait pu se faire sans les liens si précieux que j'ai pu tisser lors de nombreuses conférences internationales. Pour cela, je tiens à remercier tous les organismes qui ont pris en charge mes déplacements, parmi lesquels l'équipe Grimm, l'université de Leiden, le réseau européen GTEM, le groupe de recherche de théorie des nombres et le réseau franco-néerlandais. Je remercie également l'ENS Cachan - Ker Lann ainsi que la DGA pour leur soutien financier durant mes années de thèse.

Mes remerciements s'adressent ensuite aux auteurs de ces musiques qui m'ont accompagnée et qui rendaient mon travail plus confortable. Il y a Mickey3D, Ridan, Manu Chao, Bombes2Bal, Beautés Vulgaires, Lavilliers, Indochine... et l'accordéon de mon village. Plus généralement, je souhaiterais faire un clin d'oeil à tous les artistes sans qui mes rêves seraient ternes. J'aimerais tellement faire avec les mathématiques ce qu'ils font avec de la peinture, des mots ou des rythmes.

Plus personnellement, mes remerciements vont à Gaëtane qui m'a repêchée sur les rives de la Vilaine et a su m'encourager tout au long de mon année à Rennes avant de me laisser descendre sur Toulouse. De même, je remercie toutes ces personnes si chères qui m'ont accueillie au cours de mes voyages pendant mes années de thèse : Josée et Lise sur les rives québecoises du Saint-Laurent, Cécile et Gabor le long des multiples canaux hollandais, Léonie sur les rives de la Seine, Michelle et Michel au bord du canal du Midi, Colette depuis la source de la Garonne, Carole, Coralie, Sophie et Gersende sur le Furan stéphanois... puis, si je remonte la Loire jusqu'à mon village adoré, Monique, Pierrot et mes amis de toujours au bord du Lignon, parmi lesquels Jérôme dont la présence à ma soutenance me touche beaucoup.

Je termine le long de la rivière familiale. A ma famille, je lui écris un énorme merci. Mes cousins, petits et grands, mes oncles et tantes : leur réconfort est sans égal. Ils ont su maintenir en moi cet équilibre si vital. Mes grand-mères, qui m'ont transmis leur force de vivre. Je suis tellement fière d'être leur petite-fille. Motus qui m'attend devant la porte à Chazelles, le nez entre ses pattes... A quand la balade dans les bois ?
Mes parents, sans qui toute cette histoire n'aurait pu s'écrire : mon père mon premier supporter, ma mère qui m'a appris à ne pas baisser les bras.
Mon frère, qui comprend le mieux les galères et les joies de la thèse.

J'envoie enfin un tendre merci à mon Christophe, le plus patient de tous.

Introduction

L'objet de cette thèse est l'étude des pro-p extensions abéliennes sur un corps K de caractéristique $p > 0$, appelées extensions d'Artin-Schreier-Witt.

A l'origine, dans un papier commun de 1927 [7], Artin et Schreier décrivent les extensions cycliques de degré p sur un corps de caractéristique p afin de répondre entièrement au 17ème problème de Hilbert. Plus précisément, il s'agit de montrer qu'en caractéristique p il n'existe pas de corps algébriquement clos qui soit extension finie d'un sous-corps propre. Notons que le cas de la caractéristique 0 a déjà été traité par Artin en 1925 en terme de corps réels clos : dans [5], Artin montre que les corps réels clos sont précisément les corps de caractéristique 0 qui sont sous-extension finie de leur clôture algébrique, le degré de l'extension étant alors 2.

Soit K un corps de caractéristique $p > 0$. Le point clef de [7] est le suivant : toute extension cyclique de degré p sur K est donnée par un polynôme $X^p - X - a$ avec a dans K. C'est le théorème d'Artin-Schreier, analogue de la théorie de Kummer lorsque le degré de l'extension est égal à la caractéristique du corps de base. Par la suite, plusieurs études, dont celle menée par Albert dans [4], généralisent ce résultat à toute extension cyclique de degré p^n sur K avec $n \geq 1$, mais de façon itérative. Ce n'est qu'en 1936 que Witt [76], alors assistant à l'université de Göttingen, propose une construction directe de ces extensions en introduisant les célèbres vecteurs qui portent aujourd'hui son nom. Sa méthode est remarquable : les vecteurs de Witt forment un anneau commutatif dans lequel Witt généralise les données du théorème d'Artin-Schreier en manipulant des composantes fantômes. D'autre part, cette technique lui permet de décrire le groupe de Galois de toute extension abélienne finie d'exposant p^n sur K.

Cependant, d'après [54] il semble que l'objectif premier de l'article de Witt ne soit pas l'étude des extensions de degré p^n d'un point de vue uniquement galoisien mais plutôt la théorie locale du corps de classes sur ces extensions. Pour cela, retournons en 1927. Très vite les travaux de Hilbert puis de Takagi soulèvent la question de savoir si l'on peut définir une théorie du corps de classes sur les corps de fonctions de la même façon que cela a été fait pour les extensions abéliennes de corps de nombres. En 1927, Schmidt propose une première approche de la théorie du corps de classes sur les corps de fonctions, mais elle reste incomplète. Cette même année, Artin publie aussi une preuve de la loi de réciprocité générale basée sur le théorème de Chebotarev ([6]). Ce n'est qu'en 1936 que Hasse puis son assistant Schmid ([25] et [56]) donnent précisément la correspondance du corps de classes pour les extensions abéliennes dont le degré est égal à la caractéristique. L'article [76] de Witt approfondit cette étude en donnant une formule explicite du symbole local pour toute extension de degré p^n en caractéristique 0, exprimé en terme d'invariant d'algèbres. Puis, sans le montrer, Witt explique que cette formulation est encore valable en caractéristique p et qu'elle généralise ainsi la formule des résidus pour le cas global. Notons que la preuve de Witt utilise un résultat publié quelques mois plus tard par Teichmüller [72], étudiant en thèse de Hasse à Göttingen. Le résultat de Witt permettra ensuite à Schmid de calculer le conducteur d'Artin pour toute extension de degré p^n [57].

C'est donc tout naturellement que l'étude des extensions d'Artin-Schreier-Witt nous conduit à

la théorie de la ramification après avoir développé de façon précise la théorie de Galois infinie sur ces extensions.

Dans ce rapport, nous parlerons souvent d'extensions d'Artin-Schreier pour désigner les extensions d'exposant p sur K et d'extensions d'Artin-Schreier-Witt pour les extensions d'exposant p^n, l'étude de ces dernières nécessitant la théorie des vecteurs de Witt.

Dans la première partie, nous proposons une construction fonctorielle des vecteurs de Witt avec le souci permanent de tout montrer. Nous insisterons notamment sur les arguments topologiques afin de passer à la limite projective dans le second chapitre et donc d'écrire précisément la structure du groupe de Galois des extensions abéliennes maximales d'exposant p^n sur K, pour tout entier $n \geq 1$.

Notons $W_n(K)$ l'anneau des vecteurs de Witt de longueur n sur K et $W(K)$ celui des vecteurs infinis. L'application $\wp : x \mapsto x^p - x$ se relève en un morphisme de groupe additif $W_n(K) \to W_n(K)$ de noyau $W_n(\mathbb{F}_p) \simeq \mathbb{Z}/p^n\mathbb{Z}$ et en un morphisme de groupe additif $W(K) \to W(K)$ de noyau $W(\mathbb{F}_p) \simeq \mathbb{Z}_p$. Notons également G_{p^n} le groupe de Galois de l'extension abélienne maximale d'exposant p^n sur K. On munit les espaces $W_n(\mathbb{F}_p)$ et $W(\mathbb{F}_p)$ de la topologie discrète et de la topologie p-adique respectivement.

La première partie explique comment la théorie d'Artin-Schreier enrichie des vecteurs de Witt fournit des isomorphismes de groupes topologiques :

$$\mathfrak{as}_n : G_{p^n} \xrightarrow{\simeq} H_{p^n}$$

où H_{p^n} est le groupe d'homomorphismes continus $\mathrm{Hom}(W_n(K)/\wp(W_n(K)), W_n(\mathbb{F}_p))$. Si G_{p^∞} désigne le groupe de Galois de la pro-p extension abélienne maximale de K, le passage à la limite projective donne à nouveau un isomorphisme de groupes topologiques :

$$\mathfrak{as}_\infty : G_{p^\infty} \xrightarrow{\simeq} H_{p^\infty}$$

pour $H_{p^\infty} = \mathrm{Hom}(W(K)/\wp(W(K)), \mathbb{Z}_p)$.

Cette partie complète [73]. Elle développe en outre une étude supplémentaire sur la structure de $\mathbb{Z}_p$-module du pro-p groupe G_{p^∞}.

La seconde partie, qui regroupe les chapitres 3 et 4, est l'étude de la ramification dans les extensions d'Artin-Schreier-Witt lorsque le corps K est un corps complet pour une valuation discrète et de corps résiduel parfait : nous notons v_K la valuation de K, O_K son anneau de valuation et $\mathfrak{p}_K$ son idéal maximal. Plus précisément, pour $n = 1$, le chapitre 3 donne une correspondance bijective entre les groupes de ramification de G_p et la filtration du groupe d'homomorphismes H_p suivante :

$$\forall u \geq -1,\ H_p^{(u)} = \{\varphi \in H_p \ :\ \varphi((\mathfrak{p}_K^{-u} + \wp(K))/\wp(K)) = 0\},$$

où $\mathfrak{p}_K^{-u} = \{x \in K \ :\ v_K(x) \geq -u\}$.

La correspondance s'énonce ainsi (cf. théorème 3.3) :

Théorème 1. *Soit K un corps de caractéristique p, complet pour une valuation discrète et de corps résiduel parfait. Pour tout entier $u \geq -1$, l'isomorphisme $\mathfrak{as}_1$ induit les isomorphismes de groupes topologiques :*

i) $G_p^{(-1)} \xrightarrow{\simeq} H_p^{(-1)}$

ii) $G_p^{(0)} \xrightarrow{\simeq} H_p^{(0)}$

iii) $G_p^{(u)} \xrightarrow{\simeq} H_p^{(u-1)}$ *si* $u \geq 1$.

La preuve est directe et, pour $u = 0$, elle se généralise facilement au groupe d'inertie de toute extension abélienne maximale d'exposant p^n sur K (voir théorème 3.4) :

Proposition 1. *Pour tout entier $n \geq 1$, l'isomorphisme $\mathfrak{as}_n$ induit un isomorphisme de groupes topologiques :*

$$G_{p^n}^{(0)} \xrightarrow{\simeq} \{\varphi \in H_{p^n} \ ; \ \varphi(W_n(O_K)/\wp(W_n(O_K))) = 0\}.$$

Le théorème 1 précise ainsi un résultat de Maus ([46]) pour les extensions d'exposant p et la proposition 1 en donne une première généralisation pour le groupe d'inertie de toutes les extensions d'Artin-Schreier-Witt. Les mêmes arguments ne nous ont pas encore permis d'obtenir les groupes de ramification supérieurs pour les extensions d'exposant p^n lorsque $n \geq 2$. Pour atteindre cet objectif, nous abordons ensuite le problème avec une autre approche, celle de la théorie du corps de classe local.

Le chapitre 4 se place dans le cadre de la théorie usuelle du corps de classe local lorsque le corps résiduel de K est de plus fini. Pour toute extension abélienne maximale d'exposant p^n, il existe alors une correspondance entre la filtration des groupes de ramification et la filtration $U_K^{(u)} = 1 + \mathfrak{p}_K^u$ du groupe des unités de K, noté U_K. Généralisant la formule de Schmid [56] à toute extension de degré p^n, nous donnons une formulation explicite du symbole local sur ces extensions au moyen de vecteurs de Witt. Cette formulation est déjà évoquée dans le papier [76] de Witt mais n'est pas démontrée en caractéristique p. De plus, Witt utilisait le langage des algèbres centrales simples, le nôtre est retranscrit dans une terminologie cohomologique, comme il est plus d'usage maintenant. Nous obtenons ainsi une description explicite des groupes de ramification pour les extensions abéliennes maximales d'exposant p^n sur K en terme de groupes d'homomorphismes à valeurs dans $W_n(\mathbb{F}_p)$. Plus précisément, nous considérons dans H_{p^n} la filtration des sous-groupes $H_{p^n}^{(u)}$, pour $u \geq -1$, définis par :

$$H_{p^n}^{(u)} = \{\varphi \in H_{p^n} \ : \ \varphi(W_n^{(u)}(K) + \wp(W_n(K))/\wp(W_n(K))) = 0\}$$

avec :

$$W_n^{(u)}(K) := (\mathfrak{p}_K^{-\lfloor \frac{u}{p^{n-1}} \rfloor}, \mathfrak{p}_K^{-\lfloor \frac{u}{p^{n-2}} \rfloor}, \cdots, \mathfrak{p}_K^{-u}).$$

En conjuguant théorème d'existence et accouplement d'Artin-Schreier-Witt, la formule explicite du symbole local pour les extensions de degré p^n va nous permettre d'écrire une preuve complète et accessible du résultat suivant :

Théorème 2. *Soit K un corps de caractéristique p, complet pour une valuation discrète et de corps résiduel fini. Pour tout entier $u \geq 0$, l'isomorphisme $\mathfrak{as}_n$ induit les isomorphismes de groupes topologiques :*

$$G_{p^n}^{(u)} \xrightarrow{\simeq} H_{p^n}^{(u-1)}, \quad \textit{si } u > 0$$

et

$$G_{p^n}^{(0)} \xrightarrow{\simeq} H_{p^n}^{(0)}, \quad \textit{si } u = 0.$$

Ce sera le théorème 4.4. La preuve généralise les techniques développées dans le chapitre XIV de [60]. Au passage, on montre que chaque groupe $U_K^{(u)} K^{*p^n}/K^{*p^n}$ est l'orthogonal de $(W_n^{(u-1)}(K) + \wp(W_n(K))/\wp(W_n(K))$ pour l'accouplement d'Artin-Schreier-Witt. On retrouve ainsi un résultat de Brylinski [16] mais avec des arguments plus explicites utilisant moins d'outils techniques. On détaille également le calcul du conducteur dans une extension de degré p^n donné par Schmid dans [57]. Enfin, en passant à la limite projective, on déduit du théorème 2 des informations sur la ramification de G_{p^∞}. Soulignons aussi que l'approche dans le chapitre 4 diffère de celle du chapitre 3 dans le sens où l'on décrit la ramification directement pour les extensions d'Artin-Schreier-Witt maximales avant d'en déduire celle des extensions finies, ce qui est le cheminement inverse du chapitre 3.

La dernière partie est consacrée à l'étude de la structure galoisienne d'une extension de degré p sur K. Plus précisément, on développe un résultat récent de Aiba ([3]) qui donne une condition

pour que l'anneau des entiers soit un module libre sur l'ordre associé. D'après le chapitre 3, si L/K est une extension de degré p totalement ramifiée, elle est donnée par un polynôme $X^p - X = a$ où a est un élément de K de valuation $-m$ strictement négative. En outre, la valuation de a donne précisément le saut pour les groupes de ramification de l'extension. L'idée est alors de construire une suite d'entiers $\epsilon_i \in \{0, 1\}$ dépendant uniquement de p et du reste de m dans la division euclidienne par p. Cette suite jouit de propriétés remarquables qui nous permettront de montrer l'équivalence des critères suivants (théorème 5.2 dans la suite) :

Théorème 3. *Soit K un corps de caractéristique p, complet pour une valuation discrète et de corps résiduel parfait. Soit L/K une extension totalement ramifiée de degré p : elle est donnée par un polynôme $X^p - X = a$ avec $a \in K$ de valuation $-m < 0$ qui n'est pas divisible par p. On écrit $m = pt + s$ pour $1 \leq s \leq p - 1$. Les propositions suivantes sont équivalentes :*

(i) O_L est libre en tant que module sur l'ordre A associé à L/K.
(ii) la suite $(\epsilon_i)_{i=1}^{p-1}$ est de type $(10...0)^s$
(iii) s divise $p - 1$
(iv) l'embedding dimension de A est inférieure ou égale à 3.

Nous retrouvons la condition de Aiba (condition équivalente à *(iii)* d'après [37]) qui correspond à la condition donnée par Bertrandias et Ferton dans [12] pour le problème équivalent en caractéristque 0. Cependant, notre approche est différente. En particulier, nous considérons une autre O_K-base pour l'ordre associé à L/K. Cette base est plus naturelle dans un certain sens et son étude nous permet de rendre le résultat de Aiba plus explicite. Bien plus, avec des arguments entièrement combinatoires, notre méthode nous conduit à un nouveau critère, purement algébrique lui, portant sur l'embedding dimension de l'ordre associé.

Table des matières

Notations

Soit $p > 0$ un nombre premier fixé.
Dans tout ce qui suit, nous adopterons les notations suivantes.

Notations du Chapitre 1 :
Les résultats du Chapitre 1 sont généraux et concernent un anneau commutatif A quelconque. Nous noterons :

$W(A)$	anneau des vecteurs de Witt sur A
$W_n(A)$	anneau des vecteurs de Witt de longueur n
$x = (x_0, x_1, ...)$	un vecteur de Witt
$x^{(*)} = (x^{(0)}, x^{(1)}, ...)$	la suite des composantes fantômes de x
g_A	l'application $x \in W(A) \mapsto x^{(*)} \in A^{\mathbb{N}}$
V (resp. V_n)	l'opérateur Shift sur $W(A)$ (resp. $W_n(A)$)
t_n	l'homomorphisme de troncation $W(A) \to W_n(A)$
t_{nm}	l'application de transition-troncation $W_n(A) \to W_m(A)$ si $n \geq m$
F	l'homomorphisme d'anneaux $(x_k)_k \mapsto (x_k^p)_k$ dans $W(A)$
$\wp$	l'homomorphisme de groupes $\wp = F - Id$ dans $W(A)$
K	corps de caractéristique p.

Notations du Chapitre 2 :
A partir du Chapitre 2, on considère un corps K de caractéristique p sur lequel nous fixons une clôture séparable notée K^{sep}, toutes les extensions considérées sur K seront incluses dans K^{sep}. En plus des notations précédentes, nous utiliserons :

L	extension d'Aritn-Schreier-Witt finie sur K
$K(\wp^{-1}(x))$	l'extension $K(\zeta_0, ..., \zeta_{n-1})$ où $\wp(\zeta_0, ..., \zeta_{n-1}) = x$
B_n	sous-groupe de $W_n(K)$ contenant $\wp(W_n(K))$
K_{B_n}	compositum de toutes les extensions $K(\wp^{-1}(x))$ pour $x \in B_n$
K_{p^n}	l'extension abélienne maximale d'exposant p^n sur K
K_{p^∞}	la pro-p extension abélienne maximale sur K
G_{p^n}	groupe de Galois abélien maximal d'exposant p^n sur K
G_{p^∞}	pro-p groupe de Galois abélien maximal sur K
H_{p^n}	groupe d'homomorphismes continus $Hom(W_n(K)/\wp(W_n(K)), W_n(\mathbb{F}_p))$
H_{p^∞}	groupe d'homomorphismes continus $Hom(W(K)/\wp(W(K)), W(\mathbb{F}_p)$
$\mathfrak{as}_n$	l'isomorphisme d'Artin-Schreier-Witt de groupes topologiques $G_{p^n} \simeq H_{p^n}$
$\mathfrak{as}_\infty$	l'isomorphisme d'Artin-Schreier-Witt $G_{p^\infty} \simeq H_{p^\infty}$
$\mathcal{V}$	le groupe quotient $W(K)/\wp(W(K))$.

Notations des Chapitres 3, 4 et 5 :
Dans les chapitres 3, 4 et 5, nous restreignons l'étude à un corps K complet pour une valuation discrète et de corps résiduel κ parfait. Nous fixerons également une clôture algébrique de K ainsi qu'une clôture séparable κ^{sep} de κ. Les notations précédentes restent inchangées. Nous définirons également :

v_K	valuation discrète normalisée sur K
U_K	groupe des unités de K
O_K	anneau de valuation de K
$\mathfrak{p}_K$	idéal maximal de O_K
κ	corps résiduel de K
$K_{p^\infty}^{nr}$	sous-extension maximale non ramifiée dans K_{p^∞}/K
$G_{p^n}^{(u)}$	u-ème groupe de ramification dans G_{p^n} pour la notation supérieure
$G_{p^\infty}^{(u)}$	u-ème groupe de ramification dans G_{p^∞} pour la notation supérieure
$W_n^{(u)}(K)$	$(\mathfrak{p}_K^{-\lfloor \frac{u}{p^{n-1}} \rfloor}, \mathfrak{p}_K^{-\lfloor \frac{u}{p^{n-2}} \rfloor}, ..., \mathfrak{p}_K^{-u})$ sous-groupe de $W_n(K)$
$H_{p^n}^{(u)}$	$\{\varphi \in H_{p^n} \ : \ \varphi(W_n^{(u)}(K) + \wp(W_n(K))/\wp(W_n(K)) = 0\}$ sous-groupe de H_{p^n},

pour tout entier $u \geq -1$.

Enfin, dans le chapitre 5 seulement, si L/K est une extension de degré p, nous noterons $A = A(L/K)$ l'ordre associé.

Première partie

Préliminaires

Chapitre 1

Vecteurs de Witt

Ce premier chapitre propose une étude complète des vecteurs de Witt à coefficients dans un anneau commutatif quelconque. Plus précisément, nous nous intéresserons aux *p-vecteurs* de Witt lorsque p est un nombre premier, notion la plus courante dans la littérature. Cette notion est parfois présentée comme un cas particulier de vecteurs de Witt dits *généraux* dont une étude est suggérée dans [35] en exercice et est développée dans mon rapport de DEA.

Nous avons choisi d'ouvrir ce mémoire de thèse par le présent chapitre pour deux raisons essentielles : c'est d'abord un exposé préliminaire sur les vecteurs de Witt, outils de base pour l'étude des extensions d'Artin-Schreier-Witt d'exposant p^n dès que $n \geq 2$. C'est aussi une tentative d'unifier tous les travaux sur ces objets depuis leur introduction par Witt [76] en 1936, d'où notre souci permanent de détailler les moindres définitions et résultats généraux.

Dans tout ce qui suit, nous fixons un nombre premier $p > 0$ ainsi qu'un anneau commutatif A.

Le paragraphe 1.1 présente une construction fonctorielle des vecteurs de Witt permettant ainsi de retrouver les principales propriétés de ces objets. Cette construction est menée en trois étapes successives : les vecteurs de Witt sont d'abord définis comme foncteur de la catégorie des anneaux commutatifs dans la catégorie des ensembles, puis dans la catégorie des ensembles munis de deux lois de composition et enfin dans la catégorie des anneaux commutatifs. Les vecteurs de Witt à coefficients dans A forment ainsi un anneau commutatif que nous noterons $W(A)$. Cet anneau est appelé l'anneau de Witt sur A.

Dans le paragraphe 1.2 nous restreignons l'étude aux vecteurs de Witt de longueur finie n, pour un entier $n \geq 1$ fixé. En particulier, ces vecteurs de Witt tronqués forment encore un anneau, noté $W_n(A)$, qui est en fait quotient de l'anneau $W(A)$. Ce sera l'occasion d'introduire un opérateur de décalage sur ce dernier, couramment appelé opérateur *shift* et noté V.
Un résultat clef de ce paragraphe sera de montrer que l'anneau $W(A)$ peut s'écrire comme limite projective des anneaux $W_n(A)$ lorsque n tend vers l'infini. Entre autres conséquences, nous obtenons une description précise des unités de $W(A)$. Mais surtout, c'est ce résultat qui nous permettra dans les chapitres suivants d'aborder les extensions d'Artin-Schreier-Witt maximales sur un corps de caractéristique p, c'est-à-dire de passer à la limite projective dans les extensions finies d'exposant p^n afin de décrire précisément les pro-p extensions abéliennes sur ce corps.

Enfin, le paragraphe 1.3 offre une première illustration des résultats précédents en considérant le cas particulier où A est un corps de caractéristique p. Nous adopterons alors la notation $A = K$. Après avoir détaillé l'étude d'un homomorphisme de groupes $\wp$ défini sur le groupe additif de $W(K)$ et parfois appelé homomorphisme d'Artin-Schreier, nous nous appliquerons à développer un théorème similaire à la forme additive du théorème 90 de Hilbert. Cette version est à la base de la démonstration du théorème d'Artin-Schreier [7] sur les extensions cycliques de degré p en caractéristique p, nous en donnons ici sa généralisation aux vecteurs de Witt. Pour clore ce chapitre, nous proposons quelques résultats principaux sur les vecteurs de Witt à coefficients dans le corps

fini $\mathbb{F}_p$ à p éléments.
Soulignons que ce dernier paragraphe développe des outils cruciaux pour notre étude générale des extensions d'Artin-Schreier-Witt sur un corps de caractéristique p.

1.1 Une construction des vecteurs de Witt

L'objet de ce paragraphe est de définir les vecteurs de Witt à coefficients dans un anneau commutatif quelconque comme foncteur de la catégorie des anneaux commutatifs dans elle-même. Pour cela, rappelons qu'un foncteur W de la catégorie $\mathfrak{A}$ dans la catégorie $\mathfrak{B}$ est une loi qui à chaque objet A de $\mathfrak{A}$ associe un objet $W(A)$ de $\mathfrak{B}$ et à chaque morphisme $f : A \to B$ de $\mathfrak{A}$ associe un morphisme $W(f) : W(A) \to W(B)$ de $\mathfrak{B}$ de sorte que :
(F1) pour tout objet A dans $\mathfrak{A}$: $F(id_A) = id_{F(A)}$
(F2) pour tous morphismes $f : A \to B$ et $g : B \to C$: $F(g \circ f) = F(g) \circ F(f)$.

1.1.1 L'ensemble des vecteurs de Witt

Le foncteur W. Nous définissons un foncteur W comme suit. Soit A un anneau commutatif, notons $W(A)$ l'ensemble $A^{\mathbb{N}}$ des suites infinies à valeurs dans A. A chaque morphisme d'anneaux $f : A \to B$ associons l'application d'ensembles $W(f) : W(A) \to W(B)$ définie par :

$$\begin{array}{rccc} W(f) := & W(A) & \to & W(B) \\ & (a_k)_k & \mapsto & (f(a_k)_k). \end{array}$$

W satisfait clairement les axiomes $(F1)$ et $(F2)$ et définit ainsi un foncteur de la catégorie des anneaux commutatifs dans la catégorie des ensembles.

Définition 1.1. *On dit que $W(A)$ est l'ensemble des* vecteurs de Witt *à coefficients dans l'anneau A.*

Composantes fantômes d'un vecteur de Witt. A chaque vecteur $x = (x_k)_k$ de $W(A)$, on associe la suite $x^{(*)} := (x^{(k)})_k$ de $A^{\mathbb{N}}$ définie par :

$$\forall k \geq 0 \ : \ x^{(k)} := x_0^{p^k} + p x_1^{p^{k-1}} + \cdots + p^k x_k.$$

Définition 1.2. *Soit x un vecteur de Witt dans $W(A)$. On appelle* composantes fantômes *de x les coefficients $x^{(k)}$, $k \geq 0$, de la suite $x^{(*)}$.*

L'application g_A. Ceci définit une application, notée g_A, qui associe à chaque vecteur de Witt de $W(A)$ la suite de ses composantes fantômes dans $A^{\mathbb{N}}$:

$$\begin{array}{rccc} g_A := & W(A) & \to & A^{\mathbb{N}} \\ & (x_k)_k & \mapsto & (x^{(k)})_k. \end{array}$$

En général, l'application g_A n'est pas bijective. Cependant :

Proposition 1.1. *Si l'anneau A contient le corps $\mathbb{Q}$ des nombres rationels, l'application g_A est bijective.*

Preuve : On peut facilement écrire les composantes fantômes $x^{(0)}$ et $x^{(1)}$ comme des polynômes en $x^{(0)}$ et $x^{(1)}$ à coefficients rationnels :

$$x_0 = x^{(0)}, \ \text{ et } \ x_1 = \frac{1}{p}(x^{(1)} - x^{(0)})^p.$$

Ensuite, pour tout entier $k \geq 1$, nous remarquons :

$$x_k = \frac{1}{p^k}(x^{(k)} - \sum_{0 \leq d \leq k-1} p^d x_d{}^{p^{n-d}}),$$

ce qui permet de montrer récursivement pour $k \geq 0$ que chaque composante x_k s'écrit comme combinaison linéaire des $x^{(d)}$, avec $0 \leq d \leq k$, à coefficients rationnels, et donc que g_A est bijective. $\diamond$

Ce dernier résultat permet d'introduire deux lois de composition sur l'ensemble $W(A)$.

1.1.2 Deux lois de composition

Notons $+$ et $\times$ les lois de composition usuelles de l'anneau $A^{\mathbb{N}}$. Le but de ce sous-paragraphe est de définir sur $W(A)$ deux autres lois de composition, notées $\hat{+}$ et $\hat{\times}$ respectivement, de sorte que W soit un foncteur de la catégorie des anneaux commutatifs dans celle des ensembles munis de deux lois de composition. Pour cela, nous appliquons le procédé suivant :

• Si A contient $\mathbb{Q}$, l'application g_A est bijective d'après la proposition 1.1. Pour tous vecteurs de Witt $a = (a_k)_k$ et $b = (b_k)_k$ de $W(A)$, nous posons alors :

$$a\hat{+}b := g_A^{-1}(a^* + b^*) \text{ et } a\hat{\times}b := g_A^{-1}(a^* \times b^*).$$

Plus précisément, leur somme (resp. produit) est définie comme le vecteur de Witt dont les composantes fantômes sont données par :

$$(\bigstar) \qquad \forall k \geq 0,\ (a\hat{+}b)^{(k)} = a^{(k)} + b^{(k)}\ ,\ \text{resp. } (a\hat{\times}b)^{(k)} = a^{(k)}.b^{(k)}.$$

En particulier, ceci est satisfait lorsque A est l'anneau de polynômes :

$$A = R_{\mathbb{Q}} := \mathbb{Q}[X_0, X_1, ..., Y_0, Y_1, ...].$$

Bien plus, l'addition et la multiplication ainsi définies sur $W(R_{\mathbb{Q}})$ n'utilisent en fait que des coefficients entiers, selon la proposition suivante :

Proposition 1.2. *Soient $X = (X_0, X_1, ...)$ et $Y = (Y_0, Y_1, ...)$ deux vecteurs de Witt dans $W(R_{\mathbb{Q}})$. Pour tout entier $k \geq 0$, la k-ème composante de chaque vecteur somme et produit de X et Y est un polynôme en les variables $X_0, Y_0, ..., X_k, Y_k$ à coefficients entiers.*

Notation 1. *Nous noterons S_k (resp.P_k) le polynôme donnant la k-ème composante du vecteur somme (resp. produit) de deux vecteurs de Witt sur $W(R_{\mathbb{Q}})$:*

$$(X\hat{+}Y)_k = S_k(X_0, ..., X_k, Y_0, ..., Y_k),$$

resp. :

$$(X\hat{\times}Y)_k = P_k(X_0, ..., X_k, Y_0, ..., Y_k).$$

Preuve : Considérons la série formelle :

$$f_X(t) := \prod_{k\geq 0}(1 - X_k t^k).$$

Un simple calcul donne :

$$-t\frac{f_X'(t)}{f_X(t)} = \sum_{k\geq 0} X^{(k)} t^k.$$

Alors, en comparant les dérivées et les valeurs prises en 0 des séries $f_X(t)f_Y(t)$ et $f_{X+Y}(t)$, on montre que :

$$f_X(t)f_Y(t) = f_{X\hat{+}Y}(t),$$

c'est-à-dire :

$$\prod_{k\geq 0}(1 - X_k t^k)\prod_{k\geq 0}(1 - Y_k t^k) = \prod_{k\geq 0}(1 - (X\hat{+}Y)_k t^k).$$

En identifiant les coefficients devant chaque monôme t^k, nous obtenons finalement que chaque composante $(X\hat{+}Y)_k$ est un polynôme à coefficients entiers en les variables $X_0, Y_0, ..., X_k, Y_k$.
De même, on obtient un résultat analogue pour les composantes du produit $X\hat{\times}Y$ en considérant cette fois l'égalité suivante :

$$f_{X\hat{\times}Y}(t) = \prod_{d,e\geq 0} (1 - X_d^{m-d} Y_e^{m-e} t^m)^{d+e-m},$$

où dans chaque facteur du produit, m représente le plus petit commun multiple de d et e, les entiers d et e parcourant $\mathbb{N}$. ◇

Exemple 1.1. *Les deux premières composantes des vecteurs somme et produit sont faciles à calculer :*

$$(X\widehat{+}Y) = (X_0 + Y_0, X_1 + Y_1 - \sum_{k=1}^{p-1} \frac{1}{p}\binom{p}{k} X_0^k Y_0^{p-k}, \cdots),$$
$$(X\widehat{\times}Y) = (X_0.Y_0, X_1.Y_0^p + Y_1.X_0^p + pX_1Y_1, \cdots).$$

• Si A est un sous-anneau d'un anneau contenant $\mathbb{Q}$, la proposition 1.2 permet encore de définir sur l'ensemble $W(A)$ deux lois de composition à partir des composantes fantomes selon la relation (★) : soit a et b deux vecteurs de Witt sur A, il existe un unique vecteur de Witt dans $W(A)$, noté $a\hat{+}b$ (resp. $a\hat{\times}b$), dont les composantes fantomes sont $a^{(k)} + b^{(k)}$ (resp. $a^{(k)}.b^{(k)}$).
En particulier, ceci fonctionne lorsque A est l'anneau de polynômes $R_{\mathbb{Z}} := \mathbb{Z}[X_0, X_1, ..., Y_0, Y_1, ...]$.

• Considérons enfin un anneau commutatif quelconque A. Soit $a = (a_k)_k$ et $b = (b_k)_k$ deux vecteurs de Witt à coefficients dans A. On souhaite définir deux vecteurs de Witt $a\hat{+}b$ et $a\hat{\times}b$ dans $W(A)$ de sorte à généraliser les lois de composition définies pour les cas particuliers précédents. Dans ce but, notons ϕ_{ab} l'unique homomorphisme d'anneaux donné par :

$$\begin{array}{rccc} \phi_{ab} := & R_Z & \to & A \\ & X_k & \mapsto & a_k \\ & Y_k & \mapsto & b_k, \end{array}$$

pour tout entier $k \geq 0$.

On pose alors :

Définition 1.3. *Soit A un anneau commutatif. Pour tous vecteurs de Witt a et b dans $W(A)$, nous définissons leurs vecteurs somme et produit comme suit :*

$$a\hat{+}b := W(\phi_{ab})(X\hat{+}Y)$$

et :

$$a\hat{\times}b := W(\phi_{ab})(X\hat{\times}Y).$$

Il s'agit de montrer que cette définition coïncide avec les opérations données précédemment, ou encore que la relation (★) est toujours satisfaite. Pour cela, nous avons besoin du lemme suivant :

Lemme 1.1. *Soit Ω un foncteur de la catégorie des anneaux dans elle-même, tel que :*
i). pour tout anneau commutatif A, $\Omega(A) = A^{\mathbb{N}}$
ii). pour tout homomorphisme d'anneaux $f : A \to B$, $\Omega(f) : \Omega(A) \to \Omega(B)$ est l'homomorphisme d'anneaux défini par $(a_k)_k \mapsto (f(a_k))_k$.
Alors, si A et B sont deux anneaux commutatifs et si $\varphi : A \to B$ est un homomorphisme d'anneaux, le diagramme suivant est commutatif :

$$\begin{array}{ccc} W(A) & \xrightarrow{W(f)} & W(B) \\ \downarrow{\scriptstyle g_A} & & \downarrow{\scriptstyle g_B} \\ A^{\mathbb{N}} & \xrightarrow{\Omega(f)} & B^{\mathbb{N}} \end{array} .$$

Preuve : La preuve consiste simplement à écrire les définitions des foncteurs W et Ω, ainsi que des applications g_A et g_B puis à montrer que chaque m-ème composante fantôme du vecteur de Witt $(f(a_k))_k$ dans $W(B)$ est $f(a^{(m)})$. $\diamond$

Nous obtenons alors :

Proposition 1.3. *Soit A un anneau commutatif. Tous vecteurs de Witt a et b dans $W(A)$ satisfont les relations suivantes :*

$$g_A(a\widehat{+}b) = g_A(a) + g_A(b) \;\; et \;\; g_A(a\widehat{\times}b) = g_A(a).g_A(b).$$

En d'autres termes, la relation ($\bigstar$) est satisfaite pour tout anneau commutatif.

Preuve : Le lemme 1.1 appliqué aux anneaux A et $R_{\mathbb{Z}}$ donne le diagramme commutatif suivant :

$$\begin{array}{ccc} W(R_{\mathbb{Z}}) & \xrightarrow{W(\phi_{ab})} & W(A) \\ \downarrow{\scriptstyle g_{R_{\mathbb{Z}}}} & & \downarrow{\scriptstyle g_A} \\ R_{\mathbb{Z}}^{\mathbb{N}} & \xrightarrow{\Omega(\phi_{ab})} & A^{\mathbb{N}} \end{array} .$$

Ainsi, d'après la relation ($\bigstar$) dans $W(R_{\mathbb{Z}})$ et en raison de l'addictivité du morphisme $\Omega(\phi_{ab})$, nous obtenons :

$$\begin{aligned} g_A(a\widehat{+}b) &= g_A \circ W(\phi_{ab})(X\widehat{+}Y) \\ &= \Omega(\phi_{ab}) \circ g_{R_{\mathbb{Z}}}(X\widehat{+}Y) \\ &= \Omega(\phi_{ab})(g_{R_{\mathbb{Z}}}(X) + g_{R_{\mathbb{Z}}}(Y)) \\ &= \Omega(\phi_{ab}) \circ g_{R_{\mathbb{Z}}}(X) + \Omega(\phi_{ab}) \circ g_{R_{\mathbb{Z}}}(Y) \\ &= g_A(a) + g_B(b). \end{aligned}$$

De même, on montre que : $g_A(a\widehat{\times}b) = g_A(a).g_A(b)$. $\diamond$

Remarque 1. *La présente remarque est essentielle pour la suite. La proposition 1.3 montre en particulier que la relation ($\bigstar$) est satisfaite pour tout anneau commutatif A. Cependant, cette relation ne suffit pas en général à définir des lois d'addition et de multiplication sur $W(A)$. C'est le cas par exemple si p n'est pas inversible dans A car alors l'application g_A n'est plus bijective puisque deux vecteurs de Witt distincts peuvent avoir les mêmes composantes fantômes.*
Aussi encourageons-nous vivement le lecteur à se rappeler les différentes étapes précédentes car c'est ce processus qui nous permet de définir proprement somme et produit sur les vecteurs de Witt à coefficients dans un anneau commutatif A quelconque.

Maintenant, il reste à montrer que W satisfait les axiomes d'un foncteur de la catégorie des anneaux commutatifs dans celle des ensembles munis de deux opérations. C'est la proposition suivante :

Proposition 1.4. *Soit A et B deux anneaux commutatifs. Si $f : A \to B$ est un morphisme d'anneaux, alors l'application induite :*

$$W(f) : W(A) \longrightarrow W(B)$$

est additive et multiplicative pour les lois $\widehat{+}$ et $\widehat{\times}$.

Preuve : Pour tous vecteurs de Witt a et b dans $W(A)$, nous avons :

$$\begin{aligned} W(f)(a\widehat{+}b) &= W(f \circ \phi_{ab})(X\widehat{+}Y) \\ &= W(\phi_{W(f)(a),W(f)(b)})(X\widehat{+}Y) \\ &= W(\phi_{W(f)(a),W(f)(b)})(X)\hat{+}W(\phi_{W(f)(a),W(f)(b)})(Y) \\ &= W(f)(a)\hat{+}W(f)(b). \end{aligned}$$

Par un argument analogue, on montre également :

$$W(f)(a\widehat{\times}b) = W(f)(a)\widehat{\times}W(f)(b).$$

$\diamond$

1.1.3 L'anneau $W(A)$

Voici enfin le résultat principal de ce premier paragraphe :

Théorème 1.1. *Soit A un anneau commutatif. Notons respectivement 0 et 1 ses éléments neutres pour l'addition et la multiplication. Alors l'ensemble $W(A)$ est muni d'une structure d'anneau commutatif pour les lois de composition $\widehat{+}$ et $\widehat{\times}$ définies précédemment, d'élements neutres $(0,0,...)$ et $(1,0,0,...)$ respectivement.*

Preuve : Si A contient $\mathbb{Q}$, l'application g_A est bijective mais aussi additive et multiplicative d'après la proposition 1.3. Ainsi, g_A transfert la structure d'anneau commutatif de $(A^{\mathbb{N}}, +, \times)$ sur $(W(A), \widehat{+}, \widehat{\times})$.
Si maintenant A est un sous-anneau d'un anneau contenant $\mathbb{Q}$, $W(A)$ est encore un anneau pour les lois $\widehat{+}$ et $\widehat{\times}$ par la proposition 1.2. C'est en particulier le cas pour l'ensemble des vecteurs de Witt à coefficients dans l'anneau de polynomes $A_{\mathbb{Z}} := \mathbb{Z}[X_0, X_1, ..., Y_0, Y_1, ..., Z_0, Z_1, ...]$ dans lequel nous notons X, Y et Z les vecteurs de Witt $(X_0, X_1, ...)$, $(Y_0, Y_1, ...)$ et $(Z_0, Z_1, ...)$ respectivement.

Enfin, soit A un anneau comutatif arbitraire. Il s'agit de montrer que les lois $\widehat{+}$ et $\widehat{\times}$ satisfont dans $W(A)$ les axiomes d'un anneau. Si a, b et c sont trois vecteurs de Witt dans $W(A)$, notons ϕ_{abc} l'unique homomorphisme d'anneaux de $A_{\mathbb{Z}}$ dans $W(A)$ qui envoie les composantes X_k (resp. Y_k) (resp. Z_k) sur a_k (resp. b_k) (resp. c_k) pour tout entier $k \geq 0$. D'après la proposition 1.4, l'application $W(\phi_{abc})$ est multiplicative et additive, elle transporte donc les relations d'associativité, distibutivité et commutativité de l'anneau $W(A_{\mathbb{Z}})$ dans l'ensemble $W(A)$ pour les lois $\widehat{+}$ et $\widehat{\times}$. De plus, cette application permet de définir dans $W(A)$ l'opposé de tout vecteur a pour la loi $\widehat{+}$ en posant : $-a := W_{\phi_{abc}}(-X)$. Ainsi, $W(A)$ est muni d'une structure d'anneau commutatif pour les lois $\widehat{+}$ et $\widehat{\times}$.
Il reste à montrer que les éléments $(0,0...)$ et $(1,0,...)$ sont neutres dans $W(A)$ pour les lois $\widehat{+}$ et $\widehat{\times}$ respectivement. En effet, cela est trivial lorsque $\mathbb{Q}$ est inclus dans A car alors l'application g_A envoie $(0,0...)$ (resp. $(1,0...)$) sur l'élément nul (resp. unité) de $A^{\mathbb{N}}$, c'est-à-dire sur $(0,0,...)$ (resp. $(1,1,...)$). Alors, par un argument analogue au procédé précédent, on montre que cela reste vrai pour tout anneau commutatif A, complétant ainsi la preuve du théorème 1.1. ◇

Le corollaire qui suit clot ce paragraphe en montrant que W est un foncteur de la catégorie des anneaux commutatifs dans elle-même :

Corollaire 1.1. *Soit A et B deux anneaux commutatifs. Pour tout morphisme d'anneaux $f : A \to B$, l'application induite $W(f) : W(A) \to W(B)$ est encore un morphisme d'anneaux.*
Ainsi construit, W est alors un foncteur de la catégorie des anneaux commutatifs dans elle-même.

Preuve : La preuve est essentiellement la proposition 1.4 ainsi que le théorème 1.1. ◇

Remarque 2. *Si A contient $\mathbb{Q}$, l'application g_A est un isomorphisme d'anneaux. Cependant, dans le cas général, $A^{\mathbb{N}}$ et $W(A)$ correspondent uniquement en tant qu'ensembles. En fait, si l'anneau A est de caractéristique $p > 0$ par exemple, alors $A^{\mathbb{N}}$ est de caractéristique p aussi tandis que $W(A)$ est de caractéristique 0 : ces deux anneaux ne peuvent pas être isomorphes.*

Dans la suite, nous désignerons aussi par $+$ et $.$ les lois de composition $\widehat{+}$ et $\widehat{\times}$ sur l'anneau de Witt $W(A)$, pour tout anneau commutatif A.

Exemple 1.2. *A partir de l'exemple 1.1 écrivons les deux premières composantes pour la somme puis le produit de deux vecteurs de Witt a et b dans $W(A)$:*

$$(a+b) = (a_0 + b_0\ ,\ a_1 + b_1 - \sum_{k=1}^{p-1} [\frac{1}{p} \begin{pmatrix} p \\ k \end{pmatrix}] a_0^k b_0^{p-k}\ , ...)$$

et :

$$(a \times b) = (a_0.b_0\ ,\ a_1.b_0^p + a_0^p.b_1 + pa_1b_1\ , ...).$$

où la notation $[\frac{1}{p}\begin{pmatrix} p \\ k \end{pmatrix}]$ *désigne* $\frac{(p-1)!}{k!(p-k)!}$, *pour tout* k *dans* $\{1, ..., p-1\}$.

1.2 Les vecteurs de Witt de longueur n

Fixons un entier positif $n \geq 1$. Dans ce paragraphe nous nous restreignons à l'étude des vecteurs de Witt de longueur n. Le sous-paragraphe 1.2.1 montre que ces vecteurs tronqués forment encore un anneau que nous noterons $W_n(A)$. Dans le sous-paragraphe 1.2.2 nous introduisons un opérateur de décalage défini sur $W(A)$, permettant ainsi de préciser la structure de $W_n(A)$ comme anneau quotient de $W(A)$. Enfin, le sous-paragraphe 1.2.3 décrit l'anneau de Witt $W(A)$ comme limite projective des anneaux $W_n(A)$.

1.2.1 L'anneau $W_n(A)$

Définition 1.4. *Pour tout entier $n \geq 1$, nous notons $W_n(A)$ l'ensemble des vecteurs de Witt tronqués $(x_0, x_1, \cdots, x_{n-1})$ de longueur n.*

D'après la proposition 1.2 et puisque les composantes $(x+y)_k$ et $(x.y)_k$ dépendent uniquement des coefficients x_i et y_i pour $i \leq k$, l'ensemble $W_n(A)$ est muni d'une structure d'anneau pour les lois induites de $+$ et $.$ dans $W(A)$ par troncation :

Proposition 1.5. *Si $n \geq 1$, l'ensemble $W_n(A)$ est un anneau commutatif pour les lois $+$ et $.$ definies dans $W(A)$.*

Preuve : Evident. ◇

Exemple 1.3. *Pour $n = 1$, l'anneau des vecteurs de Witt de longueur 1 à coefficients dans A est $W_1(A) = A$.*

La proposition suivante précise la précédente :

Proposition 1.6. *L'anneau $W_n(A)$ est anneau quotient de $W(A)$.*

Preuve : A partir de la proposition 1.5, on montre facilement que $W_n(A)$ est l'image de $W(A)$ par l'homomorphisme surjectif d'anneaux t_n défini par :

$$\begin{array}{rccc} t_n := & W(A) & \longrightarrow & W_n(A) \\ & x = (x_0, \cdots, x_{n-1}, \cdots) & \mapsto & (x_0, \cdots, x_{n-1}). \end{array}$$

◇

Remarque 3. *La projection $t_n : W(A) \to W_n(A)$ est une application de troncation, appelée n-ème troncation de l'anneau de Witt $W(A)$.*

1.2.2 L'operateur shift

Nous souhaitons préciser la structure de $W_n(A)$ comme anneau quotient de $W(A)$. Ceci nous conduit à introduire un opérateur de décalage, plus brièvement l'opérateur *shift* ou encore le *Vershiebung* pour les germanophones :

Définition 1.5. *On appelle opérateur shift de l'anneau $W(A)$ l'application $V : W(A) \to W(A)$ définie par :*

$$V(x_0, x_1, ...) = (0, x_0, x_1, ...)$$

Proposition 1.7. *Pour tout anneau commutatif A, l'opérateur V est additif sur $W(A)$.*

Preuve : Nous montrons l'additivité de V lorsque A contient $\mathbb{Q}$, p étant inversible dans A. Conservant les notations du paragraphe 1.1, il existe alors une unique application, que nous noterons g_A^V, rendant le diagramme suivant commutatif :

$$\begin{array}{ccc} W(A) & \xrightarrow{g_A} & A^{(\mathbb{N})} \\ \Big\downarrow{\scriptstyle V} & & \Big\downarrow{\scriptstyle g_A^V} \\ W(A) & \xrightarrow{g_A} & A^{\mathbb{N}}. \end{array}$$

Soit $x = (x_0, x_1, ...)$ un vecteur de $W(A)$. D'après la définition des composantes fantômes, on a :

$$\begin{aligned} g_A(x) &= (x^{(0)}, x^{(1)}, ...) \\ &= (x_0, x_0^p + px_1, ...) \end{aligned}$$

et :

$$\begin{aligned} g_A \circ V(x) &= g_A(0, x_0, x_1, ...) \\ &= (0, px_0, px_0^p + p^2 x_1, ...) \\ &= (0, px^{(0)}, px^{(1)}, ...). \end{aligned}$$

Ainsi, l'application g_A^V envoie $(x^{(0)}, x^{(1)}, ...)$ sur $(0, px^{(0)}, px^{(1)}, ...)$, elle est donc additive.
Alors, par commutativité du diagramme et puisque g_A est un isomorphisme d'anneaux d'après le paragraphe 1.1, il vient :

$$V = g_A^{-1} \circ g_A^V \circ g_A$$

L'application V est donc additive, ce qui montre la proposition lorsque $\mathbb{Q} \subset A$.
La proposition est donc satisfaite également lorsque A est l'anneau de polynômes $A_{\mathbb{Z}} = \mathbb{Z}[X_0, X_1, ..., Y_0, Y_1, ...]$ puisque $A_{\mathbb{Z}}$ est un sous-anneau de $\mathbb{Q}[X_0, X_1, ..., Y_0, Y_1, ...]$.
Enfin, avec les notations du lemme 1.1, si A est quelconque, pour tous vecteurs de Witt a et b dans $W(A)$, le diagramme :

$$\begin{array}{ccc} W(A_{\mathbb{Z}}) & \xrightarrow{W(\phi_{a,b})} & W(A) \\ \Big\downarrow{\scriptstyle V} & & \Big\downarrow{\scriptstyle V} \\ W(A_{\mathbb{Z}}) & \xrightarrow{W(\phi_{a,b})} & W(A) \end{array}$$

commute par fonctorialité de W. En outre, les applications $W(\varphi_{a,b})$ et V commutent trivialement. Ainsi, d'après la proposition 1.4 il vient :

$$\begin{aligned} V(a+b) &= V \circ W(\phi_{a,b})(X+Y) \\ &= W(\phi_{a,b}) \circ V(X+Y) \\ &= W(\phi_{a,b})(V(X) + V(Y)) \\ &= W(\phi_{a,b})(V(X)) + W(\phi_{a,b})(V(Y)) \\ &= V(W(\phi_{a,b})(X)) + V(W(\phi_{a,b})(Y)) \\ &= V(a) + V(b) \end{aligned}$$

et donc V est encore additive pour tout anneau commutatif A, ce qui conclut la preuve. ◇

Retournons à l'étude de l'anneau $W_n(A)$. D'après la preuve de la proposition 1.6, $W_n(A)$ apparaît comme quotient de $W(A)$:

Proposition 1.8. *Pour tout entier $n \geq 1$, on a un isomorphisme d'anneaux :*

$$W_n(A) \xrightarrow{\simeq} W(A)/V^n W(A).$$

Preuve : Soit $x = (x_i)_i$ un vecteur de Witt dans $W(A)$. Alors on a :

$$\begin{array}{rcl} t_n(x) = 0 & \Leftrightarrow & \forall i \leq n-1 \ \ x_i = 0 \\ & \Leftrightarrow & x = (0, \cdots, 0, x_n, \cdots) \\ & \Leftrightarrow & x = V^n(x_n, x_{n+1}, \cdots) \in V^n W(A), \end{array}$$

ce qui montre que $V^n W(A)$ est le noyau de t_n. Par passage au quotient, le morphisme de troncation t_n induit alors un isomorphisme d'anneaux $W_n(A) \xrightarrow{\simeq} W(A)/V^n W(A)$. $\diamond$

Remarque 4. *En particulier, $V^n W(A)$ est un idéal de l'anneau de Witt $W(A)$.*

En outre, par passage au quotient, l'opérateur shift V induit une application additive de $W_n(k)$ dans $W_{n+1}(k)$, que nous noterons V (ou V_n lorsqu'il est nécessaire de préciser n) :

$$\begin{array}{rccc} V \ : & W_n(k) & \longrightarrow & W_{n+1}(k) \\ & (x_0, ..., x_{n-1}) & \mapsto & (0, x_0, ..., x_{n-1}). \end{array}$$

1.2.3 L'anneau $W(A)$ comme limite projective

Ce sous-paragraphe est consacré à l'écriture de l'anneau de Witt $W(A)$ comme limite projective des anneaux $W_n(A)$ lorsque n tend vers l'infini.
Si n et m sont deux entiers tels que $n \geq m \geq 1$, nous noterons t_{nm} le morphisme de troncation de $W_n(K)$ dans $W_m(K)$:

$$\begin{array}{rccc} t_{nm} \ := & W_n(A) & \to & W_m(A) \\ & (x_0, ..., x_{m-1}, ..., x_{n-1}) & \mapsto & (x_0, ..., x_{m-1}). \end{array}$$

On a :

Théorème 1.2. *Soit A un anneau commutatif. L'anneau de Witt $W(A)$ est isomorphe à la limite projective du système $(W_n(A), t_{nm})_n$:*

$$W(A) \simeq \varprojlim W_n(A),$$

lorsque $n \to +\infty$.

Preuve : Puisque toutes les troncations t_{nm} sont des morphismes d'anneaux, la limite projective $\varprojlim W_n(A)$ a une structure d'anneau. Il s'agit donc de montrer l'existence d'un isomorphisme d'anneaux entre $W(A)$ et cette limite projective. Pour tous les entiers $n \geq 1$, désignons par π_n les applications de projection $\varprojlim W_n(A) \to W_n(A)$ relatives au système projectif $(W_n(A), t_{nm})_n$. Puisque toutes les applications de transition t_{nm} sont surjectives, il en est de même des π_n.
Or, pour tous entiers $n \geq m$, il est facile de vérifier que le diagramme suivant commute :

$$\begin{array}{ccc} W(A) & \xrightarrow{t_n} & W_n(A) \\ & \searrow^{t_m} & \downarrow{\scriptstyle t_{nm}} \\ & & W_m(A) \end{array}$$

où t_n est l'application de troncation introduite dans la proposition 1.6.
Alors, d'après la propriété universelle des limites projectives, il existe une unique application Θ : $W(A) \to \varprojlim W_n(A)$ telle que le diagramme :

$$\begin{array}{ccc} W(A) & \xrightarrow{t_n} & W_n(A) \\ \downarrow{\scriptstyle \Theta} & \nearrow_{\pi_n} & \\ \varprojlim W_n(A) & & \end{array}$$

commute pour tout entier $n \geq 1$. C'est-à-dire :

$$\pi_n \circ \Theta = t_n.$$

De plus, l'application Θ est un morphisme d'anneaux, les applications t_n etπ_n étant elles-mêmes des morphismes. Il reste donc à montrer que Θ est bijective.
Il est facile de vérifier que Θ est injective puisque $\cap_n V^n W(A) = 0$. Rappelons que d'après la proposition 1.8, chaque idéal $V^n W_n(A)$ est le noyau de t_n.
Maintenant, soit $Z := (z^1, z^2, ...)$ un élément de $\varprojlim W_n(A)$. On souhaite construire un vecteur de Witt x dans $W(A)$ tel que $\Theta(x) = Z$, ce qui signifie :

$$\begin{array}{rcl} \Theta(x) = Z & \Leftrightarrow & \forall n \geq 1,\ \pi_n \circ \Theta(x) = \pi_n(Z) \\ & \Leftrightarrow & \forall n \geq 1,\ t_n(x) = z^n \\ & \Leftrightarrow & \forall n \geq 1,\ \forall k \leq n-1,\ x_k = (z^n)_k. \end{array}$$

Mais, pour tous les entiers $n \geq m$, la relation caractéristique du système projectif $(W_n(A), t_{nm})_n$:

$$t_{nm} \circ \pi_n(Z) = \pi_m(Z),$$

implique :

$$t_{nm}(z^n) = z^m.$$

D'où, pour tous les entiers $n \geq m$ et $k \in \{0, ..., m-1\}$:

$$(z^n)_k = (z^m)_k.$$

Cela entraîne que pour tout $k \geq 0$ et pour tout $n \geq k+1$, les coefficients $(z^n)_k$ sont constants et égaux à $(z^{k+1})_k$.
Alors, le vecteur de Witt x de $W(A)$ défini par ses coefficients :

$$\forall k \geq 0,\ x_k = (z^{k+1})_k,$$

satisfait les relations :

$$\forall n \geq 0,\ \forall k \leq n-1,\ (x)_k = (z^n)_k.$$

Ainsi $\Theta(x) = Z$, d'où la surjectivité de Θ et la fin de la preuve du théorème. ◇

Fixons une topologie sur A, la topologie discrète par exemple. Si l'on munit chaque anneau $W_n(A)$ de la topologie induite par le produit A^n, alors la limite projective $\varprojlim W_n(A)$ est un espace topologique pour la topologie induite par la topologie produit de $\prod_n W_n(A)$. C'est pourquoi, à partir de maintenant, identifiant l'anneau de Witt $W(A)$ avec $\varprojlim W_n(A)$, nous munirons $W(A)$ de la topologie ainsi définie. L'isomorphisme Θ devient ainsi un homéomorphisme.
En résumé :

Corollaire 1.2. *Si A est un anneau topologique, l'anneau de Witt $W(A)$ est muni de la topologie induite du produit $\prod_n W_n(A)$, où chaque anneau $W_n(A)$ a la topologie induite de A^n.*

On peut montrer facilement que cette topologie sur $W(A)$ est équivalente à la topologie de la convergence composante par composante.

Une première conséquence de ce résultat est la suivante. Etant donnée une suite de vecteurs de Witt $(z(k))_k$ dans $W(A)$, on peut définir la somme infinie $\sum_k z(k)$ comme la limite dans $W(A)$ de la suite $(\sum_{k=0}^N z(k))_N$ lorsque cette dernière converge pour la topologie donnée précédemment. Illustrons ceci avec le résultat suivant que nous utiliserons plus loin pour montrer la proposition 1.14 :

Proposition 1.9. *Pour chaque élément a de A, notons $\{a\}$ le vecteur de Witt $\{a, 0, ...\}$. Alors, tout vecteur de Witt x dans $W(A)$ vérifie l'identité :*

$$x = \sum_{k\geq 0} V^k(\{x_k\}).$$

Remarquons que cette proposition implique la formule suivante :

$$(x_0, x_1, ...) + (0, ..., 0, y_s, y_{s+1}, ...) = (x_0, ..., x_{s-1}, x_s + y_s, ...),$$

ce qui sera d'une grande utilité dans les chapitres suivants.

Preuve : D'abord, il est facile de vérifier la convergence de la série dans $W(A)$ puisque pour chaque entier $n \geq 1$ la suite :

$$(t_n(\sum_{k=0}^{N} V^k(\{x_k\}))_N$$

est constante à partir du rang $n-1$, égale à $\sum_{k=0}^{n-1} V^k(\{x_k\})$.
Alors, en suivant le processus du paragraphe 1.1 utilisé pour définir les lois de composition sur $W(A)$, il suffit de montrer la relation lorsque A contient $\mathbb{Q}$ seulement. Or dans ce cas, g_A est un isomorphisme. Il s'agit donc de montrer l'égalité :

$$g_A(x) = g_A(\sum_{k\geq 0} V^k(\{x_k\}),$$

c'est-à-dire :

$$\forall n \geq 0,\ x^{(n)} = (\sum_{k\geq 0} V^k(\{x_k\}))^{(n)}.$$

Maintenant, d'après la proposition 1.3 et la définition des composantes fantômes, il vient :

$$\begin{array}{lll} \forall n \geq 0,\ \forall N \geq 0, & (\sum_{k=0}^{N} V^k(\{x_k\})^{(n)} & = \sum_{k=0}^{N} (V^k(\{x_k\}))^{(n)} \\ & & = \sum_{k=0}^{n} (V^k(\{x_k\}))^{(n)} \\ & & = \sum_{k=0}^{n} p^k x_k^{p^{n-k}} \\ & & = x^{(n)}. \end{array}$$

D'où, en faisant tendre N vers l'infini :

$$(\sum_{k\geq 0} V^k(\{x_k\}))^{(n)} = x^{(n)},$$

ce qu'il fallait démontrer. ◇

Au passage, on a le résultat suivant :

Proposition 1.10. *Pour tout $u \in K$ et tout $x \in W(K)$, on a :*

$$\{u\}x = (ux_0, u^p x_1, u^{p^2} x_2, ..., u^{p^k} x_k, ...).$$

Preuve : La preuve est analogue à celle de la proposition 1.9 dès que l'on remarque que $(\{u\})^{(k)} = u_k^{p^k}$ pour tout $k \geq 0$. ◇

Une autre conséquence du théorème 1.2 est la caractérisation des unités de l'anneau de Witt $W(A)$:

Proposition 1.11. *Pour tout entier $n \geq 1$, un vecteur de Witt tronqué $x = (x_0, \cdots, x_{n-1})$ de $W_n(A)$ est une unité de $W_n(A)$ si et seulement si x_0 est une unité de A.*

Preuve : Si $x = (x_0, ..., x_{n-1})$ est une unité de $W_n(A)$, il existe $y = (y_0, \cdots, y_{n-1}) \in W_n(A)$ tel que :

$$x.y = (1, 0, \cdots, 0),$$

ce qui implique d'après l'exemple 1.2 que $x_0.y_0 = 1$ et donc que x_0 est une unité dans A.
Réciproquement, supposons que x_0 est inversible dans A. Considérons le vecteur $y := (x_0^{-1}, 0, \cdots, 0)$ dans $W_n(A)$. Alors, d'après la proposition 1.9 on a :

$$\begin{aligned} x.y &= x.(x_0^{-1}, 0, \cdots, 0) \\ &= (1, *, \cdots, *) \\ &= (1, 0, \cdots, 0) - (0, *, \cdots, *) \\ &= 1 - Vz, \end{aligned}$$

pour un certain vecteur z dans $W_{n-1}(A)$. On en déduit :

$$\begin{aligned} x.y.(1 + Vz + \cdots + V^{n-1}z) &= (1 - Vz)(1 + Vz + \cdots + V^{n-1}z) \\ &= \textstyle\sum_0^{n-1} V^i z - \sum_1^n V^i z \\ &= 1 - V^n z \\ &= 1, \end{aligned}$$

puisque l'anneau $W_{n-1}(A)$ est annulé par V^n. Ainsi, le vecteur x est une unité de $W_n(A)$, ce qui montre l'assertion. ◇

Corollaire 1.3. *Les unités de l'anneau de Witt $W(A)$ sont précisément les vecteurs de Witt dont la première composante est une unité de A.*

Preuve : Cela résulte du théorème 1.2 et de la proposition 1.11 :

$$\begin{aligned} x \in W(A) \text{ est une unité} &\Leftrightarrow \exists y \in W(A) \;\; x.y = 1 \\ &\Leftrightarrow \exists y \in W(A) \;\; \forall n \;\; t_n(x.y) = 1 \\ &\Leftrightarrow \exists y \in W(A) \;\; \forall n \;\; t_n(x).t_n(y) = 1 \\ &\Leftrightarrow \forall n \;\; t_n(x) = (x_0, \cdots, x_{n-1}) \text{ est une unité de } W_n(A) \\ &\Leftrightarrow x_0 \text{ est une unité de } A. \end{aligned}$$

◇

Dans le paragraphe qui suit, ce corollaire sera utilisé pour montrer le théorème 1.3.

1.3 Cas d'un corps de caractéristique p

Pour clore ce chapitre, nous proposons une étude de l'anneau de Witt $W(A)$ lorsque A est un corps de caractéristique p que nous noterons dans la suite K. Ce dernier paragraphe n'est pas seulement une illustration des propriétés précédentes : il développe surtout les principaux outils et résultats essentiels à l'étude des extensions d'Artin-Schreier-Witt. Plus précisément, le sous-paragraphe 1.3.1 offre une étude détaillée de l'endomorphisme $\wp$ défini sur le sous-groupe additif de $W(K)$. Ce morphisme, parfois dit d'Artin-Schreier, est présenté comme un relèvement aux vecteurs de Witt du polynôme $X^p - X$ servant à décrire les extensions de degré p sur K dans le théorème initial d'Artin-Schreier [7] et sera à la base de la généralisation de ce théorème pour décrire les extensions plus générales d'Artin-Schreier-Witt sur K. Il est à noter que $\wp$ peut aussi etre défini sur $W(A)$ lorsque A est simplement un anneau de caractéristique p.

A partir de ce morphisme de groupes, le sous-paragraphe 1.3.2 développe un théorème que l'on présentera comme la forme additive du théorème 90 de Hilbert pour les vecteurs de Witt sur K. Enfin, le sous-paragraphe 1.3.3 donne une description explicite des vecteurs de Witt sur le corps fini $\mathbb{F}_p$.

1.3.1 Les applications F et $\wp$

Lorsque l'anneau A est de caractéristique p, deux applications jouent un rôle particulier sur l'anneau de Witt $W(A)$. La première, notée F, est induite fonctoriellement du morphisme de Frobenius défini sur l'anneau A. La seconde, notée $\wp$, est un morphisme additif défini par $\wp = F - Id$.

Si A est de plus muni d'une structure de corps, alors noté K, nous nous intéresserons à décrire le noyau et l'image de $\wp$, obtenant ainsi une suite exacte à la base de la description du groupe de Galois des extensions d'Artin-Schreier-Witt sur K dans le chapitre suivant. Insistons sur le fait que pour ces extensions $\wp$ est amené à jouer le même rôle que joue le polynôme $X^p - X$ pour les extensions cycliques de degré p sur K, d'où l'intérêt particulier de ce sous-paragraphe pour la suite.

L'endomorphisme F. Soit A un anneau de caractéristique p. L'application $x \mapsto x^p$ est un endomorphisme d'anneaux sur A. Ainsi, d'après le paragraphe 1.1, elle définit fonctoriellement un morphisme d'anneaux sur $W(A)$ que nous notons F :

$$\begin{array}{rccc} F := & W(A) & \longrightarrow & W(A) \\ & (x_0, x_1, ...) & \mapsto & (x_0^p, x_1^p, ...). \end{array}$$

Remarque 5. *Attention ! Pour tout $x \in W(A)$, $F(x)$ n'est pas en général la puissance p-ème de x de $W(K)$.*

Remarque 6. *Si A est de plus parfait, F est un isomorphisme.*

Proposition 1.12. *Pour chaque entier $n \geq 1$, l'endomorphisme F de $W(A)$ induit par passage au quotient un endomorphisme sur l'anneau $W_n(A)$, que nous noterons encore F (où F_n si confusion) :*

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

Preuve : L'idéal $V^n W(A)$ est invariant sous l'action de F, il est donc inclus dans le noyau du morphisme composé $t_n \circ F : W(A) \to W_n(A)$ d'après la proposition 1.8. Ainsi, par passage au quotient, cela définit un morphisme d'anneaux de $W(A)/V^n W(A)$ dans $W_n(A)$, et donc un endomorphisme de $W_n(A)$. ◇

L'endomorphisme de groupes $\wp$. On considère maintenant $W(A)$ comme un groupe additif seulement et l'on pose :

Définition 1.6. *Soit $\wp$ le morphisme de groupes $F - Id$ défini sur $W(A)$ par :*

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

Fixons un entier $n \geq 1$. Par passage au quotient, $\wp$ définit encore un endomorphisme sur le groupe additif de $W_n(A)$, morphisme que nous noterons toujours $\wp$ (ou $\wp_n$ si confusion) :

$$\begin{array}{rccc} \wp : & W_n(A) & \to & W(A) \\ & (x_0, ..., x_{n-1}) & \mapsto & (x_0^p, ..., x_{n-1}^p) - (x_0, x_1, ...). \end{array}$$

Exemple 1.4. *D'après l'exemple 1.2 il est facile de calculer le premier coefficient de $\wp(x)$ pour tout vecteur $x = (x_0, x_1, ...)$ dans $W_n(A)$:*

$$\wp(x) = (x_0^p - x_0, *, *, ...) = (\wp(x_0), *, *, ...)$$

Dans toute la suite, nous nous restreignons au cas où A est un corps de caractéristique p et nous adopterons la notation $A = K$. Il vient alors deux résultats cruciaux concernant l'endomorphisme $\wp$ de $W_n(K)$. Le premier donne la surjectivité de $\wp$ sur une clôture séparable de K :

Proposition 1.13. *Soit K un corps de caractéristique p. Fixons une clôture séparable de K, désignée par K^{sep}. Pour tout vecteur x de $W_n(K)$ il existe un vecteur ξ dans $W_n(K^{sep})$ tel que $\wp(\xi) = x$.*

Preuve : La preuve se fait par récurrence sur $n \geq 1$.
Si $n = 1$, alors $W_n(K) = K$ et $\wp$ est le polynôme $X^p - X$ séparable sur K, d'où l'existence d'une solution ξ dans $K^{sep} = W_1(K^{sep})$ telle que $\wp(\xi) = x$.
Maintenant, supposons que pour un entier $n \geq 1$ la propriété est satisfaite. Soit $(x_0, ..., x_n)$ un vecteur de $W_{n+1}(K)$. On distingue alors deux cas :

- soit $x_0 = 0$: par induction il existe $\xi := (\xi_1, ..., \xi_n)$ dans $W_n(K^{sep})$ tel que $\wp(\xi_1, ..., \xi_n) = (x_1, ..., x_n)$. D'où :

$$\begin{aligned} x &= V(x_1, \cdots, x_n) \\ &= V(\wp(\xi)) \\ &= \wp(V(\xi)) \\ &= \wp(0, \xi_1, ..., \xi_n) \end{aligned}$$

puisque les applications V et $\wp$ commutent de façon évidente (voir également la propriété 1.16). Puisque le vecteur $(0, \xi_1, \cdots, \xi_n)$ est dans $W_{n+1}(K^{sep})$ par hypothèse, le résultat est démontré pour x.

- soit $x_0 \neq 0$: il existe $a \in k^{sep}$ tel que $x_0 = \wp(a)$ d'après le cas $n = 1$. Ainsi x s'écrit $(\wp(a), x_1, ..., x_n)$, d'où l'équivalence :

$$x \in \wp(W_{n+1}(K^{sep})) \Leftrightarrow (\wp(a), x_1, ..., x_n) - \wp(a, 0, ..., 0) \in \wp(W_{n+1}(K^{sep})$$

puisque $\wp$ est un morphisme de groupes.
Or d'après l'exemple 1.4, la première composante de $(\wp(a), x_1, ..., x_n) - \wp(a, 0, ..., 0)$ est $\wp(a) - \wp(a)$ donc nulle. On est donc ramené au cas précédent, c'est-à-dire x appartient bien à $\wp(W_{n+1}(K^{sep}))$, ce qui termine la preuve. ◇

Le second résultat concerne le noyau de $\wp$ sur $W(K)$:

Proposition 1.14. *Pour tout entier $n \geq 1$, le noyau de $\wp$ sur $W_n(K)$ est $W_n(\mathbb{F}_p)$.*

Preuve : D'abord, l'anneau $W_n(\mathbb{F}_p)$ est clairement inclus dans le noyau de $\wp$ puisque F est l'identité sur $\mathbb{F}_p$.
Réciproquement, montrons l'autre inclusion par récurrence sur $n \geq 1$. Si $n = 1$, $W_1(K)$ est le corps K de caractéristique p, il satisfait donc :

$$\forall \xi \in K \ : \ \xi^p - \xi = 0 \Leftrightarrow \xi \in \mathbb{F}_p.$$

Cela signifie que le noyau de $\wp$ sur $W_1(K)$ est précisément $W_1(\mathbb{F}_p) = \mathbb{F}_p$.
Maintenant supposons la propriété établie pour un entier $n \geq 1$ et considérons le noyau de $\wp$ sur $W_{n+1}(K)$. Soit $\xi = (\xi_0, ..., \xi_n) \in W_{n+1}(K)$ un élément de ce noyau. A nouveau, nous distinguons deux possibilités :

- soit $\xi_0 = 0$: par un argument analogue à la preuve précédente, nous montrons que $\wp(\xi_1, ..., \xi_n)$ est nul dans $W_n(K)$. Ainsi, par hypothèse, $(\xi_1, ..., \xi_n)$ of $W_n(K)$ a tous ses coefficients dans $\mathbb{F}_p$, c'est-à-dire : $\xi \in W_{n+1}(\mathbb{F}_p)$.

- soit $\xi_0 \neq 0$: d'après l'exemple 1.4 nous avons toujours $\wp(\xi_0) = 0$ et donc $\xi_0 \in \mathbb{F}_p$. Par la proposition 1.9 et après troncation, il vient dans $W_{n+1}(K)$:

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

d'où :

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

En particulier, cela implique :

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

puisque $(\xi_0, 0, ..., 0) \in W_{n+1}(\mathbb{F}_p)$ et donc, d'après le cas précédent, ξ est dans $W_{n+1}(\mathbb{F}_p)$.
Ainsi, par récurrence, le noyau de $\wp$ sur $W_n(K)$ est $W_n(\mathbb{F}_p)$ pour tout $n \geq 1$. $\diamond$

En conséquence, les solutions de l'équation $\wp(\xi) = x$ pour un vecteur $x \in W_n(K)$ diffèrent toutes par un vecteur de Witt à coefficients dans $\mathbb{F}_p$, et il y a exactement p^n tels vecteurs. D'où la nécessité d'un étude précise des anneaux $W(\mathbb{F}_p)$ et$W_n(\mathbb{F}_p)$, ce que nous ferons dans le sous-paragraphe 1.3.3. Mais avant, développons un autre résultat qui nous permettra de généraliser aux vecteurs de Witt les arguments de la preuve du théorème initial d'Artin-Schreier.

1.3.2 Théorème de Hilbert 90 dans $W_n(K)$

Nous désignons toujours par K un corps de caractéristique p. Soit $n \geq 1$ un entier, nous nous intéressons ici à un théorème semblable à la version additive du théorème 90 de Hilbert pour les vecteurs de Witt, version qui est le point clef dans la preuve du théorème d'Artin-Schreier décrivant les extensions cycliques de degré p sur K. Le résultat qui suit sera de même importance dans le chapitre suivant pour l'étude générale du groupe de Galois des extensions d'Artin-Schreier-Witt d'exposant p^n.

Soit L une extension finie sur K, soit G son groupe de Galois. Commençons par une définition :

Définition 1.7. *Pour chaque K-automorphisme σ de G et pour tout vecteur de Witt x dans $W_n(L)$ on note $\sigma.x$ le vecteur de $W_n(L)$ défini par :*

$$\sigma.x := (\sigma(x_0), \sigma(x_1), ..., \sigma(x_{n-1})).$$

D'où la version additive du théorème 90 de Hilbert pour les vecteurs de Witt de longueur n sur K :

Théorème 1.3. *Soit K un corps de caractéristique p. Soit L une extension galoisienne finie sur K de groupe $G = Gal(L/K)$. Alors, pour tout entier $n \geq 1$, le premier groupe de cohomologie correspondant aux vecteurs de Witt de longueur n est trivial :*

$$H^1(Gal(L/K), W_n(L)) = 0.$$

Preuve : Soit f un 1-cocycle de G dans $W_n(L)$, c'est-à-dire une fonction de G dans $W_n(L)$ telle que pour tous σ, τ dans G : $f(\sigma.\tau) = \tau f(\sigma) + f(\tau)$. Il s'agit de montrer que f est aussi un cobord, c'est-à-dire qu'il existe x dans $W_n(L)$ tel que :

$$\forall \sigma \in G \quad f(\sigma) = x - \sigma(x)$$

Soit $y = (y_0, y_1, ..., y_{n-1})$ un élément de $W_n(L)$ satisfaisant $tr_k^L(y_0) \neq 0$: l'existence d'un tel élément est due à l'indépendance linéaire sur L de tous les K-automorphismes de L (cf ([35], Chap. VI, §4)). On définit la trace de y de L dans K par :

$$tr(y) = \sum_{\sigma \in G} \sigma(y) = \sum_{\sigma \in G} (\sigma y_0, \sigma y_1, ..., \sigma y_{n-1}) = (tr(y_0), *, ..., *)$$

Puisque $tr(y_0)$ est à la fois la première composante de $tr(y)$ et une unité de L, $tr(y)$ est aussi une unité de $W_n(L)$ par la proposition 1.11. On pose alors dans $W_n(K)$:

$$x := \frac{1}{tr(y)} \sum_{\tau \in G} f(\tau)\tau(y)$$

Pour tout σ in G, il vient :

$$\begin{aligned}\sigma(x) &= \frac{1}{\sigma(tr(y))}\sum_{\tau\in G}\sigma(f(\tau))\sigma(\tau(y)) \\ &= \frac{1}{tr(y)}\sum_{\tau\in G}(f(\sigma\tau)-f(\sigma)).\sigma\tau(y) \\ &= \frac{1}{tr(y)}\sum_{\tau\in G}f(\sigma\tau)\sigma\tau(y) - \frac{1}{tr(y)}\sum_{\tau\in G}f(\sigma)\sigma\tau(y) \\ &= \frac{1}{tr(y)}\sum_{\psi\in G}f(\psi)\psi(y) - \frac{f(\sigma)}{tr(y)}\sum_{\psi\in G}\psi(y) \\ &= x - f(\sigma)\end{aligned}$$

D'où $f(\sigma) = x - \sigma(x)$, comme désiré. ◇

1.3.3 Vecteurs de Witt sur $\mathbb{F}_p$

Nous clôturons ce chapitre par une description explicite des vecteurs de Witt sur le corps fini $\mathbb{F}_p$ à p éléments. Pour tout entier $n \geq 1$ rappelons l'existence d'un isomorphisme canonique d'anneaux :

$$\mathcal{F}_n \ : \ W_n(\mathbb{F}_p) \longrightarrow \mathbb{Z}/p^n\mathbb{Z},$$

donné par :

$$(x_0, x_1, ..., x_{n-1}) \mapsto \bar{x_0} + p\bar{x_1} + ... + \bar{x_{n-1}}p^{n-1} \mod p^n,$$

où chaque $\bar{x_k} \in \mathbb{Z}$ désigne l'unique représentant modulo p de x_k dans $\{0, ..., p-1\}$.
Cet isomorphisme transforme l'opérateur shift V en la mutliplication par p, notée p, selon le diagramme commutatif suivant :

$$\begin{array}{ccc} W_n(\mathbb{F}_p) & \xrightarrow{\mathcal{F}_n} & \mathbb{Z}/p^n\mathbb{Z} \\ \downarrow V & & \downarrow \mathbf{p} \\ W_{n+1}(\mathbb{F}_p) & \xrightarrow{\mathcal{F}_{n+1}} & \mathbb{Z}/p^{n+1}\mathbb{Z} \end{array}$$

En outre, pour tout $n \geq 1$, nous avons un autre diagramme commutatif :

$$\begin{array}{ccc} W_{n+1}(\mathbb{F}_p) & \xrightarrow{\mathcal{F}_{n+1}} & \mathbb{Z}/p^{n+1}\mathbb{Z} \\ \downarrow t_n & & \downarrow \mathrm{red}_n \\ W_n(\mathbb{F}_p) & \xrightarrow{\mathcal{F}_n} & \mathbb{Z}/p^n\mathbb{Z} \end{array}$$

où t_n est le morphisme de troncation et où red_n désigne la réduction modulo p^n. Alors, en munissant les anneaux $\mathbb{Z}/p^n\mathbb{Z}$ et$W_n(\mathbb{F}_p)$ pour tout $n \geq 1$ de la topologie discrète, les isomorphismes $\mathcal{F}_n$ deviennent des homeomorphismes, d'où un isomorphisme de systèmes projectifs :

$$\varprojlim W_n(\mathbb{F}_p) \xrightarrow{\simeq} \varprojlim \mathbb{Z}/p^n\mathbb{Z}.$$

Par le théorème 1.2 il en résulte un isomorphisme d'anneaux topologiques :

$$W(\mathbb{F}_p) \xrightarrow{\simeq} \mathbb{Z}_p.$$

Ici $\mathbb{Z}_p$ est muni de la topologie p-adique qui est la topologie naturellement induite du système projectif $(\mathbb{Z}/p^n\mathbb{Z}, \mathrm{red})_n$. De plus, le précédent isomorphisme étant canonique, il nous autorise les identifications $W_n(\mathbb{F}_p) = \mathbb{Z}/p^n\mathbb{Z}$ pour tout $n \geq 1$, ainsi que $W(\mathbb{F}_p) = \mathbb{Z}_p$.
Nous résumons tout ceci dans la proposition suivante :

Proposition 1.15. *Les vecteurs de Witt à coefficients dans $\mathbb{F}_p$ satisfont :*

$$W(\mathbb{F}_p) = \mathbb{Z}_p$$

et pour tout $n \geq 1$:

$$W_n(\mathbb{F}_p) = \mathbb{Z}/p^n\mathbb{Z}.$$

De plus, l'anneau de Witt $W(\mathbb{F}_p)$ est muni de la topologie p-adique pour laquelle il est compact.

Il est alors intéressant de vérifier la proposition 1.8 pour $W(\mathbb{F}_p)$. En effet, de ce qui précède, il vient simultanément :

$$W_n(\mathbb{F}_p) = \mathbb{Z}/p^n\mathbb{Z},$$

et aussi :

$$W(\mathbb{F}_p)/V^nW(\mathbb{F}_p) = \mathbb{Z}_p/p^n\mathbb{Z}_p.$$

L'isomorphisme naturel :

$$\mathbb{Z}/p^n\mathbb{Z} \xrightarrow{\simeq} \mathbb{Z}_p/p^n\mathbb{Z}_p$$

corrobore donc l'isomorphisme de la proposition 1.8 :

$$W_n(\mathbb{F}_p) \xrightarrow{\simeq} W(\mathbb{F}_p)/V^nW(\mathbb{F}_p).$$

D'après ([60], Chap.II, §5) la proposition 1.15 se généralise à tout corps parfait de caractéristique p. Plus précisément, Serre énonce le résultat suivant :

Théorème 1.4. *Soit K un corps parfait de caractéristique p, l'anneau de Witt $W(K)$ est un p-anneau strict de corps résiduel K.*

Concrètement, cela signifie que $W(K)$ est un anneau complet pour une valuation discrète de corps résiduel K, d'idéal maximal engendré par p, et que $W(K)$ est caractérisé par ces propriétés via un unique isomorphisme.
En particulier, si $K = \mathbb{F}_p$, on retrouve une nouvelle fois l'identification $W(\mathbb{F}_p) = \mathbb{Z}_p$ par unicité du p-anneau strict pour un corps résiduel de caractéristique p donné.

De plus, grâce à ce théorème, Serre établit une formule qui sera d'un intérêt particulier pour le théorème 2.1 du chapitre 2 mais aussi dans le chapitre 4 :

Proposition 1.16. *Soit A un anneau de caractéristique p. Sur l'anneau de Witt $W(A)$ on a :*

$$V \circ F = F \circ V = \mathbf{p},$$

où $\mathbf{p}$ désigne la mutliplication par p.
En particulier, il vient : $V \circ \wp = \wp \circ V$.

Preuve : Il est facile de voir que V et$F$ commutent par la proposition 1.9.
Quant à la relation $V \circ F = \mathbf{p}$, sa preuve est basée sur l'identification $x = \sum_{i=0}^{\infty}\{x_i^{p^{-i}}\}p^i$ pour tout vecteur $x \in W(A)$ pusique A est de caractéristique p (cf. [60], Chap.II, §6).
Cependant, cette relation se montre aussi *à la main* à partir des relations de récurrence $(Vx)^{(n)} = px^{(n-1)}$ et $(Fx)^{n-1} = x^{(n)} - p^n x_n$ ainsi que de la proposition 1.3 pour l'addition de Witt. $\diamond$

Chapitre 2

Pro-p extensions abéliennes en caractéristique p

Soit $p > 0$ un nombre premier et soit K un corps de caractéristique p.

Ce second chapitre est l'étude des pro-p extensions de K d'un point de vue essentiellement galoisien. Le cadre est celui de la théorie d'Artin-Schreier, à distinguer de la théorie de Kummer dans laquelle les degrés des extensions sont premiers à la caractéristique : cette théorie a initialement été développée dans un article commun d'Artin et Schreier [7] en 1927 pour décrire le groupe de Galois des extensions cycliques de degré p sur K. L'outil essentiel qui permettra de passer des extensions d'exposant p aux extensions d'exposant p^n pour $n \geq 2$ sera la manipulation des vecteurs de Witt. C'est pourquoi, nous parlerons d'avantage de la théorie d'Artin-Schreier-Witt pour évoquer l'étude galoisienne des pro-p extensions de K.

Plus précisément, il s'agit dans ce chapitre de généraliser le théorème initial d'Artin-Schreier en donnant une description explicite du groupe de Galois des extensions abéliennes finies puis infinies d'exposant p^n sur K, pour tout entier $n \geq 1$. Le but ultime est de donner une étude complète de la pro-p extension abélienne maximale de K. Toutes les extensions considérées ici sont contenues dans une clôture séparable K^{sep} de K que nous fixerons dans la suite.

Cette généralisation est menée progressivement tout au long du présent chapitre. Le paragraphe 2.1 concerne d'abord les extensions d'Artin-Schreier-Witt finies de K, c'est-à-dire les extensions abéliennes finies d'exposant divisant p^n pour tout $n \geq 1$ (cf. théorème 2.2). Ensuite, le paragraphe 2.2 traite des extensions d'Artin-Schreier-Witt infinies en calculant explicitement le groupe de Galois des extensions abéliennes maximales d'exposant p^n sur K (cf. corollaire 2.1), puis par passage à la limite, celui de la pro-p extension abélienne maximale (cf. théorème 2.4).

Les preuves que nous proposons sont assez proches de celles de l'article initial d'Artin et Schreier : le polynôme $X^p - X$ est remplacé par l'homomorphisme de groupes $\wp$ sur $W(K)$ et le théorème 90 de Hilbert devient le théorème 1.3 du chapitre précédent. La principale innovation réside dans l'introduction des vecteurs de Witt dont la manipulation représente la difficulté de ce chapitre mais aussi et surtout sa réelle motivation. Tous ces outils ont été développés dans le chapitre 1.

Si la plupart des résultats de ces deux paragraphes sont maintenant courants dans la littérature galoisienne, ils le sont de façon éparse et leurs preuves sont rarement exposées de façon complète. C'est pourquoi nous avons tenu à les détailler toutes ici afin de présenter un tableau complet de la théorie de Galois des extensions d'Artin-Schreier-Witt.

Le paragraphe 2.3, quant à lui, pousse cette étude plus loin avec la description du groupe de Galois G_{p^∞} de la pro-p extension abélienne maximale de K comme module sur l'anneau $\mathbb{Z}_p$ des entiers p-adiques. En particulier, nous développerons la question de savoir si ce module est libre sur $\mathbb{Z}_p$: c'est le théorème 2.5, notre première contribution à cette riche théorie. Il affirme que G_{p^∞}

est libre en tant que $\mathbb{Z}_p$-module si et seulement si le groupe de l'extension abélienne maximale d'exposant p sur K est de dimension finie comme $\mathbb{F}_p$-espace vectoriel. Les outils principaux en sont une version topologique du lemme de Nakayama et quelques propriétés des nombres cardinaux.

L'étude des extensions infinies d'Artin-Schreier-Witt conduit naturellement à des questions topologiques. A ce titre, rappelons que tout groupe de Galois est muni de la topologie de Krull. De plus, chaque anneau $W_n(\mathbb{F}_p)$, identifié à $\mathbb{Z}/p^n\mathbb{Z}$, est muni de la topologie discrète et l'anneau de Witt $W(\mathbb{F}_p)$, canoniquement isomorphe à $\mathbb{Z}_p$, est muni de la topologie induite du produit $\prod_n W_n(K)$, c'est-à-dire de la topologie p-adique, conformément au corollaire 1.2 du chapitre 1.

2.1 Extensions finies d'Artin-Schreier-Witt

Ce paragraphe concerne la théorie de Galois dans les extensions abéliennes finies d'exposant p^n sur K, pour tout entier $n \geq 1$, que nous appelons extensions finies d'Artin-Schreier-Witt.

2.1.1 Extensions cycliques de degré p^n

Fixons un entier $n \geq 1$ et considérons d'abord les extensions cycliques de degré p^n sur K.

Les notations sont celles du chapitre 1. Pour un vecteur de Witt $x \in W_n(K)$, nous désignerons également par $K(\wp^{-1}(x))$ l'extension $K(\zeta_0, ..., \zeta_{n-1})$ où $\zeta = (\zeta_0, ..., \zeta_{n-1})$ est un vecteur dans $W_n(K^{\text{sep}})$ tel que $\wp(\zeta) = x$.

Le théorème qui suit est la généralisation directe du théorème d'Artin-Schreier. Bien plus, il représente un résultat clef pour tout ce qui suit et c'est pourquoi nous avons décidé de conserver la preuve aussi détaillée.

Théorème 2.1 (Extensions cycliques de degré p^n)**.** *Soit K un corps de caractéristique $p > 0$ et soit $n \geq 1$ un entier positif. On a :*

a). *Pour $x = (x_0, ..., x_{n-1}) \in W_n(K)$, soit l'équation $\wp(\xi) = x$ n'admet aucune solution dans $W_n(K)$, soit elle admet une solution dans $W_n(K)$ auquel cas toutes ses solutions sont dans $W_n(K)$ et il y a p^n telles solutions.*

b). *Si l'équation n'admet aucune solution dans $W_n(K)$, l'extension $K(\wp^{-1}x)$ est cyclique sur K de degré divisant p^n. Le degré est exactement p^n si et seulement si $x_0 \notin \wp(K)$.*

c). *Réciproquement, si L/K est une extension cyclique de degré p^n, il existe x dans $W_n(K)$ tel que $L = K(\wp^{-1}x)$ et $x_0 \notin \wp(K)$.*

Preuve : **assertion a) :** D'après la proposition 1.14 et puisque $\mathbb{F}_p$ s'injecte dans 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 exactement p^n telles solutions puisqu'elles diffèrent deux à deux par un élément de $W_n(\mathbb{F}_p)$

assertion b) : Supposons maintenant que l'équation n'admet aucune solution. On montre d'abord que l'extension $K(\wp^{-1}x)/K$ est normale. Soit $\xi \in W_n(K(\wp^{-1}x))$ tel que $\wp(\xi) = x$. Soit $\varphi : K(\wp^{-1}x) \to \bar{K}$ un K-morphisme de corps, $\bar{K}$ étant une clôture algébrique de K fixée. Ce morphisme définit fonctoriellement un homomorphisme d'anneaux :

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

en posant :

$$W_n(\varphi)(\xi_0, ..., \xi_{n-1}) = (\varphi(\xi_0), ..., \varphi(\xi_{n-1}))$$

de telle sorte que $W_n(\varphi)_{|W_n(K)} = id_{W_n(K)}$.
Alors, d'après la définition de $\wp$ il vient :

$$\begin{aligned} \wp(W_n(\varphi)(\xi)) &= (W_n(\varphi)(\xi)) - W_n(\varphi)(\xi) \\ &= W_n(\varphi)F(\xi) - W_n(\varphi)(\xi) \end{aligned}$$

car $W_n(\varphi)$ et F agissent linéairement sur les composantes des vecteurs de Witt. D'où :

$$\begin{aligned}\wp(W_n(\varphi)(\xi)) &= W_n(\varphi)(F\xi - \xi)\\ &= W_n(\varphi)(x)\\ &= x\end{aligned}$$

puisque x est dans $W_n(K)$.
Ainsi, d'après la proposition 1.14, $W_n(\varphi)(\xi)$ appartient à $W_n(K(\wp^{-1}x))$ et donc l'application φ fixe globalement $K(\wp^{-1}x)$, ce qui montre que l'extension est normale.
En outre, d'après la proposition 1.13, $K(\wp^{-1}x)$ l'extension est séparable sur K, donc galoisienne.

Montrons ensuite que son groupe de Galois, noté G_n est cyclique et déterminons sont degré.
Par la proposition 1.13 toujours, il existe ξ in $W_n(K^{\text{sep}})$ tel que $\wp(\xi) = x$. De plus, en posant $\xi = (\xi_0, \xi_1, ..., \xi_{n-1})$, alors d'après la remarque 1.4 il vient :

$$\wp(\xi_0) = x_0.$$

Considérons d'abord le groupe G_1 défini par : $G_1 = Gal(K(\wp^{-1}x_0)/K) = Gal(K(\xi_0)/K)$. Puisque G_1 agit sur les racines du polynômes $\wp(X) - x_0 = X^p - X - x_0$ et d'après la proposition 1.14, nous avons :

$$\forall \sigma \in G_1 \ , \ \sigma(\xi_0) - \xi_0 \in W_1(\mathbb{F}_p)$$

avec $W_1(\mathbb{F}_p) = \mathbb{F}_p$.
On définit alors l'application suivante :

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

C'est un morphisme de groupes, en effet :

$$\begin{aligned}\forall \sigma, \tau \in G_1 \quad \varphi_1(\sigma\tau) &= \sigma\tau(\xi_0) - \xi_0\\ &= \sigma(\tau(\xi_0) - \xi_0) + \sigma(\xi_0) - \xi_0\\ &= \varphi_1(\tau) + \varphi_1(\sigma)\end{aligned}$$

où σ désigne un K-isomorphisme de corps.
Bien plus, nous avons :

$$\begin{aligned}\forall \sigma \in G_1 \quad \sigma(\xi_0) - \xi_0 = 0 \quad &\Rightarrow \quad \sigma(\xi_0) = \xi_0\\ &\Rightarrow \quad \sigma = id\end{aligned}$$

d'où l'injectivité de φ_1.
De même, pour tout $n \geq 1$, on peut définir l'application suivante :

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

avec : $\sigma(\xi) - \xi = (\sigma(\xi_0), \sigma(\xi_1), ..., \sigma(\xi_{n-1})) - (\xi_0, \xi_1, ..., \xi_{n-1}) = (\varphi_1(\xi_0), *, ...)$.
En développant un argument semblable au précédent, il est alors facile de montrer que φ_n est aussi un homomorphisme de groupes injectif.
D'où le diagramme suivant :

$$\begin{array}{ccc}G_n & \xrightarrow{\varphi_n} & W_n(\mathbb{F}_p)\\ \downarrow{\scriptstyle r_n} & & \downarrow{\scriptstyle t_n}\\ G_1 & \xrightarrow{\varphi_1} & W_1(\mathbb{F}_p).\end{array}$$

Ici, r_n est l'application de restriction :

$$\begin{array}{rccc}r_n : & G_n & \longrightarrow & G_1\\ & \sigma & \mapsto & \sigma_{|K(\xi_0)}\end{array}$$

et t_n l'application de troncation :

$$\begin{array}{rccc} t_n : & W_n(\mathbb{F}_p) & \longrightarrow & W_1(\mathbb{F}_p) \\ & (x_0, ..., x_{n-1}) & \mapsto & x_0 \end{array}$$

Ces deux morphismes sont surjectifs.
Clairement, le diagramme commute puisque pour tout $\sigma \in G_n$ on a :

$$t_n \circ \varphi_n(\sigma) = t_n(\sigma(\xi) - \xi) = t_n(\sigma(\xi_0) - \xi_0, *, ...) = \sigma(\xi_0) - \xi_0$$

et aussi :

$$\varphi_1 \circ r_n(\sigma) = \varphi_1(\sigma_{|k(\xi_0)}) = \sigma_{|k(\xi_0)} - \xi_0 = \sigma(\xi_0) - \xi_0.$$

On distingue alors deux cas précisément :

- cas 1 : $x_0 \notin \wp(K)$, ce qui signifie que l'extension $K(\xi_0)/K$ est de degré p . Dans ce cas, comme G_1 agit transitivement sur les racines de $\wp(X) - x_0$ et d'après la proposition 1.14, on a $\varphi_1(G_1) = W_1(\mathbb{F}_p) = \mathbb{F}_p$ et donc φ_1 est surjective. Par commutativité du diagramme, φ_n est surjective aussi, c'est donc un isomorphisme de groupes :

$$\varphi_n : G_n \xrightarrow{\simeq} W_n(\mathbb{F}_p)$$

Comme $W_n(\mathbb{F}_p) \simeq \mathbb{Z}/p^n\mathbb{Z}$, cela montre que G_n est cylcique d'ordre exactement p^n.

- cas 2 : soit $x_0 \in \wp(k)$, c'est-à-dire $\xi_o \in K$. Dans ce cas, $G_1 = \{id\}$ et φ_1 est trivial. L'homomorphisme φ_n ne peut donc être surjectif et le groupe de Galois G_n est isomorphe à un sous-groupe strict du groupe cyclique $\mathbb{Z}/p^n\mathbb{Z}$, d'où la preuve de l'assertion b).

assertion c) : Réciproquement, soit L/K une extension cyclique de degré p^n. Notons G son groupe de Galois. On affirme :

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

En effet, nous avons la suite exacte :

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

Puisque $H^1(G, W_n(L)) = 0$ d'après le théorème 1.3, la suite exacte de cohomologie s'écrit :

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

où φ envoie x sur $\{\sigma \mapsto \sigma(\xi) - \xi\}$ avec $\xi \in W_n(L)$ tel que $\wp(\xi) = x$.
Comme 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 G et $W_n(\mathbb{F}_p)$ sont tous deux cycliques de degré p^n et donc $H^1(G, W_n(\mathbb{F}_p))$ aussi. Alors, en posant $PW := \wp(W_n(L)) \cap W_n(K)$, le quotient $PW/\wp(W_n(K))$ est cyclique d'ordre p^n et son groupe dual est canoniquement isomorphe à $\mathrm{Hom}(PW, W_n(\mathbb{F}_p))$.

Soit x un vecteur dans PW tel que $x + \wp(W_n(K))$ engendre $PW/\wp(W_n(K))$. Nécessairement : $x_o \notin \wp(K)$.
Maintenant, montrons que $L = K(\wp^{-1}x)$. Clairement, comme chaque solution ξ de l'équation $\wp(\xi) = x$ est dans $W_n(L)$, on a : $K(\wp^{-1}x) \subset L$.
Pour montrer l'autre inclusion, considérons l'accouplement suivant :

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

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 (cf. [35], Chap. I,§9), puisque les noyaux sont triviaux et comme G est fini, on obtient un isomorphisme de groupes :

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

Chaque automorphisme $\sigma \in G$ tel que $\sigma_{|K(\wp^{-1}x)} = id$ satisfait donc : $\delta(\sigma) = id$ c'est-à-dire $\sigma = id_{|L}$ puisque δ est un isomorphisme. D'où $Gal(L/K(\wp^{-1}x)) = \{id\}$, i.e. $L = K(\wp^{-1}x)$, ce qu'il fallait démontrer. $\diamond$

Ainsi, les extensions cycliques de degré p^n sur le corps K sont précisément les extensions du type $K(\wp^{-1}x)$ pour un certain vecteur de Witt x dans $W_n(k)$ tel que $x_0 \notin \wp(K)$.

2.1.2 Extensions abéliennes finies d'exposant au plus p^n

Nous développons ici l'analogue de la théorie de Kummer pour les extensions abéliennes finies d'exposant divisant p^n sur le corps K de caractéristique p.

L'étape qui suit le théorème 2.1 est le résultat suivant :

Théorème 2.2 (Extensions abéliennes finies d'exposant divisantp^n)**.** *Soit K un corps de caractéristique $p > 0$ et soit $n \geq 1$ un entier positif. Soit B_n un sous-groupe de $W_n(K)$ contenant $\wp(W_n(K))$ avec un indice fini. Notons K_{B_n} l'extension $K(\wp^{-1}B_n)$, c'est-à-dire le compositum de toutes les extensions $K(\wp^{-1}x)$ lorsque x parcourt B_n. On a :*

a). *L'extension K_{B_n}/K est une extension galoisienne, abélienne finie et d'exposant divisant p^n.*

b). *Réciproquement, si L/K est une extension abélienne finie d'exposant divisant p^n, il existe un sous-groupe B_n de $W_n(K)$ satisfaisant les propriétés précédentes et tel que $L = K_{B_n}$.*

Preuve : **assertion a).** D'après le théorème 2.1, pour chaque vecteur x de B_n, l'extension $K(\wp^{-1}x)$ est galoisienne sur K et cyclique de degré p^d avec $d \leq n$. Alors, en tant que compositum, l'extension K_{B_n}/K est aussi galoisienne et d'exposant divisant p^n, ce qui montre l'assertion a).

assertion b). Réciproquement, si L/K est une extension abélienne finie d'exposant divisant p^n et de groupe G, le théorème 2.1 induit la suite exacte :

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

où $\wp(W_n(L)) \cap W_n(K)/\wp(W_n(K))$ est d'exposant p^n.
Posons $B_n := \wp(W_n(L)) \cap W_n(K)$. Clairement $K_{B_n} \subset L$.
Pour montrer l'autre inclusion, considérons l'accouplement suivant :

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

donné par :

$$(x + \wp(W_n(K)), \sigma) \mapsto \sigma(\xi) - \xi,$$

pour un certain vecteur ξ de $W_n(L)$ tel que $\wp(\xi) = x$. Cet accouplement ne dépend pas du choix de ξ : en effet, si $\wp(\xi') = x$ aussi, alors $\sigma(\xi) - \xi = \sigma(\xi') - \xi'$ puisque ξ et ξ' diffèrent par un élément de $W_n(\mathbb{F}_p)$ (cf. proposition 1.14).
On en déduit un isomorphisme de groupes :

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

Ainsi, pour chaque $\sigma \in G$ tel que $\sigma_{|K_{B_n}} = id$, il vient : $\delta(\sigma) = id$. D'où $\sigma = id_{|L}$ puisque δ est un isomorphisme, donc $Gal(L/K_{B_n}) = \{id\}$, c'est-à-dire $L = K_{B_n}$, comme désiré. $\diamond$

Nous allons déduire du théorème précédent une description explicite du groupe de Galois des extensions finies d'Artin-Schreier-Witt sur K. C'est précisément ce résultat qui nous permettra de donner le groupe de Galois des extensions maximales d'Artin-Schreier-Witt dans le paragraphe suivant :

Corollaire 2.1. *Soit L_n une extension abélienne finie d'exposant divisant p^n sur K. D'après le théorème 2.2, il existe un sous-groupe B_{L_n} de $W_n(K)$ tel que $L_n = K(\wp^{-1}(B_{L_n}))$. Alors on a un isomorphisme de groupes :*

$$\begin{array}{ccc} Gal(L_n/K) & \xrightarrow{\simeq} & Hom(B_{L_n}/\wp(W_n(K)), W_n(\mathbb{F}_p)) \\ \sigma & \mapsto & (x + \wp(W_n(K)) \mapsto \sigma(\xi) - \xi) \end{array}$$

où ξ est un vecteur de $W_n(K^{sep})$ tel que $\wp(\xi) = x$.

Notons que cet isomorphisme est indépendant du choix de ξ comme nous l'avons déjà indiqué dans la preuve de l'assertion b) du théorème 2.2.

Preuve : C'est essentiellement la preuve de l'assertion b) du théorème 2.2. ◇

Remarque 7. *Si L/K est une extension abélienne finie d'exposant p^n, on a un isomorphisme de groupes topologiques semblable à celui du corollaire 2.1 :*

$$\begin{array}{ccc} Gal(L/K) & \xrightarrow{\simeq} & Hom(B_L/\wp(W_n(K)), W_n(\mathbb{F}_p)) \\ \sigma & \mapsto & \{x + \wp(W_n(K)) \mapsto \sigma(\xi) - \xi), \end{array}$$

pour ξ dans $W_n(K^{sep})$ tel que $\wp(\xi) = x$ et où B_L est un sous-groupe de $W_n(K)$ contenant $\wp(W_n(K))$ mais sans indice fini cette fois.
Nous ne montrerons pas ce résultat puisqu'il est sans utilité pour la suite de ce mémoire. Une preuve en est donnée dans mon rapport de DEA, elle s'appuie sur l'égalité suivante :

$$Gal(K_{B_L}/K) = \varprojlim Gal(K_{B_0}/K),$$

lorsque B_0 parcourt l'ensemble des sous-groupes de B_L contenant $\wp(W_n(K))$ avec un indice fini, les notations étant les mêmes que celles du théorème 2.2.

2.2 Extensions maximales d'Artin-Schreier-Witt

Rappelons que la théorie de Galois infinie définit le groupe de Galois G d'une extension infinie L/K comme une limite projective :

$$G = \varprojlim Gal(M/K),$$

où M parcourt l'ensemble des sous-extensions finies de L/K. En particulier, le groupe de Galois d'une extension infinie a la structure d'un groupe profini muni de la topologie dite de Krull pour laquelle une base de voisinages de l'unité est exactement l'ensemble de tous les sous-groupes distingués de G d'indice fini.

Ce paragraphe concerne les extensions infinies d'Artin-Schreier-Witt sur le corps K de caractéristique $p > 0$. Plus précisément, pour un entier $n \geq 1$, nous déterminons le groupe de Galois de l'extension abélienne maximale d'exposant p^n sur K. Notons G_{p^n} ce groupe, rappelons qu'il est donné par la limite projective :

$$G_{p^n} = \varprojlim Gal(L_n/K),$$

lorsque L_n parcourt l'ensemble des extensions abéliennes finies d'exposant divisant p^n sur K. Utilisant le corollaire 2.1, il vient alors :

Théorème 2.3 (Extension abélienne maximale d'exposant p^n)**.** *Soit K un corps de caractéristique $p > 0$ et soit $n \geq 1$ un entier positif. On a un isomorphisme canonique de groupes topologiques :*

$$\begin{array}{rccc} \mathfrak{as}_n : & G_{p^n} & \xrightarrow{\simeq} & Hom(W_n(K)/\wp(W_n(K)), W_n(\mathbb{F}_p)) \\ & \sigma & \mapsto & \{x + \wp(W_n(K)) \mapsto \sigma(\xi) - \xi), \end{array}$$

où $\xi \in W_n(K^{sep})$ est tel que $\wp(\xi) = x$.
Ici, le groupe de Galois G_{p^n} est muni de la topologie de Krull et le groupe

$$Hom(W_n(K)/\wp(W_n(K)), W_n(\mathbb{F}_p))$$

de la topologie induite du produit $\prod_n W_n(\mathbb{F}_p)$ où chaque $W_n(\mathbb{F}_p) = \mathbb{Z}/p^n\mathbb{Z}$ est discret.

Comme dans le corollaire 2.1, chaque isomorphisme $\mathfrak{as}_n(x)$ ne dépend pas du choix de ξ. Pour tout $n \geq 1$, $\mathfrak{as}_n$ sera appelé le $n$ème isomorphisme d'Artin-Schreier-Witt.

Preuve : Si L_n/K est une extension abélienne finie d'exposant divisant p^n, on a d'après le corollaire 2.1 un isomorphisme de groupes :

$$Gal(L_n/K) \xrightarrow{\simeq} \mathrm{Hom}(B_{L_n}/\wp(W_n(K)), W_n(\mathbb{F}_p)).$$

Alors, pour toute sous-extension $M_n \subset L_n$, le diagramme suivant est commutatif :

$$\begin{array}{ccc} Gal(L_n/K) & \xrightarrow{\simeq} & \mathrm{Hom}(B_{L_n}/\wp(W_n(K)), W_n(\mathbb{F}_p)) \\ \Big\downarrow{\scriptstyle r_{LM}} & & \Big\downarrow{\scriptstyle h_{LM}} \\ Gal(M_n/K) & \xrightarrow{\simeq} & \mathrm{Hom}(B_{M_n}/\wp(W_n(K)), W_n(\mathbb{F}_p)) \end{array}$$

où les flèches verticales r_{LM} et h_{LM} sont les applications de restriction.
Les groupes $Gal(L_n/K)$ et $W_n(\mathbb{F}_p)$ étant compacts pour la topologie discrète car finis et le groupe $\mathrm{Hom}(B_{L_n}/\wp(W_n(K)), W_n(\mathbb{F}_p))$ étant compact pour la topologie induite du produit $\prod W_n(\mathbb{F}_p)$, on en déduit par passage à la limite projective un isomorphisme de groupes topologiques :

$$G_{p^n} \xrightarrow{\simeq} \varprojlim \mathrm{Hom}(B_{L_n}/\wp(W_n(K)), W_n(\mathbb{F}_p)),$$

où la limite projective est prise respectivement aux applications de restriction comme applications de transition et sur tous les sous-groupes B_{L_n} de $W_n(K)$ contenant $\wp(W_n(K))$ avec un indice fini conformément à la correspondance du théorème 2.2.
Alors, par la propriété universelle des limites projectives et directes, ceci induit un isomorphisme de groupes topologiques :

$$G_{p^n} \xrightarrow{\simeq} \mathrm{Hom}(\varinjlim B_{L_n}/\wp(W_n(K)), W_n(\mathbb{F}_p)).$$

Or $W_n(K)$ est clairement la réunion de tous les sous-groupes B_{L_n} et le système projectif $\{B_{L_n}, h_{LM}\}$ est stable par union finie, ainsi on a l'égalité :

$$\varinjlim B_{L_n} = W_n(K).$$

D'où l'isomorphisme de groupes topologiques :

$$G_{p^n} \xrightarrow{\simeq} \mathrm{Hom}(W_n(K)/\wp(W_n(K)), W_n(\mathbb{F}_p)).$$

Notons $\mathfrak{as}_n$ cet isomorphisme. Par construction, pour tout $\sigma \in G_{p^n}$, il est donné par :

$$\mathfrak{as}_n(\sigma) : x + \wp(W_n(K)) \mapsto \sigma(\xi) - \xi,$$

pour un vecteur ξ dans $W_n(K^{\mathrm{sep}})$ tel que $\wp(\xi) = x$. Ceci montre le théorème. ◇

Notation 2. *Dans toute la suite et pour tout entier $n \geq 1$ nous écrirons :*

$$H_{p^n} \;=\; Hom(W_n(K)/\wp(W_n(K)), W_n(\mathbb{F}_p)),$$

de sorte que :

$$\mathfrak{as}_n \;:\; G_{p^n} \xrightarrow{\simeq} H_{p^n}.$$

Remarque 8. *D'après le théorème 2.3 le groupe H_{p^n} est compact car homéomorphe au groupe de Galois G_{p^n}. Un autre argument, n'utilisant pas le théorème, serait de considérer H_{p^n} comme le sous-groupe formé de tous les homomorphismes de $W_n(\mathbb{F}_p)^{W_n(K)/\wp(W_n(K))}$.*
En effet, munissons le groupe $W_n(\mathbb{F}_p)^{W_n(K)/\wp(W_n(K))}$ de la topologie produit pour laquelle il est compact : cette topologie est équivalente à la topologie de la convergence simple. Ainsi, H_{p^n} est un sous-groupe fermé de $W_n(\mathbb{F}_p)^{W_n(K)/\wp(W_n(K))}$ et donc compact.

2.3 Pro-p extension abélienne maximale

A partir du théorème 2.3, il suffit maintenant de passer à la limite projective lorsque n tend vers l'infini cette fois, afin d'obtenir une description explicite du groupe de Galois de la pro-p extension abélienne maximale de K. Notons G_{p^∞} ce groupe, il est donné par le système projectif :

$$G_{p^\infty} = \varprojlim G_{p^n},$$

lorsque $n \to +\infty$, les applications de transition étant les restrictions.

Alors on a :

Théorème 2.4 (Pro-p extension abélienne maximale)**.** *Soit K un corps de caractéristique p. Si G_{p^∞} désigne le groupe de Galois de la pro-p extension abélienne maximale de K, on a un isomorphisme de groupes topologiques :*

$$\mathfrak{as}_\infty \ : \ G_{p^\infty} \xrightarrow{\simeq} Hom(W(K)/\wp(W(K)), W(\mathbb{F}_p)).$$

donné par : :

$$\sigma \ \mapsto \ \{x + \wp(W(K)) \mapsto \sigma(\xi) - \xi,$$

avec ξ dans $W(K^{sep})$ tel que $\wp(\xi) = x$.
Ici G_{p^∞} est muni de la topologie de Krull et $Hom(W(K)/\wp(W(K)), W(\mathbb{F}_p))$ de la topologie induite du produit $\prod W(\mathbb{F}_p)$, où $W(\mathbb{F}_p)$, identifié à $\mathbb{Z}_p$, a la topologie p-adique.

A nouveau, $\mathfrak{as}_\infty(x + \wp(W(K)))$ ne dépend pas du choix de ξ.

Notation 3. *L'isomorphisme de groupes topologiques $\mathfrak{as}_\infty$ sera appelé l'isomorphisme d'Artin-Schreier-Witt.*

Pour démontrer le théorème 2.4 nous avons besoin du lemme suivant :

Lemme 2.1. *Pour chaque entier $n \geq 1$, on a un isomorphisme naturel de groupes topologiques :*

$$H_{p^n} \ \xrightarrow{\simeq} \ Hom(W(K)/\wp(W(K)), W_n(\mathbb{F}_p)),$$

donné par :

$$\varphi \ \mapsto \ \{x + \wp(W(K)) \mapsto \varphi((x_0, ..., x_{n-1}) + \wp(W_n(K)))\},$$

en notant $x = (x_0, x_1, ...)$ dans $W(K)$.
On considère sur $Hom(W(K)/\wp(W(K)), W_n(\mathbb{F}_p))$ est muni de la topologie induite du produit $\prod_{W(K)/\wp(W(K))} W_n(\mathbb{F}_p)$ avec $W_n(\mathbb{F}_p)$ discret.

Preuve : Notons $\mathcal{V}(K)$ le groupe quotient $W(K)/\wp(K)$. On montre d'abord l'existence d'un isomorphisme de groupes :

$$\Theta_n \ : \ W_n(K)/\wp(W_n(K)) \xrightarrow{\simeq} \mathcal{V}(K)/\mathbf{p}^n\mathcal{V}(K),$$

où $\mathbf{p}$ est la mutliplication par p sur $W(K)$, satisfaisant la relation $\mathbf{p} = VF = FV$ d'après la proposition 1.16.
Or, on a l'égalité :

$$\mathbf{p}^n W(K) + \wp(W(K)) = V^n(W(K)) + \wp(W(K)).$$

En effet, pour $x \in W(K)$, la définition de $\wp$ et la proposition 1.16 impliquent :

$$\begin{array}{lll} Vx & = FVx - FVx + Vx & \\ & = VFx - \wp(Vx) & (*) \\ & = \mathbf{p}x - \wp(Vx) & (**). \end{array}$$

Alors, par $(*)$ on a d'abord l'inclusion $V(\wp(W(K)) \subset \wp(W(K))$ et donc V agit sdur le quotient $\mathcal{V}(K)$. Ensuite, d'après $(**)$, V agit comme la mutliplication par p puisque $\wp(Vx)$ est dans $\wp(W(K))$. D'où l'égalité $V = \mathbf{p}$ sur ce quotient, et donc l'image de V^n est égale à l'image de $\mathbf{p}^n$, ce que nous affirmions.
Ainsi, d'après la proposition 1.8, nous obtenons successivement les isomorphismes de groupes suivants :

$$\begin{array}{ll} W_n(K)/\wp(W_n(K)) & \simeq W(K)/(\wp(W(K)) + V^n(W(K))) \\ & \simeq W(K)/(\wp(W(K)) + \mathbf{p}^n W(K)) \\ & \simeq \mathcal{V}(K)/\mathbf{p}^n\mathcal{V}(K), \end{array}$$

comme désiré. En outre, le dernier isomorphisme, que nous noterons Θ_n, est clairement donné par :

$$(x_0, ..., x_{n-1}) \mod \wp(W_n(K)) \mapsto (x + \wp(W(K))) \mod \mathbf{p}^n\mathcal{V},$$

où x est un vecteur de $W(K)$ tel que $t_n(x) = (x_0, ..., x_{n-1})$.

Alors, par dualité, on en déduit un isomorphisme de groupes :

$$H_{p^n} \xrightarrow{\simeq} \mathrm{Hom}(\mathcal{V}(K)/\mathbf{p}^n\mathcal{V}(K), W_n(\mathbb{F}_p)),$$

qui envoie une application f sur $f \circ \Theta_n^{-1}$.
Maintenant, le noyau de chaque homomorphisme de $\mathrm{Hom}(\mathcal{V}(K)/, W_n(\mathbb{F}_p))$ contient $\mathbf{p}^n\mathcal{V}(K)$ puisque $W_n(\mathbb{F}_p) = \mathbb{Z}/p^n\mathbb{Z}$ par la proposition 1.15. Alors, par passage au quotient, cela induit un unique homomorphisme de $\mathrm{Hom}(\mathcal{V}(K)/\mathbf{p}^n\mathcal{V}(K), W_n(\mathbb{F}_p))$, d'où un autre isomorphisme de groupes :

$$\mathrm{Hom}(\mathcal{V}(K), W_n(\mathbb{F}_p)) \xrightarrow{\simeq} \mathrm{Hom}(\mathcal{V}(K)/\mathbf{p}^n\mathcal{V}(K), W_n(\mathbb{F}_p)).$$

et donc, par composition, un isomorphisme de groupes que nous notons Φ_n :

$$\Phi_n \ : \ H_{p^n} \xrightarrow{\simeq} \mathrm{Hom}(\mathcal{V}(K), W_n(\mathbb{F}_p)).$$

Il reste à montrer que Φ_n est un homéomorphisme. Or les groupes H_{p^n} et $\mathrm{Hom}(\mathcal{V}(K), W_n(\mathbb{F}_p))$ sont compacts en tant que sous-groupes fermés de groupes compacts. Il suffit donc de prouver la continuité de l'isomorphisme Φ_n, c'est-à-dire, par la propriété universelle de la topologie produit, de montrer la continuité des applications $\varphi_a \circ \Phi_n$ pour tous a dans $\mathcal{V}(K)$, où chaque φ_a désigne la projection naturelle :

$$\begin{array}{rccc} \varphi_a : & \mathrm{Hom}(\mathcal{V}(K), W_n(\mathbb{F}_p)) & \longrightarrow & W_n(\mathbb{F}_p) \\ & h & \mapsto & h(a). \end{array}$$

Fixons un élément a de $\mathcal{V}(K)$. Soit U un sous-ensemble de $W_n(\mathbb{F}_p)$ (U est nécessairement ouvert puisque $W_n(\mathbb{F}_p)$ est discret), on a :

$$\begin{array}{rcl} (\varphi_a \circ \Phi_n)^{-1}(U) & = & \{f \in H_{p^n} \ : \ \varphi_a \circ \Phi_n(f) \in U\} \\ & = & \{f \in H_{p^n} \ : \ f(\Theta_n^{-1}(a + \mathbf{p}^n\mathcal{V}(K)) \in U\} \\ & = & \{f \in H_{p^n} \ : \ f(\bar{a}) \in U\}, \end{array}$$

où $\bar{a}$ est dans $W_n(K)/\wp(W_n(K))$ et satisfait $\Theta_n(\bar{a}) = a + \mathbf{p}^n\mathcal{V}(K)$.
Alors, si $\tau_{\bar{a}}$ désigne la projection naturelle de H_{p^n} sur $W_n(\mathbb{F}_p)$, nous obtenons :

$$(\varphi_a \circ \Phi_n)^{-1}(U) \ = \ \tau_{\bar{a}}^{-1}(U),$$

et donc $(\varphi_a \circ \Phi_n)^{-1}(U)$ est ouvert dans H_{p^n} puisque $\tau_{\bar{a}}$ est continu pour la topologie produit. D'où la continuité des applications $\varphi_a \circ \Theta_n$, $a \in \mathcal{V}(K)$, ce qu'il fallait démontrer. $\diamond$

D'où la preuve du théorème 2.4 :

Preuve : Rappelons que le groupe G_{p^∞} est la limite projective des groupes G_{p^n} par rapport aux applications de restriction.
Par composition, le théorème 2.3 et le lemme 2.1 montrent ensemble que chaque isomorphisme d'Artin-Schreier-Witt $\mathfrak{as}_n$ induit naturellement un isomorphisme de groupes topologiques :

$$G_{p^n} \xrightarrow{\simeq} \mathrm{Hom}(W(K)/\wp(W(K)), W_n(\mathbb{F}_p)),$$

donné par :

$$\sigma \mapsto \{x + \wp(W(K)) \mapsto \sigma(\xi_0, ..., \xi_{n-1}) - (\xi_0, ..., \xi_{n-1})\},$$

pour un vecteur $(\xi_0, ..., \xi_{n-1})$ de $W_n(K)$ tel que $\wp(\xi_0, ..., \xi_{n-1}) = (x_0, ..., x_{n-1})$. Nous désignerons toujours par $\mathfrak{as}_n$ cet isomorphisme.
En outre, si $n \geq m$, on a un diagramme commutatif :

$$\begin{array}{ccc} G_{p^n} & \xrightarrow{\mathfrak{as}_n} & \mathrm{Hom}(W(K)/\wp(W(K)), W_n(\mathbb{F}_p)) \\ \downarrow{\scriptstyle r_{nm}} & & \downarrow{\scriptstyle \pi_{nm}} \\ G_{p^m} & \xrightarrow{\mathfrak{as}_m} & \mathrm{Hom}(W(K)/\wp(W(K)), W_m(\mathbb{F}_p)) \end{array}$$

avec r_{nm} l'application de restriction et π_{nm} la réduction modulo $V^m W_n(\mathbb{F}_p)$.
On en déduit un isomorphisme entre deux systèmes projectifs de groupes topologiques compacts (séparables). Par passage à la limite projective lorsque $n \to +\infty$, cela induit un isomorphisme de groupes topologiques :

$$G_{p^\infty} \xrightarrow{\simeq} \varprojlim \mathrm{Hom}(W(K)/\wp(W(K)), W_n(\mathbb{F}_p)).$$

D'où l'isomorphisme de groupes topologiques, d'après la propriété universelle des limites projectives :

$$G_{p^\infty} \xrightarrow{\simeq} \mathrm{Hom}(W(K)/\wp(W(K)), \varprojlim W_n(\mathbb{F}_p)),$$

et donc, par le théorème 1.2 :

$$G_{p^\infty} \xrightarrow{\simeq} \mathrm{Hom}(W(K)/\wp(W(K)), W(\mathbb{F}_p)),$$

ce que nous voulions montrer.
Notons $\mathfrak{as}_\infty$ ce dernier isomorphisme. Par construction, pour tout automorphisme σ de G_{p^∞}, $\mathfrak{as}_\infty$ est donné par :

$$\mathfrak{as}_\infty(\sigma) \ : \ x + \wp(W(K)) \mapsto \sigma(\xi) - \xi,$$

où ξ est un vecteur de $W(K^{\mathrm{sep}})$ tel que $\wp(\xi) = x$. $\diamond$

Notation 4. *Nous noterons H_{p^∞} le groupe $Hom(W(K)/\wp(W(K)), W(\mathbb{F}_p))$, de telle sorte que l'isomorphisme de groupes topologiques du théorème 2.4 se ré-écrit :*

$$\mathfrak{as}_\infty \ : \ G_{p^\infty} \xrightarrow{\simeq} H_{p^\infty}.$$

Rappelons que H_{p^∞} est la limite projective des groupes H_{p^n} lorsque $n \to +\infty$ et par rapport aux réductions modulo V^n comme applications de transition.

2.4 G_{p^∞} comme $\mathbb{Z}_p$-module

Nous clôturons ce chapitre par un paragraphe mettant en lumière quelques propriétés algébriques du groupe de Galois G_{p^∞} de la pro-p extension abélienne maximale du corps K. Le théorème 2.4 donne un isomorphisme de groupes topologiques :

$$G_{p^\infty} \simeq \mathrm{Hom}(W(k)/\wp(W(k)), W(\mathbb{F}_p)),$$

où $W(\mathbb{F}_p)$ identifié à $\mathbb{Z}_p$ est muni de la topologie p-adique.
Une conséquence importante de ce théorème est que le pro-p groupe G_{p^∞} est un groupe topologique compact pour la topologie p-adique et surtout qu'il est sans torsion.
En outre, G_{p^∞} hérite de la structure de $\mathbb{Z}_p$-module topologique pour l'action continue $(\lambda, \varphi) \in \mathbb{Z}_p \times G_{p^\infty} \mapsto \lambda.\varphi \in G_{p^\infty}$ donnée par $\lambda.\varphi := x \in \mathcal{V} \mapsto \lambda\varphi(x) \in \mathbb{Z}_p$.

Ces remarques nous conduisent naturellement à mener une étude plus précise du pro-p groupe G_{p^∞} comme module sur $\mathbb{Z}_p$. En particulier, nous traiterons la question de savoir sous quelles conditions G_{p^∞} est libre sur $\mathbb{Z}_p$: c'est le théorème 2.5. D'autres propriétés algébriques seront rapidement évoquées dans le dernier sous-paragraphe.

2.4.1 Résultat principal

Un module sur un anneau est dit libre s'il admet une base ou s'il est le module nul.
Soit M un module libre sur un anneau principal A et soit $(x_i)_{i\in I}$ une base de ce module indexée par un ensemble I. Le cardinal de I est déterminé de façon unique : en effet, si p est premier dans A alors le quotient de M/pM est un espace vectoriel sur le corps A/pA, dont la dimension est précisément le cardinal de I. Si le module M est de plus sans torsion, cela nous permet de définir le rang de M sur A comme le cardinal de I.
Rappelons également que tout sous-module d'un module libre sur un anneau principal est libre aussi et de rang inférieur ou égal (cf. [35], p.880).

Notre résultat principal est le suivant :

Théorème 2.5. *Le pro-p groupe de Galois G_{p^∞} est libre en tant que $\mathbb{Z}_p$-module si et seulement si le $\mathbb{F}_p$-espace vectoriel $G_{p^\infty}/pG_{p^\infty}$ est de dimension finie, alors notée r_p.*
Plus précisément, si G_{p^∞} est $\mathbb{Z}_p$-libre, alors il est finiment engendré de rang r_p.

En résumé, soit G_{p^∞} est libre de type fini, soit il n'est pas libre.

La preuve du théorème 2.5 consiste à montrer les deux points suivants :

- 1. si $r_p := \dim_{\mathbb{F}_p} G_{p^\infty}$ est fini, alors G_{p^∞} est libre de rang fini égal à r_p
- 2. sinon, G_{p^∞} n'est pas libre.

Si l'on admet la version topologique du lemme de Nakayama (cf. [49], p. 242) le premier point est trivial : c'est le sous-paragraphe 2. Néanmoins, nous en donnerons à la fin de ce paragraphe une autre preuve complète en exhibant un sous-module libre qui est dense dans G_{p^∞}.

Pour traiter le cas où $G_{p^\infty}/pG_{p^\infty}$ est de dimension infinie sur $\mathbb{F}_p$, nous ferons appel à des propriétés sur les nombres cardinaux, c'est l'objet du sous-paragraphe 3.

Alors que le premier point est vrai pour tout module compact sur un anneau local qui est lui-même compact pour sa topologie $\mathfrak{m}$-adique, $\mathfrak{m}$ désignant son idéal maximal, le cas infini est essentiellement dû au fait que G_{p^∞} est un groupe profini abélien sans torsion.

2.4.2 Cas fini

Le pro-p groupe abélien G_{p^∞} est un module sur l'anneau local $\mathbb{Z}_p$ qui est compact pour la topologie p-adique et G_{p^∞} est lui-même compact pour la topologie p-adique. Ainsi, d'après le lemme de Nakayama topologique, G_{p^∞} est de type fini si (et seulement si) le $\mathbb{F}_p$-espace vectoriel $G_{p^\infty}/pG_{p^\infty}$

est de dimension finie. Lorsque c'est le cas, G_{p^∞} est un $\mathbb{Z}_p$-module libre en tant que module finiment engendré et sans torsion sur un anneau principal. De plus, son rang est $r_p = \dim_{\mathbb{F}_p} G_{p^\infty}/pG_{p^\infty}$ par le lemme de Nakayama à nouveau, d'où la preuve du point (1).

2.4.3 Cas infini

L'étude du cas infini nécessite le résultat suivant qui classifie tous les groupes abéliens profinis sans torsion (cf. [53], p.133) :

Théorème 2.6. *Soit G un groupe abélien profini sans torsion. Alors G un produit direct de copies de $\mathbb{Z}_p$:*

$$G \simeq \prod_p (\prod_{m(p)} \mathbb{Z}_p)$$

lorsque p parcourt l'ensemble des nombres premiers et où chaque $m(p)$ est un nombre cardinal.

Dans notre contexte, le pro-p groupe G_{p^∞} est alors un produit de copies de $\mathbb{Z}_p$ pour notre unique nombre premier p, caractéristique du corps K. Cela s'écrit :

$$G \simeq \prod_{\mathcal{V}} \mathbb{Z}_p,$$

pour un certain ensemble d'indices $\mathcal{V}$.

Maintenant, si nous supposons que G_{p^∞} n'est pas finiment engendré en tant que module sur $\mathbb{Z}_p$, alors nécessairement l'ensemble $\mathcal{V}$ est infini. Considérons un sous-ensemble dénombrable infini S de $\mathcal{V}$ et posons :

$$M := \{(x_v)_v \in G_{p^\infty} \ : \ \forall v \notin S,\ x_v = 0\ ,\ \forall N \geq 1\ \exists S_N \subset S \text{ finite } s.t. \forall s \in S - S_N\ p^N | x_s\}.$$

L'ensemble M est un $\mathbb{Z}_p$-sous-module de G_{p^∞}. Nous affirmons alors que M n'est pas libre.
D'abord, le quotient M/pM est un $\mathbb{F}_p$-espace vectoriel dont une base est indexée par l'ensemble infini S. En particulier, son cardinal est égal au cardinal de S.
Ensuite, montrons que le cardinal de M est strictement plus grand que celui de S. En effet, chaque élément x de M s'écrit de façon unique comme :

$$x = x_0 + px_1 + p^2x_2 + \cdots + p^n x_n + \cdots,$$

où les x_n sont dans M avec des coordonnées dans $[|0, p-1|]$, toutes étant nulles sauf un nombre fini. Cette série converge bien puisque G_{p^∞} est aussi compact pour la topologie p-adique. Ainsi, puisque l'ensemble de tous les sous-ensembles finis de S a le même cardinal que S, le cardinal de M vaut :

$$\text{card } M = (\text{ card } S)^{\aleph_0} = \aleph_0^{\aleph_0},$$

puisque S est dénombrable. Or le nombre cardinal $\aleph_0^{\aleph_0}$ est strictement plus grand que $\aleph_0$ et donc que le cardinal de S, ce que nous voulions montrer.

Supposons donc que M est libre comme $\mathbb{Z}_p$-module. Son rang est alors égal à la dimension de M/pM et donc les cardinaux de M et M/pM sont égaux, ce qui soulève une contradiction.
Ainsi, le sous-module M n'est pas libre et donc G_{p^∞} ne peut être libre en tant que module sur l'anneau principal $\mathbb{Z}_p$, ce qui finit la preuve du théorème.

2.4.4 Quelques remarques

Ce sous-paragraphe peut être survolé, il propose une étude supplémentaire des groupes quotients $G_{p^\infty}/p^nG_{p^\infty}$ pour tous $n \geq 1$, ce qui permet de retrouver le point (1) du théorème 2.5 en exhibant un sous-module libre et dense dans G_{p^∞}.

On peut montrer facilement les deux propositions suivantes :

Proposition 2.1. *Pour chaque entier $n \geq 1$, on a isomorphisme de groupes topologiques :*

$$G_{p^n} \simeq G_{p^\infty}/p^n G_{p^\infty},$$

où G_{p^n} désigne le groupe de Galois de l'extension abélienne maximale d'exposant p^n sur K.

Proposition 2.2. *Pour tout entier $n \geq 1$, le groupe quotient $G_{p^\infty}/p^n G_{p^\infty}$ a une structure de module libre sur l'anneau $\mathbb{Z}/p^n\mathbb{Z}$. Son rang ne dépend pas de n et est égal à $r_p = \dim_{\mathbb{F}_p} G_{p^\infty}/pG_{p^\infty}$.*

Par le théorème 2.3, le groupe de Galois G_p de l'extension abélienne maximale d'exposant p est isomorphe au groupe dual $\mathrm{Hom}(K/\wp(K), \mathbb{F}_p)$ de $K/\wp(K)$. Alors, puisque $G_{p^\infty}/pG_{p^\infty}$ est isomorphe à G_p, il résulte que le $\mathbb{Z}_p$-module G_{p^∞} est libre si et seulement si le $\mathbb{F}_p$-espace vectoriel $K/\wp(K)$ est de dimension finie. Par exemple, c'est ce que l'on a lorsque le corps K est fini et il serait intéressant de voir s'il existe d'autres cas semblables.

Nous concluons ce chapitre par quelques commentaires sur la structure topologique du $\mathbb{Z}_p$-module G_{p^∞} en montrant qu'il est "topologiquement" libre. On dit qu'un module topologique admet une base topologique, ou qu'il est topologiquement libre, s'il contient un sous-module libre et dense. Le théorème 2.6 qui classifie tous les groupes abéliens profinis et sans torsion montre que G_{p^∞} est homéomorphe à un produit direct de copies de $\mathbb{Z}_p$. La somme directe associée représente donc un sous-module libre et dense dans G_{p^∞} et donc G_{p^∞} est topologiquement libre.

Nous allons extraire un autre sous-module libre et dense dans G_{p^∞} qui a une signification avec le théorème 2.5.
Montrons d'abord un lemme purement algébrique :

Lemme 2.2. *On a un homomorphisme de groupes topologiques :*

$$G_{p^\infty} \simeq \varprojlim G_{p^\infty}/p^n G_{p^\infty},$$

où G_{p^∞} a la topologie p-adique et où la limite projective est prise respectivement aux morphismes de projection.

Preuve : Nous avons vu que G_{p^∞} est compact. De plus, les sous-groupes $p^n G_{p^\infty}$ forment une filtration décroissante de sous-groupes fermés pour la topologie p-adique. Alors, puisque l'on a $\cap_{n=1}^{\infty} p^n G_{p^\infty} = \{id\}$, on en déduit un homomorphisme de groupes topologiques : $\varprojlim G_{p^\infty}/p^n G_{p^\infty}$ (cf. [61], p.3). ◇

Nous énonçons également :

Lemme 2.3. *Soit A un anneau de valuation discrète, d'idéal maximal $\mathcal{P} = pA$ et de corps résiduel $k = A/pA$. Soit M un A-module sans torsion. Si $(\bar{a}_i)_{i\in I}$ est une base du k-espace vectoriel $m = M/pM$, alors tout relèvement $(a_i)_i$ de $(\bar{a}_i)_i$ à M forme une famille linéairement indépendante sur le module M.*

Preuve : Considérons une combinaison linéaire sur M :

$$(C1) \qquad \sum_i \alpha_i a_i = 0 \quad , \ \alpha_i \in A.$$

On obtient par réduction dans M/pM :

$$\sum_i \bar{\alpha}_i \bar{a}_i = 0 \quad , \ \bar{\alpha}_i \in k,$$

d'où $\bar{\alpha}_i = 0$ dans k pour tout i. On peut donc écrire $\alpha_i = p\alpha_i^{(1)}$. Maintenant, la relation $(C1)$ devient :

$$p(\sum_i \alpha_i^{(1)} a_i) = 0 \quad , \ \alpha_i^{(1)} \in A,$$

et donc :

$$(C2) \qquad \sum_i \alpha_i^{(1)} a_i = 0 \quad , \ \alpha_i \in A,$$

puisque M est sans torsion.

De même, pour tout indice i on montre par récurrence sur $n \geq 1$ que chaque p^n divise α_i. Alors $v_p(\alpha_i) = \infty$ et donc $\alpha_i = 0$ pour tout i, c'est-à-dire la famille $(a_i)_i$ est linéairement indépendante sur M. $\diamond$

En particulier, si $(\bar{a}_i)_{i \in I}$ est une $\mathbb{F}_p$-base de l'espace vectoriel $G_{p^\infty}/pG_{p^\infty}$ (card $I = r_p$), on peut la relever en une famille linéairement indépendante $(a_i)_{i \in I}$ de G_{p^∞}. Notons N le sous-module libre de G_{p^∞} que cette famille engendre.
Pour chaque entier $n \geq 1$, la famille $(a_i)_i$de G_{p^∞} se projette sur une base de $G_{p^\infty}/p^n G_{p^\infty}$. Ainsi, le sous-module N se surjecte à chaque étage fini sur la limite projective $\varprojlim G_{p^\infty}/p^n G_{p^\infty}$. Donc, d'après le lemme 2.2 et aussi ([53], p. 8), N est dense dans G_{p^∞} : $G_{p^\infty} = \bar{N}$.

Ainsi, nous aurions pu montrer la première partie du théorème 2.5 comme suit. En effet, si $G_{p^\infty}/pG_{p^\infty}$ est de dimension finie r_p, alors N est libre de rang fini égal à r_p et donc fermé dans G_{p^∞}. Le $\mathbb{Z}_p$-module G_{p^∞} est donc libre aussi, de rang fini égal à r_p.

Deuxième partie

Ramification dans les extensions d'Artin-Schreier-Witt

Chapitre 3

Extensions d'Artin-Schreier-Witt de corps résiduel parfait

On appelle corps local un corps muni d'une valuation discrète pour laquelle il est complet. Ce troisième chapitre propose de calculer les groupes de ramification des extensions d'Artin-Schreier-Witt sur un corps local K de caractéristique $p > 0$ lorsque le corps résiduel est parfait. L'objectif est atteint partiellement : nous donnons ici une étude complète des groupes de ramification de toutes les extensions abéliennes d'exposant p sur K ainsi qu'une description précise du groupe d'inertie de toutes les pro-p extensions abéliennes de K.

Le paragraphe 3.1 contient quelques définitions et propriétés de base sur les groupes de ramification d'une extension algébrique de K. Plus précisément, on rappelle d'abord la notion de groupes de ramification en notation inférieure pour une extension finie de K avant de passer à la notation supérieure, cette dernière permettant de définir les groupes de ramification dans une extension galoisienne infinie.

Le paragraphe 3.2 donne une description complète de tous les groupes de ramification pour les extensions abéliennes d'exposant p sur K à travers l'isomorphisme d'Artin-Schreier-Witt $\mathfrak{as}_1$ du chapitre 2. Le théorème 3.2 traite d'abord le cas d'une extension cyclique de degré p sur K. C'est aujourd'hui un résultat classique, mais nous avons pris le soin de détailler sa preuve car il est à la base de l'étude qui suit. En effet, le théorème 3.3 donne une première généralisation en décrivant les groupes de ramification d'une extension abélienne finie d'exposant p^n. On améliore ainsi un résultat de Maus [46] en précisant la correspondance donnée via l'isomorphisme d'Artin-Schreier-Witt et sans faire appel à la théorie du corps de classe. Ensuite, dans le corollaire 3.3 on en déduit les groupes de ramification pour l'extension abélienne maximale d'exposant p sur K.

Enfin, le paragraphe 3.3 propose une première généralisation de cette étude aux extensions abéliennes d'exposant p^n lorsque $n \geq 2$ en explicitant leur groupe d'inertie (théorème 3.4). Par passage à la limite projective, nous obtenons alors le groupe d'inertie de la pro-p extension abélienne maximale de K (corollaire 3.5).
Ce dernier paragraphe ouvre donc la question de savoir si l'on peut pousser l'étude à tous les groupes de ramification pour les extensions d'exposant p^n lorsque $n \geq 2$.

3.1 Rappels sur les groupes de ramification

Ce paragraphe est consacré à des rappels sur les groupes de ramification. Pour plus de détails, le lecteur se reportera aux deux premières parties de [60], ainsi qu'à [31], [48] et [74].

3.1.1 Extensions non ramifiées

1 Extensions finies

Dans tout ce qui suit, K désigne un corps local de valuation discrète v_K. On notera O_K l'anneau de valuation correspondant, $\mathfrak{p}_K$ son idéal maximal, U_K le groupe des unités et κ le corps résiduel que nous supposerons toujours parfait.
Toutes les extensions considérées sur K (resp. κ) seront incluses dans une clôture algébrique $\bar{K}$ (resp. $\bar{\kappa}$) fixée.

Soit L une extension finie de K. Par ([60], Chap.II, §2), L est muni d'une structure de corps local pour laquelle nous utiliserons les notations v_L, O_L, $\mathfrak{p}_L$, U_L et aussi l pour le corps résiduel.

Le corps résiduel κ étant parfait, l'extension résiduelle l/κ est séparable. En particulier, si L/K est galoisienne, l/κ l'est aussi et son groupe de Galois $Gal(l/\kappa)$ s'écrit comme quotient du groupe $Gal(L/K)$.

Indice de ramification et degré résiduel. On note n le degré de l'extension L/K et f celui de l/κ. Ces degrés sont reliés par la relation :

$$n \ = \ e \times f \ ,$$

où l'entier e est appelé l' *indice de ramification* de l'extension L/K. Cet indice satisfait :

$$\mathfrak{p}_K O_L \ = \ \mathfrak{p}_L^e .$$

Le degré f, quant à lui, est le *degré résiduel* de l'extension L/K.
Du point de vue des valuations, il apparaît :

$$\forall x \in L \ : \ v_L(x) \ = \ \frac{1}{f} v_K(N_{L/K}(x)),$$

où $N_{L/K}$ désigne la norme de l'extension L/K. En particulier, nous avons :

$$\forall x \in K \ : \ v_L(x) \ = \ e v_K(x).$$

Extensions non ramifiées et extensions totalement ramifiées. L'extension L/K est dite *non ramifiée* si $e = 1$ (et dans le cas général si l'extension résiduelle est de plus séparable). Lorsque L/K est galoisienne, cette condition implique un isomorphisme naturel entre les groupes de Galois de L/K et de $l/\bar{k}$.
On dit que l'extension est *totalement ramifée* lorsque $f = 1$, c'est-à-dire lorsque $e = n$, ce qui signifie que l'extension résiduelle est triviale.

2 Extensions infinies

Corps résiduel d'une extension infinie. Soit M une extension algébrique infinie de K. Soit m l'extension de κ définie comme la réunion des extensions résiduelles l/κ de toutes les sous-extensions L/K finies de M. On dit que m est le *corps résiduel* de M.

D'après ([60], Chap. II, §5) on a :

Proposition 3.1. *A chaque extension finie séparable l de κ correspond une extension non ramifiée L de K telle que l soit le corps résiduel de L, cette propriété définit l'extension L de façon unique à un unique isomorphisme près. De plus, l'extension L/K est galoisienne si et seulement si l'extension résiduelle l/κ est galoisienne et alors leurs groupes de Galois sont isomorphes.*

Soit κ^{sep} la clôture séparable de κ, i.e. la plus grande extension séparable de κ contenue dans la clôture algébrique $\bar{\kappa}$. Le proposition 3.1 nous mène à considérer la réunion des extensions finies non ramifiées de K correspondant à l'ensemble des sous-extensions finies de κ^{sep} : ce compositum est une extension algébrique de K que nous noterons K^{nr}. En particulier, l'extension K^{nr} a pour corps résiduel κ^{sep} et est galoisienne sur K de groupe $Gal(K^{nr}/K) \simeq \text{Gal}(\kappa^{\text{sep}}/\kappa)$.

Extensions infinies non ramifiées et extensions totalement ramifiées. Une extension infinie M/K est dite *non ramifiée* si toutes ses sous-extensions finies $K \subset L \subset M$ sont non ramifiées. De même, M/K est dite *totalement ramifiée* si elle a toutes ses sous-extensions finies qui sont totalement ramifiées.

On a :

Proposition 3.2. *L'extension K^{nr} est non ramifiée sur K, c'est l'extension maximale non ramifiée de K.*

On définit alors la sous-extension maximale non ramifiée d'une extension M/K comme l'intersection $M \cap K^{nr}$. En particulier, on peut montrer qu'elle a même corps résiduel $\bar{m}$ que M et que son groupe de Galois est précisément donné par un isomorphisme canonique $Gal((M \cap K^{nr})/K) = Gal(\bar{m}/\kappa)$.
Il est à noter qu'en général M/K est totalement ramifiée si et seulement si $M \cap K^{nr} = K$.

Extensions résiduelles de K_{p^n} et K_{p^∞}. Pour chaque entier $n \geq 1$ notons K_{p^n} l'extension abélienne maximale d'exposant p^n de K et notons K_{p^∞} la pro-p extension abélienne maximale de K. Alors, d'après ce qui précède, le corps résiduel de K_{p^n} est la réunion des corps résiduels de toutes les extensions abéliennes finies d'exposant p^n de K. De même, celui de K_{p^∞} est la réunion des corps résiduels de toutes les extensions d'Artin-Schreier-Witt finies de K. Plus précisément :

Proposition 3.3. *L'extension résiduelle de K_{p^n}/K est l'extension abélienne maximale d'exposant p^n sur k, nous la notons κ_{p^n}. L'extension résiudelle de K_{p^∞}/K est la pro-p extension abélienne maximale de κ, notée κ_{p^∞}.*

Preuve : Par définition, le corps résiduel de K_{p^n} est clairement inclus dans κ_{p^n}.
Réciproquement, soit l une extension abélienne finie d'exposant p^n sur κ. D'après la proposition 3.1 il existe une extension finie non ramifiée L de K de corps résiduel l. De plus, l'extension L/K est galoisienne, de groupe de Galois isomorphe à $Gal(l/\kappa)$: elle est donc abélienne d'exposant p^n. Par maximalité, l'extension L est incluse dans K_{p^n}. Ainsi le corps résiduel de K_{p^n} contient l'extension l, c'est donc κ_{p^n}.
On montre de même que l'extension κ_{p^∞} est le corps résiduel de K_{p^∞}. ◇

En particulier, la théorie de Galois des extensions d'Artin-Schreier-Witt sur K développée dans le chapitre 2 nous permet d'écrire explicitement le groupe de Galois de l'extension maximale non ramifiée $K_{p^n}^{nr}$ de chaque extension K_{p^n}, $n \geq 1$. On a en effet un isomorphisme de groupes topologiques :

$$Gal((K_{p^n} \cap K^{nr})/K) \xrightarrow{\simeq} Gal(\kappa_{p^n}/\kappa) \xrightarrow{\simeq} Hom(W_n(\kappa)/\wp(W_n(\kappa)), \mathbb{Z}/p^n\mathbb{Z}).$$

De même, pour la pro-p extension abélienne maximale K_{p^∞} de K, on a :

$$Gal((K_{p^\infty} \cap K^{nr})/K) \xrightarrow{\simeq} Gal(\kappa_{p^\infty}/\kappa) \xrightarrow{\simeq} Hom(W(\kappa)/\wp(W(\kappa)), \mathbb{Z}_p).$$

3.1.2 Groupes de Ramification

1 Notation inférieure

Dans ce sous-paragraphe nous fixons une extension galoisienne finie L du corps local K de caractéristique p. Puisque κ est parfait, l'extension résiduelle l/κ est toujours séparable.

La filtration des groupes de ramification. Soit G le groupe de Galois de l'extension L/K. Pour chaque entier $i \geq -1$, on définit dans G le sous-groupe suivant :

$$G_{(i)} := \{\sigma \in G \,:\, \sigma(x) - x \in \mathfrak{p}_L^{i+1},\ \forall x \in O_L\}.$$

Le groupe $G_{(i)}$ est appelé le *i-ème groupe de ramification* de G (pour la notation inférieure).

Les $G_{(i)}$ sont des sous-groupes distingués de G. Ils forment une filtration décroissante de G, avec $G_{(-1)} = G$ et $G_{(m)} = 1$ pour un certain entier $m \geq 1$ puisque G est fini :

$$G = G_{(-1)} \supset G_{(0)} \supset G_{(1)} \supset ... \supset G_{(m)} = 1.$$

Le groupe $G_{(0)}$. D'après ([60], Chap.I, §6) on a une suite exacte courte :

$$1 \longrightarrow G_{(0)} \longrightarrow G \xrightarrow{\epsilon} Gal(l/\kappa) \longrightarrow 1$$

dans laquelle ϵ désigne l'homomorphisme $\sigma \mapsto \bar{\sigma}$ défini par :

$$\forall x \in O_L \ : \ \bar{\sigma}(\bar{x}) = \bar{\sigma(x)}$$

où $\bar{x}$ représente la classe de x modulo $\mathfrak{p}_L$. En particulier, l'application ϵ induit l'isomorphisme de groupes :

$$G/G_{(0)} \simeq Gal(l/\kappa).$$

Le groupe $G_{(0)}$ est appelé *groupe d'inertie* de l'extension L/K. De plus, si l'extension L/K est galoisienne, le quotient $G/G_{(0)}$ est le groupe de Galois de la sous-extension maximale non ramifiée de L/K (cf. [60], Chap.IV, §1) :

$$G/G_{(0)} = Gal((K^{nr} \cap L)/K).$$

En particulier, si L/K est totalement ramifiée alors $G_{(0)} = G$ et si L/K est non ramifiée son groupe d'inertie $G_{(0)}$ est trivial.

Le groupe $G_{(1)}$. Considérons maintenant le sous-corps fixé par $G_{(1)}$. Pour cela, nous dirons qu'une extension de K est *modérément ramifiée* si p ne divise pas son indice de ramification. En particulier, le compositum de deux extensions modérément ramifiées est encore modérément ramifié. On définit donc la sous extension maximale modérément ramifiée de L/K comme l'union de toutes les sous-extensions modérément ramifiées de L/K, nous la noterons V. Alors, d'après ([74], Chap. 3, §6) mais aussi ([60], Chap. IV, §2, cor.1), le quotient $G/G_{(1)}$ est le groupe de Galois de V/K :

$$G/G_{(1)} \simeq Gal(V/K).$$

En particulier, si l'extension L/K est modérément ramifiée, alors $G_{(1)}$ est trivial. Dans notre cadre, une extension d'Artin-Schreier-Witt de K est modérément ramifiée si et seulement si elle est non ramifiée.

Toute sous-extension non ramifiée de L/K est modérément ramifiée, c'est pourquoi V contient la sous-extension maximale non ramifiée $K^{nr} \cap L$, ce qui confirme l'inclusion $G_{(1)} \subset G_{(0)}$. De plus, si G est un p-groupe, alors toutes les sous-extensions modérément ramifiées de L/K sont non ramifiées et donc $V = K^{nr} \cap L$, ce qui signifie $G_{(0)} = G_{(1)}$. C'est le cas des extensions d'Artin-Schreier-Witt.

A l'inverse, une extension est dite *sauvagement ramifiée* si son extension résiduelle est séparable et si p divise son indice de ramification. Par exemple, l'extension L/V est toujours sauvagement ramifiée. Bien plus, c'est seulement dans le cas sauvagement ramifié que des groupes $G_{(i)}$ non triviaux apparaissent pour $i \geq 1$. Dans ce qui suit, les pro-p extensions abéliennes de K sont sauvagement ramifiées, sauf si elles sont non ramifiées. Ceci motive l'étude des groupes de ramification d'indice supérieur à 2 dans les extensions d'Artin-Schreier-Witt.

Sauts. On dit qu'un entier $t \geq -1$ est un saut pour la filtration $\{G_{(i)}\}_i$ si :

$$G_{(t)} \neq G_{(t+1)}.$$

L'étude des groupes de ramification peut se ramener à celle des sauts de la filtration correspondante.

Il vient alors une nouvelle caractérisation pour chaque groupe de ramification d'indice i, $i \geq 1$. En effet, fixons une uniformisante π_L de L. On a :

$$G_{(i)} = \{\sigma \in G_{(0)} \ : \ \sigma(\pi_L) - \pi_L \in \mathfrak{p}_L^{i+1}\}.$$

Par exemple, c'est à partir de cette relation que l'on calculera dans le théorème 3.2 l'unique saut de la filtration $\{G_{(i)}\}_i$ lorsque l'extension L/K est cyclique de degré p totalement ramifiée. En effet, ce saut est l'unique entier $t \geq 1$ tel que :

$$v_L(\sigma(\pi_L) - \pi_L) \geq t + 1,$$

pour tous les automorphismes σ de $G_{(0)}$.

Groupes de ramification dans un sous-groupe de G. Pour finir, soit H un sous-groupe de G et soit M le sous-corps de L invariant par H. Alors, les groupes de ramification de l'extension L/K déterminent ceux de L/M de la façon suivante :

$$\forall i \geq -1 \ : \ H_{(i)} = G_{(i)} \cap H.$$

Souvent, la notation inférieure pour les groupes de ramification est dite adaptée aux sous-groupes. Cependant, afin d'étudier les groupes de ramification d'une extension infinie, il serait plus intéressant de déterminer les groupes de ramification d'une sous-extension, c'est-à-dire pour un quotient du groupe G. Cela nécessite d'introduire une nouvelle notation.

2 Notation supérieure

Indices réels. Généralisons d'abord la notation $G_{(i)}$ aux indices réels. Dorénavant, si $u \geq -1$ est un réel, nous noterons $G_{(u)}$ le groupe de ramification $G_{(i_u)}$:

$$G_{(u)} = G_{(i_u)},$$

où i_u est l'unique entier tel que :

$$i_u - 1 < u \leq i_u.$$

La fonction ψ de Herbrand. On introduit alors la fonction $\varphi = \varphi_{L/K}$ définie par :

$$\varphi(u) \ = \ \begin{cases} u & \text{si } -1 \leq u < 0 \\ \displaystyle\sum_{i=1}^{i_u} \frac{1}{(G_{(0)} : G_{(i)}} + \frac{u - i_u}{(G_{(0)} : G_{(i_u+1)})} & \text{si } u \geq 0 \end{cases}$$

On montre facilement que φ est un homéomorphisme de la demi-droite $[-1; +\infty[$ sur elle-même. Soit $\psi = \psi_{L/K}$ la fonction inverse : ψ est appelée *fonction de Herbrand* de l'extension L/K.

Groupes de ramification en notation supérieure. Enfin, pour tout réel $v \geq -1$, on définit le *groupe de ramification d'indice v pour la notation supérieure* de l'extension finie L/K par :

$$G^{(v)} := G_{(\psi(v))}.$$

Les groupes $G^{(v)}$, $v \geq -1$, forment encore une filtration décroissante de G avec $G^{(-1)} = G = G_{(-1)}$ et $G^{(0)} = G_{(0)}$, puisque ψ est l'application identité sur $[-1; 0]$. La dernière égalité est d'un intérêt certain pour la suite, en particulier dans le calcul du groupe d'inertie des extensions d'Artin-Schreier-Witt.
De plus, si G est fini, $G^{(s)} = 1$ à partir d'un réel $s \geq 0$ suffisamment grand. En résumé, on écrit :

$$G^{(-1)} = G \supset G^{(0)} \supset G^{(1)} \supset ... \supset G^{(s)} = 1.$$

Remarquons que pour tout réel $u \geq -1$, on a aussi :

$$G_{(u)} = G^{(\varphi(u))}.$$

En particulier : $G_{(1)} = G^{(\varphi(1))}$. Or si l'extension L/K est modérément ramifiée, on a vu que $G_{(0)} = G_{(1)}$. Puisque $\varphi(1) = 1$, cela entraîne l'égalité :

$$G^{(0)} = G^{(1)},$$

pour toutes les extensions d'Artin-Schreier-Witt finies.

De même que pour la notation inférieure, nous dirons qu'un réel $t \geq -1$ est un saut pour la filtration $\{G^{(v)}\}_v$, s'il satisfait :

$$\forall \epsilon > 0,\ G^{(t)} \neq G^{(t+\epsilon)}.$$

Nous verrons plus loin que lorsque G est abélien, cette relation est équivalente à la suivante :

$$G^{(t)} \neq G^{(t+1)},$$

par le théorème de Hasse-Arf (cf. théorème 3.1). Néanmoins, dans le cas général, les sauts de la filtration des groupes de ramification pour la notation supérieure ne sont pas nécessairement entiers.

Groupes de ramification dans une sous-extension. Soit M une sous-extension de L/K. Les homéomoprhismes φ et ψ vérifient les formules suivantes :

$$\varphi_{L/K} = \varphi_{M/K} \circ \varphi_{L/M}$$

et :

$$\psi_{L/K} = \psi_{L/M} \circ \psi_{M/K}.$$

Cela permet de montrer que la restriction naturelle $Gal(L/K) \twoheadrightarrow Gal(M/K)$ envoie $G(L/K)^{(v)}$ sur $G(M/K)^{(v)}$ (cf. [60], Chap.IV, §3, prop.14) :

Proposition 3.4. *Soit H un sous-groupe distingué de G. Pour tout réel $v \geq -1$ on a :*

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

Cette proposition est souvent attribuée à Herbrand. Elle signifie que la notation supérieure est adaptée aux quotients, c'est-à-dire que pour la notation supérieure les groupes de ramification d'une extension déterminent ceux de toute sous-extension. Cette propriété permet de définir les groupes de ramification pour une extension galoisienne infinie en passant à la limite projective.

Groupes de ramification dans une extension galoisienne infinie. Supposons maintenant que l'extension L/K est galoisienne et infinie. Nous notons toujours G son groupe de Galois. La proposition 3.4 permet de définir pour chaque réel $v \geq -1$ le groupe de ramification $G^{(v)}$ d'indice v comme la limite projective des groupes $Gal(M/K)^{(v)}$ lorsque M parcourt l'ensemble des sous-extensions galoisiennes finies de L/K

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

Les sous-groupes $G^{(v)}$ de G forment encore une filtration décroissante de G et sont fermés dans G pour la topologie de Krull. Cette filtration est continue à gauche, c'est-à-dire : $G^{(v)} = \cap_{w<v} G^{(w)}$.

Généralisant le cas des extensions finies, on dit qu'un réel $t \geq -1$ est un saut pour la filtration des groupes de ramification $G^{(v)}$ si :

$$\forall \epsilon > 0\ :\ G^{(t)} \neq G^{(t+\epsilon)}.$$

Une suite exacte. Nous conservons les notations précédentes. Lorsque l'extension L/K est infinie, on a encore la suite exacte :

$$1 \longrightarrow G^{(0)} \longrightarrow G \xrightarrow{\epsilon} Gal(l/\kappa) \longrightarrow 1.$$

En effet, le groupe de Galois G de L/K est défini comme la limite projective :

$$G = \varprojlim Gal(M/K),$$

lorsque M parcourt l'ensemble des sous-extensions finies de L/K, la limite étant prise par rapport aux applications de restriction $R_{MN} : Gal(M/K) \twoheadrightarrow Gal(N/K)$. De plus, on a par définition :

$$Gal(L/K)^{(0)} = \varprojlim Gal(M/K)^{(0)},$$

pour les applications de restriction $R^{(0)}_{MN} := R_{MN|Gal(M/K)^{(0)}}$.

Or, quand M parcourt l'ensemble des sous-extensions finies de L/K l'extension résiduelle associée $\bar{m}/\kappa$ parcourt l'ensemble des sous-extensions finies de l/κ par définition du corps résiduel d'une extension infinie. Il vient alors :

$$Gal(l/\kappa) = \varprojlim Gal(\bar{m}/\kappa),$$

par rapport aux applications de restrictions $r_{\bar{m}\bar{n}}$.

De plus, si M/K et N/K sont deux sous-extensions avec $M \subset N \subset L$, on montre facilement que le diagramme suivant commute :

$$\begin{array}{ccccccccc} 1 & \longrightarrow & Gal^{(0)}(N/K) & \longrightarrow & Gal(N/K) & \longrightarrow & Gal(\bar{n}/\kappa) & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle R^{(0)}_{MN}} & & \downarrow{\scriptstyle R_{MN}} & & \downarrow{\scriptstyle r_{\bar{m}\bar{n}}} & & \\ 1 & \longrightarrow & \tilde{Gal}^{(0)}(M/K) & \longrightarrow & Gal(M/K) & \longrightarrow & Gal(\bar{m}/\kappa) & \longrightarrow & 1 \end{array}$$

d'où notre assertion en prenant la limite projective et d'après ([35], Chap. III, §10.3).

Le théorème de Hasse-Arf. Nous terminons ces rappels avec un théorème qui caractérise les sauts pour les groupes de ramification en notation supérieure lorsque l'extension est abélienne. Ce théorème est souvent donné pour une extension finie mais nous montrons qu'il se généralise facilement aux extensions galoisiennes infinies. C'est le théorème dit de Hasse-Arf, nous l'énonçons ainsi :

Théorème 3.1. *[Hasse-Arf] Soit K un corps local de corps résiduel parfait. Soit L/K une extension galoisienne et soit G son groupe de Galois. Si G est abélien et si $t > -1$ est un saut pour la filtration $G^{(v)}$ alors t est un entier.*

Lorsque l'extension L/K est finie, une preuve de ce théorème est donnée dans ([48], Chap.V, §6.3) et ([60], Chap.V, §7). Nous allons montrer qu'il se généralise alors facilement aux extensions inifinies.

Soit donc L/K une extension galoisienne infinie de K. Soit G son groupe de Galois supposé abélien, G est la limite projective des groupes G_M de toutes les sous-extensions finies $K \subset M \subset L$. Soit t un saut pour la filtration $\{G^{(v)}\}_v$, on a :

$$\forall \epsilon > 0,\ G^{(t)} \neq G^{(t+\epsilon)}.$$

En particulier, pour chaque $\epsilon > 0$, il existe une sous-extension finie M telle que $G^{(t)}_M \neq G^{(t+\epsilon)}_M$. Par le théorème de Hasse-Arf pour les extensions finies, cela signifie qu'il existe un entier dans l'intervalle $[t; t+\epsilon]$ pour tout $\epsilon > 0$: le saut t est donc entier.

L'étude qui suit considère uniquement les groupes de ramification pour la notation supérieure. En outre, grâce au théorème de Hasse-Arf, nous nous restreignons essentiellement aux groupes de ramification indexés par un entier.

3.2 Groupes de ramifications dans les extensions d'Artin-Schreier-Witt d'exposant p

L'objet de ce paragraphe est de développer le théorème initial d'Artin-Schreier Iorsque le corps K est un corps local de corps résiduel parfait. Plus précisément, il s'agit de combiner la théorie d'Artin-Schreier avec la théorie de la ramification pour donner une description explicite des groupes de ramification de toute extension abélienne d'exposant p sur K. Le but est de décrire les groupes de ramification de l'extension abélienne maximale d'exposant p sur K à travers l'isomorphisme d'Artin-Schreier-Witt $\mathfrak{as}_1$ (cf. chap.2), obtenant ainsi une filtration explicite du groupe $\mathrm{Hom}(K/\wp(K), W_1(\mathbb{F}_p))$.

Le sous-paragraphe 1 considère d'abord les extensions cycliques de degré p. Soit L une extension cyclique de degré p sur K et de groupe G. Rappelons que le théorème d'Artin-Schreier décrit cette extension comme le corps de décomposition du polynôme $X^p - X - x_0$ pour un certain x_0 de K qui n'appartient pas à $\wp(K)$. D'autre part, dans le cadre de la théorie de la ramification, il existe un seul saut $n_0 \geq -1$ dans la filtration des groupes de ramification de L/K qui sont alors donnés par :

$$G = G^{(-1)} = ... = G^{(n_0)} = \mathbb{Z}/p\mathbb{Z},$$

et :

$$G^{(n_0+1)} = G^{(n_0+2)} = ... = \{id\}.$$

De plus, le saut n_0 vaut -1 si et seulement si l'extension L/K est non ramifiée.

Il s'agit donc, dans ce premier sous-paragraphe, de calculer le saut de la filtration $\{G^{(v)}\}_v$ en fonction de x_0 lorsque l'extension L/K est totalement ramifiée : c'est le théorème 3.2 qui montre que le saut est précisément la valeur absolue de la valuation de x_0. Ce problème avait déjà été abordé par Hasse [25] mais nous avons choisi de le détailler car non seulement il développe des arguments intéressants mais surtout il est à la base de l'étude que nous développons par la suite pour les extensions générales d'exposant p.
Pour le problème analogue en caractéristique 0 nous renvoyons le lecteur à [39].

Améliorant un résultat de Maus [46], le sous-paragraphe 2 généralise l'étude précédente aux extensions abéliennes finies d'exposant p sur K avec le théorème 3.3. L'outil principal est le lemme 3.2, résultat clef sur les groupes de ramification dans un compositum.

Il reste alors à passer à la limite projective. C'est ce que nous faisons dans le dernier sous-paragraphe, obtenant ainsi dans le corollaire 3.3 une description explicite des groupes de ramification de l'extension abélienne maximale d'exposant p de K.

3.2.1 Groupes de ramification dans les extensions cycliques de degré p

L'énoncé principal de ce sous-paragraphe est le suivant :

Théorème 3.2. *Soit K un corps local de caractéristique $p > 0$ et de corps résiduel κ parfait. Soit $x_0 \in K$. Notons L le corps de décomposition sur K du polynôme d'Artin-Schreier $\mathcal{P}_{x_0}$ donné par :*

$$\mathcal{P}_{x_0}(X) = X^p - X - x_0.$$

On a :

(i) si $v_K(x_0) > 0$, le polynôme $\mathcal{P}_{x_0}$ se scinde complètement sur K et l'extension L est triviale.

(ii) si $v_K(x_0) = 0$ et si $x_0 \notin \wp(K)$, le polynôme $\mathcal{P}_{x_0}$ est irréductible sur K et l'extension L/K est cyclique de degré p. De plus, L/K est non ramifiée et il existe une unité α de L telle que $L = K(\alpha)$.

(iii) si $v_K(x_0) < 0$ et si $p \nmid v_K(x_0)$, l'extension L/K est cyclique de degré p et est totalement ramifiée. Notons $n_0 = -v_K(x_0)$. Les sous-groupes de ramification de L/K sont donnés par :

$$G = G^{(-1)} = ... = G^{(n_0)} \text{ et } G^{(n_0+1)} = 1,$$

où G désigne le groupe de Galois de L/K.

En d'autres mots, dans *(ii)* le saut de la filtration des groupes de ramification de L/K est -1 puisque l'extension est non ramifiée, tandis que dans *(iii)* le saut vaut n_0. La liste est exhaustive. Le cas où $n_0 > 0$ et n_0 est divisible par p sera traité plus tard : il se ramène à une des trois situations du théorème.

Remarque 9. *Dans les rappels, nous avons déjà observé que le saut ne peut être 0 pour une extension d'Artin-Schreier-Witt, ce que confirme le théorème 3.2 pour une extension cyclique de degré p. Un argument est de dire qu'il n'y a pas de partie modérément ramifiée au-dessus de la*

sous-extension maximale non ramifiée et donc $G^{(0)} = G^{(1)}$. Le corollaire 1 à la proposition 7 de ([60], Chap.IV, §2) fournit un autre argument.

Voici une preuve détaillée du théorème 3.2 :

Preuve :

(i) Si x_0 est dans $\mathfrak{p}_K$, alors par réduction modulo $\mathfrak{p}_K$ l'équation $\mathcal{P}_{x_0}(X) = 0$ devient $\bar{X}^p - \bar{X} = 0$ sur le corps résiduel κ. Cette équation se décompose en facteurs linéaires puisque char $\kappa = p$. Alors, par le lemme de Hensel ([60], Chap.II, §4, prop.7) le polynôme $\mathcal{P}_{x_0}$ - qui appartient à $O_K[X]$- se décompose complètement dans K.

(ii) Dans ce second cas, par le théorème d'Artin-Schreier, l'extension L/K est cyclique de degré p. Son extension résiduelle $\bar{l}/\kappa$ est donc soit de degré p soit triviale. Or $v_K(x_0) = 0$: $\bar{l}$ contient le corps de décomposition du polynôme réduit $\mathcal{P}_{x_0} \mod \mathfrak{p}_L$, c'est-à-dire de $\bar{X}^p - \bar{X} - \bar{x_0}$ où $\bar{x_0} \notin \wp(\kappa)$. Toujours par le théorème d'Artin-Schreier, l'extension $\bar{l}/\kappa$ est donc cyclique de degré p et l'extension L est non ramifiée sur K. De plus, L s'écrit $L = K(\alpha)$ où α est une racine de $\mathcal{P}_{x_0}$. Mais l'égalité :

$$\alpha^p - \alpha = x_0$$

entraîne l'égalité des valuations sur L :

$$v_L(\alpha^p - \alpha) = 0$$

qui est valide seulement si $v_L(\alpha) = 0$, c'est-à-dire si α est une unité dans L.

(iii) C'est le point le plus délicat à traiter. On montre d'abord que l'extension L/K est cyclique de degré p. Par le théorème d'Artin-Schreier, soit le polynôme $\mathcal{P}_{x_0}$ est irréductible sur K soit il se décompose complètement sur K. Or, si l'on considère le polygone de Newton du polynôme $\mathcal{P}_{x_0}$, on voit facilement que $\mathcal{P}_{x_0}$ admet exactement p racines distinctes toutes de valuation $-\frac{n_0}{p}$ qui n'est pas un entier par hypothèse. Ainsi $\mathcal{P}_{x_0}$ n'a pas de racine dans K, ce qui signifie que l'extension L est à nouveau cyclique de degré p sur K.

Montrons ensuite que l'extension L/K est totalement ramifiée. Soit α une racine dans L de $\mathcal{P}_{x_0}$ telle que $L = K(\alpha)$. Sa valuation sur L satisfait :

$$v_L(\alpha) = -\frac{n_0}{p}e,$$

où e désigne l'indice de ramification de L/K. Or $v_L(\alpha)$ est entier puisque $\alpha \in L$ et n_0 est premier à p, l'indice e est donc divisble par p. Mais p est aussi le degré de L/K et donc e divise p. D'où $p = e$ et l'extension est totalement ramifiée.

Il reste à calculer le saut t de la filtration des groupes de ramification dans l'extension L/K. D'après ce qui précède, ce dernier est strictement positif, on écrit donc :

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

Nous avons d'abord besoin de décrire l'anneau d'entiers O_L, ce qui est équivalent à extraire une uniformisante de O_L puisqu'elle engendre O_L comme O_K-algèbre d'après ([60],Chap. I, §6, prop.18). Soit donc π_K une uniformisante de K. Puisque n_0 est premier à p, il existe deux entiers a et b avec a dans $\{0, ..., p-1\}$ tels que :

$$-an_0 + bp = 1.$$

Alors, comme $v_L(\alpha) = -n_0$ et $v_L(\pi_K) = 1 \times e = p$, il vient :

$$v_L(\alpha^a {\pi_K}^b) = 1,$$

et donc l'élément défini par $\pi_L := \alpha^a {\pi_K}^b$ est une uniformisante de L. En outre, les conjugués de α étant les $\alpha + i$, avec $0 \leq i \leq p-1$, ceux de π_L sont donnés par :

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

pour tous les i dans $\{0, ..., p-1\}$. Il s'agit donc de calculer chaque $v_L(\pi_L - \pi_L^{(i)})$ afin de déterminer le saut de la filtration de L/K :

$$\begin{aligned} v_L(\pi_L - \pi_L^{(i)}) &= v_L(\pi_K^b(\alpha^a - (\alpha+i)^a)) \\ &= v_L(\pi_K^b) + v_L(\sum_{k=1}^{a} \binom{a}{k} \alpha^{a-k} i^k) \\ &= bp + v_L(\alpha^{a-1} i) \\ &= bp + (a-1)(-n_0) \\ &= n_0 + 1. \end{aligned}$$

Ainsi, le saut dans la filtration des groupes de ramification pour la notation inférieure est n_0 (voir paragraphe 3.1) : $G_{(0)} = ... = G_{(n_0)}$ et $G_{(n_0+1)} = 1$. Le groupe G étant d'ordre p, n_0 est aussi le saut pour la notation supérieure : $G^{(0)} = ... = G^(n) = G$ et $G^{(n+1)} = 1$, ce qui montre le théorème. ◇

Au passage, la preuve de l'assertion (i) montre le résulat suivant qui sera d'un intérêt particulier dans la suite, se généralisant facilement au cas des vecteurs de Witt (cf. lemme 3.4 du paragraphe 3.3) :

Corollaire 3.1. *On a :*

$$\mathfrak{p}_K \subset \wp(K).$$

Un mot sur le cas où x_0 est de valuation strictement négative et divisible par p : c'est la remarque qui suit. Plus généralement, nous verrons avec le corollaire 3.2 qu'aucun saut dans une extension d'Artin-Schreier-Witt d'exposant p n'est divisible par p.

Remarque 10. **??** *Supposons que x_0 est de valuation $-n_0$ avec $n_0 > 0$ et $p|n_0$. Ecrivons $x_0 = u\pi_K^{-pk}$ où u est une unité de U_K et $k \geq 1$ un entier. L'équation :*

$$X^p - X = x_0$$

définit sur K la même extension que l'équation :

$$(X - y_0)^p - (X - y_0) = x_0 - y_0^p + y_0$$

où $y_0 = u_0\pi_K^{-k}$ dans K avec $u_0 \in U_K$ tel que $\bar{u} = \bar{u}_0^p \mod \mathfrak{p}_K$ (un tel u_0 existe puisque κ est supposé parfait).
De plus, le terme de droite $x_0 - y_0^p + y_0$ est de valuation strictement plus grande que x_0 en tant que somme des termes $(u - u_0^p)\pi_K^{-pk}$ et $u_0\pi_K^{-k}$, où $u - u_0^p$ appartient à $\mathfrak{p}_K$. Alors, par le changement de variables $Y = X - y_0$ et en posant $x_1 = x_0 - y_0^p + y_0$, les polynômes $\mathcal{P}_{x_0}$ et $\mathcal{P}_{x_1}$ définissent la même extension sur K et $v_K(x_1) > v_K(x_0)$.
En itérant le procédé, on obtient un élément x_1 de K tel que $p \nmid v_K(x_1)$ ou bien $v_K(x_1) \geq 0$. On est ainsi ramené à l'un des cas (i), (ii) ou (iii) du théorème 3.2.

3.2.2 Groupes de ramification dans les extensions abéliennes finies d'exposant p

Le but de ce sous-paragraphe est de généraliser le théorème 3.2 à toute extension abélienne finie d'exposant p sur K en décrivant explicitement ses groupes de ramification.

Dans la suite, nous fixons une extension L abélienne finie d'exposant p sur K. D'après le théorème 2.2 du chapitre 2, L est le compositum de toutes les extensions cycliques $K(\wp^{-1}(x))$ lorsque x parcourt le sous-groupe $B = \wp(L) \cap K$ de $W_1(K) = K$ contenant $\wp(K)$ avec un indice fini. Bien plus, si G désigne le groupe de Galois de L/K, l'isomorphisme d'Artin-Schreier-Witt $\mathfrak{as}_1$ induit un isomorphisme :

$$\begin{array}{rccc} \mathfrak{as}_1 : & G & \xrightarrow{\simeq} & Hom(B/\wp(K), \mathbb{Z}/p\mathbb{Z}) \\ & \sigma & \mapsto & f_\sigma : \{x + \wp(K) \mapsto \sigma(\xi) - \xi, \end{array}$$

où ξ appartenant à K^{alg} est tel que $\wp(\xi) = x$.

Notons H_B le groupe $\mathrm{Hom}(B/\wp(K), \mathbb{Z}/p\mathbb{Z})$. On introduit d'abord une filtration croissante de sous-groupes dans le quotient $B/\wp(K)$, par dualité elle définit une filtration décroissante de H_B. Le théorème 3.3 montre alors que cette dernière filtration correspond à la filtration des groupes de ramification de l'extension L/K par l'isomorphisme d'Artin-Schreier-Wîtt.

Isomorphisme entre deux filtrations.
Pour chaque entier $u \geq -1$, on définit dans $B/\wp(K)$ le sous-groupe :

$$B^{(u)} := (\mathfrak{p}_K^{-u} \cap B + \wp(K))/\wp(K),$$

en posant $\mathfrak{p}_K^0 = O_K$. D'après le corollaire 3.1, le premier quotient $B^{(-1)}$ est trivial. Clairement, les groupes $B^{(u)}$ forment une filtration croissante de $B/\wp(K)$ et puisque $B/\wp(K)$ est fini, $B^{(m)} = B/\wp(K)$ pour un certain entier $m \geq 0$:

$$B^{(-1)} = \{1\} \subset B^{(0)} \subset B^{(1)} \subset \cdots \subset B^{(m)} = B/\wp(K).$$

On dit qu'un entier $t \geq 0$ est un saut pour la filtration des $B^{(u)}$ s'il satisfait :

$$B^{(t-1)} \neq B^{(t)}.$$

Lorsque $t \geq 1$, nous énonçons déjà :

Lemme 3.1. *Si $t \geq 1$ est un saut pour la filtration $\{B^{(u)}\}_u$, alors t n'est pas divisible par p.*

Preuve : Supposons que t soit divisible par p et écrivons $t = pk$ pour un certain entier $k \geq 1$. Puisque t est un saut dans la filtration des $B^{(u)}$, il existe $x \in K$ tel que $\hat{x}$ soit dans $B^{(pk)}$ mais pas dans $B^{(pk-1)}$, si $\hat{x}$ désigne un représentant de x modulo $\wp(K)$. De plus, on peut prendre x dans $B \cap \mathfrak{p}_K^{-pk}$. En particulier, x est de valuation $v_K(x) = -pk$ et x n'appartient pas à $\wp(K)$. Alors, la sous-extension $M = K(\wp^{-1}(x))$ de L est cyclique d'ordre p et est engendrée par une racine α dans L de l'équation $\alpha^p - \alpha = x$.
De plus, si v_L désigne la valuation discrète normalisée de L qui prolonge celle de K et si e est l'indice de ramification de L/K, on a :

$$v_L(\alpha) = -ek.$$

Soit π une uniformisante de K. Il vient :

$$v_L(\alpha\pi^k) = 0,$$

et donc l'élément $z := \alpha\pi^k$ est une unité dans L.
D'autre part, l'élément x s'écrit $x = w\pi^{-pk}$ pour une unité w de K.
Alors, la relation $\alpha^p - \alpha = x$ devient après multiplication par π^{kp} :

$$z^p - \pi^{k(p-1)}z = w.$$

Si $\bar{w}$ est un représentant de w modulo $\mathfrak{p}_L$, il s'ensuit :

$$\bar{w} = \bar{w}_0^p \mod \mathfrak{p}_L,$$

où w_0 est une unité de U_K, puisque κ est parfait.
Ainsi, le corollaire 3.1 permet d'écrire dans $B/\wp(K)$:

$$\begin{aligned}
\hat{x} &= x - ((\frac{w_0}{\pi^k})^p - \frac{w_0}{\pi^k}) && \mod \wp(K) \\
&= \frac{1}{\pi^{kp}}(z^p - \pi^{k(p-1)}z - (w_0^p - \pi^{k(p-1)}w_0)) && \mod \wp(K) \\
&= \frac{1}{\pi^{kp}}(w - w_0^p + \pi^{k(p-1)}w_0) && \mod \wp(K).
\end{aligned}$$

Or dans le dernier terme de droite, $w - w_0^p$ appartient à $\mathfrak{p}_L \cap K = \mathfrak{p}_K$ et donc aussi $\pi^{k(p-1)}$ par construction. Ainsi, le terme $w - w_0^p + \pi^{k(p-1)}$ appartient à $\mathfrak{p}_K$, ce qui entraine $\hat{x} \in B^{(pk-1)}$, d'où une contradiction. $\diamond$

Ce lemme sera d'une importance cruciale pour la preuve du point (*iii*) du théorème 3.3.

Retournons à la filtration des quotients $B^{(u)}$. Par dualité, cette filtration induit une filtration décroissante dans H_B. En effet, les sous-groupes :

$$H_B^{(u)} := \{\varphi \in H_B \ : \ \varphi(B^{(u)}) = 0\}$$

forment une filtration décroissante de H_B, avec :

$$\{1\} = H_B^{(m)} \subset ... \subset H_B^{(1)} \subset H_B^{(0)} \subset H_B^{(-1)} = H_B,$$

où l'entier m est tel que $B^{(m)} = B/\wp(K)$.
Dans la filtration $H_B^{(u)}$ nous dirons cette fois qu'un entier $t \geq -1$ est un saut si :

$$H_B^{(t)} \neq H_B^{(t+1)},$$

de telle sorte que $t + 1 \geq 0$ soit un saut pour la filtration des $B^{(u)}$. On impose ainsi un décalage d'une unité entre la définition d'un saut pour les $B^{(u)}$ et celle pour les $H_B^{(u)}$.

Voici enfin le résultat principal de ce sous-paragraphe. Le théorème qui suit établit une correspondance explicite entre la filtration des sous-groupes $H_B^{(u)}$ et celle des groupes de ramification pour la notation supérieure de l'extension L/K.

Théorème 3.3. *Soit K un corps local de caractéristique $p > 0$ et de corps résiduel parfait. Soit L une extension abélienne finie d'exposant p sur K et soit G son groupe de Galois. Notons H_B le groupe $Hom(B/\wp(K), W_1(\mathbb{F}_p))$, où B est le sous-groupe $\wp(L) \cap K$ de K. L'isomorphisme d'Artin-Schreier-Witt $\mathfrak{as}_1 : G \xrightarrow{\simeq} H_B$ induit les isomorphismes suivants :*

(*i*) $G^{(-1)} \xrightarrow{\simeq} H_B^{(-1)}$

(*ii*) $G^{(0)} \xrightarrow{\simeq} H_B^{(0)}$

(*iii*) *et pour tout entier $u \geq 1$: $G^{(u)} \xrightarrow{\simeq} H_B^{(u-1)}$.*

Remarque 11. *Comme pour le théorème 3.2, on retrouve dans le théorème 3.3 l'égalité $G^{(0)} = G^{(1)}$ due au fait que l'extension L/K est sauvagement ramifiée.*

La preuve du théorème 3.3 que nous proposons nécessite un résultat sur les groupes de ramification d'un compositum, l'idée étant de considérer l'extension L/K comme le compositum de toutes ses sous-extensions cycliques et de leur appliquer le théorème 3.2. C'est le lemme qui suit.

Groupes de ramification d'un compositum.
Nous affirmons :

Lemme 3.2. *Soit K un corps local et soient L et L' deux extensions abéliennes finies de K telles que $L \cap L' = K$, de sorte que le compositum $L.L'$ soit une extension galoisienne de K. Notons G le groupe de Galois de $L.L'$ sur K. Soient H et H' les sous-groupes de G fixés par L et L' respectivement. Si H est inclus dans le plus grand sous-groupe de ramification non trivial de G, alors pour tout $u \geq -1$, on a un isomorphisme :*

$$G^{(u)} \xrightarrow{\simeq} (G/H)^{(u)} \times (G/H')^{(u)}.$$

Preuve : Notons $G^{(s)}$ le plus grand groupe de ramification non trivial de G, cela signifie :

$$G^{(s)} \neq \{1\}\ ,\ G^{(s+1)} = \{1\}.$$

Par hypothèse, $H \subset G^{(s)}$.
Fixons un entier $u \geq -1$. D'après ([60], Chap. IV, §3), on a :

$$(G/H)^{(u)} = G^{(u)}H/H \ \text{ et } \ (G/H')^{(u)} = G^{(u)}H'/H.$$

Ceci nous conduit à définir un homomorphisme :

$$F_u := G^{(u)} \longrightarrow (G/H)^{(u)} \times (G/H')^{(u)},$$

donné par :

$$\sigma \in G^{(u)} \mapsto (\sigma H, \sigma H').$$

C'est un morphisme injectif car $H \cap H' = \{1\}$, puisque $L \cap L' = K$.
Il est également surjectif dès lors que H est inclus dans $G^{(s)}$. En effet, si $u > s$, alors $G^{(u)} = \{1\}$ et F_u est clairement surjectif. Maintenant, si $u \leq s$, alors H est aussi un sous-groupe de $G^{(u)}$ et le groupe de ramification $(G/H)^{(u)}$ est isomorphe à $G^{(u)}/H$. Ainsi, pour un élément (ϕ, ϕ') de $(G/H)^{(u)} \times (G/H')^{(u)}$ donné, il existe σ dans $G^{(u)}$ tel que $\sigma = \phi \mod H$ et σ' dans $G^{(u)}H'$ tel que $\sigma' = \phi' \mod H'$. Or, par l'isomorphisme naturel $G \simeq H \times H'$, il existe aussi $h \in H$ et $h' \in H'$ tels que $\sigma h = \sigma' h'$. Cela signifie que l'élément σh de $G^{(u)}$ est envoyé sur (ϕ, ϕ') par F_u, d'où la surjectivité de F_u et la fin de la preuve ◇

Remarque 12. *Les conditions de notre lemme représentent un cas particulier d'un critère développé par Maus dans [45] : deux extensions L et L' sur K sont dites arithmétiquement disjointes sur K si la relation $G^{(v)} \simeq (G/H)^{(v)} \times (G/H')^{(v)}$ est satisfaite pour tous les réels $v \geq -1$.*

Preuve du théorème 3.3

Preuve :

(i) Cette assertion est évidente à partir des définitions.

(ii) Pour tout x de l'anneau d'entiers O_L notons $\bar{x}$ la classe de x modulo $\mathfrak{p}_L$.
D'abord, la théorie de la ramification donne un isomorphisme naturel de $G/G^{(0)}$ dans $Gal(\bar{l}, \kappa)$:

$$\begin{array}{rccl} \psi_1 : & G/G^{(0)} & \xrightarrow{\simeq} & Gal(\bar{l}/\kappa) \\ & \sigma + G^{(0)} & \mapsto & \bar{\sigma} : \{x + \mathfrak{p}_L \mapsto \sigma(x) + \mathfrak{p}_L\}. \end{array}$$

Ensuite, la théorie d'Artin-Schreier appliquée à l'extension résiduelle fournit un second isomorphisme :

$$\begin{array}{rccl} \psi_2 : & Gal(\bar{l}/\kappa) & \xrightarrow{\simeq} & Hom(\wp(\bar{l}) \cap \kappa/\wp(\kappa), \mathbb{Z}/p\mathbb{Z}) \\ & \bar{\sigma} & \mapsto & \varphi_{\bar{\sigma}} : \{\bar{x} + \wp(\kappa) \mapsto \bar{\sigma}(\bar{\xi}) - \bar{\xi}\}, \end{array}$$

où $\bar{\xi} \in \bar{l}$ est tel que $\bar{\xi}^p - \bar{\xi} = \bar{x}$ dans $\bar{l}$. Or par le lemme de Hensel, cette dernière égalité devient $\xi^p - \xi = x$ dans L. En particulier, il vient :

$$\bar{\sigma}(\bar{\xi}) - \bar{\xi} = \sigma(\xi) - \xi \mod \mathfrak{p}_L,$$

où $\sigma \in G$ est tel que $\psi_1(\sigma + G^{(0)}) = \bar{\sigma}$.
Enfin, puisque $B = \wp(L) \cap K$ et $O_K \cap \wp(K) = \wp(O_K)$, on a un isomorphisme naturel $B^{(0)} \simeq \wp(\bar{l}) \cap \kappa/\wp(\kappa)$. En effet :

$$\begin{array}{rl} B^{(0)} & = (B \cap O_K + \wp(K))/\wp(K) \\ & \simeq B \cap O_K/\wp(K) \cap B \cap O_K \ , \\ & \simeq \wp(L) \cap O_K/\wp(O_K) \end{array}$$

et puisque $\mathfrak{p}_K \subset \wp(O_K)$ par le corollaire 3.1, on en déduit :

$$\begin{array}{rl} B^{(0)} & \simeq (\wp(L) \cap O_K/\mathfrak{p}_K)/(\wp(O_K)/\mathfrak{p}_K) \\ & \simeq \wp(\bar{l}) \cap \kappa/\wp(\kappa), \end{array}$$

où le dernier isomorphisme est induit par la projection $O_K \twoheadrightarrow \kappa$.
On en déduit par dualité un troisème isomorphisme :

$$\begin{array}{rccl} \psi_3 \ : & Hom(\wp(\bar{l}) \cap \kappa/\wp(\kappa), \mathbb{Z}/p\mathbb{Z}) & \xrightarrow{\simeq} & Hom(B^{(0)}, \mathbb{Z}/p\mathbb{Z}) \\ & \varphi & \mapsto & \psi : \{x + \wp(K) \mapsto \varphi(\bar{x})\}. \end{array}$$

La composition des trois applications précédentes donne alors l'isomorphisme :

$$\begin{array}{rccl} \psi : & G/G^{(0)} & \xrightarrow{\simeq} & Hom(B^{(0)}, \mathbb{Z}/p\mathbb{Z}) \\ & \sigma + G^{(0)} & \mapsto & \psi_\sigma : \{x + \wp(K) \mapsto \sigma(\xi) - \xi\}, \end{array}$$

où $\xi \in L$ est tel que $\xi^p - \xi = x$.
De plus, puisque ψ_2 est induit par l'isomorphisme d'Artin-Schreier-Witt $\mathfrak{as}_1$ sur l'extension résiduelle, l'isomorphisme ψ rend le diagramme suivant commutatif :

$$\begin{array}{ccc} G & \twoheadrightarrow & G/G^{(0)} \\ \downarrow{\scriptstyle \mathfrak{as}_1} & & \downarrow{\scriptstyle \psi} \\ H_B & \twoheadrightarrow & Hom(B^{(0)}, \mathbb{Z}/p\mathbb{Z}). \end{array}$$

Ici, les homomorphismes horizontaux sont donnés par les morphismes de restriction dont les noyaux sont respectivement $G^{(0)}$ et $H_B^{(0)}$. Ainsi, l'isomorphisme d'Artin-Schreier-Witt $\mathfrak{as}_1$ envoie $G^{(0)}$ sur $H_B^{(0)}$, d'où un diagramme commutatif avec des lignes exactes :

$$\begin{array}{ccccccccc} 1 & \longrightarrow & G^{(0)} & \longrightarrow & G & \longrightarrow & G/G^{(0)} & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \mathfrak{as}_1} & & \downarrow{\scriptstyle \mathfrak{as}_1} & & \downarrow{\scriptstyle \psi} & & \\ 1 & \longrightarrow & H_B^{(0)} & \longrightarrow & H_B & \longrightarrow & Hom(B^{(0)}, \mathbb{Z}/p\mathbb{Z}) & \longrightarrow & 1 \end{array}$$

L'isomorphisme $\mathfrak{as}_1$ induit donc un isomorphisme $G^{(0)} \xrightarrow{\simeq} H_B^{(0)}$, d'où la preuve de l'assertion (ii).

(iii) Nous montrons l'assertion (iii) par récurrence sur l'ordre du groupe G, plus précisément sur l'exposant $n \geq 1$, où $|G| = p^n$.

a) $n = 1$
Dans ce cas, l'extension L/K est cyclique de degré p, il en est de même pour $B/\wp(K)$. En particulier, il y a seulement un saut dans la filtration des $B^{(u)}$, nous le notons $t \geq 0$. Par définition, on a :

$$B^{(t)} = B/\wp(K) \ \text{ et } \ B^{(t-1)} = \{1\},$$

de telle sorte que $t - 1$ est un saut pour la filtration des $\{H_B^{(u)}\}_u$ de H_B :

$$H_B^{(t-1)} = H_B \ \text{ and } \ H_B^{(t)} = \{1\}.$$

Il existe donc x dans B tel que son image modulo $\wp(K)$ soit dans $B^{(t)}$ mais pas dans $B^{(t-1)}$, ce qui signifie : $L = K(\wp^{-1}(x))$. De plus, sans perte de généralité, on peut supposer $v_K(x) = -t$. Nous distinguons alors trois cas :
1) Si $t = 0$, le théorème 3.2 montre que L/K est non ramifiée, i ;e. $G^{(0)} = \{1\}$, d'où, pour tout entier $u \geq 1$:

$$G^{(u)} = \{1\} \simeq H_B^{(u-1)}.$$

2) Si $t > 0$ et si t est premier à p, le théorème 3.2 montre que l'extension est totalement ramifiée et que le saut dans la filtration de ses groupes de ramification est t. Alors, pour tout entier $u \geq 1$, on a encore :

$$\begin{array}{ll} G^u = G \simeq H_B^{(u-1)} & \text{si } u \leq t \\ G^{(u)} = \{1\} \simeq H_B^{(u-1)} & \text{si } u > t. \end{array}$$

3) Le cas où $t > 0$ et p divise t est impossible par le lemme 3.1.

Ainsi, l'assertion (iii) est démontrée pour toute extension cyclique d'ordre p.

(b) $n \geq 2$

Soit $n \geq 1$. Supposons que l'assertion (iii) est vraie pour toute extension abélienne finie de K de degré inférieur ou égal à p^n. Soit L/K une extension abélienne finie d'exposant p^{n+1} et soit G son groupe de Galois. Il y a au plus $n+1$ dans la filtration de ses groupes de ramification. Notons $G^{(s)}$ son plus grand groupe de ramification non trivial, c'est-à-dire :

$$G^{(s)} \neq \{1\}\ ,\ G^{(s+1)} = \{1\}.$$

Alors $G^{(s)}$ est un p-groupe d'ordre $p^s \leq p^{n+1}$ avec $s \geq 1$. En particulier il contient un sous-groupe, noté J_1, d'ordre p. De plus, il existe un autre sous-groupe J_2 tel que l'on ait un isomorphisme naturel :

$$G \simeq J_1 \times J_2,$$

et J_2 est d'ordre inférieur ou égal à p^n.

Soient maintenant M_1 et M_2 les sous-corps de L/K fixés par J_2 et J_1 respectivement de sorte que M_1/K (resp. M_2/K) ait pour groupe de Galois G/J_1 (resp. G/J_2). On obtient simultanément :

$$M_1 \cap M_2 = K \ \text{ et } \ L = M_1.M_2.$$

Alors, d'après le lemme 3.2, l'isomorphisme naturel $G \xrightarrow{\simeq} G/J_1 \times G/J_2$ induit pour tout $u \geq 1$ un isomorphisme :

$$G^{(u)} \xrightarrow{\simeq} (G/J_1)^{(u)} \times (G/J_2)^{(u)}.$$

Notons A_1 (resp. A_2) le sous-groupe $\wp(M_1) \cap K$ (resp. $\wp(M_2) \cap K$) de B. Puisque les extensions M_1 et M_2 sont de degré inférieur ou égal à p^n sur K, on en déduit un isomorphisme pour tout $u \geq 1$:

$$G^{(u)} \xrightarrow{\simeq} H_{A_1}^{(u-1)} \times H_{A_2}^{(u-1)}$$

donné par :

$$\sigma \mapsto (\mathfrak{as}_1(\sigma_{|M_1}), \mathfrak{as}_1(\sigma_{|M_2})).$$

D'autre part, on sait que le groupe G est isomorphe au produit $G/J_1 \times G/J_2$ de façon naturelle. L'isomorphisme d'Artin-Schreier-Witt $\mathfrak{as}_1$ induit donc l'isomorphisme :

$$\mathcal{E} : H_B \xrightarrow{\simeq} H_{A_1} \times H_{A_2}.$$

Pour tout $u \geq 1$, nous affirmons alors que l'isomorphisme $\mathcal{E}$ envoie le sous-groupe $H_B^{(u-1)}$ sur :

$$\mathcal{E}(H_B^{(u-1)}) = H_{A_1}^{(u-1)} \times H_{A_2}^{(u-1)}.$$

En effet, la première inclusion est évidente puisque $A_i^{(u-1)} = B^{(u-1)} \cap A_i/\wp(K)$ pour $i = 1, 2$.

Réciproquement, soit (σ_1, σ_2) un élément de $H_{A_1}^{(u-1)} \times H_{A_2}^{(u-1)}$. Par l'isomorphisme $\mathcal{E}$, il existe f dans H_B tel que :

$$f_{|A_i/\wp(K)} = \sigma_i,\ i = 1, 2.$$

En particulier :

$$f(B^{(u-1)} \cap A_i/\wp(K)) = 0,\ i = 1, 2.$$

Or, par dualité, $\mathcal{E}$ induit un isomorphisme :

$$B/\wp(K) \xrightarrow{\simeq} A_1/\wp(K) \times A_2/\wp(K),$$

et donc f est nulle sur $B^{(u-1)}$, c'est-à-dire $f \in H_B^{(u-1)}$.

D'où un nouvel isomorphisme pour tout $u \geq 1$:

$$H_B^{(u-1)} \xrightarrow{\simeq} H_{A_1}^{(u-1)} \times H_{A_2}^{(u-1)}.$$

En conclusion, l'application d'Artin-Schreier-Witt induit par composition les isomorphismes :

$$\forall u \geq 1,\ G^{(u)} \xrightarrow{\simeq} H_B^{(u-1)},$$

ce qui montre l'assertion (iii). $\diamond$

Corollaire 3.2. *Il n'y a pas de saut divisible par p dans la filtration des groupes de ramification d'une extension abélienne finie d'exposant p sur K.*

Preuve : D'abord 0 ne peut pas être un saut puisque $G^{(0)} = G^{(1)}$. Ensuite, à la fois le lemme 3.1 et la preuve du théorème 3.3 montrent que tout saut $t > 0$ qui est strictement positif ne peut pas être divisible par p. $\diamond$

3.2.3 Groupes de ramification dans l'extension abélienne maximale d'exposant p

Ce dernier sous-paragraphe calcule les groupes de ramification pour l'extension abélienne maximale d'exposant p sur K en passant à la limite projective dans le théorème 3.3. Notons K_p cette extension et G_p son groupe de Galois sur K. D'après le chapitre 2, l'isomorphisme d'Artin-Schreier-Witt est donné par :

$$\mathfrak{as}_1 \ :\ G_p \xrightarrow{\simeq} H_p,$$

où H_p désigne le groupe d'homomorphismes continus $\mathrm{Hom}(K/\wp(K), \mathbb{Z}/p\mathbb{Z})$ et est muni de la topologie induite du produit $\prod_{K/\wp(K)} \mathbb{Z}/p\mathbb{Z}$.

Généralisant la filtration $\{B^{(u)}\}_u$ du théorème 3.3, on considère dans $K/\wp(K)$ la filtration décroissante formée des sous-groupes :

$$K^{(u)} := \mathfrak{p}_K^{-u}/\wp(K),\ \forall u \geq -1$$

Par dualité, nous définissons alors dans H_p les sous-groupes :

$$H_p^{(u)} := \{\varphi \in H_p \ :\ \varphi(K^{(u)}) = 0\}.$$

Clairement, ces sous-groupes forment une filtration décroissante de sous-groupes de H_p avec $H_p^{(-1)} = H_p$. Par contre, en général, nous n'avons plus $H^{(m)} = 1$ pour aucun entier m.

En outre, les groupes $H_p^{(u)}$ sont tous fermés dans H_p, ce sont en particulier des groupes compacts. On affirme alors :

Corollaire 3.3. *Pour tout entier $u \geq -1$, l'isomorphisme d'Artin-Schreier-Witt $\mathfrak{as}_1$ induit les isomorphismes de groupes topologiques suivants :*

(i) $G_p^{(-1)} \xrightarrow{\simeq} H_p^{(-1)}$

(ii) $G_p^{(0)} \xrightarrow{\simeq} H_p^{(0)}$

(iii) et pour tout entier $u \geq 1$, $G_p^{(u)} \xrightarrow{\simeq} H_p^{u-1}$.

Preuve : (i) Evident.

(ii) Notons $\mathcal{S}$ l'ensemble des sous-groupes de K qui contiennent $\wp(K)$ avec un indice fini. Soit $B \in \mathcal{S}$. Notons G_B le groupe de Galois de l'extension abélienne d'exposant p^n sur K correspondante, i.e. de l'extension $L = K(\wp^{-1}B)$.

D'abord, par le théorème 3.3 l'application d'Artin-Schreier-Witt $\mathfrak{as}_1$ induit un isomorphisme que nous noterons ψ_B :

$$\psi_B \ :\ G_B^{(0)} \xrightarrow{\simeq} H_B^{(0)}.$$

D'autre part, on a par définition :

$$G_p^{(0)} = \varprojlim G_B^{(0)},$$

lorsque B parcourt l'ensemble $\mathcal{S}$ et par rapport aux applications de restriction.
On a également :

$$H_p^{(0)} = \varprojlim H_B^{(0)},$$

puisque $(K \cap \mathfrak{p}_K^0)/\wp(K)$ est la réunion de tous les sous-groupes $B^{(0)}$ lorsque B parcourt $\mathcal{S}$.
Alors, pour $B \subset B'$ dans $\mathcal{S}$ le diagramme suivant est commutatif :

$$\begin{array}{ccc} G_{B'}^{(0)} & \twoheadrightarrow & G_B^{(0)} \\ \downarrow{\scriptstyle \psi'_B} & & \downarrow{\scriptstyle \psi_B} \\ H_{B'}^{(0)} & \twoheadrightarrow & H_B^{(0)} \end{array}$$

où les applications horizontales sont les restrictions.

Ainsi, par la propriété universelle des limites projectives et puisque les groupes $G_B^{(0)}$ et $H_B^{(0)}$ sont compacts, il existe un unique isomorphisme de groupes topologiques :

$$\psi^{(0)} : G_p^{(0)} \xrightarrow{\simeq} H_p^{(0)}.$$

Cet isomorphisme est de plus induit par $\mathfrak{as}_1$, ce qui montre l'assertion (ii) .

(iii) La preuve est essentiellement la même que pour (ii), en remplaçant l'indice 0 par u pour G_p et par $u-1$ pour H_p lorsque $u \geq 1$. ◇

Remarque 13. *Ecrivons le corollaire 3.3 pour les groupes de ramification indexés par un nombre réel. Puisque tous les sauts de la filtration des $G^{(v)}$ sont entiers par le théorème de Hasse-Arf, rappelons que si $v \geq -1$ est un réel, alors on a :*

$$G_p^{(v)} = G_p^{(i)},$$

où i est le plus petit entier supérieur à v $(i-1 < v \leq i)$.
Pour ce même indice, on notera donc :

$$K^{(v)} := K^{(i)},$$

et donc :

$$H_p^{(v)} := H_p^{(i)}.$$

Ainsi, adoptant ces nouvelles notations, le corollaire 3.3 devient :

Corollaire 3.4. *Pour tous réels $v \geq -1$, l'isomorphisme d'Artin-Schreier-Witt $\mathfrak{as}_1$ induit les isomorphismes de groupes topologiques :*

(i) $G_p^{(-1)} \xrightarrow{\simeq} H_p^{(-1)}$

(ii) $G_p^{(v)} \xrightarrow{\simeq} H_p^{(v)}$ si $-1 < v \leq 0$

(iii) $G_p^{(v)} \xrightarrow{\simeq} H_p^{(v-1)}$ si $v > 0$.

3.3 Le groupe d'inertie des extensions d'Artin-Schreier-Witt

Ce paragraphe tente de généraliser l'étude précédente à toutes les extensions d'Artin-Schreier-Witt sur K. On y parvient partiellement en donnant une description précise du groupe d'inertie de toutes les extensions abéliennes maximales d'exposant p^n sur K pour $n \geq 1$.

Plus précisément, pour tout entier $n \geq 1$, notons K_{p^n} l'extension abélienne maximale d'exposant p^n sur K et G_{p^n} son groupe de Galois. Nous allons calculer le groupe d'intertie de G_{p^n} en montrant que l'application d'Artin-Schreier-Witt $\mathfrak{as}_n$ induit un isomorphisme de groupes topologiques :

$$G_{p^n}^{(0)} \xrightarrow{\simeq} \{\varphi \in H_{p^n} \ : \ \varphi(W_n(O_K)/\wp(W_n(O_K))) = 0\}.$$

C'est le théorème 3.4. Par passage à la limite projective, le corollaire 3.5 en déduit le groupe d'inertie de la pro-p extension abélienne maximale K_{p^∞} de K à travers l'isomorphisme de groupes topologiques :

$$G_{p^\infty}^{(0)} \xrightarrow{\simeq} \{\varphi \in H_{p^\infty} \ : \ \varphi(W(O_K)/\wp(W(O_K)) = 0\},$$

induit par $\mathfrak{as}_\infty$ à son tour.

Cette généralisation nécessite d'abord quelques précisions sur les vecteurs de Witt à coefficients dans l'anneau O_K des entiers de K, pour lesquels nous développons quelques propriétés de base dans le sous-paragraphe 1.

3.3.1 Somme dans $W_n(O_K)$

Le présent sous-paragraphe regroupe quelques résultats préliminaires sur la somme dans l'anneau de Witt $W_n(O_K)$. Rappelons que dans le paragraphe 1.1 du chapitre 1, en notant $R_{\mathbb{Q}}$ l'anneau de polynômes $\mathbb{Q}[X_0, X_1, ..., Y_0, ...]$, nous avons défini la somme de deux vecteurs de Witt $(X_0, ..., X_{n-1})$ et $(Y_0, ..., Y_{n-1})$ dans $W_n(R_{\mathbb{Q}})$ comme le vecteur $(Z_0, ..., Z_{n-1})$ donné par ses composantes fantômes :

$$\forall i,\ 0 \leq i \leq n-1,\ Z^{(i)} = X^{(i)} + Y^{(i)},$$

De plus, d'après la proposition 1.2 du chapitre 1, il existe des polynômes S_i de $\mathbb{Z}[X_0, ..., X_i, Y_0, ..., Y_i]$ tels que chaque i-ème composante du vecteur somme s'écrit :

$$Z_i = S_i(X_0, ..., X_i, Y_0, ..., Y_i).$$

Cette relation nous permet de montrer récursivement sur l'indice i la formule :

$$\begin{aligned} Z_i = \quad & X_i + Y_i + \tfrac{1}{p^i}((X_0^{p^i} + Y_0^{p^i} - S_0(X_0, Y_0)^{p^i}) + ... \\ & ... + p^{i-1}(X_{i-1}^p + Y_{i-1}^p - S_{i-1}(X_0, ..., X_{i-1}, Y_0, ..., Y_{i-1})^p). \end{aligned}$$

Pour tout entier $i \geq 1$, cela nous conduit à introduire naturellement le polynôme suivant dans $\mathbb{Z}[X_0, ..., X_{i-1}, Y_0, ..., Y_{i-1}]$:

$$C_i(X_0, ..., X_{i-1}, Y_0, ..., Y_{i-1}) := S_i(X_0, ..., X_i, Y_0, ..., Y_i) - (X_i + Y_i),$$

et pour $i = 0$:

$$C_0 = 0 \in \mathbb{Z}.$$

Clairement, les polynômes C_i ont tous des coefficients entiers et satisfont ;

$$Z_i = X_i + Y_i + C_i(X_0, ..., X_{i-1}, Y_0, ..., Y_{i-1}).$$

Maintenant fixons deux vecteurs de Witt $(x_0, ..., x_{n-1})$ et $(y_0, ..., y_{n-1})$ dans $W_n(K)$. D'après la définition 1.3 du chapitre 1, leur vecteur somme $(z_0, ..., z_n)$ est défini directement par les relations :

$$z_i = S_i(x_0, ..., x_i, y_0, ..., y_i),$$

c'est-à-dire :

$$z_i = x_i + y_i + C_i(x_0, ..., x_{i-1}, y_0, ..., y_{i-1}),$$

pour tout $i \geq 0$.
C'est pourquoi, dans ce qui suit, nous nous intéresserons aux valeurs $C_i(x_0, ..., x_{i-1}, y_0, ..., y_{i-1})$ lorsque les vecteurs de Witt $(x_0, ..., x_{n-1})$ et $(y_0, ..., y_{n-1})$ sont tous deux dans $W_n(O_K)$. Plus précisément, nous allons montrer trois lemmes utiles pour la suite :

Lemme 3.3. *Soient $(x_0, ..., x_{n-1})$ et $(y_0, ..., y_{n-1})$ deux vecteurs de Witt dans $W_n(O_K)$. Si de plus toutes les composantes y_i sont dans $\mathfrak{p}_K$ alors on a :*

$$C_i(x_0, ..., x_{i-1}, y_0, ..., y_{i-1}) \in \mathfrak{p}_K,$$

pour tout i, $0 \leq i \leq n-1$.

Lemme 3.4. *Soit $(z_0, ..., z_{n-1})$ un vecteur de Witt dans $W_n(O_K)$. Si toutes ses composantes z_i sont dans $\mathfrak{p}_K$ alors $(z_0, ..., z_{n-1})$ appartient à $\wp(W_n(O_K))$.*

Lemme 3.5. *Soit $(x_0, ..., x_{n-1})$un vecteur de Witt dans $W_n(O_K)$ et soit $\pi_0, ..., \pi_{n-1}$ n éléments de $\mathfrak{p}_K$. On a :*

$$(x_0 + \pi_0, ..., x_{n-1} + \pi_{n-1}) - (x_0, ..., x_{n-1}) \in \wp(W_n(O_K)).$$

Avant de montrer ces lemmes, rappelons simplement que l'idéal maximal $\mathfrak{p}_K$ de O_K est inclus dans $\wp(K)$ par le corollaire 3.1. En fait, le lemme 3.4 est une généralisation de ce corollaire.

Remarque 14. *Les preuves que nous proposons sont essentiellement des manipulations sur les vecteurs de Witt et sur l'addition dans l'anneau de Witt. Le lecteur peut passer outre ces démonstrations sauf s'il désire se familiariser avec les outils de Witt.*

Remarque 15. *Le lemme 3.4 peut également se montrer par un argument topologique à partir du corollaire 1.2 du chapitre 1. En effet, munissant O_K de la topologie induite de le topologie usuelle de K pour sa valuation, l'anneau $W(O_K)$ est muni de la topologie p-adique correspondant à la convergence composante par composante induite du produit $\prod O_K$. Alors, si $z = (z_0, ..., z_{n-1})$ est un vecteur de $W_n(O_K)$ dont toutes ses composantes sont dans $\mathfrak{p}_K$, la somme $\sum_{h=0}^{\infty} z^{p^h}$ converge composante par composante, donc converge dans $W_n(O_K)$ vers un vecteur Z. Clairement, on a alors : $z = \wp(-Z)$, i.e. $z \in \wp(W_n(O_K))$.*

Preuve : [Lemme 3.3]
Pour $i = 0$ l'assertion est triviale, concentrons-nous alors sur le cas $i \geq 1$.
Montrons par itération sur $i \geq 1$ que chaque polynôme C_i de $\mathbb{Z}[X_0, ..., X_{i-1}, Y_0, ..., Y_{i-1}]$ satisfait :

$$C_i(X_0, ..., X_{i-1}, 0, ..., 0) = 0.$$

En effet, pour $i = 1$ nous avons formellement :

$$\begin{aligned} C_1(X_0, Y_0) &= \frac{1}{p}((X_0^p + Y_0^p - (X_0 + Y_0)^p) \\ &= \sum_{l=1}^{p-1} \frac{1}{p}\binom{p}{l} x_0^l y_0^{p-l}. \end{aligned}$$

Donc $C_1(X_0, Y_0)$ se factorise par Y_0, ce qui signifie $C_1(X_0, 0) = 0$.
Soit $i \geq 1$ un entier. Supposons que l'on ait dans l'anneau $\mathbb{Z}[X_0, ..., X_{j-1}, Y_0, ..., Y_{j-1}]$ et pour tout $j \in \{1, ..., i-1\}$:

$$C_j(X_0, ..., X_{j-1}, 0, ..., 0) = 0.$$

On écrit :

$$R_i(X_0, ..., X_{i-1}, Y_0, ..., Y_{i-1}) = p^i C_i(X_0, ..., X_{i-1}, Y_0, ..., Y_{i-1}),$$

c'est-à-dire, R_i est combinaison linéaire de termes du type :

$$\begin{aligned}\Gamma_j(X_0,...,X_j,Y_0,...,Y_j) &= p^j(X_j^{p^{i-j}}+Y_j^{p^{i-j}}-(X_j+Y_j+C_j(X_0,...,X_{j-1},Y_0,...,Y_{j-1}))^{p^{i-j}}\\ &= -p^j(\sum_{l=1}^{p^{i-j}-1}\binom{p^{i-j}}{l}x_j^l y_j^{p^{i-j}-l}+\sum_{l=1}^{p^{i-j}-1}\binom{p^{i-j}}{l}(X_j+Y_j)^l C_j^{p^{i-j}-l}+C_j^{p^{i-j}}).\end{aligned}$$

pour tout j de $\{0,...,i-1\}$ avec $C_0=0$.
Par récurrence, on a donc pour chaque entier j, $j\leq 0\leq i-1$:

$$\Gamma_j(X_0,...,X_j,0,...,0)=0,$$

d'où, en sommant :

$$R_i(X_0,...,X_{i-1},0,...,0)=0.$$

Maintenant, $C_i=\frac{1}{p^i}R_i$ et C_i tout comme R_i sont des polynômes de $\mathbb{Z}[X_0,...,X_{i-1},Y_0,...,Y_{i-1}]$. En particulier, tous les coefficients de R_i sont divisibles par p^i. Toujours dans $\mathbb{Z}[X_0,...,X_{i-1},Y_0,...,Y_{i-1}]$, nous avons donc :

$$C_i(X_0,...,X_{i-1},0,...,0)=0,$$

ce qui montre notre affirmation.

Il en résulte que chaque polynôme C_i est dans l'idéal de $\mathbb{Z}[X_0,...,X_{i-1},Y_0,...,Y_{i-1}]$ engendré par les éléments $Y_0,...,Y_{i-1}$:

$$C_i\ \in <Y_0,...,Y_{i-1}>.\mathbb{Z}[X_0,...,X_{i-1},Y_0,...,Y_{i-1}].$$

Or, si l'on évalue C_i en $x_0,...,x_{i-1},y_0,...,y_{i-1}$ lorsque ces variables appartiennent à O_K et si de plus $y_0,...,y_{i-1}$ sont dans $\mathfrak{p}_K$, la valeur :

$$c_i=C_i(x_0,...,x_{i-1},y_0,...,y_{i-1})$$

est dans l'idéal de O_K engendré par $y_0,...,y_{i-1}$. Ainsi, tous les coefficients c_i sont dans $\mathfrak{p}_K$, d'où la preuve du lemme 3.3. ◇

Preuve : [Lemma 3.4]
Il s'agit de montrer l'existence d'un vecteur de Witt $(w_0,...,w_{n-1})$ dans $W_n(O_K)$ tel que :

$$\wp(w_0,...,w_{n-1})=(z_0,...,z_{n-1}),$$

ce qui signifie :

$$w_i^p-w_i=z_i+C_k(w_0,...,w_{i-1},z_0,...,z_{i-1})$$

pour tout entier i, $0\leq i\leq n-1$.
L'idée est alors de construire un tel vecteur composante par composante, de façon récursive.
Pour $i=0$, l'équation :

$$W^p-W=z_0,$$

admet une solution w_0 dans K puisque z_0 est dans $\mathfrak{p}_K\subset\wp(K)$. De plus, si l'on considère les valuations, on voit que w_0 est en fait dans O_K.

Or, pour un entier i fixé, $0\leq i\leq n-1$, supposons qu'il existe des composantes $w_0,...,w_i$ dans O_K telles que pour tout j, $1\leq j\leq i$:

$$w_j^p-w_j=z_j+C_i(w_0,...,w_{j-1},z_0,...,z_{j-1}).$$

Considérons alors l'équation :

$$W^p-W=z_{i+1}+C_{i+1}(w_0,...,w_i,z_0,...,z_i).$$

Puisque $w_0,...,w_i$ sont tous dans O_K et $z_0,...,z_i$ dans $\mathfrak{p}_K$, $C_{i+1}(w_0,...,w_i,z_0,...,z_i)$ est dans $\mathfrak{p}_K$ par le lemme 3.3. Mais z_{i+1} est dans $\mathfrak{p}_K$ aussi et donc le terme de droite appartient à $\mathfrak{p}_K$.

Ainsi, l'équation admet dans K une solution w_{i+1} qui appartient à O_K. On peut donc construire récursivement un vecteur de Witt $(w_0, ..., w_{n-1})$ dans $W_n(O_K)$ tel que

$$\wp(w_0, ..., w_{n-1}) = (z_0, ..., z_{n-1}).$$

D'où le preuve du lemme 3.4. ◇

Preuve : [Lemma 3.5]
Notons $(z_0, ..., z_{n-1})$ le vecteur de Witt :

$$(z_0, ..., z_{n-1}) := (x_0 + \pi_0, ..., x_{n-1} + \pi_{n-1}) - (x_0, ..., x_{n-1}).$$

Ce vecteur est dans l'anneau $W_n(O_K)$ en tant que somme. Montrons qu'en fait toutes ses composantes sont dans $\mathfrak{p}_K$, nous conclurons alors par le lemme 3.4.

Nous raisonnons par récurrence encore, à partir de la relation :

$$z_i = \pi_i - C_i(x_0, ..., x_{i-1}, z_0, ..., z_{i-1}),$$

pour tout entier i, $0 \leq i \leq n-1$.

Pour $i = 0$, $z_0 = \pi_0$ et donc z_0 est dans $\mathfrak{p}_K$.

Pour un entier $i \geq 0$, supposons que $z_0, ..., z_i$ est dans $\mathfrak{p}_K$. Par le lemme 3.3, $C_{i+1}(x_0, ..., x_i, z_0, ..., z_i)$ est aussi dans $\mathfrak{p}_K$. Il en est de même pour z_{i+1} en tant que somme.

Ainsi, par récurrence sur i, toutes les composantes z_i de $(z_0, ..., z_{n-1})$ sont dans $\mathfrak{p}_K$. Appliquant le lemme 3.4, on en déduit que le vecteur de Witt $(z_0, ..., z_{n-1})$ appartient à $\wp(W_n(O_K))$. ◇

3.3.2 Groupe d'inertie de G_{p^n}

Nous avons maintenant tous les outils en main pour calculer le groupe d'inertie de chaque extension abélienne maximale d'exposant p^n sur K, notée K_{p^n}.

Fixons un entier $n \geq 1$. On note G_{p^n} le groupe de Galois de l'extension K_{p^n}/K et H_{p^n} le groupe $\mathrm{Hom}(W_n(K)/\wp(W_n(K)), \mathbb{Z}/p^n\mathbb{Z})$. Rappelons que la théorie d'Artin-Schreier-Witt établit un isomorphisme de groupes topolgiques entre ces deux groupes, noté $\mathfrak{as}_n$. En outre, d'après la proposition 3.3, l'extension résiduelle de K_{p^n}/K est l'extension κ_{p^n} abélienne maximale d'exposant p^n sur κ, son groupe de Galois satisfait donc :

$$Gal(\kappa_{p^n}/\kappa) \xrightarrow{\simeq} \bar{h}_{p^n},$$

où $\bar{h}_{p^n}$ désigne le groupe $\mathrm{Hom}(W_n(\kappa)/\wp(W_n(\kappa)), \mathbb{Z}/p^n\mathbb{Z})$.

Le lemme 3.5 nous permet alors de définir un homomorphisme de groupes :

$$\phi_n : H_{p^n} \longrightarrow \bar{h}_{p^n},$$

en posant :

$$\phi_n(\varphi) := \{(\bar{x}_0, ..., \bar{x}_{n-1}) + \wp(W_n(\kappa)) \mapsto \varphi((x_0, ..., x_{n-1}) + \wp(W_n(K)))\},$$

où pour tout i, x_i appartient à O_K et satisfait $x_i = \bar{x}_i \mod \mathfrak{p}_K$.

En effet, montrons d'abord que cette application est bien définie. Soit $(x_0, ..., x_{n-1})$ et $(y_0, ..., y_{n-1})$ deux vecteurs de $W_n(K)$ tels que pour chaque indice i les composantes x_i et y_i sont respectivement des représentants de $\bar{x}_i$ modulo $\mathfrak{p}_K$:

$$x_i = y_i = \bar{x}_i \mod \mathfrak{p}_K.$$

En particulier, $(y_0, ..., y_{n-1})$ s'écrit $(x_0+\pi_0, ..., x_{n-1}+\pi_{n-1})$ pour des éléments π_i de $\mathfrak{p}_K$. Ainsi, par le lemme 3.5, la différence $(y_0, ..., y_{n-1})-(x_0, ..., x_{n-1})$ est dans $\wp(W_n(O_K))$ et donc $\phi_n(\varphi(\bar{x}_0, ..., \bar{x}_{n-1}))$ ne dépend pas du choix des représentants $\bar{x}_0, ..., \bar{x}_{n-1}$ in O_K.

Ensuite, l'application ϕ_n est clairement un morphisme de groupes. De plus, son noyau est donné par le sous-groupe :

$$\mathfrak{K}_n := \{\varphi \in H_{p^n} \ : \ \varphi((W_n(O_K) + \wp(W_n(K)))/\wp(W_n(K)), \mathbb{Z}/p^n\mathbb{Z}) = 0\}.$$

D'où une suite exacte :

$$0 \to \mathfrak{K}_n \to H_{p^n} \to Hom(W_n(\kappa)/\wp(W_n(\kappa, \mathbb{Z}/p^n\mathbb{Z}).$$

Or d'après la théorie de la ramification on a aussi :

$$0 \to G_{p^n}^{(0)} \to G_{p^n} \stackrel{\epsilon_n}{\to} Gal(\kappa_{p^n}/\kappa) \to 0,$$

où l'application ϵ_n est définie comme suit :

$$\epsilon_n(\sigma) := \bar{x} \mapsto \sigma(\bar{x}),$$

pour un certain représentant x de $\bar{x}$ modulo $\mathfrak{p}_L$, où L désigne l'extension finie non ramifiée de K correspondant à la sous-extension séparable $\bar{l} = \kappa(\wp^{-1}(\bar{x}))$ de κ_{p^n}/κ par la proposition 3.1.
L'isomorphisme $\mathfrak{as}_n$ d'Artin-Schreier-Witt rend alors le diagramme suivant commuttaif :

$$\begin{array}{ccc} G_{p^n} & \xrightarrow{\epsilon_n} & Gal(\kappa_{p^n}/\kappa) \\ \downarrow{\scriptstyle \mathfrak{as}_n} & & \downarrow{\scriptstyle \bar{\mathfrak{as}}_n} \\ H_{p^n} & \xrightarrow{\phi_n} & \bar{h}_{p^n} \end{array}$$

où $\bar{\mathfrak{as}}_n$ est l'isomorphisme d'Artin-Schreier-Witt de l'extensionκ_{p^n}/κ).
D'où le diagramme commutatif :

$$\begin{array}{ccccccccc} 0 & \longrightarrow & G_{p^n}^{(0)} & \longrightarrow & G_{p^n} & \xrightarrow{\epsilon_n} & Gal(\kappa_{p^n}/\kappa) & \longrightarrow & 0 \\ & & \| & & \downarrow{\scriptstyle \mathfrak{as}_n} & & \downarrow{\scriptstyle \bar{\mathfrak{as}}_n} & & \\ 0 & \longrightarrow & \mathfrak{K}_n & \longrightarrow & H_{p^n} & \xrightarrow{\phi_n} & \bar{h}_{p^n} & & \end{array}$$

où les deux lignes verticales de droite sont des isomorphismes. On en déduit un isomorphisme de groupes topologiques entre $G_{p^n}^{(0)}$ et $\mathfrak{K}_n$.

Voici enfin le résultat principal de ce paragraphe :

Théorème 3.4. *Soit K un corps local de caractéristique $p > 0$ et de corps résiduel parfait. Soit $n \geq 1$ un entier. Le groupe d'inertie de l'extension abélienne maximale d'exposant p^n sur K est donné par l'isomorphisme de groupes topologiques suivant :*

$$G_{p^n}^{(0)} \stackrel{\simeq}{\longrightarrow} \{\varphi \in H_{p^n} \ ; \ \varphi(W_n(O_K)/\wp(W_n(O_K))) = 0\},$$

induit par l'isomorphisme d'Artin-Schreier-Witt $\sigma \mapsto \mathfrak{as}_n(\sigma)$.

Nous montrons d'abord un résultat préliminaire :

Lemme 3.6. *On a :*

$$\wp(W_n(O_K)) = \wp(W_n(K)) \cap W_n(O_K).$$

Preuve : La première inclusion est triviale puisque $\wp$ est un morphisme de groupes sur $W_n(O_K)$. Réciproquement, soit $(z_0, ..., z_{n-1})$ un vecteur dans $\wp(W_n(K) \cap W_n(O_K)$. Toutes ses composantes z_i sont dans O_K et il existe un vecteur $(w_0, ..., w_{n-1})$ de $W_n(K)$ tel que :

$$\wp(w_0, ..., w_{n-1}) = (z_0, ..., z_{n-1}).$$

D'après le sous-paragraphe 3.3.1, cette relation est équivalente au système

$$\{w_k^p - w_k = z_k + C_k(z_0, ..., z_{k-1}, w_0, ..., w_{k-1})\}_k,$$

lorsque k parcourt $\{0, ..., n-1\}$ et où $C_0 = 0$.
Si $k = 0$, la relation $w_0^p - w_0 = z_0$ implique que w_0 est dans O_K aussi en considérant les valuations.
Pour un entier k fixé, $0 \leq k \leq n-1$, supposons que toutes les composantes $w_0, ..., w_k$ sont dans O_K. Alors le terme de droite :

$$z_{i+1} + C_{i+1}(z_0, ..., z_i, w_0, ..., w_i)$$

est aussi dans O_K puisque C_{i+1} est un polynôme à coefficients entiers. Pour les mêmes raisons, w_{i+1} est dans O_K.
On montre ainsi par récurrence sur i que chaque w_i est dans O_K. Donc $(z_0, ..., z_{n-1})$ est dans $\wp(W_n(O_K))$, ce qui prouve le lemme 3.6. ◇

D'où la preuve du théorème 3.4 :

Preuve : Nous avons déjà montré l'existence d'un isomorphisme entre $G_{p^n}^{(0)}$ et le noyau $\mathfrak{K}_n$ de ϕ_n. Il reste à montrer l'isomorphisme :

$$\mathfrak{K}_n \xrightarrow{\simeq} \{\varphi \in H_{p^n} \ ; \ \varphi(W_n(O_K)/\wp(W_n(O_K))) = 0\},$$

ce qui revient à montrer :

$$(W_n(O_K) + \wp(W_n(K)))/\wp(W_n(K)) \xrightarrow{\simeq} W_n(O_K)/\wp(W_n(O_K)).$$

Or ce dernier isomorphisme est une conséquence directe de l'égalité :

$$\wp(W_n(O_K)) = \wp(W_n(K) \cap W_n(O_K),$$

donnée par le lemme 3.6.
Par composition, nous obtenons un isomorphisme :

$$G_{p^n}^{(0)} \xrightarrow{\simeq} \{\varphi \in H_{p^n} \ ; \ \varphi(W_n(O_K)/\wp(W_n(O_K))) = 0\}$$

qui est clairement induit par l'iosmorphisme d'Artin-Schreier-Witt. En particulier cet isomorphisme est continu pour les topologies induites.
Or les groupes $G_{p^n}^{(0)}$ et $\{\varphi \in H_{p^n} \ ; \ \varphi(W_n(O_K)/\wp(W_n(O_K))) = 0\}$ sont compacts, c'est donc un homéomorphisme. Ceci termine la preuve du théorème 3.4. ◇

Notation 5. *Pour tout entier $n \geq 1$ nous noterons :*

$$H_{p^n}^{(0)} := \{\varphi \in H_{p^n} \ : \ \varphi(W_n(O_K))/\wp(W_n(O_K))) = 0\}.$$

Le théorème 3.4 donne donc l'isomorphisme de groupes topologiques :

$$G_{p^n}^{(0)} \xrightarrow{\simeq} H_{p^n}^{(0)}$$

induit par $\mathfrak{as}_n$.

3.3.3 Groupe d'inertie de G_{p^∞}

En passant à la limite projective dans 3.4 on obtient le corollaire suivant :

Corollaire 3.5. *Le groupe d'inertie $G_{p^\infty}^{(0)}$ de la pro-p extension abélienne maximale K_{p^∞} de K est donné par l'isomorphisme de groupes topologiques :*

$$G_{p^\infty}^{(0)} \xrightarrow{\simeq} \{\varphi \in H_{p^\infty} \ ; \ \varphi(W(O_K)/\wp(W(O_K))) = 0\},$$

induit par l'isomorphisme d'Artin-Schreier-Witt $\mathfrak{as}_\infty$.

Rappelons que H_{p^∞} désigne le groupe $\mathrm{Hom}(W(K)/\wp(W(K)), W(\mathbb{F}_p))$ qui est muni de la topologie induite du produit $\prod W(\mathbb{F}_p)$ où $W(\mathbb{F}_p) \simeq \mathbb{Z}_p$ a la topologie p-adique. D'après le théorème 2.4 du chapitre 2, l'application d'Artin-Schreier-Witt $\mathfrak{as}_\infty$ établit un isomorphisme de groupes topologiques du groupe G_{p^∞} de la pro-p extension abélienne maximale de K sur H_{p^∞}.

Voici la preuve du corollaire 3.5 :

Preuve : Pour chaque couple d'entiers $n \geq m$ nous noterons π_{nm} la surjection naturelle :

$$\begin{array}{ccccc} H_{p^n} & \longrightarrow & & & H_{p^m} \\ \varphi & \mapsto & \varphi & \mod V^m W_n(\mathbb{F}_p). & \end{array}$$

On obtient ainsi un système projectif $\{H_{p^n}, \pi_{nm}\}_n$ dont la limite projective est H_{p^∞} (cf. théorème 2.4 du chapitre 2).

D'autre part, un argument semblable à la preuve du lemme 2.1 conduit pour tout n à l'identification :

$$H_{p^n}^{(0)} = \{\varphi \in H_{p^n} \ : \ \varphi(W(O_K)/\wp(W(O_K))) = 0\},$$

qui reste compatible avec les isomorphismes du théorème 3.4.

On introduit alors dans H_{p^∞} le sous-groupe :

$$H_{p^\infty}^{(0)} := \{\varphi \in H_{p^\infty} \ : \ \varphi(W(O_K)/\wp(W(O_K))) = 0\}.$$

C'est un sous-groupe fermé de H_{p^∞}, donc compact. De plus, si π_n désigne la projection :

$$\begin{array}{rccccc} \pi_n : & H_{p^\infty} & \longrightarrow & & & H_{p^n} \\ & \varphi & \mapsto & \varphi & \mod p^n W(\mathbb{F}_p) & \end{array}$$

qui est compatible avec le système projectif $\{H_{p^n}, \pi_{nm}\}_n$, on a :

$$H_{p^\infty}^{(0)} = \varprojlim \pi_n(H_{p^\infty}^{(0)}),$$

d'après l'assertion a) de ([53], cor. 1.1.8).

Or, pour chaque $n \geq 1$, on a aussi par définition :

$$\pi_n(H_{p^\infty}^{(0)}) \subset H_{p^n}^{(0)},$$

d'où l'inclusion :

$$H_{p^\infty}^{(0)} \subset \varprojlim H_{p^n}^{(0)}.$$

Réciproquement, si φ est un morphisme de H_{p^∞}, on a :

$$\begin{array}{rl} \varphi \in \varprojlim H_{p^n}^{(0)} & \Longrightarrow \varphi(W(O_K)/\wp(W(O_K))) \in \cap_n V^n W(\mathbb{F}_p) \\ & \Longrightarrow \varphi(W(O_K)/\wp(W(O_K))) = 0 \ \text{ dans } W(\mathbb{F}_p) \\ & \Longrightarrow \varphi \in H_{p^\infty}^{(0)}, \end{array}$$

d'où l'égalité :

$$H_{p^\infty}^{(0)} = \varprojlim H_{p^n}^{(0)}.$$

D'autre part, la théorie de la ramification permet d'écrire la limite projective :

$$G_{p^\infty}^{(0)} = \varprojlim G_{p^n}^{(0)}$$

prise par rapport aux restrictions r_{nm} comme applications de transition.

Or, pour $n \geq m$, le diagramme suivant commute :

$$\begin{array}{ccc} G_n^{(0)} & \xrightarrow{\mathfrak{as}_{n\,|G_n^{(0)}}} & H_{p^n}^{(0)} \\ \Big\downarrow{\scriptstyle r_{nm}} & & \Big\downarrow{\scriptstyle \pi_{nm}} \\ G_m^{(0)} & \xrightarrow{\mathfrak{as}_{m\,|G_m^{(0)}}} & H_m^{(0)} \end{array}$$

où les lignes horizontales sont des isomorphismes par le théorème 3.4.

Ainsi, puisque tous les groupes $G_{p^n}^{(0)}$ et $H_{p^n}^{(0)}$ sont compacts, on en déduit un isomorphisme de groupes topologiques :

$$\varprojlim G_{p^n}^{(0)} \xrightarrow{\simeq} \varprojlim H_{p^n}^{(0)},$$

c'est-à-dire :

$$G_{p^\infty}^{(0)} \xrightarrow{\simeq} H_{p^\infty}^{(0)}.$$

De plus, par construction, cet isomorphisme est induit par l'isomorphisme d'Artin-Schreier-Witt $\mathfrak{as}_\infty$, ce qui montre le corollaire 3.5. ◇

Chapitre 4

Le symbole d'Artin-Schreier-Witt

Soit K un corps local de caractéristique p. Dans le chapitre 3 précédent, il s'agissait de décrire les groupes de ramification pour les extensions d'Artin-Schreier-Witt du corps K quand son corps résiduel est parfait. L'interaction entre la théorie d'Artin-Schreier-Witt et la théorie de la ramification nous a permis de décrire explicitement tous les groupes de ramification pour les extensions abéliennes d'exposant p ainsi que le groupe d'inertie de toutes les extensions abéliennes maximales d'exposant p^n sur K.

L'objet du présent chapitre est d'utiliser la théorie usuelle du corps de classes local pour compléter cette étude, i.e. donner tous les groupes de ramification de toutes les extensions maximales d'Artin-Schreier-Witt sur K lorsque le corps résiduel de ce dernier est fini. Soit K^{sep} une clôture séparable de K, une conséquence importante du théorème d'existence est la correspondance bijective entre la filtration des groupes de ramification de l'extension abélienne maximale de K et la filtration $(U_K^{(u)} = 1 + \mathfrak{p}_K^u)_{u\geq 0}$ du groupe des unités de K. Cette correspondance va nous permettre d'expliciter les groupes de ramification de chaque extension abélienne maximale d'exposant p^n sur K.

Bien que la stratégie développée ici est plus directe, les outils algébriques utilisés font appel à une théorie bien plus profonde. En outre, pour être valide, cela impose de se placer dans le cadre usuel de la théorie du corps de classes local qui est plus restrictif : dorénavant le corps résiduel de K est supposé fini.

Tout ce chapitre s'articule autour du symbole local d'Artin-Schreier : c'est notre baguette magique. Il s'agit d'un accouplement non dégénéré $K/\wp(K) \times K^*/K^{*p} \to \mathbb{Z}/p\mathbb{Z}$ qui fait correspondre la filtration du groupe des unités de K^* avec la filtration $H_p^{(v)}$ du dual de $K/\wp(K)$ définie dans le chapitre 3. Par le théorème d'existence, on retrouve ainsi les groupes de ramification de l'extension abélienne maximale d'exposant p sur K tels qu'ils ont été décrits dans le chapitre précédent.

Afin d'étendre ce procédé aux extensions abéliennes d'exposant p^n sur K pour tout $n \geq 1$, la principale tâche consistera donc à généraliser le symbole d'Artin-Schreier aux vecteurs de Witt de longueur n et à en donner une formulation explicite qui généralise la formule de Schmid.

Le résultat principal de ce chapitre est le théorème 4.4 : il donne la description complète des groupes de ramification des extensions abéliennes maximales d'exposant p^n sur K pour tout entier $n \geq 1$. Cette description est donnée à travers l'isomorphisme d'Artin-Schreier-Witt $\mathfrak{as}_n$ défini dans le chapitre 2. On l'obtient en particulier en manipulant les vecteurs de Witt sous une forme réduite qui permet de simplifier considérablement les calculs.

Pour montrer ce théorème, le résultat clef est la proposition 4.34. On retrouve ainsi de façon naturelle un résultat de Brylinski [16] mais avec des arguments plus explicites et sans les outils de Kato. Comme conséquence du théorème 4.4, on retrouve aussi - et de façon plus détaillée - le calcul donné dans [57] du conducteur d'Artin pour une extension cyclique de degré p^n sur K.

Par passage à la limite projective, on obtient enfin la filtration complète des groupes de ramification de la pro-p extension abélienne maximale de K : c'est le corollaire 4.6 qui clôt cette

étude.

Le présent chapitre s'organise comme suit. Les deux premiers paragraphes préparent l'étude en introduisant les définitions et propriétés de base qui seront largement utilisées dans la suite. Plus précisément, le paragraphe 4.1 est consacré au théorème d'existence de la théorie du corps de classe local et introduit le symbole local d'Artin-Schreier. Ensuite, le paragraphe 4.2 rappelle quelques résultats essentiels de la dualité de Pontryagin pour les groupes abéliens localement compacts.

A partir du théorème d'existence et surtout du symbole local d'Artin-Schreier, le paragraphe 4.3 permet alors de vérifier les résultats obtenus dans le chapitre 3 pour l'extension abélienne maximale d'exposant p sur K lorsque le corps résiduel est fini. Ces outils de la théorie du corps de classes local se généralisent aux extensions abéliennes d'exposant p^n sur K : après avoir défini un accouplement non-dégénéré $W_n(K)/\wp(W_n(K) \times K^*/K^{*p^n} \to W_n(\mathbb{F}_p)$ qui étend le symbole d'Artin-Schreier, le paragraphe 4.4 décrit enfin les groupes de ramification pour toutes les extensions maximales d'Artin-Schreier-Witt sur K.

Insistons ! Dans tout ce chapitre, le corps résiduel κ de K est supposé fini : c'est le cadre de la théorie usuelle du corps de classes local.

4.1 Quelques résultats de théorie du corps de classes local

Ce paragraphe rappelle les grandes lignes du théorème d'existence pour un corps local K de corps résiduel fini. Lorsque K est de caractéristique $p > 0$, cela nous mène à considérer un accouplement particulier : le symbole local d'Artin-Schreier.

Le cadre usuel de la théorie du corps de classes local est celui d'un corps local de corps résiduel fini. Dans ce paragraphe seulement, nous ne ferons aucune hypothèse sur la caractéristique du corps K considéré, excepté lors de l'introduction du symbole local d'Artin-Schreier.

Dans toute la suite, on se fixe une clôture séparable K^{sep} de K dans K^{alg}. Nous noterons G_K le groupe de Galois de l'extension K^{sep}/K et G_K^{ab} son groupe de Galois abélianisé, c'est-à-dire le groupe de Galois de l'extension abélienne maximale de K dans K^{sep}.

Le sous-paragraphe 4.1.1 rappelle d'abord la loi de réciprocité pour une extension finie de K puis introduit le théorème d'existence développé dans le sous-paragraphe 4.1.2. Ce théorème est central dans la théorie usuelle du corps de classes local : il affirme que les sous-groupes fermés d'indice fini de K^* sont précisément les groupes de normess sur K donnant ainsi un isomorphisme de groupes topologiques entre la complétion de K^* pour ses sous-groupes fermés d'indice fini et le groupe G_K^{ab}. En d'autres termes, si H est un sous-groupe fermé d'indice fini de K^*, alors il existe une unique extension abélienne finie L/K telle que $N_{L/K}(L^*) = H$.
Le point clef dans la preuve du théorème d'existence est de montrer la trivialité du groupe des normes universelles $\mathcal{D}_K$ de K^*, c'est-à-dire de l'intersection de ses groupes du normes. Lorsque le corps K est de caractéristique p, cela nous conduit à introduire dans le sous-paragraphe 4.1.3 le symbole d'Artin-Schreier dont une formulation explicite est donnée par la formule de Schmid et utilisée pour prouver le théorème d'existence selon la démonstration proposée par Serre dans [60].
Conséquence du théorème d'existence : il induit un isomorphisme entre la filtration des groupes de ramification de G_K^{ab} et la filtration des sous-groupes $(1 + \mathfrak{p}_K^u)$ du groupe des unités de K. Cette propriété est notre point de départ pour l'étude des groupes de ramification des extensions d'Artin-Schreier-Witt dans le cadre de la théorie usuelle du corps de classes local, c'est pourquoi nous la détaillons dans le sous-paragraphe 4.1.4.

Le symbole local d'Artin-Schreier est donc initialement introduit comme outil pour démontrer le théorème d'existence. Très vite, il jouera un rôle crucial dans la recherche des groupes de ramification pour toutes les pro-p extensions abéliennes de K.

Pour plus de détails sur le théorème d'existence, le lecteur se rapportera aux chapitres XI et XIV de [60] ainsi qu'au chapitre V de [66].

4.1.1 La loi de réciprocité

Loi de réciprocité pour une extension finie de K. Soit L une extension finie sur K de groupe de Galois $G(L/K)$ et de degré m. Le groupe de cohomologie $H^2(L/K) := H^2(G(L/K), L^*)$ est naturellement isomorphe à $\mathbb{Z}/n\mathbb{Z}$, il admet donc un générateur canonique appelé classe fondamentale de L/K et noté $a_{L/K}$.
Selon un théorème de Tate (cf. e.g. [66], Chap.V, §2), le cup-produit par la classe fondamentale induit un isomorphisme entre groupes cohomologiques de Tate :

$$\begin{array}{ccc} \hat{H}^{-2}(L/K) & \xrightarrow{\simeq} & \hat{H}^0(L/K) \\ x & \mapsto & a_{L/K} \cup x \end{array}$$

qui donne lieu à l'isomorphisme (cf. [60], Chap. XI, §3) - appelé *isomorphisme de Nakayama* :

$$\Theta_{L/K} : G(L/K)^{\mathrm{ab}} \xrightarrow{\simeq} K^*/N_{L/K}L^*.$$

On appelle *loi de réciprocité* de la théorie du corps de classe local l'isomorphisme réciproque :

$$\omega_{L/K} : K^*/N_{L/K}L^* \xrightarrow{\simeq} G(L/K).$$

L'homomorphisme composé :

$$K^* \twoheadrightarrow K^*/N_{L/K}L^* \xrightarrow{\simeq} G(L/K)$$

est parfois appelé *application de reste normique*.
Si $b \in K^*$, son image est notée par le symbole :

$$b \mapsto (b, L/K)$$

appelé *symbole d'Artin* ou encore *symbole de reste normique* de b dans L/K.

Remarque 16. *La terminologie "reste normique" s'explique par la propriété suivante :*

$$(b, L/K) = 1 \iff b \in N_{L/K}L^*,$$

$N_{L/K}$ désignant la norme de l'extension L/K.

La loi de réciprocité entraîne :

Proposition 4.1. *Si L/K est une extension finie, alors $(K^* : N_{L/K}L^*)$ est fini.*

Cet indice est appelé *indice normique* de l'extension L/K. Il divise $[L : K]$ et lui est égal si et seulement l'extension L/K est abélienne.

Topologie de la norme sur K^*. On dit qu'un sous-groupe de K^* est un groupe de normes s'il s'écrit $N_{L/K}L^*$ pour une extension abélienne finie L/K. Par la théorie de Galois, tout sous-groupe de K^* qui contient un groupe de normes est encore un groupe de normes.

Proposition 4.2. *La correspondance $L \leftrightarrow N_{L/K}L^*$ est une bijection de l'ensemble des extensions abéliennes finies de K dans l'ensemble des groupes de normes de K^* qui renverse l'inclusion et satisfait les relations :*

$$N_{L.M/K}(L.M)^* = N_{L/K}L^* \cap N_{M/K}M^* \;\; et \;\; N_{L\cap M/K}(L \cap M)^* = N_{L/K}L^*.N_{M/K}M^*,$$

pour toutes extensions abéliennes finies M et L de K.

Rappelons que K^* est muni de la topologie induite de la topologie usuelle de K donnée par sa valuation. Maintenant, la proposition 4.2 nous permet de définir une nouvelle topologie sur K^* en

considérant l'ensemble des groupes de normes de K^* comme une base de voisinages de 1 : c'est la *topologie de la norme.*

Alors, si l'on passe à la limite projective sur toutes les extensions abéliennes finies de K, la loi de réciprocité fournit un isomorphisme de groupes topologiques :

$$\hat{K}^* \xrightarrow{\simeq} G_K^{ab},$$

où $\hat{K}^*$ est le complété de K^* pour la topologie de la norme :

$$\hat{K}^* := \varprojlim \{K^*/N_{L/K}L^* \mid L/K \text{ abélien }, [L:K] < \infty\}.$$

La topologie des sous-groupes ouverts d'indice fini. On peut également munir K^* de la topologie de ses sous-groupes ouverts d'indice fini et considérer le complété de K^* pour cette topologie, noté $\tilde{K}^*$:

$$\tilde{K}^* := \varprojlim \{K^*/U \mid U \text{ ouvert }, (K^* : U) < \infty\}.$$

4.1.2 Le théorème d'existence

Le théorème d'existence affirme essentiellement que ces deux topologies sont équivalentes sur K^*, d'où un isomorphisme continu :

$$\tilde{K}^* \xrightarrow{\simeq} G_K^{ab}.$$

Ce théorème s'énonce ainsi :

Théorème 4.1 (Théorème d'existence)**.** *Soit K un corps local de corps résiduel fini. Les groupes de normes sur K^* sont précisément ses sous-groupes ouverts d'indice fini.*

En particulier, la loi de réciprocité induit alors un isomorphisme, noté ω_K, du complété de K^* pour la topologie de ses sous-groupes ouverts d'indice fini dans le groupe de Galois de l'extension abélienne maximale de K :

$$\omega_K : \tilde{K}^* \xrightarrow{\simeq} G_K^{ab}.$$

Par la suite, l'isomorphisme ω_K sera encore appelé loi de réciprocité.

Une preuve du théorème d'existence consiste à montrer successivement les trois étapes suivantes :

Etape 1. *Pour chaque extension abélienne finie L/K, l'application norme $N_{L/K} : L^* \to K^*$ est continue et propre. L'image $N_{L/K}L^*$ est donc un sous-groupe ouvert de K^* d'indice fini.*

Il en résulte que l'application identité $K^* \to K^*$ (le premier muni de la topologie usuelle, le second de la topologie de la norme) est continue.

Etape 2. *Supposons que K est de caractéristique $p > 0$ ou bien que K est de caractéristique 0 et contient les racines p-ièmes de l'unité. Pour chaque élément $\zeta \in K^*$, si ζ est une norme dans toute extension cyclique de degré p sur K, alors $\zeta \in K^{*p}$.*

Cette étape entraine en particulier que le groupe des normes universelles de K, c'est-à-dire $\mathcal{D}_K = \cap_{L/K} N_{L/K}L^*$, est égal à $\cap_n K^{*n}$ et donc trivial (cf. [66], Chap.V, §4, prop.57). Or $\mathcal{D}_K$ est aussi le noyau de l'homomorphisme canonique $K^* \to \hat{K}^*$, $\hat{K}^*$ étant le complété de K^* pour la topologie de la norme.

Etape 3. *Tout sous-groupe ouvert d'indice fini de K^* et contenant U_K est un groupe de normes pour une extension non-ramifiée de K.*

Cette étape est une conséquence du fait que le symbole de reste normique $(-, L/K)$ est calculable explicitement dès que l'extension L/K est non ramifiée (cf. [60], Chap.XIII, §4, prop.18) :

Lemme 4.1. *Soit L/K une extension abélienne finie non ramifiée d'extension résiduelle l/κ. Soit F le générateur canonique du groupe $Gal(l/\kappa)$, i.e. son automorphisme de Frobenius. Alors, en identifiant les groupes $Gal(L/K)$ et $Gal(l/\kappa)$, pour tout élément $b \in K^*$ on a : :*

$$(b, L/K) = F^{v_K(b)}.$$

En particulier, chaque unité $b \in U_K$ est une norme dans une extension non ramifiée de K.

En pratique, l'étape 2 est la plus difficile à montrer. Or c'est une étape décisive puisqu'elle entraîne que la topologie normique sur K^* est séparée et que la loi de réciprocité induit une injection continue de K^* dans G_K^{ab}, condition nécessaire à la validité du théorème d'existence.

Lorsque car $K = p$, l'étape 2 se montre par la profonde théorie de Lubin-Tate. On peut également donner la très belle preuve de Serre ([60], Chap. XI, §5, and Chap. XIV, §6) qui s'articule autour d'un accouplement particulier : le symbole d'Artin-Schreier. Nous nous proposons de développer ce dernier argument.

4.1.3 Le symbole local d'Artin-Schreier

Fixons un nombre premier p et notons G_p le groupe de Galois de l'extension abélienne maximale d'exposant p sur K. On a : $G_p = G_K^{ab}/(G_K^{ab})^p$.

Le symbole local d'Artin-Schreier est un accouplement que Serre [60] introduit pour montrer l'étape 2 dans la preuve du théorème d'existence lorsque le corps K est de caractéristique p.

Quand le corps K est de caractéristique 0, cela conduit à un autre accouplement qui provient de la théorie de Kummer et que l'on appelle le symbole de Hilbert. Nous expliquons d'abord brièvement ce symbole puisque le mécanisme est le même que celui du symbole d'Artin-Schreier mais l'étude en est plus facile.

Le symbole de Hilbert. Considérons rapidement le cas où K est de caractéristique 0, ce qui signifie que K est une extension finie de $\mathbb{Q}_p$, i.e. un corps p-adique. Notons μ_p le groupe des racines p-ièmes de l'unité.

Lorsque le corps K contient μ_p, la théorie de Kummer fournit un accouplement :

$$\begin{array}{ccc} K^* \times G_K^{\mathrm{ab}} & \to & \mu_p \\ (a, \sigma) & \mapsto & \frac{\sigma(\alpha)}{\alpha}, \end{array}$$

où α est une racine p-ième de a dans K^{sep}. En particulier, cet accouplement induit une bijection entre les sous-groupes de K^* contenant K^{*p} et les extensions abéliennes de K d'exposant p.

Alors, en combinant la théorie de Kummer avec la loi de réciprocité, on obtient un nouvel accouplement :

$$\begin{array}{ccc} K^* \times K^* & \to & \mu_p \\ (a, b) & \mapsto & \dfrac{(b, L/K)(\alpha)}{\alpha}, \end{array}$$

où $\alpha^p = a$ et $L = K(\alpha)$. Cela conduit au symbole :

$$(a, b) := \frac{(b, L/K)(\alpha)}{\alpha}$$

appelé le symbole de Hilbert de a et b.

Le symbole de Hilbert est une application bilinéaire qui satisfait :

$(i)_H$. $(a, b) = 1 \iff b \in N_{L/K}L^*$, avec $L = K(\alpha)$ et $\alpha^p = a$.

$(ii)_H$. Si $(a, b) = 1$ pour tout $b \in K^*$, alors $a \in K^{*p}$.

En outre : $(b, a) = (a, b)^{-1}$. D'où la proposition suivante :

Proposition 4.3. *Si un élément $b \in K^*$ est une norme dans toute extension cyclique de degré p sur K, alors $b \in K^{*p}$.*

Ce résultat montre l'étape 2 en caractéristique 0. Il montre aussi que l'accouplement suivant est non-dégénéré :

$$\begin{array}{ccc} K^*/K^{*p} \times K^*/K^{*p} & \to & \mu_n \\ (a.K^{*p}, b.K^{*p}) & \mapsto & \dfrac{(b, L/K)(\alpha)}{\alpha}, \end{array}$$

et cet accouplement est encore appelé symbole de Hilbert.

Lorsque K est de caractéristique p la preuve de l'étape 2 est plus difficile et conduit au symbole d'Artin-Schreier.

Le symbole d'Artin-Schreier. Nous supposons maintenant que K est de caractéristique p. En particulier, on identifie K avec le corps $\kappa((t))$ des séries formelles sur κ lorsque t est une uniformisante de K (cf. [60], Chap.II, §4, thm 2).

Sur le groupe additif de K, on définit un homomorphisme de groupes $\wp$ par (cf. Chap.1) :

$$\forall x \in K,\ \wp(x) := x^p - x.$$

Rappelons que la théorie d'Artin-Schreier fournit un isomorphisme de groupes topologiques :

$$G_p \to Hom(K/\wp(K), \mathbb{Z}/p\mathbb{Z}),$$

donné par :

$$\sigma \mapsto \{\varphi_\sigma : a + \wp(K) \mapsto \sigma(\alpha) - \alpha\},$$

où $\alpha \in K^{\text{sep}}$ est tel que $\wp(\alpha) = a$ et où φ_σ ne dépend pas du choix de α puisque deux telles racines diffèrent d'un élément dans $\mathbb{Z}/p\mathbb{Z}$.

Alors, l'interaction entre la théorie d'Artin-Schreier et la loi de réciprocité donne l'accouplement :

$$\begin{array}{ccc} K \times K^* & \to & \mathbb{Z}/p\mathbb{Z} \\ (a, b) & \mapsto & (b, L/K)(\alpha) - \alpha, \end{array}$$

avec $\wp(\alpha) = a$ et $L = K(\alpha)$.

Pour tout $a \in K$ et pour tout $b \in K^*$, on définit le symbole d'Artin-Schreier de a et b en posant :

$$[a, b) := (b, L/K)(\alpha) - \alpha.$$

Le crochet est du à l'additivité du groupe K considéré dans l'accouplement précédent. C'est pour cette raison que le symbole d'Artin-Schreier est aussi appelé symbole semi-additif de Hilbert.

Le symbole d'Artin-Schreier est une application bilinéaire qui satisfait :

$(i)_{AS}$. $[a, b) = 0 \iff b \in N_{L/K}L^*,\ L = K(\alpha),\ \wp(\alpha) = a$.

$(ii)_{AS}$. Si $[a, b) = 0$ pour tout $b \in K^*$, alors $a \in \wp(K)$.

Il est à noter que $(ii)_{AS}$ est assez différente de la propriété $(ii)_H$. Cette propriété ne nous permettra pas de montrer l'étape 2 en caractéristique p aussi facilement qu'en caractéristique 0, il aurait été préférable d'avoir K^{*p} à la place de $\wp(K)$.

Une formulation plus explicite du symbole d'Artin-Schreier s'impose donc.

La formule de Schmid. Rappelons l'identification $K = \kappa((t))$, où t est une uniformisante de K. Si f est un élément de K, fdt est une forme différentielle sur K. Le coefficient devant t^{-1} est appelé le *résidu* de la forme fdt et sera noté $Res(fdt)$:

$$Res(fdt) = Res_{t=0}(fdt).$$

La formule de Schmid est une formule du résidu qui permet de calculer explicitement le symbole d'Artin-Schreier :

Proposition 4.4 (Formule de Schmid)**.** *Soit K un corps local de caractéristique p et de corps résiduel fini. Pour tout $a \in K$ et tout $b \in K^*$, on a :*

$$[a, b) = Tr_{\kappa/\mathbb{F}_p}(Res(a\frac{db}{b})).$$

Cette formule, due à Schmid [56], s'appuie sur le résultat suivant :

Lemme 4.2. *Pour tout $a \in K$ et pour tout $b \in K^*$, notons $c = Res(a\frac{db}{b}) \in \kappa$. Alors on a :*

$$[a, b) = [c, t).$$

Pour une preuve complète de la formule de Schmid, le lecteur se rapportera à ([60], Chap.XIV,§5).

A partir de la formule de Schmid, il est maintenant facile de montrer le résultat suivant :

Proposition 4.5. *Soit K un corps local de caractéristique p et de corps résiduel fini. Si un élément $b \in K^*$ est norme dans toute extension cyclique de degré p sur K, alors $b \in K^{*p}$.*

Preuve : Par la propriété $(i)_{AS}$, l'hypothèse revient à dire que $[a, b) = 0$ pour tout $a \in K$. Alors, si b n'était pas une puissance p-ième dans K, la forme différentielle db/b ne serait pas identiquement nulle. Pour chaque constante $c \in \kappa$, on pourrait donc choisir $a \in K$ tel que $adb/b = cdt/t$, d'où $Res(adb/b) = c$. Alors la formule de Schmid donnerait $Tr_{\kappa/\mathbb{F}_p}(c) = 0$, ce qui contredit la surjectivité de la trace $\kappa \to \mathbb{Z}/p\mathbb{Z}$. ◇

La proposition 4.5 complète la preuve de l'étape 2 du théorème d'existence. Elle montre également le résultat suivant qui sera crucial pour la suite :

Proposition 4.6. *Le symbole d'Artin-Schreier induit un accouplement non dégénéré :*

$$\begin{array}{ccc} K/\wp(K) \times K^*/K^{*p} & \to & \mathbb{Z}/p\mathbb{Z} \\ (a + \wp(K), b.K^{*p}) & \mapsto & (b, L/K)(\alpha) - \alpha, \end{array}$$

où $\wp(\alpha) = a$, $\alpha \in K^{sep}$ et $L = K(\alpha)$.

Preuve : Le noyau de gauche est trivial par la propriété $(ii)_{AS}$, le noyau de droite aussi d'après la proposition 4.5 et la propriété $(i)_{AS}$. ◇

Dans tout ce qui suit, le symbole d'Artin-Schreier fera référence à ce dernier accouplement défini sur $K/\wp(K) \times K^*/K^{*p}$.

4.1.4 Unités et groupes de ramification

Dans ce sous-paragraphe, nous expliquons pourquoi le théorème d'existence induit une correspondance bijective entre la filtration $(1 + \mathfrak{p}_K^u)_u$ du groupe des unités de K et la filtration des groupes de ramification de G_K^{ab}. Cette conséquence essentielle du théorème d'existence nécessite d'abord de préciser quelques résultats sur la topologie du groupe U_K des unités de K.

Topologie sur U_K. Rappelons que le corps K est muni d'une valuation discrète v_K pour laquelle il complet et que son corps résiduel κ est fini. Nous notons toujours O_K l'anneau de valuation de K et $\mathfrak{p}_K$ son idéal maximal. D'après ([31], Chap.II), K est un corps localement compact et non discret. Pour tous les entiers $u \geq 0$, les puissances u-ièmes $\mathfrak{p}_K^u$ avec $\mathfrak{p}_K^0 = O_K$ sont des sous-groupes ouverts et fermés de K et forment une base de voisinage de 0 dans K comme dans O_K. Ainsi, puisque K est complet on en déduit un isomorphisme de groupes topologiques (cf. e.g. [48], Chap.II, §4, prop.4.5) :

$$O_K \xrightarrow{\simeq} \varprojlim O_K/\mathfrak{p}_K^u.$$

Or, étant donnée une uniformisante t de O_K fixée, la correspondance $at^u \mapsto a \mod \mathfrak{p}_K$ induit un isomorphisme $\mathfrak{p}_K^u/\mathfrak{p}_K^{u+1} \simeq O_K/\mathfrak{p}_K = \kappa$ pour tout entier $u \geq 0$. Les anneaux $O_K/\mathfrak{p}_K^u$ sont donc finis et O_K est profini, donc compact. Il en résulte que K est localement compact, totalement discontinu et non discret pour la topolgie induite de sa valuation (voir aussi [31], Chap.II).

Maintenant, le groupe des unités U_K est fermé dans O_K, il est alors séparé et compact, donc complet. De plus, les sous-groupes $U_K^{(u)} := 1 + \mathfrak{p}_K^u$, $u \geq 1$, sont ouverts et fermés et ils forment une base de voisinages de 1 dans U_K. D'après ([60], Chap.IV, §2, prop.6), le quotient $U_K/U_K^{(1)}$ est isomorphe au groupe κ^* et chaque quotient $U_K^{(u)}/U_K^{(u+1)}$ est isomorphe non canoniquement au groupe additif de κ. Les groupes $U_K^{(u)}$ sont donc d'indice fini dans U_K. Alors, d'après ([53], Chap.III, §1 et §2), il en résulte un isomorphisme de groupes topologiques :

$$U_K \xrightarrow{\simeq} \varprojlim U_K/U_K^{(u)},$$

lorsque $u \to +\infty$ et donc U_K est profini. Cela montre que K^* est aussi localement compact, totalement disconnexe et non discret pour la topologie induite de celle de K.

En particulier, la topologie sur U_K induite de celle de K correspond à la topologie définie par ses sous-groupes fermés d'indice fini et U_K est compact pour cette topologie. Il est alors intéressant de voir comment le théorème d'existence se comporte sur U_K.

Le théorème d'existence sur U_K. On a :

Proposition 4.7. *Soit $G_K^{(0)}$ le groupe d'inertie de G_K^{ab}. Le théorème d'existence fournit le diagramme commutatif suivant :*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & U_K & \longrightarrow & K^* & \xrightarrow{v_K} & \mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \omega_K|_{U_K}} & & \downarrow{\scriptstyle \omega_K} & & \downarrow{\scriptstyle i} & & \\ 0 & \longrightarrow & G_K^{(0)} & \longrightarrow & G_K^{ab} & \longrightarrow & \hat{\mathbb{Z}} & \longrightarrow & 0 \end{array}$$

où la flèche de droite est l'inclusion canonique.

En particulier, la loi de réciprocité induit sur U_K un isomorphisme de groupes topolgiques :

$$\omega_{K|U_K} : U_K \xrightarrow{\simeq} G_K^{(0)}.$$

Preuve : La première ligne du diagramme est donnée par la valuation de K.
Montrons que la loi de réciprocité ω_K envoie U_K sur le groupe d'inertie de G_K^{ab}. Une conséquence du lemme 4.1 est que si L/K est une extension abélienne finie de groupe de Galois G, la loi de réciprocité envoie U_K sur le groupe d'inertie $G^{(0)}$ de G (cf. [60], Chap. XIII, §4). En passant à la limite projective sur toutes les extensions abéliennes finies de K, la loi de réciprocité induit donc une surjection $U_K \twoheadrightarrow G_K^{(0)}$ puisque U_K est compact.

Il reste alors à montrer la commutativité du diagramme pour la colonne de droite. Cela résulte de l'identification de $\hat{\mathbb{Z}}$ avec $G_K^{\mathrm{ab}}/G_K^{(0)}$ qui est le groupe de Galois de la sous-extension maximale non ramifiée de K^{ab} sur K. En effet, cette identification est due à la finitude du corps résiduel κ qui entraine que toute extension de degré fini sur κ est cyclique.

L'isomorphisme $U_K \xrightarrow{\simeq} G_K^{(0)}$ résulte alors de la commutativité du diagramme puisque les deux flèches de droite sont des applications injectives. Cet isomorphisme est de plus bicontinu car ω_K est continu et parce que U_K est compact. En d'autres termes, la loi de réciprocité ω_K identifie U_K avec $G_K^{(0)}$, ce qui montre la proposition. ◇

En poussant l'étude plus loin, on obtient un résultat analogue pour les groupes de ramification supérieurs :

Corollaire 4.1. *Pour tout entier $u \geq 0$, le théorème d'existence induit un isomorphisme de groupes topologiques :*

$$\omega_{K_{U_K^{(u)}}} : U_K^{(u)} \xrightarrow{\simeq} G_K^{(u)},$$

où $U_K^{(u)} = 1 + \mathfrak{p}_K^u$ et où $G_K^{(u)}$ est le groupe de ramification d'indice u de G_K^{ab}.

Preuve : Voir ([60], Chap. XV, §2) puis passer à la limite projective. ◇

Retour à notre problème initial, i.e. à la recherche des groupes de ramification dans les pro-p extensions abéliennes de K lorsque K est de caractéristique p. Le théorème d'existence nous permet d'identifier K^*/K^{*p} avec le groupe G_p de l'extension abélienne maximale d'exposant p sur K (cf. proposition 4.16). Il s'agit donc de développer des arguments de dualité afin de mettre en correspondance la filtration des groupes de ramification de G_p avec une certaine filtration du groupe $\mathrm{Hom}(K/\wp(K), \mathbb{Z}/p\mathbb{Z})$ via le symbole d'Artin-Schreier. C'est le rôle de la dualité de Pontryagin qui fait l'objet du paragraphe suivant.

4.2 Quelques rappels sur la dualité de Pontryagin

Ce paragraphe rappelle les propriétés de base de la dualité de Pontryagin pour les groupes abéliens localement compacts (sous-paragraphes 1 et 2) avant de les traduire dans les catégories particulières des groupes abéliens profinis et des groupes abéliens discrets de torsion (sous-paragraphe 3) afin d'adapter cette dualité au cadre de la théorie d'Artin-Schreier-Witt.

4.2.1 Groupes abéliens localement compacts

Définition. Soit G un groupe topologique abélien d'élément unité 1.

Définition 4.1. *Le groupe topologique G est dit localement compact s'il est séparé et si 1 possède un voisinage compact.*

Exemple 4.1. *Tout groupe discret est localement compact.*

Sous-groupes et groupes quotients. On a :

Proposition 4.8. *Soit G un groupe localement compact. Tout sous-groupe H de G est localement compact si et seulement s'il est fermé dans G.*

Preuve : Si H est fermé dans G, alors $H \cap V$ est un voisinage compact de 1 dans H pour tout voisinage compact V de 1 dans G.
La réciproque est le corollaire 2 de ([15], Chap.III, §.3.3). ◇

La propriété suivante caractérise les groupes quotients d'un groupe localement compact :

Proposition 4.9. *Soit G un groupe localement compact et soit H un sous-groupe de G. Si H est fermé dans G, alors le quotient G/H est aussi localement compact pour la topologie quotient.*

Preuve : D'après la proposition 18 de ([15], Chap.III, §2.6), le groupe quotient G/H est séparé. De plus il est facile de montrer que son élément unité admet un voisinage compact puisque la projection canonique $G \twoheadrightarrow G/H$ est continue et ouverte. ◇

La topologie compacte-ouverte. Soient G et H deux groupes abéliens localement compacts. Le groupe $\mathrm{Hom}(G, H)$ des homomorphismes continus de G dans H est muni d'une topologie naturelle, la topologie compacte-ouverte, dont une base est donnée par la collection des sous-ensembles :

$$B(C, U) = \{f \in \mathrm{Hom}(G, H) \ : \ f(C) \subset U\}$$

lorsque K parcourt les sous-ensembles compacts de G et U les sous-ensembles ouverts de H.

4.2.2 Dualité de Pontryagin

La dualité de Pontryagin est un outil essentiel lorsque l'on travaille avec les groupes abéliens localement compacts. Selon un célèbre théorème dû à Pontryagin et van Kampen, cette dualité induit un isomorphisme entre chaque groupe abélien localement compact et son bidual. Autre résultat que nous présenterons dans ce sous-paragraphe : la dualité de Pontryagin établit une correspondance entre la catégorie des groupes abéliens compacts et celle des groupes abéliens discrets.

Dans tout ce qui suit, le tore $\mathbb{R}/\mathbb{Z}$ est considéré comme un groupe topologique pour la topologie quotient provenant du groupe additif $\mathbb{R}$.

Le groupe dual de Pontryagin. Soit G un groupe abélien localement compact.

Définition 4.2. *On appelle dual de Pontryagin $G^\wedge$ du groupe G le groupe :*

$$G^\wedge = Hom(G, \mathbb{R}/\mathbb{Z})$$

de tous les homomorphismes continus de G dans $\mathbb{R}/\mathbb{Z}$, muni de la topologie compacte-ouverte.

Proposition 4.10. *Le dual $G^\wedge$ est un groupe abélien localement compact pour la topologie compacte-ouverte.*

Exemple 4.2. $(\mathbb{Z})^\wedge = Hom(\mathbb{Z}, \mathbb{R}/\mathbb{Z}) = \mathbb{R}/\mathbb{Z}$,
et $(\mathbb{R}/\mathbb{Z})^\wedge = Hom(\mathbb{R}/\mathbb{Z}, \mathbb{R}, \mathbb{Z}) = \mathbb{Z}$.

La proposition qui suit est une correspondance entre les catégories des groupes compacts abéliens et celle des groupes abéliens discrets :

Proposition 4.11. *Si G est compact (resp. discret) alors $G^\wedge$ est discret (resp. compact).*

Preuve : Soit $\pi : \mathbb{R} \twoheadrightarrow \mathbb{R}/\mathbb{Z}$ la projection canonique. L'unique sous-groupe de $\mathbb{R}/\mathbb{Z}$ contenant l'ouvert $U = \pi(-\frac{1}{3}; +\frac{1}{3})$ est le groupe trivial $\{0\}$. Alors, si G est compact, l'ouvert $B(G, U)$ de $G^\wedge$ consiste uniquement en l'application nulle : $G^\wedge$ est donc discret.

Réciproquement, si G est discret les sous-ensembles compacts de G sont précisément ses sous-ensembles finis. Alors, la topologie compacte-ouverte coïncide sur $G^\wedge$ avec la topologie issue du produit $\prod_G \mathbb{R}/\mathbb{Z}$. Or $G^\wedge$ est fermé dans $\prod_G \mathbb{R}/\mathbb{Z}$, puisque $\prod_G \mathbb{R}/\mathbb{Z} - G^\wedge$ est ouvert et $\mathbb{R}/\mathbb{Z}$ est séparé (cf. [53], prop. 2.9.1). D'où la compacité de $G^\wedge$ par le théorème de Tychonov. ◇

Remarque 17. *La dualité de Pontryagin établit aussi une correspondance entre les sous-catégories des groupes abéliens profinis et des groupes abéliens discrets de torsion. Voir également le sous-paragraphe* 3.

Le bidual de Pontryagin. De même, on peut considérer le bidual $G^{\wedge\wedge}$ d'un groupe abélien localement compact G :

$$G^{\wedge\wedge} = \mathrm{Hom}(G^\wedge, R/\mathbb{Z}) = \mathrm{Hom}(\mathrm{Hom}(G, \mathbb{R}/\mathbb{Z}), \mathbb{R}/\mathbb{Z}).$$

On a un homomorphisme canonique de G dans $G^{\wedge\wedge}$ donné par :

$$\begin{array}{rccl} \alpha_G : & G & \to & G^{\wedge\wedge} \\ & g & \mapsto & (\chi \mapsto \chi(g)). \end{array}$$

Le théorème de Pontryagin - van Kampen affirme que α_G est un isomorphisme :

Théorème 4.2 (Pontryagin - van Kampen)**.** *Soit G un groupe abélien localement compact. L'homomorphisme canonique α_G de G dans son bidual $G^{\wedge\wedge}$ est un isomorphisme de groupes topologiques.*

Une preuve de ce théorème est donnée dans ([53], 2.9) pour les cas particuliers où G est un groupe abélien profini ou un groupe abélien discret et de torsion. Quant à la preuve originale, [49] fait référence au théorème 5.3 du livre de Pontryagin (*Topological groups*, Gordon and Brach, New York, London, Paris 1966). Une liste de preuves complètes est également disponible dans ([53], 2.9). Cependant, plus loin dans la remarque 19, nous ébaucherons une esquisse de preuve pour le théorème 4.2.

Applications transposées. Soient G et H deux groupes abéliens localement compacts. Soit $\varphi : G \to H$ un homomorphisme continu.

Définition 4.3. *L'application transposée de φ est l'homomorphisme continu défini par :*

$$\begin{array}{cccc} \varphi^\wedge & H^\wedge & \to & G^\wedge \\ & \chi' & \mapsto & (g \mapsto \chi'(\varphi(g))). \end{array}$$

Proposition 4.12. *Soit G un groupe abélien localement compact et soit H un sous-groupe ouvert de G. Alors l'homomorphisme transposé $i^\wedge : G^\wedge \to H^\wedge$ de l'injection canonique $i : H \hookrightarrow G$ est surjectif.*

Démonstration. Par construction, l'homomorphisme $i^\wedge$ est continu. Il s'agit donc de montrer sa surjectivité. Soit χ' un caractère de $H^\wedge$. Selon ([35], Chap.XX, §4), le groupe $\mathbb{R}/\mathbb{Z}$ est injectif dans la catégorie des groupes abéliens puisqu'il est divisible. Alors, χ' s'étend en un homomorphisme χ de G dans $\mathbb{R}/\mathbb{Z}$ tel que $\chi' = \chi \circ i$. De plus, puisque H est ouvert dans G, l'injection i est ouverte et donc χ est continu. En résumé, χ est un caractère de $G^\wedge$ et vérifie $i^\wedge(\chi) = \chi'$. Ceci montre la surjectivité de $i^\wedge$. □

Remarque 18. *En fait, $i^\wedge$ induit un isomorphisme de groupes topologiques de $G^\wedge/H^\perp$ sur $H^\wedge$, où l'on note $H^\perp$ le sous-groupe orthogonal de H dans G i.e. l'ensemble des caractères χ de $G^\wedge$ qui annulent H. On peut montrer que si H est compact (resp. ouvert) alors $H^\perp$ est ouvert (resp. compact).*

Remarque 19. *Nous présentons ici une idée générale pour montrer le théorème 4.2.*
On a en effet un résultat analogue à la proposition 4.12 pour les projections :

Proposition 4.13. *Soit G un groupe abélien localement compact et soit H un sous-groupe fermé de G. Alors, l'application transposée $\pi^\wedge$ de la projection canonique$\pi : G \to G/H$ induit un isomorphisme de groupes topologiques de $(G/H)^\wedge$ sur $H^\perp$.*

Les propositions 4.12 et 4.13 montrent que la dualité de Pontryagin est compatible avec les extensions de groupes, plus précisément :

Proposition 4.14. *Soit G un groupe abélien localement compact et soit H un sous-groupe compact et ouvert de G. Si H et G/H sont tous deux isomorphes à leur bidual de Pontryagin comme groupes topologiques, alors G l'est aussi.*

De même, signalons que la dualité de Pontryagin est compatible avec les limites projectives et inductives. Par exemple, si $(G_i, \varphi_{ij})_i$ est un système projectif de groupes abéliens localement compacts tel que les morphismes de transition φ_{ij} sont tous stricts, surjectifs et de noyau compact et si la limite projective $G = \varprojlim G_i$ est un groupe abélien localement compact, alors le système $(G_i^\wedge, \varphi_{ij}^\perp)_i$ est projectif aussi et l'on a un isomorphisme de groupes topologiques :

$$G^\wedge \xrightarrow{\simeq} \varprojlim G_i^\wedge.$$

Si de plus chaque groupe G_i est isomorphe à son bidual, il en est de même pour G.
Sous d'autres conditions, on a un résultat analogue pour les limites inductives.

Ces compatibilités fournissent une preuve pour le théorème 4.2. L'idée est de considérer des groupes élémentaires qui sont des groupes localement compacts de la forme $\mathbb{R}^p \times (\mathbb{R}/\mathbb{Z})^q \times \mathbb{Z}^r \times F$ où F est un groupe abélien fini. Il s'agit alors de montrer que tout groupe abélien localement compact s'écrit à l'aide de limites inductives et projectives de groupes élémentaires et que chaque groupe élémentaire satisfait le théorème de Pontryagin - van Kampen.

4.2.3 La dualité $\mathbf{Hom}(-, \mathbb{Q}/\mathbb{Z})$

Plus que la dualité sur $\mathbb{R}/\mathbb{Z}$, il est courant en algèbre de manipuler la dualité $\mathrm{Hom}(-, \mathbb{Q}/\mathbb{Z})$ qui associe à chaque groupe topologique le groupe d'homomorphismes continus $\mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$ lorsque $\mathbb{Q}/\mathbb{Z}$ est muni de la topologie discrète.

Le dualité de Pontryagin usuelle et la dualité $\mathrm{Hom}(-, \mathbb{Q}/\mathbb{Z})$ ne coïncident pas toujours. Par exemple $\mathrm{Hom}(\mathbb{Z}, \mathbb{R}/\mathbb{Z}) = \mathbb{R}/\mathbb{Z}$ alors que $\mathrm{Hom}(\mathbb{Z}, \mathbb{Q}/\mathbb{Z}) = \mathbb{Q}/\mathbb{Z}$.

Cependant, ces dualités coïncident sur certaines catégories de groupes abéliens localement compacts, c'est le cas en particulier pour les sous-catégories des groupes abéliens profinis mais aussi des groupes abéliens discrets de torsion, ce qui sera d'un grand intérêt pour notre étude.

Proposition 4.15. *Lorsque le groupe G est soit abélien profini soit abélien discret de torsion, on a un isomorphisme de groupes topologiques :*

$$Hom(G, \mathbb{R}/\mathbb{Z}) \xrightarrow{\simeq} Hom(G, \mathbb{Q}/\mathbb{Z})$$

pour la topologie compacte-ouverte.

Preuve : Nous renvoyons encore à ([53], thm 2.9.6). ◇

Un fait essentiel est que tout ce qui a été formulé plus haut pour la dualité de Pontryagin peut s'énoncer de façon analogue pour la dualité $\mathrm{Hom}(-, \mathbb{Q}/\mathbb{Z})$ sur les catégories des groupes abéliens profinis et des groupes abéliens discrets de torsion, les preuves étant de plus fort similaires. En particulier, cela conduit au résultat suivant :

Théorème 4.3. *La dualité $Hom(-, \mathbb{Q}/\mathbb{Z})$ établit une équivalence de catégories entre les groupes abéliens profinis et les groupes abéliens discrets de torsion. Plus précisément, le groupe dual d'un groupe abélien profini (resp. discret et de torsion) est un groupe abélien discret de torsion (resp. profini).*
De plus, lorsque le groupe abélien G est soit profini soit discret de torsion, l'homomorphisme canonique :

$$G \longrightarrow Hom(Hom(G, \mathbb{Q}/\mathbb{Z}), \mathbb{Q}/\mathbb{Z})$$

est un isomorphisme de groupes topologiques.

Pour plus de détails, le lecteur pourra se reporter à ([53], thm 2.9.3) par exemple.

4.3 Symbole d'Artin-Schreier et extensions abéliennes maximales d'exposant p

Soit K un corps local de caractéristique p et de corps résiduel κ fini. Soit G_p le groupe de Galois de l'extension abélienne maximale d'exposant p sur K. D'après le chapitre 2, l'isomorphisme d'Artin-Schreier-Witt est un isomorphisme de groupes topologiques :

$$\mathfrak{as}_1 : G_p \xrightarrow{\simeq} H_p,$$

où H_p est le groupe $\mathrm{Hom}(K/\wp(K), \mathbb{Z}/p\mathbb{Z})$ (cf. théorème 2.3).

Le corollaire 3.3 du chapitre 3 complète ce résultat en explicitant une bijection entre la filtration des sous-groupes de ramification de G_p et la filtration $(H_p^{(u)})_u$ de H_p donnée par :

$$H_p^{(u)} = \{\varphi \in H_p \ : \ \varphi(K^{(u)}) = 0\}$$

où $K^{(u)} = (\mathfrak{p}_K^{-u} + \wp(K))/\wp(K)$, pour tout entier $u \geq -1$.

Le but de ce paragraphe est de développer une méthode plus directe issue de la théorie du corps de classes local pour retrouver cette correspondance. Néanmoins les outils seront plus élaborés donc plus difficiles à manipuler puisque cela nécessite à la fois les théories profondes du théorème d'existence et de la dualité de Pontryagin.

Soulignons aussi que les hypothèses sont maintenant plus restrictives : alors que le corps résiduel κ du corps K était auparavant parfait, la théorie usuelle du corps de classes local impose maintenant de supposer κ fini.

Le sous-paragraphe 4.3.1 est un panorama des propriétés topologiques pour les objets utilisés précisant ainsi le cadre de l'étude. Le sous-paragraphe 4.3.2 concerne uniquement l'isomorphisme d'Artin-Schreier-Witt $G_p \xrightarrow{\simeq} H_p$ en montrant comment le symbole d'Artin-Schreier et la dualité de Pontryagin permettent de le retrouver. Ces méthodes sont généralisées dans le sous-paragraphe 4.3.3 et redonnent la description explicite des sous-groupes de ramification de G_p. Nous avons pris soin de détailler ces méthodes afin de passer plus facilement dans le paragraphe qui suit aux extensions abéliennes maximales d'exposant p^n pour $n \geq 2$.

4.3.1 Panorama

Ce sous-paragraphe détaille notre cadre de travail pour le rendre compatible avec la dualité de Pontryagin, ceci afin de justifier l'utilisation élégante du symbole local d'Artin-Schreier.

Le corps K est toujours muni de sa topologie usuelle, donnée par sa valuation discrète, pour laquelle il est complet. D'après le sous-paragraphe 4.1.4, cette topologie induit une topologie sur le groupe abélien K^* qui le rend localement compact.

Première conséquence du théorème d'existence pour l'extension abélienne maximale d'exposant p sur K : la loi de réciprocité applique $(K^*)^p$ sur G_p. Plus précisément :

Proposition 4.16. *Le théorème d'existence induit un isomorphisme de groupes topologiques, encore noté ω_K :*

$$\omega_K : K^*/(K^*)^p \xrightarrow{\simeq} G_p,$$

où $K^*/(K^*)^p$ est muni de la topologie quotient.

Preuve : C'est une conséquence du diagramme commutatif de la proposition 4.7 :

$$\begin{array}{ccccccccc} 0 & \longrightarrow & U_K & \longrightarrow & K^* & \xrightarrow{v_K} & \mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \omega_K|U_K} & & \downarrow{\scriptstyle \omega_K|K^*} & & \downarrow{\scriptstyle i} & & \\ 0 & \longrightarrow & G_K^{(0)} & \longrightarrow & G_K^{\mathrm{ab}} & \longrightarrow & \hat{\mathbb{Z}} & \longrightarrow & 0 \end{array}$$

où la flèche de gauche est un isomorphisme. La suite exacte de la première ligne est clairement scindée puisque tout élément de K s'écrit de façon unique $\epsilon.t^v$ avec $\epsilon \in U_K$ et $n \in \mathbb{Z}$ dès que l'on s'est fixé une uniformisante t de K.

Etudions la seconde ligne. Puisque G_K^{ab} est un groupe profini, il a la structure d'un $\hat{\mathbb{Z}}$-module. Alors, comme $\hat{\mathbb{Z}}$ est libre sur lui-même donc projectif, la suite $0 \to G_K^{(0)} \to G_K^{\mathrm{ab}} \to \hat{\mathbb{Z}} \to 0$ est scindée aussi.

D'où la commutativité du diagramme :

$$\begin{array}{ccccccccc} 0 & \longrightarrow & U_K/U_K^p & \longrightarrow & K^*/K^{*p} & \longrightarrow & \mathbb{Z}/p\mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \omega_K} & & \downarrow{\scriptstyle \omega_K} & & \downarrow & & \\ 0 & \longrightarrow & G_p^{(0)} & \longrightarrow & G_p & \longrightarrow & \hat{\mathbb{Z}}/p\hat{\mathbb{Z}} & \longrightarrow & 0 \end{array}$$

en appliquant le produit tensoriel $\otimes\mathbb{Z}/p\mathbb{Z}$. Maintenant, $\mathbb{Z}/p\mathbb{Z}$ et $\hat{\mathbb{Z}}/p^n\hat{\mathbb{Z}}$ sont canoniquement isomorphes. Les deux flèches de droite et de gauche sont donc des isomorphismes de groupes de topologiques et ω_K induit bien un isomorphisme de K^*/K^{*p} dans G_p. $\diamond$

En particulier, K^*/K^{*p} est alors un groupe abélien profini.

De plus, le groupe $K/\wp(K)$ est abélien discret pour la topologie quotient et de torsion. En effet, l'idéal $\mathfrak{p}_K$ est un voisinage ouvert de 0 dans K et d'après la proposition 3.1 du chapitre 3, $\mathfrak{p}_K \subset \wp(K)$. Alors, modulo $\wp(K)$, $\{0\}$ est ouvert dans $K/\wp(K)$. Enfin, puisque K est de caractéristique p, le quotient $K/\wp(K)$ est clairement annulé par p, donc de torsion.

Ainsi la dualité de Pontryagin coïncide avec la dualité $\mathrm{Hom}(-,\mathbb{Q}/\mathbb{Z})$ sur les groupes $K/\wp(K)$ et K^*/K^{*p} d'après la proposition 4.15. Or ces deux groupes sont tous deux annulés par p et donc la dualité $\mathrm{Hom}(-,\mathbb{Q}/\mathbb{Z})$ coïncide avec la dualité $\mathrm{Hom}(-,\mathbb{Z}/p\mathbb{Z})$ puisque $\frac{1}{p}\mathbb{Q}/\mathbb{Z}$ et $\mathbb{Z}/p\mathbb{Z}$ sont canoniquement isomorphes. Dans la suite, on se restreindra à l'étude de la dualité $\mathrm{Hom}(-,\mathbb{Z}/p\mathbb{Z})$ sur $K/\wp(K)$ et K^*/K^{*p} pour laquelle le théorème 4.3 reste valide.

4.3.2 L'isomorphisme $G_p \xrightarrow{\simeq} H_p$

Nous vérifions d'abord que le symbole d'Artin-Schreier induit un isomorphisme de groupes topologiques $G_p \xrightarrow{\simeq} H_p$ qui coïncide avec l'isomorphisme $\mathfrak{as}_1$ d'Artin-Schreier du chapitre 2. Rappelons que cet isomorphisme est donné par :

$$\mathfrak{as}_1 \ : \ \sigma \mapsto \varphi_\sigma = \{a + \wp(K) \mapsto \sigma(\alpha) - \alpha\}$$

avec $\alpha \in K^{\mathrm{sep}}$ tel que $\wp(\alpha) = a$.

On a :

Proposition 4.17. *Le symbole d'Artin-Schreier établit un isomorphisme de groupes topologiques :*

$$\psi_p : K^*/K^{*p} \xrightarrow{\simeq} Hom(K/\wp(K), \mathbb{Z}/p\mathbb{Z})$$

donné par $(b.K^{*p}) \mapsto \{(a + \wp(K)) \mapsto [a, b)\}$.

Preuve : D'après la proposition 4.6, le symbole d'Artin-Schreier est un accouplement non dégénéré, cela signifie qu'il induit des homomorphismes injectifs :

$$\begin{array}{rccc} f: & K^*/K^{*p} & \hookrightarrow & \mathrm{Hom}(K/\wp(K), \mathbb{Z}/p\mathbb{Z}) \\ & b.K^{*p} & \mapsto & \{f_b : a + \wp(K) \mapsto [a, b)\} \end{array}$$

et :

$$\begin{array}{rccc} g: & K/\wp(K) & \hookrightarrow & \mathrm{Hom}(K^*/K^{*p}, \mathbb{Z}/p\mathbb{Z}) \\ & a + \wp(K) & \mapsto & \{g_a : b.K^{*p} \mapsto [a, b)\}. \end{array}$$

Or $K/\wp(K)$ est discret, l'injection g est donc continue. Ainsi, selon la proposition 4.12, son morphisme transposé fournit une surjection continue :

$$\begin{array}{rccc} g^\wedge: & \mathrm{Hom}(\mathrm{Hom}(K^*/K^{*p}, \mathbb{Z}/p\mathbb{Z}), \mathbb{Z}/p\mathbb{Z}) & \twoheadrightarrow & \mathrm{Hom}(K/\wp(K), \mathbb{Z}/p\mathbb{Z}) \\ & \chi & \mapsto & \{a + \wp(K) \mapsto \chi \circ g(a + \wp(K))\}. \end{array}$$

Maintenant, par le théorème 4.3, les groupes K^*/K^{*p} et $\mathrm{Hom}(\mathrm{Hom}(K^*/K^{*p}, \mathbb{Z}/p\mathbb{Z}), \mathbb{Z}/p\mathbb{Z})$ sont canoniquement isomorphes comme groupes topologiques via la correspondance $b \mapsto (\chi \mapsto \chi(b))$. Par composition, on obtient un morphisme surjectif continu :

$$\begin{array}{rccc} K^*/K^{*p} & \twoheadrightarrow & \mathrm{Hom}(K/\wp(K), \mathbb{Z}/p\mathbb{Z}) \\ b.K^{*p} & \mapsto & \{a + \wp(K) \mapsto [a, b)\} \end{array}$$

et ce dernier est identiquement égal à l'application f définie ci-dessus. Ainsi, f est un isomorphisme continu. Comme K^*/K^{*p} et $\mathrm{Hom}(K/\wp(K), \mathbb{Z}/p\mathbb{Z})$ sont profinis donc compacts, f est même un isomorphisme de groupes topologiques. Désormais nous noterons ψ_p l'isomorphisme f. $\diamond$

En combinant la proposition 4.17 avec le théorème d'existence, on obtient :

Corollaire 4.2. *Par composition avec l'isomorphisme réciproque de la loi de réciprocité, ψ_p induit un isomorphisme de groupes topologiques :*

$$G_p \xrightarrow{\simeq} Hom(K/\wp(K), \mathbb{Z}/p\mathbb{Z})$$

qui coïncide avec l'isomorphisme d'Artin-Schreier-Witt $\mathfrak{as}_1$. En d'autres termes :

$$\mathfrak{as}_1 = \psi_p \circ \omega_K^{-1}.$$

Preuve : D'après la proposition 4.16 l'application composée $\omega_K^{-1} \circ \psi_p$ est un isomorphisme de groupes topologiques :

$$G_p \xrightarrow{\simeq} \mathrm{Hom}(K/\wp(K), \mathbb{Z}/p\mathbb{Z})$$

donné par : $\sigma \mapsto \{a + \wp(K) \mapsto [a, b)\}$, où $b = \omega_K^{-1}(\sigma) \in K^*$. Cet isomorphisme est précisément l'isomorphisme d'Artin-Schreier-Witt puisque $[a, b) = \omega_K(b)(\alpha) - \alpha = \sigma(\alpha) - \alpha$ avec $\wp(\alpha) = a$. $\diamond$

En d'autres termes, le symbole local d'Artin-Schreier est simplement la traduction directe de l'accouplement d'Artin-Schreier dans le langage du théorème d'existence.

Cela étant fait, il s'agit maintenant de considérer la filtration des groupes de ramification de G_p et voir comment elle correspond à la filtration des $H_p^{(v)}$ du groupe H_p par le symbole d'Artin-Schreier.

4.3.3 Groupes de ramification dans l'extension abélienne maximale d'exposant p

Dans ce sous-paragraphe, on applique le mécanisme de dualité précédent aux sous-groupes $U_K^{(u)}K^{*p}/K^{*p}$ de K^*/K^{*p}, pour tous $u \geq 0$. On sait en effet par le théorème d'existence et la proposition 4.16 que ces groupes forment une filtration décroissante de K^*/K^{*p} et qu'ils correspondent bijectivement aux groupes $G_p^{(u)}$ de G_p.

Conservant les notations du chapitre 3, nous noterons pour tout $u \geq -1$:

$$K^{(u)} = (\mathfrak{p}_K^{-u} + \wp(K))/\wp(K),$$

avec $\mathfrak{p}_K^0 = O_K$ et $\mathfrak{p}_K^{-1} = K$. Pour $u \geq 0$, les groupes $K^{(u)}$ forment une filtration croissante de $K/\wp(K)$. Rappelons aussi que pour tout entier $u \geq 1$, l'isomorphisme d'Artin-Schreier $\mathfrak{as}_1$ induit un isomorphisme de groupes topologiques :

$$G_p^{(u)} \xrightarrow{\simeq} \{\varphi \in H_p \ : \ \varphi(K^{(u-1)}) = 0\},$$

d'après le chapitre 3. Il s'agit pour nous de retrouver ces correspondances à partir du théorème d'existence cette fois. L'intérêt de cette méthode est qu'elle se généralisera plus facilement aux extensions d'exposant p^n sur K dès que $n \geq 2$.

Sauts. Nous vérifions d'abord qu'aucun saut n'est divisible par p. On dit qu'en entier $t \geq 0$ est un saut pour la filtration $\{U_K^{(n)}K^{*p}/K^{*p}\}_u$ si :

$$U_K^{(t)}K^{*p}/K^{*p} \neq U_K^{(t+1)}K^{*p}/K^{*p}.$$

Ainsi définis et grâce au théorème d'existence, les sauts pour la filtration des $U_K^{(n)}K^{*p}/K^{*p}$ correspondent précisément aux sauts de la filtration des groupes de ramification de G_p.

Comme κ est parfait, on a le résultat suivant :

Proposition 4.18. *Aucun saut n'est divisible par p dans la filtration $\{U_K^{(u)}K^{*p}/K^{*p}\}_u$.*

Preuve : Soit $u \geq 0$ un entier positif. Supposons que u est divisible par p et écrivons $u = lp$. Soit $b \in K^*$ tel que son image modulo K^{*p} appartienne à $U_K^{(u)}.K^{*p}/K^{*p}$. On a :

$$b = (1 + \beta t^{lp} + h.o.t.) \times \epsilon^p,$$

avec $\beta \in \kappa$ et $\epsilon \in K^*$, où l'abbréviation *h.o.t.* (*higher other terms* en anglais) regroupe des termes de plus haut degré dans la série formelle.
Or puisque κ est parfait, il existe $\gamma \in \kappa$ tel que $\beta = \gamma^p$. Il vient alors :

$$b = (1 + \gamma t^l)^p (1 + \beta' t^{lp+1} + h.o.t.)\epsilon^p,$$

avec $\beta' \in \kappa$. Ainsi, modulo K^{*p}, l'image de b est dans $U_K^{(u+1)}K^{*p}/K^{*p}$ et donc $U_K^{(u)}.K^{*p}/K^{*p} = U_K^{(u+1)}K^{*p}/K^{*p}$. ◇

Cette proposition entraîne qu'aucun saut dans la filtration des groupes de ramification de G_p n'est divisible par p. On retrouve en particulier $G_p^{(0)} = G_p^{(1)}$.

De même, on dit qu'un entier $t \geq -1$ est un saut pour la filtration $\{K^{(u)}\}_u$ de $K/\wp(K)$ si $K^{(u)} \neq K^{(u-1)}$, d'où l'existence d'un décalage d'une unité entre la définition des sauts pour les $U_K^{(u)}K^{*p}/K^{*p}$ et celle pour les $K^{(u)}$.

Proposition 4.19. *Si $u \geq 1$ est divisible par p, alors $K^{(u)} = K^{(u-1)}$. Cela signifie qu'aucun saut strictement positif n'est divisible par p dans la filtration des $K^{(u)}$.*

Preuve : Clairement, $K^{(u-1)} \subset K^{(u)}$. Réciproquement, soit $a \in K$ tel que $\bar{a} \in K^{(u)}$ où l'on désigne par une barre la classe modulo $\wp(K)$. On a donc $a = a_u T^{-u} + \sum_{i \geq -u+1} a_i T^i$, avec $a_u \in \kappa^*$ et $a_i \in \kappa$. Or, $u = lp$ pour $l \geq 1$ et a_u est de la forme γ^p, avec $\gamma \in \kappa$, car κ est parfait. On en déduit :

$$a = \gamma T^{-l} + \sum_{i \geq -(u-1)} a_i T^i + \wp(\gamma T^{-l}),$$

d'où $\bar{a} \in K^{(u-1)}$ aussi et donc $K^{(u)} = K^{(u-1)}$, ce qu'il fallait démontrer. ◇

Cela nous conduit à considérer les groupes quotients $U_K^{(u)}.K^{*p}/K^{*p}$ quand $u \geq 1$ est premier à p. Il s'agit alors de montrer que ces groupes correspondent bijectivement aux orthogonaux pour le symbole d'Artin-Schreier des groupes $K^{(v)}$, $v \geq 0$.

Calcul du symbole local d'Artin-Schreier. Pour déterminer l'orthogonal de chaque groupe, nous allons utiliser la formule explicite de Schmid (cf. proposition 4.4). A ce titre, calculons :

Lemme 4.3. *Soient i et j deux entiers positifs tels que $0 \leq i \leq j$.*
Soit $a \in K$ dont l'image modulo $\wp(K)$ est dans $K^{(i)} \backslash K^{(i-1)}$. On écrit : $a = a_{-i}T^{-i} + h.o.t.$ avec $a_{-i} \in \kappa^*$.
Soit $b \in K^*$ dont l'image modulo K^{*p} est dans $(U_K^{(j)}K^{*p}/K^{*p}) \backslash (U_K^{(j+1)}K^{*p}/K^{*p})$. On écrit : $b = 1 + b_j T^j + h.o.t.$ avec $b_j \in \kappa^*$.
En particulier, j n'est pas divisible par p. Alors on a :

$$Res(a\frac{db}{b}) = \begin{cases} a_{-i}b_j j & \text{if } j = i \\ 0 & \text{if } j > i. \end{cases}$$

Ici, l'abbréviation *h.o.t* est toujours utilisée pour désigner des termes de degré strictement plus grand que $-i$ resp. j.

Preuve : En effet, puisque j n'est pas divisible par p, on obtient :

$$a\frac{db}{b} = (a_{-i}T^{-i} + h.o.t.)\frac{jb_jT^{j-1} + h.o.t.}{1 + b_jT^j + h.o.t.},$$

d'où $a\frac{db}{b} = a_{-i}b_jjT^{j-i-1} + h.o.t.$. Alors le coefficient devant T^{-1} est soit $a_{-i}b_jj$ si $j = i$ soit 0 si $j > i$, comme désiré. ◇

Groupes de ramification supérieurs dans G_p. Pour chaque entier positif $u \geq 0$, notons :

$$\mathcal{S}_p^{(u)} := \{b.K^{*p} \in K^*/K^{*p} \ : \ [a, b) = 0, \ \forall a \in \mathfrak{p}_K^{-u}\}.$$

C'est un sous-groupe K^*/K^{*p}. Autrement dit, $\mathcal{S}_p^{(u)}$ est le groupe orthogonal de $K^{(u)} = (\mathfrak{p}_K^{-u} + \wp(K))/\wp(K)$ dans K^*/K^{*p} pour le symbole d'Artin-Schreier. En particulier, pour $u = 0$, c'est l'orthogonal de $O_K/\wp(O_K)$. Clairement, les groupes $\mathcal{S}_p^{(u)}$ forment une filtration décroissante de K^*/K^{*p}.

Le lemme 4.3 entraîne le résultat suivant :

Proposition 4.20. *Pour tout entier $u \geq 1$, on a :*

$$\mathcal{S}_p^{(u-1)} = (U_K^{(u)}K^{*p})/K^{*p},$$

par le symbole d'Artin-Schreier.

Preuve : La formule de Schmid donne $[a, b) = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mathrm{Res}(a\frac{db}{b}))$ pour tout $a \in K$ et pour tout $b \in K^*$, si $\kappa = \mathbb{F}_q$ où q désigne une puissance de p.

Soit $b \in K^*$, notons $\bar{b}$ son image modulo K^{*p}. D'abord, par le lemme 4.3, si $\bar{b}$ est dans $U_K^{(u)}K^{*p}/K^{*p}$, alors $[a, b) = 0$ pour tout $a \in K$ tel que $a+\wp(K) \in K^{(i)}$ dès que $u > i$. D'où $U_K^{(u)}K^{*p}/K^{*p} \subset \mathcal{S}_p^{(u-1)}$.

Prouvons l'autre inclusion. Soit $b \in K^*$ tel que $\bar{b}$ n'appartient pas à $U_K^{(u)}K^{*p}/K^{*p}$ et montrons qu'alors $\bar{b}$ n'appartient pas à $\mathcal{S}_p^{(u-1)}$ non plus.

Pour un tel élément b, soit $j \geq 0$ le plus grand indice tel que $\bar{b}$ soit dans $U_K^{(j)}K^{*p}/K^{*p}$. En particulier, $j \leq u - 1$ et j est premier à p d'après la proposition 4.18. De plus, on peut écrire $b = 1 + b_jT^j + h.o.t.$ avec $b_j \in \kappa^*$. Alors, puisque l'application $\mathrm{Tr}_{b_j} : \alpha \in \kappa \mapsto \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\alpha b_j) \in \mathbb{Z}/p\mathbb{Z}$ n'est pas identiquement nulle, il existe $\alpha \in \kappa = \mathbb{F}_q$ tel que $\mathrm{Tr}(\alpha b_j) \neq 0$.

Comme p ne divise pas j, on a aussi $\alpha = j\gamma$ avec $\gamma \in \kappa$ tel que $\gamma \neq 0$. Chaque élément a du type $a = \gamma T^j + h.o.t.$ est donc modulo $\wp(K)$ dans $K^{(j)}$, doù $[a, b) \neq 0$ par la formule de Schmid. En particulier, puisque $j \leq u - 1$, un tel a appartient à $K^{(u-1)}$ et alors $\bar{b}$ n'appartient pas à $\mathcal{S}_p^{(u-1)}$.

Ainsi, $\mathcal{S}_p^{(u-1)} = (U_K^{(u)}K^{*p})/K^{*p}$ pour tout entier $u \geq 1$ qui n'est pas divisible par p. Maintenant cette égalité est encore vraie pour tous les entiers $u \geq 1$ grâce aux propositions 4.18 et 4.19. ◇

Corollaire 4.3. *La loi de réciprocité induit les isomorphismes de groupes topologiques :*

$$G_p^{(u)} \xrightarrow{\simeq} \{\varphi \in H_p \ : \ \varphi(K^{(u-1)}) = 0\}, \quad \textit{pour tout } u > 0$$

et :

$$G_p^{(0)} \xrightarrow{\simeq} \{\varphi \in H_p \ : \ \varphi(K^{(0)}) = 0\}, \quad \textit{pour } u = 0.$$

Ces isomorphismes coïncident avec l'isomorphisme d'Artin-Schreier $\mathfrak{as}_1$ restreint à $G_p^{(u)}$.

Preuve : On sait que chaque $G_p^{(u)}$ est isomorphe à $U_K^uK^{*p}/K^{*p}$ par le théorème d'existence. Alors, d'après la proposition 4.20, pour $u \geq 1$ ce corollaire est essentiellement le fait que l'orthogonal $\mathcal{S}_p^{(u-1)}$ du groupe $K^{(u-1)}$ pour le symbole d'Artin-Schreier est isomorphe en tant que groupe topologique à l'annulateur de $K^{(u-1)}$ dans $\mathrm{Hom}(K/\wp(K), \mathbb{Z}/p\mathbb{Z})$: ceci est donné par l'isomorphisme ψ_p de la proposition 4.17. Le reste est une conséquence du corollaire 4.2.

Pour $u = 0$, l'isomorphisme résulte de l'égalité $G_p^{(0)} = G_p^{(1)}$. ◇

4.4 Groupes de ramification dans les extensions maximales d'Artin-Schreier-Witt d'exposant p^n

Nous considérons toujours un corps local K de caractéristique p et de corps résiduel fini. Ce paragraphe a pour but de généraliser les méthodes précédentes à toutes les extensions abéliennes maximales d'exposant p^n sur K, pour $n \geq 1$.

Plus précisément, fixons un entier $n \geq 1$. Soit G_{p^n} le groupe de Galois de l'extension abélienne maximale d'exposant p^n sur K. Comme pour le cas $n = 1$, l'interaction entre la théorie d'Artin-Schreier-Witt et la théorie du corps de classes local fournit un symbole local sur $W_n(K)/\wp(W_n(K)) \times K^*/K^{*p^n}$. Il s'agit de préciser ce symbole et d'en donner une formulation explicite qui généralise la formule de Schmid de la proposition 4.4. Bien entendu, l'idée est d'utiliser les vecteurs de Witt et donc en particulier de voir le symbole d'Artin-Schreier comme un accouplement à valeurs dans $W_1(\mathbb{F}_p)$ et non plus dans $\mathbb{Z}/p\mathbb{Z}$.

Notre but est d'exhiber une correspondance $1-1$ explicite entre les groupes de ramification de G_{p^n} et une certaine filtration du groupe d'homomorphismes continus :

$$H_{p^n} = \mathrm{Hom}(W_n(K)/\wp(W_n(K)), W_n(\mathbb{F}_p)).$$

Cette correspondance sera induite par l'isomorphisme d'Artin-Schreier-Witt $\mathfrak{as}_n$ du chapitre 2 :

$$\begin{array}{rccc} \mathfrak{as}_n : & G_{p^n} & \xrightarrow{\simeq} & H_{p^n} = \mathrm{Hom}(W_n(K)/\wp(W_n(K)), W_n(\mathbb{F}_p)) \\ & \sigma & \mapsto & \varphi_\sigma : \{a + \wp(W_n(K)) \mapsto \sigma(\alpha) - \alpha\} \end{array}$$

avec $\alpha \in W_n(K^{\mathrm{sep}})$ tel que $\wp(\alpha) = a$.

Pour tout entier $u \in \mathbb{Z}$, posons :

$$W_n^{(u)}(K) := (\mathfrak{p}_K^{-\lfloor \frac{u}{p^{n-1}} \rfloor}, \mathfrak{p}_K^{-\lfloor \frac{u}{p^{n-2}} \rfloor}, \cdots, \mathfrak{p}_K^{-u}).$$

Les ensembles $W_n^{(u)}(K)$ forment une suite croissante de sous-groupes de $W_n(K)$ avec $W_n^{(0)} = W_n(O_K)$ et $W_n^{(-1)} = (\mathfrak{p}_K, ..., \mathfrak{p}_K)$.
Nous allons considérer ces sous-groupes modulo $\wp(W_n(K))$. Leurs images forment une filtration croissante du groupe quotient $W_n(K)/\wp(W_n(K))$. De plus, d'après le lemme 3.4 du chapitre 3, on a $W_n^{(u)} \subset \wp(W_n(K))$ pour tout $u \leq -1$, de sorte que dans la suite nous considérerons uniquement les groupes $W_n^{(u)}(K)$ pour $u \geq -1$.

Maintenant pour tout entier $v \geq -1$, posons :

$$H_{p^n}^{(v)} := \{\varphi \in H_{p^n} \ : \ \varphi(W_n^{(v)}(K) + \wp(W_n(K))/\wp(W_n(K))) = 0\}.$$

Clairement, les groupes $H_{p^n}^{(v)}$ forment une filtration décroissante de H_{p^n} lorsque $v \geq -1$:

$$H_{p^n} = H_{p^n}^{(-1)} \supset H_{p^n}^{(0)} \supset H_{p^n}^{(1)} \supset \cdots \supset H_{p^n}^{(v)} \cdots .$$

Ce paragraphe s'articule autour de la preuve du résultat suivant :

Théorème 4.4. *Pour tout entier $u \geq 0$, l'interaction entre la loi de réciprocité et la théorie d'Artin-Schreier-Witt induit les isomorphismes de groupes topologiques :*

$$G_{p^n}^{(u)} \xrightarrow{\simeq} H_{p^n}^{(u-1)}, \ \ \textit{si } u > 0 \ \ \textit{et} \ \ G_{p^n}^{(0)} \xrightarrow{\simeq} H_{p^n}^{(0)}, \ \ \textit{si } u = 0,$$

qui coïncident avec l'isomorphisme d'Artin-Schreier-Witt $\mathfrak{as}_n$ restreint aux $G_{p^n}^{(u)}$.

Ces isomorphismes sont obtenus à travers le symbole d'Artin-Schreier-Witt, généralisation du symbole d'Artin-Schreier aux vecteurs de Witt de longueur n.

4.4.1 Le symbole d'Artin-Schreier-Witt

La théorie d'Artin-Schreier-Witt du chapitre 2 fournit un accouplement :

$$\begin{array}{ccc} W_n(K) \times G_{p^n} & \to & W_n(\mathbb{F}_p) \\ (a, \sigma) & \mapsto & \sigma(\alpha) - \alpha, \end{array}$$

avec $\alpha \in W_n(K^{\text{sep}})$ tel que $\wp(\alpha) = a$. Rappelons que l'action du groupe de Galois G_{p^n} sur $W_n(K)$ est définie composante par composante :

$$\sigma(\alpha) = (\sigma(\alpha_0), \sigma(\alpha_1), ..., \sigma(\alpha_{n-1})).$$

D'autre part, le théorème d'existence induit un homéomorphisme de K^*/K^{*p^n} dans G_{p^n} :

Proposition 4.21. *Pour tout entier $n \geq 1$, le théorème d'existence induit un isomorphisme de groupes topologiques que nous noterons encore ω_K :*

$$\omega_K : K^*/K^{*p^n} \xrightarrow{\simeq} G_{p^n}.$$

Preuve : C'est une généralisation de la proposition 4.16. Comme les deux lignes du diagramme de la proposition 4.7 sont des suites exactes scindées, on obtient un nouveau diagramme commutatif en prenant le produit tensoriel avec $\mathbb{Z}/p^n\mathbb{Z}$:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & U_K/U_K^n & \longrightarrow & K^*/K^{*p^n} & \longrightarrow & \mathbb{Z}/p^n\mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \omega_K} & & \downarrow{\scriptstyle \omega_K} & & \downarrow & & \\ 0 & \longrightarrow & G_{p^n}^{(0)} & \longrightarrow & G_{p^n} & \longrightarrow & \hat{\mathbb{Z}}/p^n\hat{\mathbb{Z}} & \longrightarrow & 0 \end{array}$$

Puisque $\hat{\mathbb{Z}}/p^n\hat{\mathbb{Z}}$ est canoniquement isomorphe à $\mathbb{Z}/p^n\mathbb{Z}$, les flèches de gauche et de droite sont des isomorphismes, la loi de réciprocité ω_K induit donc un isomorphisme de groupes topologiques : $K^*/K^{*p^n} \xrightarrow{\simeq} G_{p^n}$, ce qu'il fallait démontrer. ◇

Ainsi, par le théorème d'existence, l'accouplement d'Artin-Schreier-Witt précédent donne lieu à l'accouplement suivant :

$$\begin{array}{ccc} W_n(K)/\wp(W_n(K)) \times K^*/K^{*p^n} & \to & W_n(\mathbb{F}_p) \\ (a + \wp(W_n(K)), b.K^{*p^n}) & \mapsto & [a, b) := (b, L/K)(\alpha) - \alpha, \end{array}$$

avec $\wp(\alpha) = a$ et $L = K(\alpha)$.

Cet accouplement est appelé *symbole d'Artin-Schreier-Witt*. Il satisfait les propriétés suivantes :

Proposition 4.22. *(i) Le symbole d'Artin-Schreier-Witt est bilinéaire.*

(ii) Pour tout $a \in K$, $[a, b) = 0$ si et seulement si b est norme dans l'extension $K(\alpha_0, ..., \alpha_{n-1})/K$ où $\wp(\alpha_0, ..., \alpha_{n-1}) = a$.

(iii) Pour tout $a \in K$ et pour tout $b \in K^*$, $[Va, b) = V[a, b)$ où V est l'opérateur shift.

(iv) $[a, b) = 0$ si et seulement si b est norme dans l'extension $K(\alpha_0, ..., \alpha_{n-1})/K$, où $\alpha = (\alpha_0, ..., \alpha_{n-1})$ est tel que $\wp(\alpha) = a$.

Preuve : Les assertions (i) et (ii) résultent directement de la définition de l'accouplement d'Artin-Schreier-Witt.

Quant à la propriété (iii), on a : $V[a, b) = V(\omega_K(\alpha) - \alpha)$ et $[Va, b) = \omega_K(\alpha') - \alpha'$ avec $\wp(\alpha) = a$ et $\wp(\alpha') = Va$. Or, on a aussi $Va = V\wp(\alpha) = \wp(V(\alpha))$ puisque V et $\wp$ commutent par la proposition 1.16 du chapitre 2, ainsi α' et $V\alpha$ diffèrent d'un élément de $W_n(\mathbb{F}_p)$. D'où $[Va, b) = \omega_K(b)(V\alpha) - V\alpha = V(\omega_K(b)(\alpha) - \alpha)$ puisque l'action de $\omega_K(b)$ sur un vecteur de Witt est définie composante par composante.

Enfin, (iv) est essentiellement due à la relation $[a,b) = (b, L/K)(\alpha) - \alpha$, c'est-à-dire $[a,b) = 0$ si et seulement si $(b, L/K) = 1$ dans $\mathrm{Gal}(K(\alpha)/K)$, i.e. si et seulement si b est norme dans $K(\alpha)$ d'après la loi de réciprocité sur les extensions finies. $\diamond$

Montrons maintenant que le symbole d'Artin-Schreier-Witt est un accouplement non-dégénéré. Cette propriété essentielle est une conséquence du théorème d'existence :

Proposition 4.23. *Le symbole d'Artin-Schreier-Witt est non-dégénéré.*

Preuve : Soit $a \in W_n(K)$ tel que $\omega_K(b)(\alpha) - \alpha = 0$ pour tout $b \in K^*$ si $\wp(\alpha) = a$. D'après le théorème d'existence, $\omega_K(K^*)$ est dense dans G_K. Donc G_K fixe l'extension $K(\alpha)$, d'où $\alpha \in W_n(K)$ i.e. $a \in \wp(W_n(K))$.

Maintenant, soit $b \in K^*$. Si $\omega_K(b)(\alpha) - \alpha = 0$ pour tout $a \in W_n(K)$ avec $\wp(\alpha) = a$, alors $\omega_K(b)$ fixe toutes les extensions cycliques de degré divisant p^n sur K, $\omega_K(b)$ fixe donc toutes les extensions abéliennes finies d'exposant p^n sur K et, en prenant la réunion, fixe l'extension abélienne maximale d'exposant p^n sur K. Ainsi, $\omega_K(b)$ est l'identité dans G_{p^n}, ce qui signifie que $b \in K^{*p^n}$ par la proposition 4.21. La réciproque est évidente.

On vient donc de montrer que les noyaux à gauche et à droite pour le symbole d'Artin-Schreier-Witt sont triviaux et donc que cet accouplement est non dégénéré. $\diamond$

Si $a \in W_n(K)$ et $b \in K^*$, nous noterons $[a,b)$ l'image de leurs représentants modulo $\wp(W_n(K))$ et modulo K^{*p^n} respectivement par le symbole d'Artin-Schreier-Witt.

Pour clore ce sous-paragraphe, nous vérifions que le symbole d'Artin-Schreier-Witt fournit un isomorphisme de G_{p^n} sur H_{p^n} qui coïncide avec l'isomorphisme d'Artin-Schreier-Witt $\mathfrak{as}_n$.

Théorème 4.5. *Le symbole d'Artin-Schreier-Witt induit un isomorphisme de groupes topologiques :*

$$\psi_{p^n} : K^*/K^{*p^n} \xrightarrow{\simeq} Hom(W_n(K)/\wp(W_n(K)), W_n(\mathbb{F}_p))$$

donné par $(b.K^{*p^n}) \mapsto \{(a + \wp(W_n(K))) \mapsto [a,b)\}$.

En particulier, par le théorème d'existence, on en déduit un isomorphisme de groupes topologiques :

$$\psi_{p^n} \circ \omega_K^{-1} \ : \ G_{p^n} \xrightarrow{\simeq} Hom(W_n(K)/\wp(W_n(K)), W_n(\mathbb{F}_p))$$

qui correspond identiquement à l'isomorphisme d'Artin-Schreier-Witt $\mathfrak{as}_n$.

Preuve : Rappelons que $W_n(K)$ est muni de la topologie p-adique, i.e. la topologie de la convergence composante par composante et qui est induite par la topologie du produit K^n lorsque K a la topologie usuelle provenant de sa valuation. En particulier, $(\mathfrak{p}_K, ..., \mathfrak{p}_K)$ est un voisinage ouvert de 0 dans $W_n(K)$ pour cette topologie. Or, d'après le lemme 3.4 du chapitre 3, $(\mathfrak{p}_K, ..., \mathfrak{p}_K) \subset \wp(W_n(K))$. Donc $W_n(K)/\wp(W_n(K))$ est discret pour la topologie quotient.

D'autre part, puisque $VF = FV$ est la multiplication par p sur $W_n(K)$ d'après la proposition 1.16 du chapitre 2, il vient : $p^n = V^n F^n = 0$ sur $W_n(K)$. Le groupe abélien $W_n(K)/\wp(W_n(K))$ est donc discret de p^n-torsion.

Par la proposition 4.21, on a aussi que le groupe K^*/K^{*p^n} est abélien profini et d'exposant p^n.

Alors, sur ces groupes, la dualité de Pontryagin coïncide avec la dualité $\mathrm{Hom}(-, \mathbb{Z}/p^n\mathbb{Z})$ et donc avec la dualité $\mathrm{Hom}(-, W_n(\mathbb{F}_p))$ puisque $\mathbb{Z}/p^n\mathbb{Z}$ et $W_n(\mathbb{F}_p)$ sont canoniquement isomorphes. Ainsi la preuve du théorème 4.5 est essentiellement la même que celles de la proposition 4.17 et du corollaire 4.2 lorsque l'on remplace $\mathbb{Z}/p\mathbb{Z}$ par $W_n(\mathbb{F}_p)$. $\diamond$

4.4.2 La formule de Schmid-Witt

Dans ce sous-paragraphe, nous allons développer une formulation explicite du symbole d'Artin-Schreier-Witt qui généralise la formule de Schmid aux vecteurs de Witt de longueur n. Nous

l'appellerons la *formule de Schmid-Witt*. Comme pour le cas d'exposant p, cette formulation sera très utile pour le calcul des groupes de ramification de G_{p^n} en correspondance avec la filtration des $H_{p^n}^{(v)}$ du groupe $\mathrm{Hom}(W_n(K)/\wp(W_n(K))/W_n(\mathbb{F}_p))$.

L'idée est de considérer la formule de Schmid initiale comme une relation donnée par les composantes fantômes d'un certain vecteur de Witt. Pour $a \in W_n(K)$ et $b \in K^*$, il s'agit précisément de passer temporairement en caractéristique 0 en relevant a et b en des éléments A et B de $W_n(R((T)))$ et $R((T))^*$ respectivement, où R est un anneau de valuation discrète complet de caractéristique 0 et de même corps résiduel que K. Or, l'anneau $R = W(\mathbb{F}_q)$ satisfait ces propriétés (cf. [60], Chap. II, §6, Thm.7). On définit donc un accouplement explicite $W_n(R((T))) \times R((T))^*$ à valeurs dans $W_n(R)$: étant donnés deux éléments A et B cet accouplement retourne un vecteur (A, B) de $W_n(R)$ donné par ses composantes fantômes que l'on exprime comme les résidus d'éléments de $R((T))$, généralisant ainsi la formule de Schmid. C'est le "Residuenvektor" de [76].

Cet accouplement est tel qu'en revenant sur $W_n(K) \times K^*$, nous obtenons un accouplement que nous appellerons *symbole de Schmid-Witt* et qui correspond en fait au symbole d'Artin-Schreier-Witt. Ce sera la proposition 4.6. Plus loin, la proposition 4.30 fournira une autre formulation pour la formule de Schmid-Witt qui évite la réduction dans $W_n(K) \times K^*$.

Enfin, notons que, puisque $X_0 = X^{(0)}$, l'application g_A qui à un vecteur de Witt associe ses composantes fantômes est bijective de $W_1(A) = A$ sur A quelque soit la caractéristique de l'anneau A considéré. C'est pourquoi, suivant notre raisonnement, la formule initiale de Schmid pour $n = 1$ n'utilise aucun relèvement.

Le présent sous-paragraphe est l'écriture détaillée de tout ce procédé.

Le symbole de Schmid-Witt. D'après ([60], Chap.II,§4), le corps K est isomorphe au corps des séries formelles $\kappa((T))$ via l'identification $\pi_K \mapsto T$ après avoir choisi une uniformisante π_K de K. Si $\kappa = \mathbb{F}_q$ pour une puissance q de p, on identifiera donc K avec le corps $\mathbb{F}_q((T))$.

Soit $a \in W_n(\mathbb{F}_q((T)))$, écrivons $a = (a_i)_i$ avec $a_i = \sum_{v \geq v_i} a_{i,v} T^i \in \mathbb{F}_q((T))$ et $a_{i,v_i} \neq 0$. De même, soit $b \in \mathbb{F}_q((T))^*$, écrivons $b = b_m T^m + h.o.t.$ avec $b_m \in \mathbb{F}_q^*$ (l'abbreviation *h.o.t.* désignant toujours des termes de degré strictement plus grand).
Nous relevons a en un élément A de $W_n(W(\mathbb{F}_q((T))))$ et b en un élément B de $W(\mathbb{F}_q)((T))^*$ comme suit :

$$A = (A_i)_{i=0}^{n-1} \in W_n(W(\mathbb{F}_q)((T))),$$

tel que, pour tout $i \geq 0$:

$$A_i = \sum_{v \geq v_i} A_{i,v} T^i, \text{ with } A_{i,v} \in W(\mathbb{F}_q),\ (A_{i,v})_0 = a_{i,v}$$

et :

$$B = \sum_{l \geq m} B_l T^l \in W(\mathbb{F}_q)((T))^*,$$

avec $(B_l)_0 = b_l$ pour tous $l \geq m$.

En particulier, si l'on munit $W(\mathbb{F}_q)((T))$ de la valuation polynômiale usuelle, alors chaque A_i est de valuation $v_K(a_i)$ et B de valuation $v_K(b)$.

Par l'identification $K = \mathbb{F}_q((T))$, on définit alors un accouplement $W_n(K) \times K^* \to W_n(\mathbb{F}_p)$ qui

est donné par la colonne de gauche dans le diagramme commutatif suivant :

$$\begin{array}{ccccc}
\mathbf{W_n}(\mathbb{F}_\mathbf{q}((\mathbf{T}))) & \xleftarrow[W_n(T_0)]{} & W_n(W(\mathbb{F}_q)((T))) & \xrightarrow{\Gamma_{W(\mathbb{F}_q)((T))}} & W(\mathbb{F}_q)((T))^n \\
\times & & \times & & \times \\
\mathbb{F}_\mathbf{q}((\mathbf{T}))^* & \xleftarrow[T_0]{} & W(\mathbb{F}_q)((T))^* & \xrightarrow{\text{"}d\log\text{"}} & W(\mathbb{F}_q)((T))^* \\
\downarrow & & \downarrow & & \downarrow \\
\mathbf{W_n}(\mathbb{F}_\mathbf{q}) & \xleftarrow[W_n(t_0)]{} & W_n(W(\mathbb{F}_q)) & \xrightarrow{\Gamma_{W(\mathbb{F}_q)}} & W(\mathbb{F}_q)^n \\
\downarrow{\scriptstyle \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}} & & & & \\
\mathbf{W_n}(\mathbb{F}_\mathbf{p}) & & & &
\end{array}$$

où les flèches sont définies comme suit :

$$\begin{array}{ccccc}
a=(a_i)_{i=0}^{n-1} & \longleftarrow\!\shortmid & A=(A_i)_{i=0}^{n-1} & \longmapsto & (A^{(i)})_{i=0}^{n-1} \\
\times & & \times & & \times \\
b=b_mt^m+\text{h.o.t.} & \longleftarrow\!\shortmid & B=B_mt^m+\text{h.o.t.} & \longmapsto & \frac{dB}{B} \\
\downarrow & & \downarrow & & \downarrow \\
(a,b) & \xleftarrow[W_n(t_0)]{}\!\shortmid & (A,B) & \longmapsto & (\mathrm{Res}(\frac{dB}{B}A^{(i)}))_i \\
\downarrow & & & & \\
\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(a,b) & & & &
\end{array}$$

Ici, la trace sur $W_n(\mathbb{F}_q)$ est définie par :

$$\forall x \in W_n(\mathbb{F}_q), \quad \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(x) := \sum_{i=0}^{d-1} F^i.x,$$

pour l'addition de Witt et où d est l'exposant dans $q=p^d$.

Remarquons que le vecteur (A,B) donné par ses composantes fantômes appartient *a priori* à l'anneau $W_n(W(\mathbb{F}_q)[\frac{1}{p}])$ puisque p n'est pas inversible dans $W(\mathbb{F}_q)$, i.e. $g_{W_n(W(\mathbb{F}_q))}$ n'est pas surjective. Mais d'après la proposition "Satz 4" de [76], chaque composante de (A,B) est un polynôme à coefficients entiers en les indéterminées B_m^{-1}, B_l et $A_{i,v}$, pour tous les indices $l \geq m$, $i \geq 0$ et $v \geq v_i$. De plus, B_m^{-1} est dans $W(\mathbb{F}_q)$ puisque sa première composante b_m est une unité de $\mathbb{F}_q$ (cf. corollaire 1.3 du chapitre 1). Le vecteur (A,B) appartient donc bien à l'anneau $W_n(W(\mathbb{F}_q))$ et le diagramme est bien défini.

Cela entraîne aussi :

Proposition 4.24. *Le vecteur de Witt (a,b), ainsi défini, ne dépend pas du choix des relèvements A et B.*

Preuve : D'après ce qui précède, chaque composante du vecteur (a,b) est un polynôme à coefficients entiers évalué en b_m^{-1}, b_l et $a_{i,v}$ puisque la première composante de la somme (resp. le produit) de deux vecteurs de Witt est la somme (resp. le produit) de leurs premières composantes (cf. chapitre 1). ◇

L'accouplement précédent $W_n(K) \times K^* \to W_n(\mathbb{F}_p)$, avec $K=\mathbb{F}_q((T))$, est donc bien défini. Nous l'appellerons *symbole de Schmid-Witt*.

Ce symbole satisfait les propriétés suivantes :

Proposition 4.25. *(i) Le symbole de Schmid-Witt est un accouplement bilinéaire.*
(ii) Pour tout $a \in W_n(K)$ et pour tout $b \in K^*$: $(Va, b) = V(a, b)$.

Preuve : La propriété (i) provient du fait que la somme dans l'anneau de Witt correspond à la somme des composantes fantômes (cf. chapitre 1).
La propriété (ii) résulte des formules $(Vx)^{(0)} = 0$ et $(Vx)^{(i)} = x^{i-1}$ pour tout vecteur de Witt x sur un anneau R et pour tout $i \geq 1$. ◇

La formule de Schmid-Witt. Généralisant la proposition 4.4, le théorème suivant montre que le symbole de Schmid-Witt est identique au symbole d'Artin-Schreier-Witt :

Théorème 4.6 (SchmidWitt)**.** *Si $a \in W_n(K)$ et $b \in K^*$, on a :*

$$[a, b) = Tr_{\mathbb{F}_q/\mathbb{F}_p}((a, b)).$$

La preuve de cette formule utilise la proposition suivante que nous montrerons plus loin :

Proposition 4.26. *Soit $a \in W_n(K)$ et soit $b \in K^*$. Si $c = (a, b) \in W_n(\mathbb{F}_q)$, alors :*

$$[a, b) = [c, T),$$

où $[-,-) : W_n(K) \times K^* \to W_n(\mathbb{F}_p)$ est le symbole d'Artin-Schreier-Witt.

Montrons alors le théorème 4.6 :

Preuve : La proposition 4.26 nous permet de prendre $b = T$ et supposer a constant, i.e. $a \in W_n(\mathbb{F}_q)$ où $\mathbb{F}_q = \kappa$. Alors le théorème 4.6 revient à dire :

$$[a, T) = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(a),$$

puisque $(a, T) = a$ lorsque a est une constante.
Soit donc $\alpha \in W_n(\kappa^{\mathrm{sep}})$ une racine de l'équation $\wp(\alpha) = a$ et soit κ'/κ l'extension cyclique correspondante de degré $p^k \leq p^n$. Posons $K' := \kappa'((T))$: c'est une extension non ramifiée de K. Alors, par le lemme 4.1 on obtient $(T, K'/K) = F_q$, où F_q désigne le générateur canonique de $\mathrm{Gal}(K'/K) \simeq \mathrm{Gal}(\kappa'/\kappa)$ défini par $x \mapsto x^q$. Ecrivant $q = p^d$ et puisque F_q commute avec $\wp$ il vient :

$$\begin{aligned}
[a, T) &= F_q\alpha - \alpha \\
&= (\alpha_0^q, ..., \alpha_{n-1}^q) - (\alpha_0, ..., \alpha_{n-1}) \\
&= (\alpha_0^{p^d}, ...) - (\alpha_0^{p^{d-1}}, ...) + (\alpha_0^{p^{d-1}}, ...) + ... + (\alpha_0^p, ...) - (\alpha_0, ...) \\
&= \wp(\alpha_0^{p^{d-1}}, ...) + ... + \wp(\alpha_0, ...) \\
&= \wp(F_q^{d-1}(\alpha)) + \wp(F_q^{d-2}(\alpha)) + ... + \wp(\alpha) \\
&= F_q^{d-1}(a) + ... + F_q(a) + a \\
&= \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(a)
\end{aligned}$$

car l'extension $\mathbb{F}_q/\mathbb{F}_p$ est cyclique d'ordre l. Ceci montre le théorème 4.6. ◇

Preuve de la proposition 4.26. La proposition 4.26 est une conséquence du lemme suivant dû à Teichmüller :

Lemme 4.4. *Soit $a_0 \in K^*$ et soit $a = \{a_0\}$ un vecteur de Witt de longueur n tel que $a_0 = \sum_{v>0} a_{0,v} T^{-v}$, i.e. a_0 est une combinaison linéaire de puissances strictement négatives de T. Alors $[a, T) = 0$.*

Preuve : Voir [72]. ◇

D'où la preuve de la proposition 4.26 :

Preuve : Supposons d'abord que $b = T$ et écrivons $a_0 = \sum_{v\in\mathbb{Z}} a_{0,v}T^v$ de telle sorte que :

$$a = \{a_{0,0}\} + \{\sum_{v>0} a_{0,v}T^v\} + \sum_{v>0}\{a_{0,-v}T^{-v}\} + \Omega a$$

pour un certain vecteur de Witt Ωa dans $W_n(K)$. Notons que comme la première composante d'un vecteur somme est la somme des premières composantes, on a $(\Omega a)_0 = 0$. On écrira alors $\Omega a = V\omega$ où $\omega = (\omega_0, \omega_1, ...)$ est un vecteur sur K.

Par bilinéarité du symbole d'Artin-Schreier-Witt, on obtient :

$$[a, T) = [\{a_{0,0}\}, T) + [\{\sum_{v>0} a_{0,v}T^v\}, T) + \sum_{v>0}[\{a_{0,-v}T^{-v}\}, T) + \Omega a.$$

D'une part, puisque $\{a_{0,0}\}$ est dans $W_n(\mathbb{F}_q)$, le symbole de Schmid-Witt vaut $(\{a_{0,0}\}, T) = \{a_{0,0}\}$. En effet, soit A un relèvement du vecteur $\{a_{0,0}\}$ pour le symbole de Schmid-Witt, alors A est un vecteur de $W_n(W(\mathbb{F}_q))$ tel que toutes ses composantes fantomes $A^{(i)}$ sont constantes. D'où $\mathrm{Res}(\frac{dB}{B}A^{(i)}) = A^{(i)}$ pour tout i et donc $(A, T) = A$, ce qui implique $(\{a_{0,0}\}, T) = \{a_{0,0}\}$. On a alors $[(\{a_{0,0}\}, T), T) = [\{a_{0,0}\}, T)$.

D'autre part, le vecteur $a_{>0} = \{\sum_{v>0} a_{0,v}T^v\}$ appartient clairement à l'ensemble $(\mathfrak{p}_K, ..., \mathfrak{p}_K)$. Par le lemme 3.4 du chapitre 3, $a_{>0}$ est donc dans $\wp(W_n(K))$. Alors $[a_{>0}, T) = 0$ d'après la proposition 4.23. En outre, si A est un relèvement de $a_{>0}$ pour le symbole de Schmid-Witt, toutes ses composantes sont de valuation strictement positives et ses composantes fantomes $A^(i)$ aussi. D'où $\mathrm{Res}(\frac{dT}{T}A^{(i)}) = 0$ pour tout i et donc $(a_{>0}, T) = 0$. Alors $[(a_{>0}, T), T) = [a_{>0}, T)$ encore.

D'après le lemme 4.4, chaque vecteur $\{a_{0,-v}T^{-v}\}$, $v > 0$, est tel que $[\{a_{0,-v}T^{-v}\}, T) = 0$. Notons $a_{<0}$ le vecteur $\{a_{0,-v}T^{-v}\}$. Pour calculer le symbole de Schmid-Witt $(a_{<0}, T)$ on relève $a_{<0}$ en un vecteur A de la forme $\{A_{0,-v}T^{-v}\}$ avec $A_{0,-v} \in W(\mathbb{F}_q)$ de telle sorte que les composantes fantômes $A^{(i)}$ sont combinaisons linéaires de puissances strictement négatives de T et satisfont donc $\mathrm{Res}(\frac{dT}{T}A^{(i)}) = 0$. D'où $(a_{<0}, T) = 0$ et $[(a_{<0}, T), T) = [(a_{<0}, T)$.

Alors, par bilinéarité des symboles d'Artin-Schreier-Witt et de Schmid-Witt, il vient :

$$[(a, T), T) - [a, T) = [(\Omega a, T), T) - [\Omega a, T).$$

Puisque $\Omega a = V\omega$ pour $\omega \in W_n(K)$, en itérant le procédé on construit successivement des vecteurs de Witt $\Omega^i a$ du type $V^i\omega_i$, avec $\omega_i \in W_n(K)$, tels que :

$$\forall i \geq 0,\ [(a, T), T) - [a, T) = [(\Omega^i a, T), T) - [\Omega^i a, T).$$

En particulier, pour $i = n$ on obtient $\Omega^n a = V^n\omega_n = 0$ et donc $[(a, T), T) - [a, T) = 0$, ce qu'il fallait démontrer.

Pour finir, soit $b \in K^*$ quelconque. On écrit $b = \epsilon T^m$, où ϵ est une unité de K et $m > 0$. En particulier, $T' := bT^{1-m}$ est une uniformisante de K. Alors par bilinéarité du symbole d'Artin-Schreier-Witt on obtient :

$$[a, b) = [a, T'T^{m-1}) = (m-1)[a, T) + [a, T') = (m-1)[(a, T), T) + [(a, T'), T')$$

et on conlut par bilinéarité du symbole de Schmid-Witt grâce à ce qui précède. On a en effet :

$$\begin{aligned}[(a, b), T) &= (m-1)[(a, T), T) + [(a, T'), T) \\ &= (m-1)[(a, T), T) + [(a, T'), T') - [(a, T'), bT^{-m}),\end{aligned}$$

où bT^{-m} est une unité de K. Or (a, T') est dans $W_n(\mathbb{F}_q)$ donc dans $W_n(O_K)$ et d'après le théorème 3.4 du chapitre 3 cela signifie que l'extension d'Artin-Schreier-Witt correspondante est non ramifiée. D'où $[(a, T'), bT^{-m}) = 0$ par le lemme 4.1 et donc $[(a, b), T) = [a, b)$. Ceci termine la preuve de la proposition 4.26. ◇

Notons que le lemme 4.4 de Teichmüller est en fait valide lorsque le corps résiduel de K est parfait alors que la formule de Schmid-Witt n'est vraie que pour un corps résiduel fini, telle que nous l'avons montrée. Cette formule implique en particulier que dans le cadre de la théorie du corps de classe local, le symbole de Scmid-Witt est également non-dégénéré.

4.4.3 La forme réduite d'un vecteur de Witt

On propose ici de réduire les vecteurs de Witt sous une forme qui rend le calcul du symbole de Schmid-Witt plus facile.

Vecteurs de Witt réduits. Nous allons montrer que chaque vecteur de Witt de longueur n sur K est congruent modulo $\wp(W_n(K))$ à un vecteur de Witt dont les composantes sont appropriées au calcul du symbole d'Artin-Schreier-Witt. Cette réduction est déjà mentionnée dans le papier de Schmid [57] :

Proposition 4.27. *Soit $a = (a_0, ..., a_{n-1})$ un vecteur de Witt dans $W_n(K)$. Alors a est congruent modulo $\wp(W_n(K))$ à un vecteur $a' = (a'_0, ..., a'_{n-1})$ tel que, pour chaque indice i, soit a'_i est dans O_K soit sa valuation $v_K(a'_i)$ est strictement négative et non divisible par p.*

On dit que le vecteur a' est réduit et on l'appelle forme réduite de a.

Preuve : Nous montrons cette proposition successivement. Elle est vraie pour $n = 1$ par la remarque **??** du chapitre 3. Supposons avoir déjà réduit a sous la forme $(a'_0, ..., a'_s, \alpha_{s+1}, ..., \alpha_{n-1})$ où chaque α_i, pour $0 \leq i \leq s$, est soit dans O_K, soit de valuation négative première à p. Considérons la composante α_{s+1}. Supposons $v_K(\alpha_{s+1}) < 0$ et $v_K(\alpha_{s+1}) = -pl$ pour un certain entier $l \geq 1$. Alors puisque κ est parfait, on peut écrire $\alpha_{s+1} = uT^{-l} + \wp(uT^{-l})$ avec $u \in \kappa$. En itérant si nécessaire, on construit a'_{s+1} et h_{s+1} dans K tels que $\alpha_{s+1} = a'_{s+1} + \wp(h_{s+1})$ et $v_K(a'_{s+1}) > v_K(\alpha_{s+1})$ avec soit $v_K(a'_{s+1}) \geq 0$ soit $p \not| v_K(a'_{s+1})$. On a donc réduit a au vecteur $a - V^{s+1}\wp(\{h_{s+1}\}) = a - \wp(V^{s+1}\{h_{s+1}\})$ puisque V et $\wp$ commutent (cf. proposition 1.16 du chapitre I). On obtient la forme $a = (a'_0, ..., a'_s, a'_{s+1}, \beta_{s+2}, ...) \mod \wp(W_n(K))$ où les $s+2$ premières composantes satisfont les conditions de la proposition. On itère le procédé aux autres composantes. ◇

Remarque 20. *Dans sa thèse (Université d'Amsterdam, 2001), V. Shabat pousse la réduction plus loin (cf. [62], Chap.8, §2). En effet, il montre que tout vecteur $a \in W_n(K)$ admet modulo $\wp(W_n(K)$ un représentant de la forme :*

$$(a_0, ..., a_{s-1}, a_s, ..., a_{r-1}, a_r, ..., a_{n-1})$$

où $a_0 = ... = a_{s-1} = 0$, $a_s, ..., a_{r-1}$ sont dans O_K, $a_s \notin \wp(K)$, a_r est de valuation strictement négative première à p et $a_{r+1}, ..., a_{n-1}$ sont soit dans O_K soit de valuation première à p. En particulier, si a est un tel vecteur réduit, il est facile de voir que a définit sur K une extension cyclique de degré exactement p^{n-s} par la théorie d'Artin-Schreier-Witt.

La fonction M_n. On introduit alors la fonction suivante :

Définition 4.4. *Pour $a = (a_0, ..., a_{n-1}) \in W_n(K)$, on définit :*

$$M_n(a) := \max_i \{-p^{n-1-i} v_K(a_i)\}.$$

Comme $v_K(0) = +\infty$, la valeur de $M_n(a)$ est soit un entier soit $+\infty$. Mais si a est un vecteur non nul, alors $M_n(a)$ est toujours un entier.

Remarque 21. *Si $n = 1$, $M_1(a_0) = -v_K(a_0)$. De plus, pour $n \geq 2$, on a la relation de récurrence :*

$$M_n(a_0, ..., a_{n-1}) = \max\{pM_{n-1}(a_0, ..., a_{n-2}), -v_K(a_{n-1})\},$$

d'où une autre définition, récursive cette fois, de $M_n(a)$.

On définit ainsi une fonction $M_n : W_n(K) \to \mathbb{Z} \cup +\infty$ qui satisfait les propriétés suivantes :

Proposition 4.28. *Soient x et y des vecteurs de Witt dans $W_n(K)$. On a :*

1. *Soit $u \geq 0$. Si $x \in W_n^{(u)} \backslash W_n^{(u-1)}$, alors $M_n(x) = u$.*

2. *Si x est réduit et si $M_n(x) \geq 1$, alors $M_n(x) = -p^{n-j-1}v_K(x_j)$ pour un unique indice j de $\{0, ..., n-1\}$.*
3. *$M_n(x+y) \leq \max\{M_n(x), M_n(y)\}$.*
4. *Si $c \in W_n(\mathbb{F}_p)$, alors $M_n(cx) \leq M_n(x)$.*
5. *Si $c \in W_n(\mathbb{F}_p)$ est une unité, alors $M_n(cx) = M_n(x)$. En particulier : $M_n(-x) = M_n(x)$.*
6. *Si $M_n(x) \neq M_n(y)$, on a l'égalité $M_n(x+y) = \max(M_n(x), M_n(y))$.*
7. *Soit $M_n(\wp(x)) \leq 0$, soit p divise $M_n(\wp(x))$.*

Preuve :

1. On note $x = (x_0, ..., x_{n-1})$. Si $x \in W_n^{(u)}$, alors pour tout i on a : $-v_K(x_i) \leq \lfloor \frac{u}{p^{n-1-i}} \rfloor$, d'où $-p^{n-1-i}v_K(x_i) \leq u$. En prenant le maximum, il vient : $M_n(x) \leq u$.

   Maintenant, x n'appartient pas à $W_n^{(u-1)}$, cela signifie qu'il existe x_i tel que $v_K(x_i) < -\lfloor \frac{u-1}{p^{n-1-i}} \rfloor$, i.e. $-p^{n-1-i}v_K(x_i) > u-1$. Donc $M_n(x) \geq u$ et $M_n(x) = u$.

   En particulier, $M_n(x) = 0$ si et seulement si l'extension cyclique $K(\alpha_0, ..., \alpha_{n-1})/K$ est non-ramifiée, où $\wp(\alpha_0, ..., \alpha_{n-1}) = a$.
2. Conséquence du point (1). Si $u \geq 1$, alors $M_n(x) > 0$, i.e. $M_n(x) = -p^{n-1-j}v_K(x_j)$ pour un certain indice j tel que $v_K(a_j) < 0$. Alors, si x est réduit et si $M_n(x) = -p^{n-1-l}v_K(x_l) = -p^{n-1-j}v_K(x_j)$ avec $l \neq j$, le nombre p devrait diviser soit $v_K(x_j)$ soit $v_K(a_l)$, ce qui contredit la définition des vecteurs réduits.
3. Rappelons (chapitre 1) que la i-ème composante du vecteur somme $x+y$ est donnée par un polynôme $S_i(x_0, ..., x_i, y_0, ..., y_i)$ à coefficients entiers. Il est en fait facile de voir que $S_i(x_0, ..., x_i, y_0, ..., y_i)$ est homogène de poids p^i, i.e. le polynôme S_i est combinaison linéaire de monômes :
$$x_0^{v_0} y_0^{w_0} ... x_i^{v_i} y_i^{w_i}$$
avec :
$$\sum_{k=0}^{i} p^k(v_k + w_k) = p^i.$$
Ecrivons $M := \max\{M_n(x), M_n(y)\}$. Pour chaque indice i, on obtient :
$$v_K(x_i) \geq \frac{-M}{p^{n-1-i}} \text{ and } v_K(y_i) \geq \frac{-M}{p^{n-1-i}},$$
d'où :
$$v_K((x+y)_i) \geq \sum_{k=0}^{i}(v_k + w_k)\frac{-M}{p^{n-1-k}} = \frac{-M}{p^{n-1}}p^i.$$
Alors, pour tout $i \geq 0$, il vient :
$$-p^{n-1-i}v_K((x+y)_i) \leq M.$$
En prenant le maximum on a donc :
$$M_n(x+y) \leq M,$$
ce qu'il fallait démontrer.
4. Ecrivons $cx = \sum_{i=0}^{n-1} V^i(\{c_i\})x$. Il s'agit de montrer la formule $M_n((V^i\{c_i\})x) \leq M_n(x)$ pour tout i. Or, d'après la proposition 1.16 du chapitre 1, on a $V^i\{c_i\} = p^i\{a_i\}$, où chaque a_i est tel que $a_i^{p^i} = c_i$. Par la proposition 1.10 du même chapitre, $M_n(\{a_i\}x) = M_n(x)$, d'où $M_n(p^i\{a_i\}x) \leq M_n(x)$.
5. C'est une conséquence du point (4). Si c est une unité, alors $M_n(x) \geq M_n(cx) \geq M_n(c^2x) ... \geq M_n(x)$ et donc $M_n(cx) = M_n(x)$.

6. Supposons par exemple $M_n(x) > M_n(y)$. On a :

$$M_n(x) = M_n((x+y)-y) \leq \max\{M_n(x+y), M_n(y)\}$$

puisque $M_n(y) = M_n(-y)$. D'où $M_n(x) = M_n(x+y)$ par le point (3).

7. On a $M_n(\wp(a)) = M_n(Fa-a) \leq \max(M_n(Fa), M_n(a))$ et la propriété résulte alors de l'égalité $M_n(Fa) = pM_n(a)$.

◇

Remarque 22. *Si l'on pose $m_n = -M_n$, la fonction m_n satisait la relation :*

$$\forall x, y \in W_n(K),\ m_n(x+y) \leq \min\{m_n(x), m_n(y\}.$$

C'est la fonction que V. Shabat utilise à la place de M_n. Il montre en particulier que m_n se comporte comme la valuation v_K de K.

Ceci entraîne :

Proposition 4.29. *Soient x et h deux vecteurs de l'anneau $W_n(K)$. Si x est un vecteur réduit, alors soit $M_n(x) \leq 0$, soit $M_n(x) \leq M_n(x + \wp(h))$.*

Preuve : Supposons $M_n(x) > 0$ et soit $j \leq 0$ l'unique indice tel que $M_n(x) = -p^{n-1-j}v_K(x_j)$. Alors, d'après la construction récursive de $M_n(x)$ on obtient :

$$M_n(x) = p^{n-1-j}M_{j+1}(x_0, ..., x_j),$$

et $M_n(\wp(h)) = \max_{i \geq j+1}\{p^{n-1-j}M_{j+1}\wp(h_0, ..., h_j), -p^{n-1-i}v_K(\wp(h)_i)\}$.
Si $M_n(x) > M_n(x + \wp(h))$, d'après le point (6) de la proposition 4.28, on a $M_n(\wp(h)) = M_n(x)$. Or, $M_{j+1}(x_0, ..., x_j)$ n'est pas divisible par p, d'où $M_n(\wp(h)) = p^{n-1-j}M_{j+1}(\wp(h_0, ..., h_j))$, i.e. $M_{j+1}(x_0, ..., x_j) = M_{j+1}(\wp(h_0, ..., h_j))$, ce qui contredit le point (7). ◇

Remarque 23. *Tous ces énoncés sur les vecteurs de Witt réduits utilisent essentiellement le fait que κ soit parfait. Ils restent donc valides dans le cadre plus général où K est un corps local de corps résiduel parfait.*

4.4.4 Calcul du symbole de Schmid-Witt

Toujours dans l'idée de simplifier les calculs du symbole d'Artin-Schreier-Witt par la formule de Schmid-Witt, nous présentons dans ce sous-paragraphe une construction équivalente du symbole de Schmid-Witt correspondant à l'idée que la $(n-1)$-ième composante fantôme d'un vecteur de Witt contiendrait toute l'information de ce vecteur.

Une définiton équivalente pour le symbole de Schmid-Witt. Montrons d'abord le lemme suivant :

Lemme 4.5. *Soit $Y = (Y_0, Y_1, ...)$ un vecteur de $W(\mathbb{F}_q)$. Alors, pour tout entier $k \geq 1$, il existe $Z_k \in W(\mathbb{F}_q)$ tel que :*

$$Y^{p^k} = \{Y_0^{p^k}\} + p^{k+1}Z_k.$$

Preuve : D'après la proposition 1.9 du chapitre 1, on a la formule $Y = \sum_{i \geq 0} V^i\{Y_i\}$ où $\{Y_i\} = (Y_i, 0, ..., 0)$. D'autre part, comme $\mathbb{F}_q$ est parfait, il existe $W_i \in \mathbb{F}_q$ tel que $Y_i = W_i^{p^i}$ pour tout i, i.e. $\{Y_i\} = F^i\{W_i\}$. Alors, puisque $VF = FV = p$, on a :

$$Y = \{Y_0\} + p\sum_{i \geq 1} p^{i-1}\{W_i\}.$$

Or, par récurrence sur k, si a et b sont dans un anneau commutatif A, il est facile de montrer la relation $(a+pb)^{p^k} = a^{p^k} + p^{k+1}c$ pour un certain élément $c \in A$. D'où $Y^{p^k} = \{Y_0\}^{p^k} + p^{k+1}Z$. On conclut avec la proposition 1.10 du chapitre 1 selon laquelle $\{Y_0\}^{p^k} = \{Y_0^{p^k}\}$. $\diamond$

Le lemme 4.5 entraîne l'identité suivante qui concerne le symbole de Schmid-Witt :

Proposition 4.30. *Soit $a \in W_n(K)$ et soit $b \in K^*$. Si A et B sont des relèvements de a et b respectivement pour le symbole de Schmid-Witt, on a la formule :*

$$Tr_{\mathbb{F}_q/\mathbb{F}_p}(a,b) = t_n(\,Tr_{\mathbb{F}_q/\mathbb{F}_p} Res(\frac{dB}{B}A^{(n-1)})),$$

où $t_n : W(\mathbb{F}_p) \twoheadrightarrow W_n(\mathbb{F}_p)$ est le morphisme de troncation.

Preuve : Notons $X = (X_i)_i$ avec $X_i \in W(\mathbb{F}_q)$ le vecteur de Witt (A, B) et notons $x = (x_i)_i$ le vecteur (a, b). Rappelons les relations $(X_i)_0 = x_i$ pour tous i. Il s'agit de montrer la formule :

$$\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p} x = t_n(\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p} X^{(n-1)}),$$

où $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p} = \sum_{i=0}^{d-1} F^i$ avec $q = p^d$.
Or, d'après le lemme 4.5, il existe des vecteurs $Z_i \in W_n(\mathbb{F}_q)$ tels que :

$$\begin{aligned}
\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p} X^{(n-1)} &= \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p} \sum_{i=0}^{n-1} p^i X_i^{p^{n-1-i}} \\
&= \sum_{i=0}^{n-1} p^i \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(X_i^{p^{n-1-i}}) \\
&= \sum_{i=0}^{n-1} p^i \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\{(X_i)_0^{p^{n-1-i}}\} + p^{n-i} Z_i)
\end{aligned}$$

Puisque F est l'application identité sur $W_n(\mathbb{F}_p)$, on a $p^i = V^i$ sur $W_n(\mathbb{F}_p)$. D'où, par linéarité de la trace :

$$\begin{aligned}
\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p} X^{(n-1)} &= \sum_{i=0}^{n-1} V^i \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\{(X_i)_0^{p^{n-1-i}}\}) + V^n \sum_{i=0}^{n-1} \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(Z_i) \\
&= \sum_{i=0}^{n-1} V^i \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\{(X_i)_0^{p^{n-1-i}}\}) \mod V^n W(\mathbb{F}_q).
\end{aligned}$$

Alors, par la relation $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\{w^{p^k}\}) = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\{w\})$ pour tout $w \in \mathbb{F}_q$ et pour tout entier $k \geq 1$ et puisque la trace commute avec l'opérateur V, on en déduit :

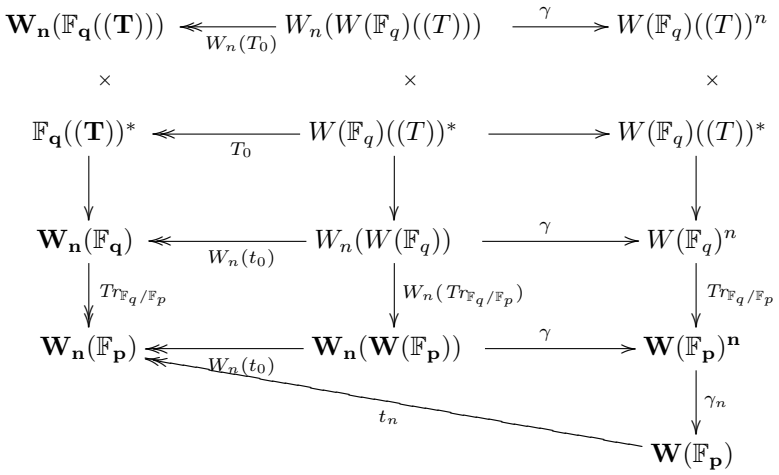
$$\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p} X^{(n-1)} = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p} \sum_{i=0}^{n-1} V^i \{(X_i)_0\} \mod V^n W(\mathbb{F}_q),$$

ce qui signifie que $t_n(\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p} X^{(n-1)}) = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p} x$, ce qu'il fallait démontrer. $\diamond$

Remarque 24. *Ainsi, nous obtenons sur le corps K une formule analogue à la proposition Satz 18 de [76] qui concerne les vecteurs de Witt de longueur n sur un corps p-adique.*

Remarque 25. *Le diagramme suivant est commutatif et complète celui du symbole de Schmid-Witt*

donné dans le sous-paragraphe 4.4.2 :



où l'application γ_n envoie la séquence des composantes fantômes sur la $(n-1)$-ième composante fantôme.

Calculs. Généralisant le lemme 4.3 et grâce aux deux simplifications précédentes, nous obtenons finalement le calcul suivant :

Proposition 4.31. *Soient $0 \leq m \leq u$ deux entiers positifs.*
Soit $a \in W_n^{(m)}(K) \backslash W_n^{(m-1)}(K)$ un vecteur de Witt réduit. On écrit $a = (a_0, ..., a_{n-1})$ avec $a_i = \sum_{v \geq v_i} a_{i,v} T^v$ et $a_{i,v_i} \in \kappa^*$ pour tout $i \geq 0$.
Soit $b \in K^*$ dont l'image modulo K^{*p^n} est dans $U_K^{(u)} K^{*p^n}/K^{*p^n}$ mais pas dans $U_K^{(u-1)} K^{*p^n}/K^{*p^n}$. On écrit $b = 1 + b_u T^u + h.o.t.$ avec $b_u \in \kappa^*$.
Alors :

$$Tr_{\mathbb{F}_q/\mathbb{F}_p}(a,b) = \begin{cases} (0, ..., 0, Tr_{\mathbb{F}_q/\mathbb{F}_p}((-v_j) b_u a_{j,v_j}^{p^{n-1-j}})) & si\ u = m \\ 0 & si\ u > m \end{cases}$$

où j est l'unique indice tel que $M_n(a) = -p^{n-1-j} v_j = m$, avec $v_j = v_K(a_j)$.

Preuve : Soient $A \in W_n(W(\mathbb{F}_p)((T)))$ et $B \in W(\mathbb{F}_p)((T))^*$ deux relèvements pour le symbole de Schmid-Witt de a et b respectivement. En particulier, ils sont de la forme :

$$A = (A_0, ..., A_{n-1}) \text{ t.q. } \forall i,\ A_i = \sum_{i \geq v_i} A_{i,v} T^v \in W(\mathbb{F}_q)((T)) \text{ et } (A_{i,v})_0 = a_{i,v},$$

et :

$$B = 1 + B_u T^u + h.o.t. \text{ t.q. } B_u \in W(\mathbb{F}_q) \text{ et } (B_u)_0 = b_u.$$

Alors, d'après la proposition 4.30, on a :

$$\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(a,b) = t_n(\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mathrm{Res}(\frac{dB}{B} A^{(n-1)})).$$

Soit v la valuation usuelle sur $W(\mathbb{F}_q)((T))$. Puisque $W(\mathbb{F}_q)((T))$ est de caractéristique 0, la $(n-1)$-ième composante fantôme de A est $A^{(n-1)} = \sum_{i \geq v_{n-1}} p^i A_i^{p^{n-1-i}}$. Comme a est réduit, il vient :

$$v(A^{(n-1)}) = \min_i \{p^{n-1-i} v_i\} = p^{n-1-j} v_j = -M_n(a) = -m$$

où $v_i = v_K(a_i) = v(A_i)$.

Par un calcul analogue à celui du lemme 4.3, on obtient alors :

$$\frac{dB}{B}A^{(n-1)} = uB_u p^j A_{j,v_j}^{p^{n-1-j}} T^{u-m-1} + h.o.t..$$

Donc, si $u > m$, $\mathrm{Res}(\frac{dB}{B}A^{(n-1)}) = 0$ d'où $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(a,b) = 0$.
Mais si $u = m$, i.e. $u = -p^{n-1-j}v_j$, on a alors :

$$\mathrm{Res}(\frac{dB}{B}A^{(n-1)}) = (-v_j)p^{n-1}B_u A_{j,v_j}^{p^{n-1-j}},$$

avec v_j premier à p. D'où, en prenant la trace de $\mathbb{F}_q$ sur $\mathbb{F}_p$:

$$\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mathrm{Res}(\frac{dB}{B}A^{(n-1)})) = p^{n-1}\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}((-v_j)B_u A_{j,v_j}^{p^{n-1-j}})$$

par linéarité. Or $p^{n-1} = V^{n-1}$ sur $W_n(\mathbb{F}_p)$, on en déduit :

$$\begin{aligned}\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mathrm{Res}(\tfrac{dB}{B}A^{(n-1)})) &= V^{n-1}(\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}((-v_j)B_u A_{j,v_j}^{p^{n-1-j}})) \\ &= V^{n-1}(\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}((-v_j)b_u a_{j,v_j}^{p^{n-1-j}}), *, *...),\end{aligned}$$

car $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(x_0, x_1, ...) = (\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(x_0), ...)$ et $(x_0, x_1, ...)^{p^k} = (x_0^{p^k}, ...)$.
Alors :

$$\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(a,b) = (0, ..., 0, \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}((-v_j)b_u a_{j,v_j}^{p^{n-1-j}}),$$

ce qui montre la proposition. ◇

4.4.5 Groupes de ramification de G_{p^n}

Le calcul du symbole d'Artin-Schreier-Witt pour les vecteurs de longueur n nous permet finalement grâce à la formule de Schmid-Witt d'expliciter une correspondnace bi-univoque entre la filtration des groupes de ramification du groupe G_{p^n} de l'extension abélienne maximale d'exposant p^n sur K et la filtration des $H_{p^n}^{(v)}$ du groupe $H_{p^n} = \mathrm{Hom}(W_n(K)/\wp(W_n(K), W_n(\mathbb{F}_p))$ donnée par :

$$\forall u \geq -1,\ H_{p^n}^{(v)} := \{\varphi \in H_{p^n}\ :\ \varphi(W_n^{(v)}(K) + \wp(W_n(K))/\wp(W_n(K))) = 0\}.$$

En particulier, $H_{p^n}^{(-1)} = H_{p^n}$ et :

$$H_{p^n}^{(0)} = \{\varphi \in H_{p^n},\ \varphi(W_n(O_K)/\wp(W_n(O_K)) = 0)\}.$$

Sauts de la filtration $\{H_{p^n}^{(u)}\}_u$. On dit qu'un entier $t \geq -1$ est un saut pour la filtration des $H_{p^n}^{(v)}$ si :

$$H_{p^n}^{(t)} \neq H_{p^n}^{(t-1)}.$$

Notons encore l'existence d'un décalage d'une unité entre la définition d'un saut pour la filtration des $H_{p^n}^{(v)}$ et celle pour les groupes de ramification de G_{p^n}.
Le résultat suivant généralise le proposition 4.19 :

Proposition 4.32. *Soit $u \geq 1$. Si p^n divise u, alors :*

$$W_n^{(u)}(K) = W_n^{(u-1)}(K) \mod \wp(W_n(K)).$$

En conséquence, aucun saut strictement positif dans la filtration des $H_{p^n}^{(v)}$ n'est divisible par p^n.

Preuve : Ecrivons $u = lp^n$ avec $l \geq 1$. Pour simplifier, notons également $A^{(u)} := (W_n^{(u)} + \wp(W_n(K)))/\wp(W_n(K))$.
Supposons qu'il existe $x \in W_n(K)$ tel que son image $\bar{x}$ modulo $\wp(W_n(K))$ soit dans $A^{(u)}\backslash A^{(u-1)}$. Par la proposition 4.27, il existe un vecteur réduit $y \in W_n(K)$ tel que $\bar{x} = \bar{y}$, en particulier $\bar{y} \in A^{(u)}\backslash A^{(u-1)}$.

Le vecteur y est donc dans $W_n^{(u-1)}(K)$, ce qui signifie qu'il existe i, $0 \leq i \leq n-1$, tel que $y_i \notin \mathfrak{p}_K^{-\lfloor \frac{u-1}{p^{n-1-i}} \rfloor}$, i.e. :

$$v_K(y_i) < -lp^{i+1} + 1.$$

En particulier, $v_K(y_i) < 0$ et donc p ne divise pas $v_K(y_i)$ puisque y est réduit. D'où :

$$v_K(y_i) < -lp^{i+1} = \frac{u}{p^{n-1-i}}.$$

Ainsi y n'appartient pas à $W_n^{(u)}(K)$. Or, puisque $\bar{y} \in A^{(u)}$, il existe $z \in W_n^{(u)}(K)$ et $h \in W_n(K)$ tels que $y = z + \wp(h)$, i.e. $z = y + \wp(-h)$. Par la proposition 4.28, on a donc $M_n(y) \geq u+1$ et $M_n(z) \leq u$. Mais d'après la proposition 4.29, on a aussi $M_n(z) \geq M_n(y)$, contradiction. ◇

Au passage, on a montré le résultat suivant qu'il est important de citer :

Corollaire 4.4. *Soit $u \geq 1$. Si y est un vecteur réduit tel que son image modulo $\wp(W_n(K))$ est dans*

$$(W_n^{(u)} + \wp(W_n(K)))/\wp(W_n(K))\backslash(W_n^{(u-1)} + \wp(W_n(K)))/\wp(W_n(K)),$$

alors y appartient à $W_n^{(u)}(K)\backslash W_n^{(u-1)}(K)$.

Preuve : Ce corollaire a été démontré dans la proposition 4.32. ◇

Sauts dans la filtration $\{U_K^{(u)}K^{*p^n}/K^{*p^n}\}_u$. En généralisation de la proposition 4.18, on a :

Proposition 4.33. *Aucun saut n'est divisible par p^n dans la filtration $\{U_K^{(u)}K^{*p^n}/K^{*p^n}\}_u$ de $U_K K^{*p^n}/K^{*p^n}$.*
En particulier, par le théorème d'existence, aucun saut n'est divisible par p^n dans la filtration des groupes de ramification de G_{p^n}.

Preuve : Puisque $\kappa = \mathbb{F}_q$ est parfait, on a $\kappa \subset \kappa^{p^n}$. Cette proposition est donc une généralisation directe de la proposition 4.18. ◇

Orthogonalité pour le symbole d'Artin-Schreier-Witt. Dans la lignée des notations du sous-paragraphe 4.3.3 nous posons :

$$\forall u \geq 0,\ \mathcal{S}_{p^n}^{(u)} := \{b.K^{*p^n} \in K^*/K^{*p^n}\ :\ [a,b) = 0,\ \forall a \in W_n^{(u)}\}.$$

Ainsi défini, chaque groupe $\mathcal{S}_{p^n}^{(u)}$ est l'orthogonal du groupe $W_n^{(u)}(K)$ modulo $\wp(W_n(K))$ in K^*/K^{*p} pour le symbole d'Artin-Schreier-Witt. En particulier, pour $u = 0$, $\mathcal{S}_{p^n}^{(0)}$ est l'orthogonal du groupe $(W_n(O_K)/\wp(W_n(O_K)))$.
Tout comme les $\mathcal{S}_p^{(u)}$ dans K^*/K^{*p}, les groupes $\mathcal{S}_{p^n}^{(u)}$ forment clairement une filtration décroissante de K^*/K^{*p^n}.

Le lemme 4.31 entraîne le résultat clef suivant :

Proposition 4.34. *Pour tout entier $u \geq 1$, on a l'égalité :*

$$\mathcal{S}_{p^n}^{(u-1)} = (U_K^{(u)}K^{*p^n})/K^{*p^n}.$$

Preuve : D'après la proposition 4.31 et le corollaire 4.4, il est facile de montrer l'inclusion $(U_K^{(u)}K^{*p^n})/K^{*p^n} \subset \mathcal{S}_{p^n}^{(u-1)}$, lorsque u n'est pas divisible par p^n.
Réciproquement, généralisant la preuve de la proposition 4.20, si $b \in K^*$ est tel que $\bar{b}$ n'appartient pas à $(U_K^{(u)}K^{*p^n})/K^{*p^n}$, montrons que $\bar{b}$ n'est pas dans $\mathcal{S}_{p^n}^{(u-1)}$ non plus.

Soit donc $j \leq u-1$ le plus petit entier tel que $\bar{b} \in U_K^{(j)}K^{*p^n})/K^{*p^n}$. En particulier, j n'est pas divisible par p^n d'après la proposition 4.33, d'où $j = p^k v$ avec $0 \leq k \leq n-1$ et $v \geq 1$ premier à p. D'autre part, on peut écrire : $b = 1 + b_j T^j + h.o.t.$ avec $b_j \in \mathbb{F}_q^*$. Alors, puisque l'application trace n'est pas nulle, il existe $\gamma \in \mathbb{F}_q^*$ tel que $\mathrm{tr}_{\mathbb{F}_q/\mathbb{F}_p}(\gamma v b_j) \neq 0$. Or $\gamma = \alpha^{p^{n-1-j}}$ avec $\alpha \in \mathbb{F}_q^*$. Considérons le vecteur $a = (a_i)_i$ donné par $a_j = \alpha T^{-v} + h.o.t$ et $a_i = 0$ pour tout $i \neq j$. Clairement, ce vecteur a est réduit et appartient à $W_n^{(v)}$ donc à $W_n^{(u-1)}$ puisque $v \leq j \leq u-1$. De plus, par le théorème 4.6 et la proposition 4.31, $[a, b) \neq 0$. Donc $\bar{b}$ n'appartient pas à $\mathcal{S}_{p^n}^{(u-1)}$.

D'où finalement l'égalité $\mathcal{S}_{p^n}^{(u-1)} = U_K^{(u)}K^{*p^n})/K^{*p^n}$ pour tout entier $u \geq 1$ non divisible par p^n.
On conclut pour tous les entiers $u \geq 1$ avec les propositions 4.32 et 4.33. ◇

Preuve du théorème 4.4. Pour $u \geq 1$, le théorème 4.4 est une conséquence directe de la proposition 4.34 et du théorème 4.5, de la même façon que nous avions montré la proposition 4.3 à partir de la proposition 4.20.

Pour $u = 0$, c'est essentiellement l'égalité $G_{p^n}^{(0)} = G_{p^n}^{(1)}$. Ceci termine la preuve du théorème 4.4.

4.4.6 Conséquences

Nous fermons ce chapitre avec deux corollaires du théorème 4.4.

Conducteur d'Artin pour une extension cyclique de degré p^n sur K. Une première conséquence du théorème 4.4 concerne le conducteur d'Artin des extensions cycliques de degré p^n sur le corps K :

Corollaire 4.5. *Soit a un vecteur de Witt de longueur n dans $W_n^{(u)}(K) \backslash W_n^{(u-1)}(K)$. Notons K_a l'extension cyclique de degré $p^k \leq p^n$ sur K définie par :*

$$K_a = K(\alpha_0, ..., \alpha_{n-1})$$

où $\alpha = (\alpha_0, ..., \alpha_{n-1}) \in W_n(K^{sep})$ est tel que $\wp(\alpha) = a$.
Alors, le conducteur d'Artin de l'extension K_a/K est $\mathfrak{p}_K^{u+1}$. En particulier, si $u = 0$, l'extension K_a/K est non ramifiée.

Comme l'extension K_a/K est cyclique, rappelons que d'après la proposition 5 de ([60], Chap.VI,§2), le conducteur d'Artin de K_a/K est précisément l'idéal $\mathfrak{p}_K^f$ où f est le plus petit indice pour lequel le groupe de ramification $\mathrm{Gal}(K_a/K)^{(f)}$ est trivial. Avec les hypothèses du corollaire 4.5, cet indice est donc u.

Preuve : Supposons $u \geq 1$. Puisque a est réduit, son image modulo $\wp(W_n(K))$ est dans $W_n^{(u)}$ mod $\wp(W_n(K))$ mais pas dans $W_n^{(u-1)}$ mod $\wp(W_n(K))$. Ainsi, d'après le théorème 4.4, K_a est fixé par $G_{p^n}^{(u+1)}$ mais pas par $G_{p^n}^{(u)}$. Puisque le groupe de Galois de K_a/K est quotient de G_{p^n}, on en déduit par le théorème de Herbrand (cf. proposition 3.4 du chapitre 3) que u est le plus petit indice pour lequel $\mathrm{Gal}(K_a/K)^{(u)}$ est trivial. ◇

Exemple 4.3. *Par exemple, si $a \in W_n(K)$ est le vecteur de Witt $(T^{-1}, 0, ..., 0)$ alors $M_n(a) = p^{n-1}$ et K_a/K est cyclique de degré p^n car $T^{-1} \notin \wp(K)$. Si G désigne le groupe de Galois de K_a/K on a donc :*

$$G^{(p^{n-1})} \neq 1 \ \ mais \ \ G^{(p^{n-1}+1)} = 1.$$

On retrouve ainsi le théorème 1 de [16] mais avec une preuve différente utilisant des arguments plus explicites sans les outils de Kato. En même temps on précise la proposition de la partie 3 [57] en détaillant chaque étape de la preuve et en particulier la formule de Schmid-Witt pour les vecteurs de Witt. Bien plus, nous donnons un résultat plus général qui correspond à la limite projective de ceux de Schmid et Brylinski dans le sens où nous avons obtenu directement les groupes de ramification pour toutes les extensions abéliennes maximales d'exposant p^n sur K.

Nous renvoyons également à [23] pour un calcul explicite de ce conducteur et nous remercions M. Matignon de nous avoir indiqué cette référence.

Groupes de ramification de G_{p^∞}. Notons H_{p^∞} le groupe $\mathrm{Hom}(W(K)/\wp(W(K)), W(\mathbb{F}_p))$. Le chapitre 2 donne un isomorphisme de groupes topologiques :

$$\mathfrak{as}_\infty : G_{p^\infty} \xrightarrow{\simeq} H_{p^\infty}$$

défini par $\sigma \mapsto \varphi_\sigma = \{a + \wp(W(K)) \mapsto \sigma(\alpha) - \alpha\}$ avec $\alpha \in W(K^{\mathrm{sep}})$ tel que $\wp(\alpha) = a$.

En prenant la limite projective sur tous les $G_{p^n}^{(u)}$ pour $n \geq 1$ et $u \geq -1$, on obtient finalement :

Corollaire 4.6. *Pour tout $n \geq 1$ et pour tout $u \geq -1$, posons :*

$$H_{p^\infty}^{(u,n)} := \{\varphi \in H_{p^\infty},\ \varphi((\mathfrak{p}_K^{-\lfloor \frac{u}{p^{n-1}} \rfloor}, ..., \mathfrak{p}_K^{-u}, *, ...) \ mod\ \wp(W(K)) \subset V^n W(\mathbb{F}_p)\}.$$

L'isomorphisme d'Artin-Schreier-Witt $\mathfrak{as}_\infty$ induit les isomorphismes de groupes topologiques :

$$G_{p^\infty}^{(0)} \xrightarrow{\simeq} \bigcap_{n\geq 1} H_{p^\infty}^{(0,n)} \ \ et\ \ G_{p^\infty}^{(u)} \xrightarrow{\simeq} \bigcap_{n\geq 1} H_{p^\infty}^{(u-1,n)}, \forall u \geq 1.$$

En particulier, pour $u = 0$, $G_{p^\infty}^{(0)}$ est isomorphe au groupe $\{\varphi \in H_{p^\infty} \ :\ \varphi(W(O_K)/\wp(O_K)) = 0\}$. Nous retrouvons ainsi le corollaire 3.5 du chapitre 3.

Troisième partie

Structure galoisienne

Chapitre 5

Anneaux d'entiers dans les extensions d'Artin-Schreier

5.1 Introduction

Soit K un corps local de caractéristique p et de corps résiduel parfait. Notons v_K sa valuation discrète, O_K son anneau de valuation et $\mathfrak{p}_K$ l'idéal maximal de O_K. Soit L/K une extension cyclique de degré p et soit G son groupe de Galois. Par la théorie d'Artin-Schreier, il existe $a \in K$ tel que cette extension soit donnée par l'équation :

$$X^p - X = a.$$

En particulier, $L = K(\alpha)$ avec $\alpha \in K^{\text{sep}}$ satisfaisant $\alpha^p - \alpha = a$.

L'objet du présent chapitre est l'étude de la structure de module galoisien de l'anneau O_L des entiers de L. D'après ([60], Chap.II, §2, prop. 3), O_L est un O_K-module libre de rang fini. D'autre part, l'action naturelle de G sur L induit une action sur O_L qui munit O_L d'une structure de module finiment engendré sur l'algèbre de groupe $O_K[G]$. Notre premier but est alors de déterminer les conditions pour que O_L soit libre sur $O_K[G]$.

Lorsque l'extension L/K est non ramifiée, nous avons le résultat suivant :

Proposition 5.1. *Si l'extension L/K est non ramifiée, l'anneau O_L est un $O_K[G]$-module libre de rang* 1.

Preuve : Soit π_K une uniformisante de K. Puisque l'extension L/K est non ramifiée, π_K est aussi une uniformisante de O_L. Alors $O_L/\pi_K O_L = l$ et l est une extension de κ de groupe canoniquement isomorphe à G. Par le théorème de la base normale (Bourbaki, *Alg.*, Chap.V, §10, no. 8), on en déduit que $O_L/\pi_K O_L$ est libre de rang 1 comme $\kappa[G]$-module :

$$\exists \beta \in O_L \ : \ O_L/\pi_K O_L = \kappa[G].\bar{\beta},$$

où $\bar{\beta}$ désigne la classe de β modulo $\pi_K O_L$.

Par le lemme de Nakayama, β engendre donc O_L comme $O_K[G]$-module. Pour conclure que O_L est un $O_K[G]$-module libre de rang 1 il reste à montrer que β est sans torsion sur $O_K[G]$, c'est-à-dire que les éléments β, $\sigma(\beta)$,..., $\sigma^{p-1}(\beta)$ sont linéairement indépendants sur O_K. Soit donc $\sum_i a_i\sigma^i(\beta) = 0$ une combinaison linéaire à coefficients dans O_K. Modulo π_K elle devient $\sum_i \bar{a}_i\sigma^i = 0$ dans $\kappa[G]$ puisque $\bar{\beta}$ est linéairement indépendant sur $\kappa[G]$. Alors tous les $\bar{a}_i$ sont nuls modulo π_K, i.e. tous les a_i sont divisibles par π_K dans O_K. En divisant par π_K et en itérant, s'il existe un coefficient a_i non nul on obtient par intégralité de l'anneau O_L une combinaison linéaire $\sum_i b_i\sigma^i(\beta) = 0$ dont un coefficient b_j est non nul et non divisible par π_K, mais ceci est impossible d'après ce qui précède. ◇

Néanmoins lorsque l'extension L/K est totalement ramifiée, l'anneau O_L n'est plus libre en tant que $O_K[G]$-module (cf. proposition 5.5 plus loin). Cette situation nous conduit alors à considérer dans $K[G]$ le sous-anneau suivant :

$$A = A(L/K) = \{\lambda \in K[G] \ : \ \lambda.O_L \subset O_L\},$$

pour l'action de $K[G]$ sur O_L induite par celle sur L. En d'autres termes, l'anneau A est l'ensemble des éléments de $K[G]$ qui induisent un endomorphisme sur O_L. C'est un O_K-ordre de $K[G]$ que l'on appelle couramment *ordre associé* à l'extension L/K mais *anneau multiplicateur* de O_L serait tout aussi approprié. De plus, l'anneau O_L a clairement une structure de A-module pour laquelle il est finiment engendré puisque $O_K[G] \subset A$.

En fait, l'anneau A est le seul O_K-ordre de $K[G]$ sur lequel O_L peut être éventuellement libre. C'est pourquoi nous nous placerons maintenant dans le cas totalement ramifié et considérerons exclusivement la question suivante : sous quelles conditions l'anneau O_L est-il un A-module libre ?

Voilà précisé l'objet du présent chapitre, notre but étant de donner une condition nécessaire et suffisante pour que l'anneau O_L des entiers de L soit libre sur l'ordre associé et lorsque c'est le cas de construire une base explicite. Aiba [3] a déjà proposé un tel critère. Il s'agira alors d'améliorer son résultat, d'une part en le rendant plus explicite et d'autre part en donnant un nouveau critère, purement algébrique, qui est relié à l'*embedding dimension* de l'anneau A. Nous manipulerons à la fois des arguments combinatoires et algébriques avec en filigrane une étude approfondie de l'ordre A associé à l'extension L/K.

Les notations utilisées seront les suivantes. Tout au long du chapitre, l'extension L/K sera supposée totalement ramifiée. D'après le chapitre 3, on peut poser $v_K(a) = -m$, où m est un entier strictement positif qui n'est pas divisible par p. On écrira donc :

$$m = pt + s,$$

avec t et s deux entiers positifs déterminés de façon unique par la condition $1 \leq s \leq p-1$.

Nous noterons également σ l'automorphisme du groupe G défini par : $\sigma(\alpha) = \alpha + 1$. C'est un générateur de G, une base du K-espace vectoriel $K[G]$ est alors $1, \sigma, ...\sigma^p$.

Maintenant, pour simplifier, nous considérerons davantage l'automorphisme $\sigma - 1$ car il satisfait $(\sigma - 1)(\alpha) = 1$. Clairement, les puissances de $\sigma - 1$ forment toujours une K-base de $K[G]$:

$$K[G] = K \oplus K.(\sigma - 1) \oplus \cdots \oplus K.(\sigma - 1)^{p-1}.$$

En particulier, on obtient un isomorphisme canonique par l'identification $\sigma \mapsto X + 1$:

$$K[G] \xrightarrow{\simeq} K[X]/X^p.$$

Si $\{x\}$ désigne la partie fractionnaire d'un réel x, i.e. $\{x\} = x - \lfloor x \rfloor$, où $\lfloor x \rfloor$ est l'unique entier tel que $\lfloor x \rfloor \leq x < \lfloor x \rfloor - 1$, Aiba [3] donne le critère suivant :

Théorème 5.1 (Aiba, 2003)**.** *Les propositions suivantes sont équivalentes :*

1. *O_L est un A-module libre.*
2. *Il n'existe pas d'entiers u et v avec $p - 1 > u > v > 1$ tels que :*

$$\left\{\frac{s}{p}\right\} > \left\{\frac{us}{p}\right\} > \left\{\frac{vs}{p}\right\}.$$

De plus, si l'anneau O_L est libre sur A, il est nécessairement de rang 1 et dans ce cas Aiba donne explicitement un générateur.

En fait, la condition (2) initiale de Aiba contenait une erreur que Lettl signale dans un papier à venir ([37]) et nous tenons à remercier B. Angles pour nous avoir communiqué cette référence. De plus, Lettl montre que cette condition est équivalente à :

3. s divise $p-1$

N.Byott aussi a noté cette équivalence dans le Mathematical Review on the Web de l'article de Aiba pré-cité. Avec d'autres arguments, nous retrouverons cette dernière condition à partir de l'étude qui suit. Soulignons également que Bertrandias et Ferton [12] ont donné le même critère pour la problème analogue en caractéristique 0.

Les arguments développés dans le papier de Aiba nous ont menés à introduire une suite $\{\epsilon_i\}_i$ de $\{0,1\}$ entièrement définie par p et par l'entier s, résidu dans la division euclidienne de $v_K(a)$ par p. L'étude de cette suite ré-explique la base de O_L sur O_K que Aiba considère. En outre, ses nombreuses propriétés combinatoires fournissent une O_K-base plus naturelle pour l'ordre A, conduisant ainsi à notre version suivante du théorème de Aiba :

Théorème 5.2. *Soit K un corps de caractéristique p, complet pour une valuation discrète et de corps résiduel parfait. Soit L/K une extension totalement ramifiée de degré p : elle est donnée par un polynôme $X^p - X = a$ avec $a \in K$ de valuation $-m < 0$ qui n'est pas divisible par p. On écrit $m = pt + s$ pour $1 \leq s \leq p-1$. Les propositions suivantes sont équivalentes :*
(i) O_L est libre en tant que module sur l'ordre A associé à L/K.
(ii) la suite $(\epsilon_i)_{i=1}^{p-1}$ est de type $(10...0)^s$
(iii) s divise $p-1$
(iv) l'embedding dimension de A est inférieure ou égale à 3.

L'intérêt principal du théorème 5.2 est qu'il fournit une preuve du critère (iii) différente de celle de Aiba et Lettl, le rendant plus explicite. Mais surtout, il donne une nouvelle condition, purement algébrique elle, liée à ce que Matsumura appelle l'*embedding dimension* de A. Une propriété essentielle de l'ordre A est d'être un anneau local noethérien de corps résiduel canoniquement isomorphe au corps résiduel de K que nous noterons κ. Alors, si $\mathfrak{m}_A$ est l'idéal maximal de A, l'embedding dimension de A n'est autre que la dimension du κ-espace vectoriel $\mathfrak{m}_A/\mathfrak{m}_A^2$.

Afin de montrer le théorème 5.2, nous commençons ce chapitre avec l'étude de l'anneau O_L comme O_K-module. Ensuite, le paragraphe 5.3 enquête sur les propriétés algébriques qui concernent l'ordre A associé à L/K. Les paragraphes 5.4, 5.5 et 5.6 montrent les équivalences de la propriété (i) avec les critères (ii), (iii) et (iv) respectivement. En particulier, dans le paragraphe 5.4 nous introduirons la suite combinatoire $\{\epsilon_i\}_i$ qui fournit une O_K-base naturelle pour l'ordre A. Quant au paragraphe 5.6, il contient d'abord quelques rappels sur la dimension d'un anneau local noethérien avant d'expliquer l'embedding dimension de A et de la ré-écrire dans un langage purement combinatoire pour enfin montrer la condition (iv) directement à partir des conditions (ii) et (iii).

Signalons que ce chapitre fera très probablement l'objet d'un article, en cours de rédaction. En particulier, il s'agit de pousser l'étude encore plus loin en donnant une relation explicite entre l'embedding dimension de A et le nombre minimal de générateurs de O_L en tant que A-module. Egalement, il fournit un algorithme qui permet de calculer directement ce dernier paramètre, donnant ainsi une étude complète de la structure galoisienne de l'anneau O_L.

Il se posera alors naturellement la question des extensions L/K de degré p^n pour $n \geq 2$.

5.2 Structure de O_L comme O_K-module

Ce paragraphe propose une étude détaillée de la base sur O_K de l'anneau O_L que Aiba utilise dans [3]. Le lecteur pourra survoler rapidement le sous-paragraphe 5.2.1 qui concerne essentiellement la recherche d'une O_K-base formée par les puissances d'un élément de O_L, mais qui est sans intérêt pour la suite.

5.2.1 A la recherche d'un générateur

D'après la proposition 3 de ([60], Chap.II, §2) et la proposition 12 de ([60], Chap.III, §7) et puisque K est un corps local, l'anneau O_L des entiers de L est un O_K-module libre de rang

$p = [L : K]$. Il existe $x \in O_L$ tel que $\{1, x, ..., x^{p-1}\}$ forme une O_K-base pour O_L. En d'autres termes, O_L est la O_K-algèbre $O_K[x]$. On peut alors s'intéresser à la recherche d'un tel élément x.

Rappelons que l'extension L est de la forme $L = K(\alpha)$, avec $\alpha^p - \alpha = a$ pour un élément $a \in K$. Si $v_K(a) > 0$, c'est-à-dire si $a \in \wp(K)$, on sait (cf. Chap 3, prop. 3.1) que L/Kest triviale, d'où $O_L = O_K$.
Si $v_K(a) = 0$ et $a \notin \wp(K)$, l'extension L/K est non ramifiée. Modulo $\mathfrak{p}_K$, le polynôme $X^p - X - a$ devient $\bar{X}^p - \bar{X} - \bar{a}$ dans l'extension résiduelle l/κ de degré p . Par le lemme de Hensel et la théorie d'Artin-Schreier, $\bar{a}$ n'appartient pas à $\wp(\kappa)$, le polynome $\bar{X}^p - \bar{X} - \bar{a}$ est donc irréductible sur κ et $l = \kappa[\bar{\alpha}]$ puisque $\bar{\alpha}$ est clairement une racine de ce polynome. Alors, d'après la proposition 16 de ([60], Chap.I, §6), on a : $O_L = O_K[\alpha]$.

Selon le théorème 3.2 du chapitre 3, le seul cas qui reste à traiter est lorsque $v_K(a) < 0$ et $p \not| v_K(a)$, i.e. lorsque l'extension L/K est totalement ramifiée. La proposition 18 de ([60], Chap.I, §6) affirme alors que $O_L = O_K[\pi_L]$, si π_L est une uniformisante de O_L qu'il s'agit donc de déterminer. Par le théorème de Bezout, il existe u et v tels que $up + vv_K(a) = 1$, l'élément $\pi_K^u \alpha^v$ est donc de valuation 1 sur L, c'est ce que nous recherchions.

Ainsi, une O_K-base pour O_L est formée des puissances de $\pi_K^u \alpha^v$. Cependant cette base n'est pas canonique puisque chaque sous-O_K-module engendré par les i premiers termes dépendent du choix de cette uniformisante. De plus, ce module n'est pas en général un module sur $O_K[G]$, ce qui complique l'étude de la structure galoisienne de O_L.

5.2.2 La base de Aiba

Dans notre contexte, il est plus naturel de considérer sur O_L la O_K-base que Aiba introduit dans [3]. Nous allons voir que cette base a l'avantage de prendre en compte l'action galoisienne puisque chaque O_K-module engendré par ses i premiers termes consécutifs est un sous-$O_K[G]$-module de O_L. De plus, ces modules sont canoniques : ils correspondent aux sous O_K-modules maximaux qui sont annulés par les puissances i-ièmes du nilradical de $O_K[G]$. Décrivons d'abord cette base et justifions ses propriétés.

Dans toute la suite, nous noterons T une uniformisante de K au lieu de π_K. Le théorème 2 de ([60], Chap.II, §4) nous permet d'identifier K avec le corps des séries formelles $\kappa((T))$.

La base de Aiba pour le O_K-module O_L est la famille :

$$\{1, \alpha T^{x_1}, \cdots, \alpha^{p-1} T^{x_{p-1}}\},$$

où pour chaque indice $i \in [1; p-1]$ l'exposant x_i est défini par la condition :

$$v_L(\alpha^i T^{x_i}) \in \{0, ..., p-1\}.$$

De façon équivalente, chaque x_i est le plus petit entier positif tel que $x_i p > mi$ pour $m = -v_K(a) = -v_L(\alpha)$. En écrivant $m = tp + s$ avec $0 \leq s \leq p-1$, cela signifie : :

$$\forall i \geq 0,\ x_i = it - \lfloor -\frac{si}{p} \rfloor$$

où l'on a posé $x_0 := 0$. Les valuations des éléments $\alpha^i T^{x_i}$, $i = 0...p-1$, sont donc distinctes deux à deux et parcourent l'ensemble $\{0, ..., p-1\}$. Cela montre que la famille $\{\alpha^i T^{x_i}\}_{i=0...p-1}$ forme bien une O_K-base pour O_L selon le résultat général suivant :

Proposition 5.2. *Soit L/K une extension galoisienne finie de corps locaux et soit l/κ son extension résiduelle. Notons $f = [l : \kappa]$ le degré d'inertie de L/K et e son indice de ramification. Soient $\xi_1, ..., \xi_f$ des représentants dans O_L d'une base de l/κ et soient e éléments $\omega_0, ..., \omega_{e-1}$ de O_L dont les valuations sont disctinctes deux à deux dans $\{0, ..., e-1\}$.*

Alors, les produits $\omega_j \xi_i$, pour $i = 1...f$ et $j = 0...e-1$, sont linéairement indépendants sur K et forment une base de O_L sur O_K.

Preuve : Le lecteur se reportera à la preuve de la proprosition 6.8 de ([48], Chap. II), ou encore à celle du lemme 1.4 dans ([31], Chap.I). ◇

Observons maintenant que la suite des x_i est croissante. On a en effet pour tout i :

$$t + \frac{1}{p} - 1 \leq x_{i+1} - x_i \leq t + \frac{1}{p} + 1,$$

d'où :

$$0 \leq t \leq x_{i+1} - x_i \leq t + 1.$$

puisque les x_i sont entiers. Cela entraîne la proposition suivante :

Proposition 5.3. *Pour tout entier i, $0 \leq i \leq p-1$, le sous O_K-module de O_L engendré par $1, \cdots, \alpha^i T^{x_i}$ a la structure d'un $O_K[G]$-module.*
Nous noterons $\mathfrak{I}_i$ ce sous-module :

$$\forall i, 0 \leq i \leq p-1, \mathfrak{I}_i = O_K \oplus O_K.\alpha T^{x_1} \oplus ... \oplus O_K.\alpha^i T^{x_i}.$$

Preuve : Il s'agit de montrer chaque $\mathfrak{I}_i$ est globalement invariant sous l'action de G. Cela est clair pour $i = 0$ puisque $\mathfrak{I}_0 = O_K$. Pour i dans $\{1, ..., p-1\}$, on a :

$$\begin{aligned} \forall j \leq i, \sigma.(\alpha^j T^{x_j}) &= T^{x_j} \sigma(\alpha)^j \\ &= T^{x_j} (\alpha + 1)^j \\ &= \textstyle\sum_{k=0}^{j} \binom{j}{k} T^{x_j - x_k} T^{x_k} \alpha^k. \end{aligned}$$

Or, pour tout $j \leq i$, $\sigma.(\alpha^j T^{x_j})$ appartient à $\mathfrak{I}_i$ puisque tous les $T^{x_j - x_k}$ sont dans O_K, d'où la proposition. ◇

En fait, la base de Aiba jouit d'une propriété plus forte : pour tout i, ses i premiers termes consécutifs engendrent sur O_L le noyau de l'endomorphisme $(\sigma - 1)^{i-1}$. C'est pour cela que nous disons que la base de Aiba est canonique. Or, par l'identification $K[G] \simeq K[X]/X^p$ avec $\sigma \mapsto X + 1$, il est facile de montrer que $XK[G]$ est le nilradical de $K[G]$ et donc que $XO_K[G]$ celui de $O_K[G]$. Ainsi, le noyau de $(\sigma - 1)^{i-1}$ sur O_L est précisément le sous-module maximal contenant la puissance i-ième de $XO_K[G]$. Si $\ker(\sigma - 1)^i$ est le noyau de $(\sigma - 1)^i$ dans O_L pour tout i, on a plus précisément :

Proposition 5.4. *Avec les notations de la proposition 5.3, pour tout indice i, $0 \leq i \leq p$, on a :*

$$\ker(\sigma - 1)^i = \mathfrak{I}_{i-1},$$

où $\mathfrak{I}_{-1} = 0$ et $\mathfrak{I}_p = O_L$.
En particulier, les sous-modules $\mathfrak{I}_i$, $-1 \leq i \leq p$, forment une filtration croissante de O_L.

Preuve : On raisonne par récurrence sur i. Les cas $i = 0$ et $i = p$ sont évidents. Soit donc $i \in \{0, ..., p-1\}$ et supposons que $\ker(\sigma - 1)^i = \mathfrak{I}_{i-1}$. On a une suite exacte :

$$0 \to \ker(\sigma - 1)^i \hookrightarrow \ker(\sigma - 1)^{i+1} \overset{(\sigma-1)^i}{\to} O_K.$$

En particulier, le quotient $\ker(\sigma - 1)^{i+1} / \ker(\sigma - 1)^i$ n'a pas de torsion sur O_K puisque O_K est sans torsion en tant que module sur lui-même.
Or, l'anneau O_K est principal et $\ker(\sigma - 1)^{i+1} / \ker(\sigma - 1)^i$ est de type fini puisque $\ker(\sigma - 1)^{i+1}$ l'est. Alors, d'après ([35], Chap.III, §7), $\ker(\sigma - 1)^{i+1} / \ker(\sigma - 1)^i$ est libre sur O_K. L'idée est donc de compléter une O_K-base de $\ker(\sigma - 1)^i = \mathfrak{I}_{i-1}$ en une O_K-base de $\ker(\sigma - 1)^{i+1}$ à partir d'éléments de $\ker(\sigma - 1)^{i+1} - \ker(\sigma - 1)^i$.

Pour tout $j \geq 0$, soit K_j le noyau de $(\sigma-1)^j$ dans le corps L considéré comme K-espace vectoriel, de sorte que $\ker(\sigma-1)^j = K_j \cap O_L$. Il est bien connu que la suite :

$$0 \subset K = K_1 \subset \cdots \subset K_j \subset K_{j+1} \subset \cdots \subset K_p = L$$

est strictement croissante et que $\dim_K K_j = j$ pour tout j, $0 \leq j \leq p$, puisque $\sigma - 1$ est un endomorphisme de L d'indice de nilpotence p. Alors par itération sur l'indice j et comme $L = K[\alpha]$, on montre facilement :

$$\forall j \in \{1, ..., p\},\ K_j = \bigoplus_{l=0}^{j-1} K.\alpha^l$$

car $(\sigma-1)^{j+1}.\alpha^j = (\sigma-1)^j(\sigma-1).\alpha^j = 0$ puisque $(\sigma-1).\alpha^j = ((\alpha+1)^j - \alpha^j)$ est dans $\bigoplus_{l\leq j-1} K.\alpha^l$. Retour à l'indice i. On a un O_K-morphisme injectif :

$$\ker(\sigma-1)^{i+1} / \ker(\sigma-1)^i \hookrightarrow K_{i+1}/K_i,$$

et donc $\ker(\sigma-1)^{i+1} / \ker(\sigma-1)^i$ est aussi un sous O_K-module de $K\alpha^i$. Or, $\ker(\sigma-1)^{i+1} \neq \ker(\sigma-1)^i$ comme α^i est dans $\ker(\sigma-1)^{i+1}$ mais pas dans $\ker(\sigma-1)^i$.

Ainsi, $\ker(\sigma-1)^{i+1} / \ker(\sigma-1)^i$est un O_K-module de rang 1 dont un générateur est $\alpha^i T^{x_i}$. Par récurrence, $\ker(\sigma-1)^{i+1}$ est un sous O_K-module de O_L engendré par 1, αT^{x_1},..., $\alpha^{i-1}T^{x_{i-1}}$ et $\alpha^i T^{x_i}$, ce qu'il fallait démontrer. ◇

5.3 L'ordre associé à L/K

5.3.1 Motivation

D'après la proposition 5.1, O_L est un $O_K[G]$-module libre dès que l'extension L/K est non ramifiée. Ce n'est plus le cas quand l'extension est totalement ramifiée :

Proposition 5.5. *Si L/K est totalement ramifiée, son anneau de valuation O_L n'est pas libre sur $O_K[G]$ en tant que module.*

Preuve : Supposons par l'absurde que O_L est libre sur $O_K[G]$. Alors il est de rang 1 par transitivité du rang et parce que $\text{rank}_{O_K} O_K[G] = \text{card}\ G = \text{rank}_{O_K} O_L$. En particulier, on obtient un isomorphisme de $O_K[G]$-modules entre O_L et $O_K[G]$. L'idée est de montrer que cela conduit à une contradiction en appliquant l'élément :

$$N_G := \sum_{\tau \in G} \tau = \sum_{i=0}^{p-1} \sigma^i$$

de $\mathbb{Z}[G]$ appelé *norme* selon les notations de ([60], Chap. $VIII$, §1)).

Pour tout G-module M, l'application N_G induit un endomorphisme $N_G : M \to M$ défini par $N_G.m = \sum_i \sigma^i.m$ dont l'image appartient à M^G. Cela s'applique en particulier à O_L et $O_K[G]$. Montrons alors que $N_G : O_L \to (O_L)^G$ n'est pas surjective alors que $N_G : O_K[G] \to (O_K[G])^G$ l'est.

Sur O_L, N_G est l'application trace usuelle à valeurs dans $(O_L)^G = O_K$. Elle induit un κ-homomorphisme sur les corps résiduels :

$$\begin{array}{rccc} \bar{N_G} : & O_L/\pi_L & \longrightarrow & O_K/\pi_K \\ & x + \pi_L & \mapsto & \text{Tr}(x) + \pi_K. \end{array}$$

Or, l'extension L/K est totalement ramifiée, donc $O_L/\pi_L = O_K/\pi_K = \kappa$ et $\bar{N}_G$ est précisément la multiplication par $[L:K]$ modulo π_K. Puisque p divise $[L:K]$, on en déduit que l'application $\bar{N}_G$ est nulle et que $N_G : O_L \to O_K$ n'est pas surjective.

A l'inverse, montrons que N_G induit un morphisme surjectif $O_K[G] \twoheadrightarrow (O_K[G])^G$. Soit $x = \sum_i a_i\sigma^i \in O_K[G]$. C'est un élément fixé par G si et seulement $\sigma.x = x$, i.e. si et seulement si

tous les a_i sont égaux. Cette condition signifie que x est de la forme $x = a\sum_i \sigma^i$ avec $a \in O_K$, c'est-à-dire $x = N_G.(a.1)$. Donc $(O_K[G])^G = N_G O_K[G]$ et $N_G : O_K[G] \to (O_K[G])^G$ est surjective, ce qu'il fallait démontrer. $\diamond$

Ceci nous conduit à l'étude de la structure de O_L comme module sur un anneau plus *grand* que $O_K[G]$.

5.3.2 Autour de la notion d'ordre

Ordres d'algèbres. Ce sous-paragraphe est un rappel sur les ordres dans les algèbres, le lecteur se reportera au chapitre II de [51] pour plus de détails.

Reiner [51] définit un O_K-ordre de la K-algèbre $K[G]$ comme un sous-anneau $\mathcal{O}$ de $K[G]$ tel que :

1. $\mathcal{O}$ est un sous O_K-module de $K[G]$ de type fini ;
2. on a l'égalité $K.\mathcal{O} = K[G]$, où :

$$K.\mathcal{O} = \{ \sum_{\text{finite sum}} x_i\lambda_i \, ; \, x_i \in K, \, \lambda_i \in \mathcal{O}\}.$$

La condition 2. signifie que $\mathcal{O}\otimes_{O_K} K = K[G]$, ou encore $\dim_K \mathcal{O}\otimes_{O_K} K = \text{card } G$. Un sous-module de $K[G]$ qui satisfait à la fois les propriétés 1.) et 2.) est réseau de $K[G]$ de rang maximal sur O_K.

Clairement, $O_K[G]$ est un O_K-ordre de $K[G]$. Il s'agit donc de trouver un O_K-ordre plus grand sur lequel O_L pourrait éventuellement être libre en tant que module. Il n'y a en fait qu'un O_K-ordre possible dans $K[G]$ (cf. proposition 5.8).

L'ordre associé à L/K. Considérons dans $K[G]$ le sous-anneau A défini par :

$$A = A(L/K) = \{\lambda \in K[G] \ : \ \lambda.O_L \subset O_L\}.$$

De façon évidente, cet anneau contient $O_K[G]$.

Proposition 5.6. *L'anneau A est un O_K-module libre de rang fini et un O_K-ordre de la K-algèbre $K[G]$. On l'appelle ordre associé à l'extension L/K.*

Preuve : Le fait que A soit un sous-anneau et même un sous O_K-module de $K[G]$ est évident. De plus, A se plonge dans le groupe des O_K-endomorphismes de O_L qui est aussi l'O_K-module des matrices $p \times p$ à valeurs dans O_K puisque $p = \text{card } G$. C'est donc un sous-module d'un O_K-module libre de type fini. Puisque O_K est principal, on en déduit que A est aussi un O_K-module libre de type fini, d'où la condition 1.

Or, l'anneau $O_K[G]$ est clairement un O_K-ordre de $K[G]$, d'où l'égalité $K.O_K[G] = K[G]$. Puisque $O_K[G] \subset A \subset K[G]$ on a aussi $K.A = K[G]$, qui est la condition 2. $\diamond$

5.3.3 Structure de $A(L/K)$ comme O_K-module

Afin de préciser la structure de l'anneau O_L comme module sur l'ordre associé à L/K, l'étude de cet ordre comme O_K-module s'impose d'abord.

Proposition 5.7. *L'ordre A associé à L/K est un O_K-module libre de rang $p = \text{card } G$, où G est le groupe de Galois de l'extension.*

Preuve : D'après la proposition 5.6, A est un O_K-module libre de rang fini. Puisque le K-espace vectoriel $K[G]$ est de dimension card G et à cause de la relation $K \otimes_{O_K} A = K[G]$ on en déduit $\text{rank}_{O_K} A = \text{card } G$ (cf. [35], Chap. XVI, §4). $\diamond$

Corollaire 5.1. *Si O_L est un module libre sur l'ordre associé A, alors il est nécessairement de rang 1.*

Preuve : Supposons que O_L est libre sur A. Puisque O_L est de type fini sur O_K, il l'est aussi sur A. De plus, en tant que A-module son rang satisfait :

$$\mathrm{rank}_A(O_L) = \frac{\mathrm{rank}_{O_K}(O_L)}{\mathrm{rank}_{O_K}(A)} = 1,$$

d'où le corollaire. ◇

Une autre conséquence est que l'ordre associé à l'extension L/K a la propriété d'être l'unique O_K-ordre de $K[G]$ sur lequel O_L est éventuellement libre comme module. C'est la proposition qui suit et qui justifie notre étude :

Proposition 5.8. *Soit L/K une extension de corps locaux. Si l'anneau O_L est un module libre sur un O_K-ordre $\mathcal{O}$ de $K[G]$, alors $\mathcal{O} = A$.*

Preuve : D'abord, puisque O_L est un $\mathcal{O}$-module, O_L est globalement invariant sous l'action de $\mathcal{O}$ induite par celle de $K[G]$. L'ordre $\mathcal{O}$ est donc inclus dans l'ordre associé A. De plus, par l'application $\mathcal{O}$-linéaire $\lambda \mapsto \{x \mapsto \lambda.x\}$, chaque élément de A est naturellement envoyé sur un $\mathcal{O}$-endomorphisme de O_L, ce qui justifie l'écriture :

$$\mathcal{O} \subset A \subset \ \mathrm{End}_{\mathcal{O}}(O_L),$$

en considérant A comme $\mathcal{O}$-module.
L'idée est alors de montrer l'égalité $\mathcal{O} = \ \mathrm{End}_{\mathcal{O}}(O_L)$. Par un argument analogue au corollaire 5.1, on montre que le module O_L est nécessairement de rang 1 sur $\mathcal{O}$ dès qu'il est libre sur $\mathcal{O}$, d'où l'existence d'une élément $b \in O_L$ tel que :

$$O_L = \mathcal{O}.b.$$

Soit donc ϕ un $\mathcal{O}$-endomorphisme de O_L. Il envoie b sur un élément du type $\beta.b$ avec $\beta \in \mathcal{O}$. Or, si $x \in O_L$, on peut écrire $x = \lambda_x.b$, avec $\lambda_x \in \mathcal{O}$. Il vient :

$$\phi(x) = \phi(\lambda_x.b) = \lambda_x \beta b = \beta.x,$$

par la linéarité de ϕ par rapport à $\mathcal{O}$ et parce que $\mathcal{O}$ est abélien.
Ainsi, le $\mathcal{O}$-endomorphisme ϕ agit sur O_L par multiplication par β, il est alors naturellement identifié avec β dans $\mathcal{O}$. On en déduit l'inclusion :

$$\mathrm{End}_{\mathcal{O}}(O_L) \subset \mathcal{O},$$

et donc l'égalité :

$$\mathcal{O} = A,$$

ce qu'il fallait démontrer. ◇

Remarque 26. *Lorsque l'extension L/K est non ramifiée, ceci confirme la proposition 5.1 qui affirme qu'alors O_L est un $O_K[G]$-module libre de rang 1. En effet, une conséquence est que l'ensemble des $O_K[G]$-endomorphismes de O_L est un $O_K[G]$-module libre de rang 1. Puisque A s'injecte dans ce module et comme il contient déjà $O_K[G]$, on a $A = O_K[G]$ nécessairement.*

5.3.4 Compléments sur les O_K-ordres de $K[G]$

Nous développons ici des remarques supplémentaires sur les O_K-ordres de $K[G]$ pour des extensions arbitraires L/K de corps locaux et de degré p. Elles font suite au théorème 8.6 de ([51], Chap.II, §8) selon lequel tout élément d'un O_K-ordre est intégral sur O_K. Nous renvoyons également au bel article [42] pour d'autres compléments sur les ordres associés.

Dans toute la suite nous noterons O_K^{cl} la clôture inétgrale de O_K dans $K[G]$. Les résultats qui suivent ne dépendent pas de la ramification dans l'extension L/K.

Lemme 5.1. *Par l'identification $X = \sigma - 1$, la clôture intégrale de O_K dans $K[G]$ est :*

$$O_K^{cl} = O_K + XK[G].$$

Preuve : L'inclusion $O_K + XK[G] \subset O_K^{\mathrm{cl}}$ est claire. Pour montrer l'autre inlcusion, considérons un élement $\lambda \in K[G]$ entier sur O_K. De l'isomorphisme naturel $K[G] \simeq K[X]/X^p$, on peut écrire :

$$\lambda = a_0 + a_1 X + ... + a_{p-1} X^{p-1},$$

où tous les a_i sont dans K. Il s'agit alors de montrer que a_0 est en fait dans O_K. Or, λ est intégral sur O_K, i.e. il existe un polynôme unitaire P à coefficients dans O_K tel que $P(\lambda) = 0$ dans $K[G]$. En particulier, cela implique $P(a_0) = 0 \mod X$ dans $K[G]$ et donc $P(a_0) \in K \cap XK[G]$. Mais considérant $K[G]$ comme la somme directe $K \oplus K.X \oplus \cdots \oplus K.X^{p-1}$ avec $X = \sigma - 1$ et puisque $X^p = 0$, on a $K \cap XK[G] = 0$. Donc $P(a_0) = 0$ et a_0 est entier sur O_K. D'où $a_0 \in O_K$ puisque O_K est intégralement clos dans K, ce qui montre le lemme. ◇

Nous appellerons O_K-ordre maximal dans l'algèbre $K[G]$, un O_K-ordre qui n'est pas strictement inclus dans aucun autre O_K-ordre de $K[G]$.

Proposition 5.9. *Il n'existe pas de O_K-ordre maximal dans $K[G]$.*

Preuve : Notons qu'il y a au plus un unique O_K-ordre maximal dans $K[G]$ puisque le produit de deux ordres est encore un ordre : cela est dû à la commutativité du groupe G et donc de l'algèbre $K[G]$.

Supposons alors qu'il exsite dans $K[G]$ un ordre sur O_K maximal. D'après le théorème 8.6 de ([51], Chap.II, §8), $\mathcal{O}$ est inclus dans O_K^{cl}. Réciproquement, tout $\lambda \in O_K^{\mathrm{cl}}$ est dans $\mathcal{O}$. Le module $O_K[\lambda]$ est clairement un O_K-ordre dans $K[\lambda]$. Donc $O_K[\lambda].\mathcal{O}$ est un O_K-ordre de $K[G]$ et est inclus dans $\mathcal{O}$ par maximalité, d'où $\lambda \in \mathcal{O}$. Cela signifie que si l'ordre $\mathcal{O}$ est maximal, alors nécessairement $\mathcal{O} = O_K^{\mathrm{cl}}$.

Or, d'après le lemme 5.1, la clôture intégrale O_K^{cl} de O_K n'est pas un O_K-ordre : en effet, $K[G]$ n'est pas de type fini sur O_K en tant que module, donc O_K^{cl} non plus.

Il n'existe donc pas d'ordre sur O_K maximal dans l'algèbre $K[G]$. ◇

Remarque 27. *Soulignons que cette propriété ne dépend que du groupe G, mais pas de l'extension L/K. En particulier, quelle que soit la ramification dans L/K, la clôture intégrale de O_K dans $K[G]$ est toujours $O_K^{cl} = O_K + XK[G]$, avec $X = \sigma - 1$. En fait, l'absence d'ordre maximal dans $K[G]$ est essentiellement due au fait que la K-algèbre $K[G]$ n'est pas séparable.*

Pour information : si R est un anneau noethérien intégralement clos et si K est son corps de fraction, on peut montrer l'existence de R-ordres maximaux dans toute K-algèbre séparable (cf. [51], §10).

5.3.5 Structure algébrique de $A(L/K)$

Nous fermons ce paragraphe avec une étude des propriétés algébriques de l'ordre associé à l'extension L/K. Plus précisément :

Proposition 5.10. *L'ordre A associé à l'extension L/K est un anneau local noethérien. De plus, son anneau réduit A_{red} est O_K.*

On appelle anneau local tout anneau qui possède un unique idéal maximal. D'autre part, rappelons qu'un anneau commutatif est dit noethérien si tous ses idéaux sont de type fini, ou, de façon équivalente, si toute chaîne croissante d'idéaux est finie.

Enfin, on définit l'anneau réduit de A l'anneau quotient $A_{\mathrm{red}} = A/\mathrm{nil}(A)$, où $\mathrm{nil}(A)$ désigne le nilradical de A, c'est-à-dire l'ensemble des éléments nilpotents de A. On rappelle que le nilradical

d'un anneau est un idéal égal à l'intersection de tous les idéaux premiers de l'anneau (cf. [9], Chap.I, prop.1.8).

Preuve : Le O_K-module A est clairement noethérien puisqu'il est de type fini sur O_K qui est noethérien en tant qu'anneau de valuation discrète (cf. [60], Chap.I, §2).

Pour montrer que A est aussi un anneau local, il suffit de montrer que son anneau réduit est local. En effet, supposons que A_{red} possède un unique idéal maximal. Si A avait deux idéaux maximaux distincts, par exemple $\mathfrak{m}_1$ et $\mathfrak{m}_2$, ils contiendraient tous les deux nil(A) et donc correspondraient dans A_{red} à deux idéaux distincts $\mathfrak{m}'_1$ et $\mathfrak{m}'_2$ via la correspondance bijective entre les idéaux de A contenant nil$A$ et les idéaux de A_{red} par la projection $f : A \twoheadrightarrow A_{\text{red}}$. Or, puisque cette correspondance est strictement croissante, si $\mathfrak{I}'$ est un idéal contenant $\mathfrak{m}'_1$, alors $f^{-1}(\mathfrak{I}')$ est un idéal de A contenant $\mathfrak{m}_1$ et par maximalité ils sont égaux. D'où $\mathfrak{m}'_1 = f \circ f^{-1}(\mathfrak{I}') = \mathfrak{I}'$ et $\mathfrak{m}'_1$ est maximal dans A_{red}. De même, $\mathfrak{m}'_2$ est maximal dans A et donc $\mathfrak{m}'_1 = \mathfrak{m}'_2$, contradiction. Ainsi l'anneau A est bien local.

Il s'agit donc de montrer que l'anneau A_{red} est local. Nous allons plus précisément montrer que $A_{\text{red}} = O_K$. Les inclusions suivantes sont évidentes :

$$\text{nil}(O_K[G]) \subset \text{nil}(A) \subset \text{nil}(K[G]).$$

En particulier, le O_K-morphisme composé $O_K[G] \hookrightarrow A \twoheadrightarrow A_{\text{red}}$ - où la première application est l'inclusion et la seconde est la surjection canonique - induit un O_K-morphisme $(O_K[G])_{\text{red}} \to A_{\text{red}}$ qui est en fait injectif puisque son noyau est exactement $O_K[G] \cap \text{nil}(A) = \text{nil}(O_K[G])$. Un argument similaire montre que l'on obtient canoniquement un O_K-morphisme injectif $A_{\text{red}} \hookrightarrow (K[G])_{\text{red}}$, d'où les inclusions :

$$O_K[G]_{\text{red}} \subset A_{\text{red}} \subset K[G]_{\text{red}}.$$

Il est alors immédiat que le nilradical de l'algèbre $K[G]$, identifiée à $K[X]/X^p$, est l'idéal engendré par X et donc que l'anneau réduit de $K[G]$ est K. De même, celui de $O_K[G]$ est O_K. Il vient :

$$O_K \subset A_{\text{red}} \subset K.$$

Pour conclure, A_{red} est un O_K-module de type fini en tant que quotient de A. C'est donc un O_K-ordre de K puisque O_K est un O_K-ordre de K. Or, $O_K$est maximal par la proposition 8.6 de ([51], §8). D'où $A_{\text{red}} = O_K$, ce qu'il fallait démontrer. ◇

Par la suite, nous noterons $\mathfrak{m}_A$ l'unique idéal maximal de l'ordre A.

Corollaire 5.2. *Le corps résiduel $A/\mathfrak{m}_A$ de A est canoniquement isomorphe à κ.*

Preuve : Puisque le nilradical d'un anneau est l'intersection de ses idéaux premiers, il est inclus dans chaque idéal maximal. Alors $\text{nil}(A) \subset \mathfrak{m}_A \subset A$ et on a un isomorphisme canonique d'anneaux :

$$A/\mathfrak{m} \simeq (A/\text{nil}(A))/(\mathfrak{m}_A/\text{nil}(A)).$$

Or, d'après la proposition 5.10, l'anneau réduit $A_{\text{red}} = A/\text{nil}(A)$ est O_K. De plus, $A/\mathfrak{m}$ est un corps et donc $O_K/(\mathfrak{m}_A/\text{nil}(A))$ aussi. Ainsi, l'idéal $(\mathfrak{m}_A/\text{nil}(A))$ est $\mathfrak{p}_K$ puisqu'il est maximal dans O_K. On a donc montré :

$$A/\mathfrak{m}_A \simeq O_K/\mathfrak{p}_K = \kappa.$$

◇

Remarque 28. *L'ordre A n'est pas un anneau de valuation puisqu'il n'est pas intègre.*

Nous pouvons maintenant montrer les équivalences des assertions du théorème 5.2.

5.4 La suite $\{\epsilon_i\}_i$ et la propriété (ii)

Nous montrons l'équivalence $(i) \Leftrightarrow (ii)$ du théorème 5.2 dans le sous-paragraphe 5.4.3. Pour cela, le sous-paragraphe 5.4.1 introduit d'abord une suite combinatoire de 0 et de 1 qui nous permet de donner naturellement une O_K-base pour l'ordre associé à L/K.

A partir de maintenant et pour toute la suite, nous modifions nos notations en posant :

$$X := \frac{\sigma - 1}{T^t},$$

où l'entier $t \geq 0$ a déjà été défini par la relation $m = pt + s$ avec $0 < s < p$.
Ce nouvel élément X appartient toujours à l'ordre associé A via l'identification $K[G] \simeq K[X]/X^p$. De plus, tous les résultats précédents restent valides.

5.4.1 Construction des ϵ_i's

La suite ϵ. Nous condérons à nouveau la O_K-base de Aiba pour O_L que nous avons décrite dans le sous-paragraphe 5.2.2. Rappelons qu'elle est donnée par :

$$\{1, \alpha T^{x_1}, \cdots, \alpha^{p-1} T^{x_{p-1}}\},$$

avec :

$$\forall i \geq 0,\ x_i = it - \lfloor -\frac{si}{p} \rfloor.$$

Nous allons modifier nos notations afin de les améliorer. Nous écrivons chaque x_i comme la somme :

$$x_i = a_1 + \cdots + a_i,$$

où chaque a_i est un entier positif donné par :

$$a_i = t + \epsilon_i,$$

pour un certain entier $\epsilon_i \in \{0, 1\}$. Plus précisément, chaque ϵ_i est défini par :

$$\epsilon_i = \lfloor -\frac{s(i-1)}{p} \rfloor - \lfloor -\frac{si}{p} \rfloor$$

et il est alors facile de voir que chaque ϵ_i prend bien la valeur 0 ou 1 car $0 < s < p$.
La définition est valable pour tout entier $i \in \mathbb{Z}$. En outre, si l'on considère toute la suite $\{\epsilon_i\}_i$, on voit qu'elle est p-cyclique, c'est-à-dire :

$$\forall i \in \mathbb{Z},\ \epsilon_{i+p} = \epsilon_i,$$

et en particulier :

$$\forall k \in \mathbb{Z},\ \epsilon_{kp} = \epsilon_0 = \epsilon_p = 0.$$

Notons aussi que :

$$\epsilon_1 = -\lfloor -\frac{s}{p} \rfloor = 1,$$

puisque l'on a supposé s tel que $0 < s < p$.
Avant d'aller plus loin, insistons sur une propriété cruciale pour la suite : la suite des ϵ_i est *équilibrée*. On dit qu'une suite est équilibrée si deux blocs quelconques de même longueur ont un poids qui diffèrent d'au plus 1. Ici, un bloc signifie une sous-suite finie de termes consécutifs, sa longueur est le nombre de termes qu'il contient et son poids est défini comme la somme de ses termes. Habituellement, si x est un bloc de longueur l, on note $|x|$ son poids.

Remarque 29. *Dans sa thèse (*2001*), Alex Heinis, étudiant de Tijdeman à l'université de Leiden, explique que les suites équilibrées ont été initialement introduites par Morse et Hedlund mais que ces derniers utilisaient davantage le nom de "suite sturmiennes" en référence au mathématicien suisse J.C.F. Sturm (*$1803 - 1855$*).*

Proposition 5.11. *La suite $\{\epsilon_i\}_i$ est équilibrée.*

Preuve : Cela résulte de la définition des ϵ_i. Soient $x = \{\epsilon_{i+1}, ..., \epsilon_{i+l}\}$ et $y = \{\epsilon_{j+1}, ..., \epsilon_{j+l}\}$ deux blocs de longueur $l \geq 1$. Leurs poids sont donnés par :

$$|x| = \lfloor -\frac{si}{p} \rfloor - \lfloor -\frac{s(i+l)}{p} \rfloor$$

et de même :

$$|y| = \lfloor -\frac{sj}{p} \rfloor - \lfloor -\frac{s(j+l)}{p} \rfloor$$

Alors, à partir de la formule $r - s - 1 < \lfloor r \rfloor - \lfloor s \rfloor < r - s + 1$ pour tous réels r et s, la différence entre les poids de x et y est :

$$-\frac{si}{p} + \frac{s(i+l)}{p} + \frac{sj}{p} - \frac{s(j+l)}{p} - 2 < |x| - |y| < -\frac{si}{p} + \frac{s(i+l)}{p} + \frac{sj}{p} - \frac{s(j+l)}{p} + 2$$

d'où $-2 < |x| - |y| < 2$ et donc $||x| - |y|| \leq 1$, ce qui montre la proposition. ◇

Dorénavant, le terme **suite** ϵ fera référence à la sous-suite $\epsilon_1, ..., \epsilon_{p-1}$ et nous nous restreignons à l'étude de cette sous-suite uniquement.

Soulignons que la suite ϵ ne dépend que des entiers p et s. En outre :

Proposition 5.12. *La suite ϵ $(\epsilon_1, ..., \epsilon_{p-1})$ est de poids s.*

Preuve : Par construction, la suite ϵ contient exactement s fois le terme 1, d'où son poids. ◇

Problème de points. Pour clore ce sous-paragraphe, nous donnons à travers deux exemples une interprétation géométrique de la suite ϵ qui rend son calcul encore plus facile.

Exemple 5.1 ($X^{-7} - X = T^{-4}$)**.** *Prenons $p = 7$ et $m = 4 = s$. Puisque m n'est pas divisible par 7, l'extension L considérée est totalement ramfiée sur le corps local $K = \mathbb{F}_7((T))$. Elle est donnée par $L = K(\alpha)$, où $\alpha \in K^{sep}$ est tel que $\alpha^7 - \alpha = T^{-4}$.*

D'après le sous-paragraphe 5.2.2, la O_K-base de Aiba pour O_L est du type :

$$1, \alpha T^{x_1}, \alpha^2 T^{x_2} ..., \alpha^6 T^{x_6},$$

où chaque x_i est tel que $7x_i$ soit le plus petit multiple de 7 qui est supérieur à $4i$. Concrètement, écrivons sur une ligne les multiples $4i$ pour i variant de 0 à 6, puis sur une seconde ligne située au-dessous et lui correspondant les multiples $7k$ jusqu'à ce que l'on obtienne $4 \times 6 = 28$, typiquement :

0	4		8	12		16	20		24	28		
0		7			14			21		28		

On voit donc que 7×1 est le plus petit multiple de 7 qui suit 4 et donc $x_1 = 1$. Ensuite $14 = 7 \times 2$ est le plus petit entier multiple de 7 qui suit immédiatement $8 = 4 \times 2$ et aussi $12 = 4 \times 3$, d'où $x_2 = x_3 = 2$. De même on trouve : $x_4 = x_5 = 3$ and $x_6 = 4$.

On vérifie alors que $x_0 = 0$, i.e. $\epsilon_1 = x_1 - x_0 = 1$, et que $x_7 = x_6$, i.e. $\epsilon_7 = x_7 - x_6 = 0$, ce qui confirme certaines propriétés des ϵ_i que nous avons mentionnées plus haut.

La base de Aiba pour O_L est la suivante :

$$1, \alpha T, \alpha^2 T^2, \alpha^3 T^2, \alpha^4 T^3, \alpha^5 T^3, \alpha^6 T^4.$$

Bien entendu, on peut calculer directement les ϵ_i et en déduire les x_i à partir de la formule :

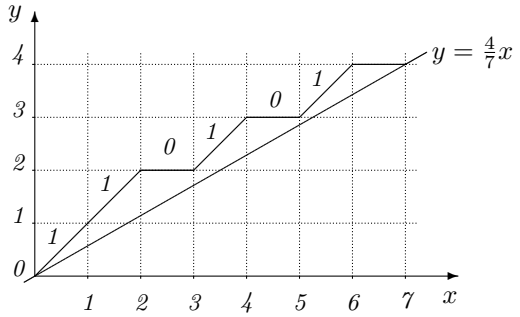
$$x_i = \epsilon_1 + \cdots + \epsilon_i$$

puisque l'on a pris $t = 0$ *ici.*

On peut aussi utiliser la méthode suivante qui utilise nos deux lignes de multiples précédentes. On a $\epsilon_i = 0$ *si et seulement si le plus petit multiple de* 7 *qui suite* $4i$ *est le même que celui qui suit immédiatement* $4(i-1)$*. Pour notre exemple, cela donne la suite* ϵ *suivante :*

$$110101.$$

Il existe encore une autre méthode géométrique qui permet de calculer très facilement les ϵ_i*. Il s'agit en effet de tracer la droite* $y = \frac{s}{p}x = \frac{4}{7}x$ *et de mettre une croix sur tous les points à coordonnées entières qui sont les plus proches de la droite sur son demi-plan supérieur. Ces point sont précisément donnés par les coordonnées* $(i, -\lfloor -\frac{4i}{7} \rfloor)$ *pour* $i \in \{0, ..., 7\}$*. Nous joignons alors ces points pour obtenir un polygone. Concrètement, cela donne :*



Chaque ϵ_i *est la pente du segment qui lie les points* $(i, -\lfloor -\frac{4i}{7} \rfloor)$ *et* $(i-1, -\lfloor -\frac{4(i-1)}{7} \rfloor)$ *: il prend bien les valeurs* 0 *ou* 1*. Ici, cela donne la suite :*

$$110101$$

qui est la même que celle obtenue par la méthode précédente.

Exemple 5.2 $(X^{-7} - X = T^{-3})$**.** *Prenons* $p = 7$ *et* $s = 3$*, en particulier* s *divise* $p-1$*. Une nouvelle fois, nous calculons les* x_i *en comprant les multiples de* 3 *et ceux de* 7 *sur les lignes suivantes :*

$$\begin{array}{cccccccccc} 0 & 3 & 6 & & 9 & 12 & & 15 & 18 & 21 \\ 0 & & & 7 & & & 14 & & & 21 \end{array}$$

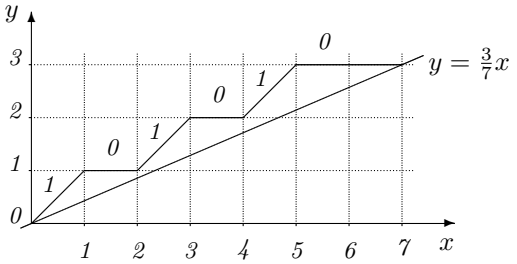
La base de Aiba pour O_L *est donc ici :*

$$1, \alpha T, \alpha^2 T, \alpha^3 T^2, \alpha^4 T^2, \alpha^5 T^3, \alpha^6 T^3.$$

On en déduit également la suite des ϵ_i*' pour* i *allant de* 1 *à* 6 *:*

$$101010,$$

que l'on retrouve aussi à l'aide du graphe suivant :



On obtient ainsi une suite ϵ de la forme $(10..0)^s$. Cet exemple satisfait les conditions (ii) et (iii) du théorème 5.2.

5.4.2 Une O_K-base pour l'ordre associé $A(L/K)$

Dans ce sous-paragraphe, la suite ϵ apparaît naturellement dans la construction d'une O_K-base pour l'ordre associé A, base que l'on obtient en considérant les matrices des puissances de X dans la base de O_L donnée par Aiba .

La construction de la base de Aiba de O_L sur O_K est basée sur l'identification des algèbres $K[G]$ et $K[X]/X^p$, où maintenant $X = \dfrac{\sigma - 1}{T^t}$. Puisque A est un O_K-ordre dans $K[G]$, une idée naturelle est alors de chercher une O_K-base pour A du type $a_0, a_1X, ..., a_{p-1}X^{p-1}$, où les a_i' sont dans K.
Cela nous mène à introduire une autre suite combinatoire composée des minima de i termes consécutifs dans la suite ϵ lorsque i varie de 0 à $p-1$. Précisément, nous posons :

$$\forall i,\ 0 \leq i \leq p-1,\ \ m_i := \inf_{j=1\ldots p-i} \{\epsilon_j + \cdots + \epsilon_{j+i-1}\},$$

avec $m_0 = 0$.
Nous avons déjà observé que tout élement de A peut naturellement être identifié avec un O_K-endomorphisme de O_L. En outre, chaque X^i, pour $0 \leq i \leq p-1$, est clairement dans A. En effet, si l'on regarde l'action de X sur les éléments de base de Aiba pour O_L, on obtient par la proposition 5.3 :

$$\forall j \geq 1,\ \ (\sigma - 1)(\alpha^j T^{x_j}) = \sum_{k=0}^{j-1} \binom{j}{k} T^{x_j - x_k} T^{x_k} \alpha^k$$

et donc :

$$X(\alpha^j T^{x_j}) = \sum_{k=0}^{j-1} \binom{j}{k} T^{x_j - x_k - t} T^{x_k} \alpha^k,$$

avec $x_j - x_k - t = (j-1-k)t + (\lfloor \frac{sk}{p} \rfloor - \lfloor \frac{sj}{p} \rfloor) \geq 0$ pour tout $k \leq j-1$. Ainsi $X.\alpha^j T^{x_j}$ appartient bien à O_L (et même à l'idéal $\mathfrak{I}_{j-1}$).
On calcule alors la matrice de chaque puissance X^i dans la base de Aiba. Pour $i = 0$, on a :

$$X = \begin{pmatrix} 0 & T^{\epsilon_1} & \star & \cdots & \star \\ 0 & 0 & 2T^{\epsilon_2} & \star & \vdots \\ \vdots & \ddots & \ddots & \ddots & \star \\ & & & 0 & (p-1)T^{\epsilon_{p-1}} \\ 0 & \cdots & 0 & 0 & 0 \end{pmatrix}$$

où l'étoile $*$ désigne des éléments de $O_K.T^{\inf_j\{\epsilon_j\}}$.

Notons que cette matrice est triangulaire supérieure de diagonale nulle. Alors, en prenant les puissances de X, nous obtenons toujours des matrices triangulaires supérieures avec De plus, en plus de 0. Plus précisément, pour tout indice $i = 0...p-1$, la matrice de X^i dans la base de Aiba est du type :

$$X^i = \begin{pmatrix} 0 & \cdots & 0 & c_1^{(i)} T^{\epsilon_1 + \ldots + \epsilon_i} & \star & \cdots & \star \\ \vdots & \ddots & & 0 & c_2^{(i)} T^{\epsilon_2 + \ldots + \epsilon_{i+1}} & & \star \\ \vdots & & & & & \ddots & \vdots \\ \vdots & & & & & \ddots & \star \\ 0 & \cdots & \cdots & \cdots & 0 & c_{p-i}^{(i)} T^{\epsilon_{p-i} + \ldots + \epsilon_{p-1}} & \\ 0 & \cdots & \cdots & \cdots & 0 & 0 & \\ \vdots & & & & & \vdots & \\ 0 & \cdots & \cdots & \cdots & \cdots & 0 & \end{pmatrix}$$

où les coefficients $c_j^{(i)}$ sont des éléments non nuls de $\mathbb{F}_p$. Dans le coin supérieur droit de la matrice, i.e. au-dessus des termes $c_j^{(i)} T^{\epsilon_j+\ldots+\epsilon_{j+i-1}}$, tous les coefficients sont dans $O_K.T^{m_i}$, ce que nous signifions par des étoiles $\star$. En conséquence, on peut diviser chaque puissance X^i par T^{m_i} et conserver une matrice à coefficients dans O_K. De plus, il semble que ce soit la plus grande puissance de T qui vérifie ces propriétés. Plus précisément, on a le résultat suivant :

Proposition 5.13. *Une O_K-base de l'ordre A associé à l'extension L/K est donnée par la famille :*

$$\left\{ \frac{X^i}{T^{m_i}} \right\}_{i=0\ldots(p-1)},$$

où $X = \dfrac{\sigma - 1}{T^t}$.

Preuve : Notons A_0 le O_K-module engendré par la famille :

$$\left\{ \frac{X^i}{T^{m_i}} \right\}_{i=0\ldots p-1}.$$

D'après ce qui précède, A_0 est un sous- O_K-module de A. De plus, il est clairement de rang p puisque les $\frac{X^i}{T^{m_i}}$ sont linéairement indépendants sur O_K.

Il s'agit alors de montrer l'égalité $A_0 = A$, ce que nous faisons progressivement. Notre preuve est essentiellement basée sur l'observation que les quotients A_0/TA_0 et A/TA sont des κ-espaces vectoriels de même dimension. On justifie d'abord l'existence d'un κ-morphisme $\phi : A_0/TA_0 \to \text{End}_{\kappa}(O_L/TO_L)$ qui est injectif. On montre ensuite que l'on peut construire un κ-homomorphisme $A/TA \to \text{End}_{\kappa}(O_L/TO_L)$ qui commute avec ϕ par l'homomorphisme canonique $f : A_0/TA_0 \to A/TA$. Ceci entraînera que f est injective et donc bijective, puis nous conclurons par le lemme de Nakayama.

Maintenant, détaillons la preuve.

Le O_K-morphisme $A_0 \to \text{End}_{O_K}(O_L)$ donné par $\lambda \mapsto \varphi_\lambda : \{x \mapsto \lambda.x\}$ induit une application bilinéaire :

$$A_0 \times \kappa \to \text{End}_{O_K}(O_L) \otimes_{O_K} \kappa$$

donnée par $(\lambda, \bar{\epsilon}) \mapsto \varphi_\lambda \otimes \bar{\epsilon}$. Par la propriété universelle du produit tensoriel, on obtient un morphisme de O_K-modules :

$$\begin{array}{rccc} \phi : & A_0 \otimes_{O_K} \kappa & \longrightarrow & \text{End}_{O_K}(O_L) \otimes_{O_K} \kappa \\ & \lambda \otimes \bar{\epsilon} & \mapsto & \varphi_\lambda \otimes \bar{\epsilon}. \end{array}$$

De plus, d'après ([35], Chap. XVI, §4), les produits tensoriels $A_0 \otimes_{O_K} \kappa$ et $\text{End}_{O_K}(O_L) \otimes_{O_K} \kappa$ sont aussi munis d'une structure d'espaces vectoriels sur κ pusique l'on peut les voir comme extensions de O_K dans κ par rapport à l'homomorphisme d'anneaux $O_K \twoheadrightarrow \kappa$. En particulier, ϕ est aussi un morphisme de κ-espaces vectoriels.

Alors, d'après ([35], Chap. XVI, §2) et puisque l'idéal maximal $\mathfrak{p}_K$ de K est engendré par T, il existe un isomorphisme canonique de κ-espaces vectoriels $A_0/TA_0 \to A_0 \otimes_{O_K} \kappa$ tel que $(\lambda + TA_0) \mapsto \lambda \otimes \bar{1}$, où $\bar{1}$ est la classe de 1 dans κ. De plus, on obtient aussi un isomorphisme canonique $\text{End}_{O_K}(O_L) \otimes_{O_K} \kappa \to \text{End}(O_L \otimes_{O_K} \kappa)$ et donc encore un κ-isomorphisme $O_L \otimes_{O_K} \kappa \to O_L/TO_L$. Ainsi, ϕ induit un κ -homomorphisme que nous noterons toujours ϕ :

$$\begin{array}{rccc} \phi : & A_0/TA_0 & \longrightarrow & \text{End}_{O_K}(O_L/TO_L) \\ & \lambda + TA_0 & \mapsto & \phi_\lambda : \{(x + TO_L) \mapsto (\lambda.x + TO_L)\}. \end{array}$$

Nous montrons que ce morphisme ϕ est injectif. Soit donc λ dans A_0. Ecrivons $\lambda = \sum_{i=0}^{p-1} \omega_i \frac{X^i}{T^{m_i}}$, où tous les ω_i sont dans O_K. Supposons que pour tout $x \in O_L$, $\lambda.x$ est dans TO_L. Il s'agit de montrer que ω_i est divisible par T dans O_K. Pour cela, nous allons utiliser les matrices des puissances X^i. Faisons l'observation suivante. Si V_j est le j-ième terme dans la base de Aiba pour O_L, alors V_j correspond au vecteur colonne :

$$\forall j,\ 0 \leq j \leq p-1, V_j = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix}$$

où 1 est sur la $(j+1)$-ième ligne. Alors, en lui appliquant la matrice $\lambda = \sum_i \omega_i \frac{X^i}{T^{m_i}}$, on obtient $\omega_0 = 0 \mod T$ pour $j = 0$ ainsi que le sytème suivant pour tous les $j \geq 1$:

$$\begin{array}{ll} \omega_0 & = 0 \mod T \\ \omega_1 T^{\epsilon_j - m_1} & = 0 \mod T \\ (\omega_1 + \omega_2) T^{\epsilon_{j-1} + \epsilon_j - m_2} & = 0 \mod T \\ \vdots & \\ (\omega_1 + \omega_2 + ...\omega_j) T^{\epsilon_1 + ... + \epsilon_j - m_j} & = 0 \mod T. \end{array}$$

En particulier, si j_1 est tel que $\epsilon_{j_1} = m_1$ alors on a $\omega_1 = 0 \mod T$ à partir de la seconde équation. Ensuite, il existe $j_2 \geq 2$ tel que $m_2 = \epsilon_{j_2 - 1} + \epsilon_{j_2}$, d'où $\omega_1 + \omega_2 = 0(\mod T)$ et donc $\omega_2 = 0(\mod T)$ aussi. On itère ce procédé en considérant à chaque étape un indice $j_i \geq i$ tel que $m_i = \epsilon_{j-i+1} + ... + \epsilon_j$. Par récurrence, on montre ainsi que pour tous les indices i, $0 \leq i \leq p-1$, on a $\omega_i = 0(\mod T)$. Cela signifie que λ est dans TA_0 et donc que ϕ est injective.

Maintenant, de la même façon que nous avons défini ϕ, on considère l'homomorphisme de κ-espaces vectoriels :

$$\begin{array}{rccc} \psi : & A/TA & \longrightarrow & \mathrm{End}_{O_K}(O_L/TO_L) \\ & \lambda + TA & \mapsto & \psi_\lambda : \{x + TO_L \mapsto \lambda.x + TO_L\}, \end{array}$$

et l'on remarque qu'il rend le diagramme suivant commutatif :

$$\begin{array}{rccc} \psi : & A_0/TA_0 & \xrightarrow{\phi} & \mathrm{End}_{O_K}(O_L/TO_L) \\ & \downarrow f & \nearrow_{\psi} & \\ & A/TA & & \end{array}$$

où f est l'homomorphisme canonique $A_0/TA_0 \to A/TA$ induit par l'injection $A_0 \hookrightarrow A$. En particulier, puisque ϕ est injective, f l'est aussi. Or, les κ-espaces vectoriels A_0/TA_0 et A/TA sont de même dimension : ils sont en effet κ-isomorphes aux espaces vectoriels $A_0 \otimes_{O_K} \kappa$ qui eux-mêmes sont isomorphes en d'eux car de même dimension par ([35], Chap. XVI, §4), précisément :

$$\dim_\kappa(A_0 \otimes_{O_K} \kappa) = \mathrm{rank}_{O_K} A_0 = p = \mathrm{rank}_{O_K} A = \dim_\kappa(A \otimes_{O_K} \kappa).$$

Ainsi, f est l'isomorphisme $A_0/TA_0 \xrightarrow{\simeq} A/TA$ et comme $\{A_0 + TA\}/TA \simeq A_0/TA_0$ on obtient l'identité de O_K-modules :$A = A_0 + TA$. Enfin, puisque A est de type fini sur O_K, on a par le lemme de Nakayama : $A = A_0$. Ceci termine la preuve. $\diamond$

En résumé, on considère, sur l'ordre associé A, la base de O_K-module suivante :

$$\{\frac{X^i}{T^{m_i}}\}_i,\ 0 \leq i \leq p-1,$$

où $m_0 = 0$ et pour tout $i \leq 1$, m_i est le minimum $\inf\{\epsilon_j + ... + \epsilon_{j+i-1}\}$ dasn la suite ϵ associée à l'extension L/K.

Soulignons que ce n'est pas la O_K-base que Aiba utilise dans [3].

Une conséquence importante de la proposition 5.13 concerne la structure algébrique de l'idéal maximal $\mathfrak{m}_A$ dans A. En identifiant T avec la mutliplication par T, on obtient en effet :

Corollaire 5.3. *L'idéal maximal $\mathfrak{m}_A$ de A est un O_K-module libre de rang p dont une base est donnée par la famille :*

$$\{T, \frac{X}{T^{m_1}}, ..., , \frac{X^{p-1}}{T^{m_{p-1}}}\}.$$

Preuve : L'idéal $\mathfrak{m}_A$ est un sous-O_K-module de A, il est donc libre de rang inférieur ou égal à celui de A. Or, d'après le corollaire 5.2, $A/\mathfrak{m}_A$ est fini. D'où $\text{rank}_{O_K}(\mathfrak{m}_A) = \text{rank}_{O_K} A = p$.

De plus, tous les $\frac{X^i}{T^{m_i}}$, $1 \leq i \leq p-1$, sont dans $\mathfrak{m}_A$ puisqu'ils sont nilpotents et T aussi en raison de l'isomorphisme $A/\mathfrak{m}_A \simeq \kappa$. On montre alors que les éléments T et $\frac{X^i}{T^{m_i}}$, $1 \leq i \leq p-1$, sont linéairement indépendants sur O_K et forment donc une base sur O_K de $\mathfrak{m}_A$. $\diamond$

Ce dernier résultat sera à la base du calcul de l'embedding dimension de A dans le sous-paragraphe 5.6.2.

5.4.3 L'équivalence $(i) \Leftrightarrow (ii)$

On rappelle que la suite ϵ est la suite finie $\{\epsilon_1, \cdots, \epsilon_{p-1}\}$. Dans ce sous-paragraphe, nous montrons l'équivalence $(i) \Leftrightarrow (ii)$ du théorème 5.2. Nous donnons d'abord un lemme très utile :

Lemme 5.2. *L'anneau de valuation O_L est libre sur A si et seulement si $O_L = A.\beta$, où $\beta = \alpha^{p-1}T^{x_{p-1}}$ est le dernier terme dans la base de Aiba de O_L sur O_K.*

Preuve : Si O_L est libre sur A, il est de rang 1 d'après le corollaire 5.1, i.e. il existe $\beta \in O_L$ tel que $O_L = A.\beta$. On écrit $\beta = \sum_{i=0}^{p-1} b_i \alpha^i T^{x_i}$ dans la base de Aiba, avec tous les b_i dans O_K. Nous allons d'abord montrer que l'on peut prendre $\beta = b_{p-1}\alpha^{p-1}T^{x_{p-1}}$ où $b_{p-1} \in U_K$ est de plus une unité de O_K.

Puisque O_L est libre sur A de rang 1, par le lemme de Nakayama, on a $O_L = A.\beta$ si et seulement $(\beta \mod \mathfrak{m}_A O_L)$ engendre le κ-espace vectoriel $O_L/\mathfrak{m}_A O_L$.

Identifiant $O_L/m_A O_L$ avec $O_L \otimes_A \kappa$ via l'application de réduction (cf. [35], Chap.XVI, §4), on voit que $O_L/\mathfrak{m}_A O_L$ est de dimension 1 sur κ et donc que les espaces vectoriels $O_L/\mathfrak{m}_A O_L$ et κ sont κ-isomorphes.

On considère alors l'application suivante :

$$\begin{array}{rccc} f: & O_L & \longrightarrow & O_K \\ & z & \mapsto & \zeta_{p-1} \end{array}$$

avec $z = \sum_{i=0}^{p-1} \zeta_i \alpha^i T^{x_i}$ dans la base de Aiba. Il est clair que f est un morphisme surjectif de O_K-modules.

Montrons : $f(\mathfrak{m}_A O_L) \subset \mathfrak{p}_K$. Pour cela, on introduit à nouveau l'homomorphisme $\frac{X^{p-1}}{T^{m_{p-1}}} : O_L \to O_L$.

On a $f(m_A O_L) \subset \mathfrak{p}_K$ si et seulement si $\frac{X^{p-1}}{T^{m_{p-1}}}(m_A O_L) \subset \mathfrak{p}_K \alpha^{p-1} T^{x_{p-1}}$. Cela se voit sur la matrice de X^{p-1} donnée dans le sous-paragraphe 5.4.2 dont la forme traduit en particulier la relation :

$$\frac{X^{p-1}}{T^{m_{p-1}}}.\sum_{i=0}^{p-1} \zeta_i \alpha^i T^{x_i} = c\zeta_{p-1}\alpha^{p-1}T^{x_{p-1}},$$

où c est une constante dans $\mathbb{F}_p$.

Soit z dans $\mathfrak{m}_A O_L$. Calculons son image par $\frac{X^{p-1}}{T^{m_{p-1}}}$. Par le corollaire 5.3, on peut écrire $z = \lambda.y$ avec $\lambda \in \mathfrak{m}_A$ avec $\lambda = \lambda_0 T + \sum_{i=1}^{p-1} \lambda_i \frac{X^i}{T^{m_i}}$, où $\lambda_i \in O_K$ et $y \in O_L$, $y = \sum_{i=0}^{p-1} y_i \alpha^i T^{x_i}$, tel que $y_i \in O_K$. Alors, considérant X^{p-1} comme un élément dans A, il vient :

$$\frac{X^{p-1}}{T^{m_{p-1}}}.z = \frac{X^{p-1}}{T^{m_{p-1}}}.(\lambda.y) = (\frac{X^{p-1}}{T^{m_{p-1}}}\lambda).y.$$

Or, , l'annulateur de $\frac{X^{p-1}}{T^{m_{p-1}}}$ dans A contient tous les $\frac{X^i}{T^{m_i}}$', pour $1 \leq i \leq p-1$, puisque $X^p = 0$. D'où $\frac{X^{p-1}}{T^{m_{p-1}}}\lambda = \lambda_0 T \frac{X^{p-1}}{T^{m_{p-1}}}$ et donc :

$$\begin{aligned} \frac{X^{p-1}}{T^{m_{p-1}}}.z &= \lambda_0 T.(\frac{X^{p-1}}{T^{m_{p-1}}}y) \\ &= (c\lambda_0 T y_{p-1})\alpha^{p-1}T^{x_{p-1}}, \end{aligned}$$

avec $c \in \mathbb{F}_p$, à partir de la matrice de X^{p-1}. En particulier, $c\lambda_0 T y_{p-1}$ appartient à $\mathfrak{p}_K$, comme désiré.

Ainsi $f(m_A O_L) \subset \mathfrak{p}_K$ et le morphisme f se factorise par $m_A O_L$: il existe un unique morphisme $\bar{f}$ de O_K-modules tel que le diagramme suivant soit commutatif :

$$\begin{array}{ccc} O_L & \xrightarrow{f} & O_K \\ \downarrow & & \downarrow \\ O_L/\mathfrak{m}_A O_L & \xrightarrow{\bar{f}} & O_K/\mathfrak{p}_K = \kappa \end{array}$$

De plus, $\bar{f}$ est surjectif. Etant clairement linéaire sur κ, f est aussi un morphisme surjectif de κ-espaces vectoriels de $O_L/\mathfrak{m}_A O_L$ sur κ, c'est donc un isomorphisme.

Alors, ($\beta \mod \mathfrak{m}_A O_L$) n'engendre pas $O_L/\mathfrak{m}_A O_L$ comme espace vectoriel sur κ si et seulement s'il est envoyé sur $0 \in \kappa$ par $\bar{f}$, i.e. si et seulement si b_{p-1} appartient à $\mathfrak{p}_K$.

Ainsi, le fait que β engendre O_L comme A-module ou non ne dépend que de b_{p-1}. On peut prendre donc tous les b_i, $0 \leq i \leq p-2$, nuls et on a que $\beta = b_{p-1}\alpha^{p-1}T^{x_{p-1}}$ est un générateur de O_L sur A si et seulement si b_{p-1} est une unité de O_K. En particulier, cela est vrai pour $b_{p-1} = 1$, i.e. pour $\beta = \alpha^{p-1}T^{x_{p-1}}$.

D'autre part, si $O_L = A.\beta$ avec $\beta = \alpha^{p-1}T^{x_{p-1}}$, alors O_L est nécessairement libre sur A de rang 1 puisqu'un tel β est sans torsion sur A, i.e. les $\frac{X^i}{T^{m_i}}.\beta$ sont linéairement indépendants sur O_K, pour $i = 0, ..., p-1$ (il suffit d'appliquer pour tout i la matrice de $\frac{X^i}{T^{m_i}}$ à β et de voir que l'on obtient un élément de $\mathfrak{I}_{p-i} - \mathfrak{I}_{p-i-1}$, conclure alors par laproposition 5.2). Ceci complète la preuve du lemme. ◇

D'où la preuve de l'assertion (ii) dans le théorème 5.2 :

Proposition 5.14. *L'anneau O_L dans l'extension L/K est un module libre sur l'ordre associé A si et seulement si la suite ϵ correspondante est du type $(10...0)^s$.*

Preuve : Supposons d'abord que O_L est libre sur A. D'après le lemme 5.2, cela entraîne que $O_L = A.\beta$ avec $\beta = \alpha^{p-1}T^{a_1+\cdots+a_{p-1}}$, c'est-à-dire :

$$O_L = \bigoplus_{i=0}^{p-1} O_K.\frac{X^i}{T^{m_i}}(\beta),$$

où $m_i = \inf\{\epsilon_j + ... + \epsilon_{j+i-1}\}$.

Nous avons déjà vu que chaque $\frac{X^i}{T^{m_i}}.\beta$ est dans $\mathfrak{I}_{p-i} - \mathfrak{I}_{p-i-1}$, avec les notations de la proposition 5.4, et que son coefficient devant $\alpha^{p-i-1}T^{a_1+...+a_{p-i-1}}$ est $T^{\epsilon_{p-i-1}+...+\epsilon_{p-1}}$.

Or, $\alpha^{p-i-1}T^{a_1+...+a_{p-i-1}}$ appartient aussi à $\mathfrak{I}_{p-i} - \mathfrak{I}_{p-i-1}$, il existe donc $y_0, ..., y_{p-1}$ dans O_K tels que $\alpha^{p-i-1}T^{a_1+...+a_{p-i-1}} = \sum_j y_j \frac{X^i}{T^{m_i}}.\beta$. En particulier, il vient :

$$y_{p-i}\frac{T^{\epsilon_{p-i}+...+\epsilon_{p-1}}}{T^{m_i}} = .$$

Donc $\frac{T^{\epsilon_{p-i}+...+\epsilon_{p-1}}}{T^{m_i}}$ est une unité de O_K, d'où nécessairement :

$$m_i = \epsilon_{p-i} + ... + \epsilon_{p-1}.$$

Cela signifie que si O_L est libre sur A alors chaque minimum m_i est atteint à la fin de la suite ϵ. Soit alors ϵ_{p-1-l} le dernier 1 dans la suite ϵ, avec $l \geq 0$: la suite se termine par 10...0 avec précisément l zeros et c'est le plus grands bloc de 0 qu'elle contient. Alors, puisque la suite est équilibrée, il y a exactement l ou $l-1$ zéros entre deux 1 consécutifs. Or, si l'on considère maintenant la suite des ϵ_i jusqu'à $i = p+1$, on obtient un bloc de $l+1$ zéros entre deux 1 qui sont ϵ_{p-1-l} et ϵ_{p+1}. Mais comme la suite entière est encore équilibrée, tous les blocs de zéros doivent donc être de longueur l entre les indices $i = 1$ et $i = p-1$. Ceci montre que la suite ϵ est nécessairement du type $(10...0)^s$ puisque tous les blocs de 0 sont alors de même longueur et parce que le chiffre 1 apparaît exactement s fois dans la suite ϵ.

Réciproquement, supposons que la suite ϵ soit du type $(10...0)^s$. En particulier, cela signifie que les minima m_i sont atteints à la fin de la suite ϵ. Une O_K-base de A est alors donnée par :

$$\left\{ \frac{X^i}{T^{\epsilon_{p-1-i}+...+\epsilon_{p-1}}} \right\}_i .$$

Maintenant, on vérifie comme précédemment que chaque $\frac{X^i}{T^{\epsilon_{p-1-i}+...+\epsilon_{p-1}}}.\beta$ est dans $\mathfrak{I}_{p-i-1} - \mathfrak{I}_{p-i-2}$. Ainsi, les p éléments $\frac{X^i}{T^{\epsilon_{p-1-i}+...+\epsilon_{p-1}}}.\beta$ sont de valuations deux à deux distinctes dans $\{0, ..., p-1\}$. Alors, d'après la proposition 5.2, ils forment une base de O_L sur O_K, c'est-à-dire $O_L = A.\beta$ et on conclut par le lemme 5.2. ◇

5.5 L'équivalence $(i) \Leftrightarrow (iii)$

La condition (iii) du théorème 5.2 surprend par sa simplicité. C'est la plus facile à tester, d'où son importance. Avant de la prouver, donnons encore un lemme :

Lemme 5.3. *Si s divise $p-1$, alors $s = p-1$ si et seulement si $\epsilon_{p-1} = 1$.*
Da façon équivalente, il n'y a aucun 0 dans la suite ϵ si et seulement si son dernier terme est 1.

Preuve : Il est évident que si $s = p-1$ tous les ϵ_i valent 1 puisque s est le nombre de 1 dans la suite ϵ (cf. proposition 5.12).
Réciproquement, supposons $\epsilon_{p-1} = 1$, ce qui signifie :

$$\lfloor -s + \frac{2s}{p} \rfloor - \lfloor -s + \frac{s}{p} \rfloor = 1,$$

et donc :

$$\lfloor -s + \frac{2s}{p} \rfloor = -s + 1,$$

puisque $s < p$.Alors on a :

$$\frac{p-1}{2} < s$$

et puisque s divise $p-1$ on en déduit $s = p-1$, ce qu'il fallait démontrer. ◇

D'où la condition (iii) du théorème 5.2 :

Proposition 5.15. *L'anneau de valuation O_L dans l'extension L/K est un module libre sur A si et seulement si s divise $p-1$.*

Preuve : La première implication est triviale puisque c'est une conséquence directe de la condition (ii) du théorème 5.2, déjà montrée dans le sous-paragraphe 5.4.3.

Réciproquement, supposons que s divise $p-1$. Il s'agit de montrer que la suite ϵ est du type $(10...0)^s$. On écrit $p-1 = sk$ avec $k \geq 1$. Puisque s est le nombre de 1 dans la suite ϵ, il reste donc à placer $s(k-1)$ termes 0 dans la suite.

D'après le lemme 5.3 on peut donc supposer $s \neq p-1$, i.e. si l est la longueur maximale d'un bloc de 0 dans la suite ϵ. Alors $l \geq 1$ et $\epsilon_{p-1} = 0$. Autrement dit, puisque $\epsilon_1 = 1$, il y a exactement s intervalles dans lesquels nous pouvons placer des 0, ce qui signifie que la suite est du type :

$$(10...0)(10...0) \cdots (10..0).$$

On considère alors deux cas : soit le dernier bloc de 0 est le plus long soit il ne l'est pas.

Supposons d'abord que le dernier bloc de 0 est de longueur 0. Puisque la suite est équilibrée, tout autre bloc de 0 dans la suite est soit de longueur l soit de longueur $l-1$ par maximalité de l. Notons r le nombre de blocs de 0 qui sont de longueur $l-1$. On a $r < s$ et le nombre total de 0 dans la ϵ donne la relation :

$$s(k-1) = sl - r,$$

d'où :

$$k - 1 = l - \frac{r}{s}.$$

Alors, si $r \neq 0$, on obtient $l-1 = k-1$ en prenant la partie entière. Dans ce cas, il y a précisément $s(l-1)$ termes 0 dans la suite, ce qui signifie que tous les blocs de 0 sont nécessairement de longueur $l-1$, absurde.

Donc $r = 0$ et tous les blocs de 0 dans la suite ϵ sont de longueur l, d'où la première implication par la proposition 5.4.3.

Considérons maintenant l'autre cas, i.e. supposons que le dernier bloc de 0 dans la suite ne soit pas maximal. La longueur d'un bloc de 0 entre deux 1 consécutifs dans la suite ϵ est toujours l ou $l-1$.

Pour déterminer la longueur du dernier bloc de 0, il faut prendre en compte le fait que $\epsilon_p = 0$ et que $\epsilon_{p+1} = \epsilon_1 = 1$ dans la suite $\{\epsilon_i\}_{i\in\mathbb{Z}}$ entière qui est encore équilibrée. Cette longueur est donc soit $l-1$ soit $l-2$. Mais si l'on note r le nombre de blocs de longueur $l-1$ dans la suite ϵ et q celui des blocs de longueur $l-2$, on a les relations :

$$0 \leq r \leq s-1 \text{ and } 0 \leq q \leq 1,$$

avec De plus, $r + q \leq s - 1$ puisqu'il y a au moins un bloc de 0 de longueur l et au moins un (le dernier précisément) qui n'est pas de longueur l. Alors, en calculant le nombre total de 0 dans la suite ϵ, on obtient l'égalité :

$$s(k-1) = sl - r - q,$$

ce qui entraîne :

$$k - 1 = \lfloor l - \frac{r+q}{s} \rfloor$$

et donc :

$$k - 1 = l - 1.$$

Le nombre total de 0 est donc $s(k-1) = sk - (r+q)$, d'où $r + q = s$, ce qui est impossible.

Ainsi, on vient de montrer que lorsque s divise $p-1$, tous les blocs de 0 sont de même longueur l. Cette longueur est nulle uniquement pour $s = p-1$. La suite ϵ est donc de la forme $(10...0)^s$ et O_L est libre sur A, une nouvelle fois d'après la proposition 5.14. $\diamond$

5.6 L'embedding dimension de A

Ce dernier paragraphe met en valeur la notion d'embedding dimension pour un anneau local noethérien. Cette notion conduira à une nouvelle condition, purement algébrique cette fois, pour que O_L soit libre sur l'ordre associé à l'extension L/K.

Précisément, d'après la proposition 5.10, l'ordre A est un anneau local noethérien et à ce titre possède une *embedding dimension*, d'où l'équivalence des propriétés (i) et (iv) du théorème 5.2 :

Proposition 5.16. *L'anneau de valuation O_L est un module libre sur A si et seulement si l'embedding dimension de A est inférieure ou égale à 3.*

Le sous-paragraphe 5.6.1 est un rappel sur la dimension d'un anneau local noethérien. Le sous-paragraphe 5.6.2 concerne plus précisément ce qu'on appelle *embedding dimension* pour l'ordre A, dimension qu'il s'agit de traduire en termes combinatoires à partir de la notion de points spéciaux associés à l'extension L/K. Dans le dernier sous-paragraphe, un simple dénombrement de ces points spéciaux permettra alors de montrer la proposition 5.16, ce qui complètera la preuve du théorème 5.2.

5.6.1 L'embedding dimension d'un anneau local noethérien

Nous donnons ici une brève présentation de l'embedding dimension pour un anneau local noethérien.

Théorie de la dimension. La dimension d'un anneau R, parfois appelée dimension de Krull, est définie comme la longueur maximale des chaînes d'idéaux premiers de R. Ici, la longueur d'une chaîne $P_0 \subset P_1 \subset ... \subset P_r$ contenant $r+1$ idéaux premiers distincts est r. Rappelons que l'anneau R n'est pas un idéal premier et que l'idéal (0) est premier seulement lorsque R est intègre.

Ce maximum peut donc être infini, même pour un anneau noethérien. Cependant, si R est local et noethérien, alors sa dimension est nécessairement finie (cf. e.g. [9], Chap.11, cor.11.11). C'est pourquoi on se restreint en général à l'étude de la dimension pour les anneaux locaux noethériens et déjà la théorie est très riche.

Exemple 5.3. *Tout anneau intègre est de dimension ≥ 0. Les anneaux intègres de dimension 0 sont précisément les corps. Plus généralement, les anneaux artiniens sont de dimension 0.*

Maintenant, si l'anneau R est intègre et principal, il est de dimension 1 car toute chaîne d'idéaux premiers est nécessairement de la forme $(0) \subset (\pi)$ pour un idéal premier (π). Typiquement, $\dim O_K = 1$ et sa seule chaîne d'idéaux premiers est $(0) \subset \mathfrak{p}_K$.

Une propriété fondamentale pour la dimension d'un anneau est qu'elle n'est pas affectée par les éléments nilpotents :

Proposition 5.17. *Soit R un anneau local noethérien et soit I un idéal nilpotent. Alors, $\dim R = \dim(R/I)$.*

En particulier, si l'on considère l'anneau réduit de l'ordre A associé à L/K, cela donne :

$$\dim A_{\text{red}} = \dim A.$$

Alors, $\dim A = 1$ puisque $A_{\text{red}} = 0_K$.

Nous donnons ensuite plusieurs caractérisations équivalentes de la dimension d'un anneau local noethérien R. Pour cela, rappelons qu'un idéal $\mathfrak{a}$ de R est dit $\mathfrak{m}$-primaire si son radical, défini par $r(\mathfrak{a}) = \{x \in R \,:\, \exists n > 0 \; x^n \in \mathfrak{a}\}$, est $\mathfrak{m}$. On a :

Proposition 5.18. *Soit R un anneau local noethérien d'idéal maximal $\mathfrak{m}$. Alors, la dimension de R est le plus petit nombre de générateurs d'un idéal $\mathfrak{m}$-primaire de R.*

Dans ([20] , cor. 10.7), on trouve la reformulation suivante :

Proposition 5.19. *Soit R un anneau local noethérien d'idéal maximal $\mathfrak{m}$. Alors,* $\dim R$ *est le plus petit entier d pour lequel il existe d éléments $x_1, ..., x_d \in \mathfrak{m}$ tels que :*

$$\mathfrak{m}^n \subset (x_1, ..., x_d), \quad \textit{pour, } n >> 0.$$

On dit que les éléments $x_1, ..., x_d$ forment un *système de paramètres* pour A.

Il existe encore d'autres caractérisations, en particulier celles qui sont liées aux polynômes de Hilbert-Samuel dans le contexte des anneaux gradués (cf. [20], Chap.12 et [43], Chap.5, §13).

Notons enfin qu'il existe une interprétation géométrique de la théorie de la dimension : le chapitre 8 de [20] en offre une agréable lecture.

Embedding dimension. Si R est un anneau local noethérien d'idéal maximal $\mathfrak{m}$ et de corps résiduel κ, le R-module $\mathfrak{m}/\mathfrak{m}^2$ est annulé par $\mathfrak{m}$: c'est donc un espace vectoriel sur κ. Or, $\mathfrak{m}$ est de type fini puisque R est noethérien. Alors, modulo $\mathfrak{m}^2$, les classes d'un ensemble de générateurs de $\mathfrak{m}$ engendrent $\mathfrak{m}/\mathfrak{m}^2$ par le lemme de Nakayama. La dimension $\dim_\kappa \mathfrak{m}/\mathfrak{m}^2$ est donc finie. Cette remarque nous conduit à la notion d'embedding dimension :

Définition 5.1 (Embedding dimension)**.** *Soit R un anneau local noethérien d'idéal maximal $\mathfrak{m}$ et de corps résiduel κ. On appelle embedding dimension de l'anneau R la dimension sur κ de l'espace vectoriel $\mathfrak{m}/\mathfrak{m}^2$. Cette dimension est notée embed R :*

$$\textit{embed } R = \dim_\kappa \mathfrak{m}/\mathfrak{m}^2.$$

Le terme *embedding dimension* semble avoir été introduit par Matsumura. On a la relation

Proposition 5.20. $\dim R \leq$ *embed R.*

Preuve : Si $x_i \in \mathfrak{m}$, $1 \leq i \leq s$, sont tels que leurs images dans $\mathfrak{m}/\mathfrak{m}^2$ forment une base de cet esace vectoriel sur κ, par le lemme de Nakayama ils engendrent $\mathfrak{m}$. D'où :

$$\dim_\kappa(\mathfrak{m}/\mathfrak{m}^2) = s \geq \dim R,$$

d'après la proposition 5.19. ◇

Il existe un lien plus précis entre la dimension de Krull et l'embedding dimension pour un anneau local noethérien (nous l'énonçons pour l'ordre associé A même s'il existe un énoncé plus général) :

Proposition 5.21. *L'embedding dimension de l'ordre A associé à l'extension est $d+1$ si d est le nombre minimal d'éléments de $\mathfrak{m}_A$ qui engendrent A comme O_K-algèbre.*

Anneaux locaux réguliers. Nous fermons ces rappels par une courte présentation de la notion d'anneau local régulier. Un anneau local R est dit *régulier* si $\dim R =$ embed R. En particulier, si l'anneau est De plus, noethérien, alors R est régulier lorsque son idéal maximal $\mathfrak{m}$ peut être engendré par exactement $\dim R$ éléments en tant que R-module. Dans ce cas, on appellera *système régulier* de paramètres pour R, un système minimal de paramètres engendrant $\mathfrak{m}$.
Un exemple d'anneau local régulier est donné par l'anneau des séries formelles $k[[x_1, ..., x_d]]$ sur un corps k. Un tel anneau est de dimension d d'après ([20], Chap.10, cor. 10.13).

Pour finir, donnons le résultat suivant que l'on trouvera dans ([44], Chap.14, §3) :

Théorème 5.3. *Tout anneau local régulier est intègre.*

Dans notre contexte, l'ordre associé A n'est pas intègre puisqu'il contient des éléments nilpotents, cet anneau n'est donc pas régulier.

5.6.2 Embedding dimension de A et points spéciaux

Dans ce sous-paragraphe, il s'agit d'exprimer l'embedding dimension de l'ordre A dans le langage combinatoire. Plus précisément, nous allons montrer que l'embedding dimension de A se calcule en comptant le nombre de *points spéciaux* associés à la suite ϵ.

Points spéciaux. Nous allons introduire la notion de *points spéciaux* en relation avec les minima m_i de la suite ϵ :

$$\forall i,\ m_i = \inf_j \{\epsilon_j + ... + \epsilon_{j+i-1}\}.$$

Cette nouvelle terminologie fait suite à l'inégalité suivante obtenue par minimalité des m_i :

$$\forall i,\ \forall j < i,\ m_i \geq m_j + m_{i-j}.$$

Cette inégalité signifie que le plus petit poids d'un bloc de longueur i dans la suite ϵ est supérieur ou égal à la somme des plus petits poids des blocs de longueurs j et $i-j$ respectivement. Plus généralement, si a, b et c sont trois entiers positifs tels que $ab + c \in \{1, ..., p-1\}$, on a :

$$m_{ab+c} \geq a m_b + m_c.$$

Par la suite, on appellera *points spéciaux* les indices i pour lesquels l'inégalité est toujours stricte. Plus précisément :

Définition 5.2. *Un indice i, $1 \leq i \leq p-1$, est un point spécial pour la suite ϵ si :*

$$\forall j < i,\ m_i > m_j + m_{i-j}.$$

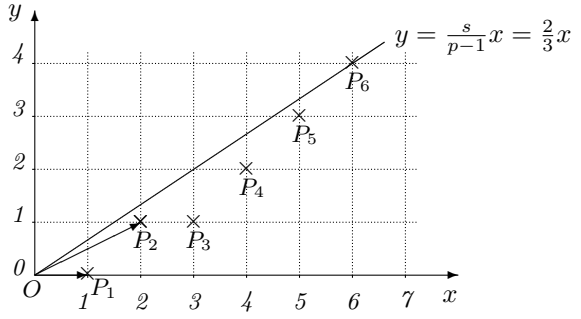
Nous noterons $\mathcal{S}$ l'ensemble des points spéciaux dans $\{1, ..., p-1\}$.

Exemple 5.4. *L'indice $i = 1$ est toujours un point spécial, quelques soient les valeurs prises par la suite ϵ. En outre, si tous les ϵ_i valent 1, alors 1 est l'unique point spécial puisque pour tout i on alors $m_i = i$, i.e. $m_i = m_1 + m_{i-1}$.*

Maintenant, si au moins un des ϵ_i est nul, soit l la longueur du plus grand bloc de 0 dans le suite ϵ. Alors les indices $i = 1$ et $i = l + 1$ sont les deux premiers points spéciaux, ils correspondent précisément aux minima $m_1 = ... = m_l = 0$ et $m_{l+1} = 1$.

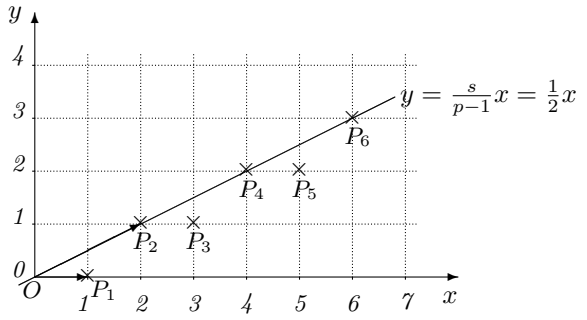
Interprétation graphique. Graphiquement, si P_i est le point de coordonnées (i, m_i) dans un repère (O, x, y), alors i est un point spécial si et seulement si le vecteur $\overrightarrow{OP_i}$ ne peut pas être atteint comme somme de deux vecteurs $\overrightarrow{OP_j}$ et $\overrightarrow{OP_{i-j}}$, avec $j < i$. Illsutrons ceci à partir des exemples 5.1 et 5.2 :

Exemple 5.5. *Considérons d'abord l'exemple $K = \mathbb{F}_p((T))$, avec $p = 7$ et $L = K(\alpha)$, où $\alpha^7 - \alpha = T^{-4}$. D'après l'exemple 5.1, la suite ϵ correspondante est $\{110101\}$. D'où les minima m_i : $m_1 = 0$, $m_2 = 1 = m_3$, $m_4 = 2$, $m_5 = 3$ et $m_6 = 4$. Graphiquement, cela donne :*



On a donc ici exactement quatre points spéciaux, ce sont les indices : 1, 2, 5 *et* 6. *Pour les autres indices, chaque vecteur* $\overrightarrow{OP_i}$ *est bien du type* $\overrightarrow{OP_j}+\overrightarrow{OP_{i-j}}$ *pour un certain* $j < i$ *:* $\overrightarrow{OP_3} = \overrightarrow{OP_1}+\overrightarrow{OP_2}$ *et* $\overrightarrow{OP_4} = \overrightarrow{OP_2} + \overrightarrow{OP_2}$.
On observe aussi que tous les points P_i *sont dessous ou sur la droite d'équation* $y = \frac{s}{p-1}x$. *Ceci est un fait plus général que l'on pourrait montrer facilement.*

Considérons maintenant le cas $K = \mathbb{F}_p((T))$, *pour* $p = 7$ *et* $L = K(\alpha)$, *avec* $\alpha^7 - \alpha = T^{-3}$. *D'après l'exemple 5.2, la suite* ϵ *correspondante est la suite* 101010, *associée aux minima :* $m_1 = 0$, $m_2 = 1 = m_3$, $m_4 = 2 = m_5$ *et* $m_6 = 3$. *D'où le graphe des points* P_i (i, m_i) *:*



Nous avons précisément deux points spéciaux, qui sont 1 *et* 2. *Une nouvelle fois, on voit facilement que pour chaque autre indice, le vecteur* $\overrightarrow{OP_i}$ *s'écrit comme une somme* $\overrightarrow{OP_j} + \overrightarrow{OP_{i-j}}$ *avec* $j < i$.
Maintenant, on peut aussi observer que chaque vecteur $\overrightarrow{OP_i}$ *est combinaison linéaire des vecteurs* $\overrightarrow{OP_1}$ *et* $\overrightarrow{OP_2}$ *seulement. Ceci est un résultat plus général qui mérite d'être énoncé, c'est la proposition qui suit.*

Suite aux exemples précédents, nous citons le résultat suivant :

Proposition 5.22. *Pour tout* i, $1 \leq i \leq p-1$, *il existe des entiers positifs* $\omega_j^{(i)}$ *tel que le vecteur* $\overrightarrow{OP_i}$ *soit combinaison linéaire :*

$$\overrightarrow{OP_i} = \sum_{j\in\mathcal{S}, j<i} \omega_j^{(i)} \overrightarrow{OP_j},$$

avec :

$$\sum_{j\in\mathcal{S}, j<i} \omega_j^{(i)} j = i.$$

Preuve : Notons toujours l la longueur du plus grand bloc de 0 dans la suite ϵ. Si $l = 0$, 1 est l'unique point spécial de la suite. De plus, pour tout i on $m_i = i$ et donc $\overrightarrow{OP_i} = i\overrightarrow{OP_1}$.
On se restreint ensuite au cas où $l \geq 1$. Si i est un point spécial, la proposition est évidente. Sinon, il existe $j < i$ tel que $m_i = m_j + m_{i-j}$. Il s'agit donc de montrer la proposition pour le plus petit indice qui n'est pas un point spécial, nous noterons i_s cet indice. La preuve complète se fait alors facilement par récurrence sur i.
Si $l = 1$, alors 1 et 2 sont les deux premiers points spéciaux et $i_s = 3$, les minima étant $m_3 = m_2 = 1$ et $m_1 = 0$. On a donc $\overrightarrow{OP_3} = \overrightarrow{OP_2} + 2\overrightarrow{OP_3}$.
Si $l > 1$, les deux premiers points spéciaux sont 1 et $l + 1 \geq 3$. Alors $i_s = 2$ car $m_2 = m_1 = 0$, d'où $\overrightarrow{OP_2} = 2\overrightarrow{OP_1}$, ce qu'il fallait démontrer. ◇

L'embedding dimension de l'ordre A**.** Nous avons déjà écrit une condition pour que O_L soit libre sur A en terme de propriété combinatoire que doit satisfaire la suite ϵ. Pour prouver une autre condition liée à l'embedding dimension de A, nous allons encore utiliser des arguments

combinatoires mais qui sont cette fois donnés par les points spéciaux associés à l'extension L/K. La proposition qui suit est une relation entre l'embedding dimension de A et le nombre de points spéciaux, c'est le résultat essentiel qui permettra de montrer la condition (iv) du théorème 5.2 :

Proposition 5.23. *L'embedding dimension de l'ordre A associé à l'extension L/K est donnée par la relation :*

$$\textit{embed } A = 1 + \textit{card } S,$$

où S est l'ensemble des points spéciaux de $\{1, ..., p-1\}$.

Preuve : Il s'agit d'étudier la dimension sur κ de l'espace vectoriel $\mathfrak{m}_A/\mathfrak{m}_A^2$. Pour cela, précisons d'abord les structures de $\mathfrak{m}_A$ puis de $\mathfrak{m}_A^2$ comme O_K-modules libres de rang p. Plus précisément, nous allons construire une O_K-base de $\mathfrak{m}_A^2$ à partir des points spéciaux associés à L/K.
D'après le corollaire 5.3, une O_K-base de $\mathfrak{m}_A$ est donnée par la famille :

$$T, \frac{X}{T^{m_1}}, \frac{X^2}{T^{m_2}}, \cdots, \frac{X^{p-1}}{T^{m_{p-1}}},$$

où les m_i sont les minima $\inf_j\{\epsilon_j + ... + \epsilon_{j+i-1}\}$.
Maintenant, l'idéal $\mathfrak{m}_A^2$ est aussi un sous-O_K-module libre de A de rang p puisque $\mathfrak{m}_A/\mathfrak{m}_A^2$ est fini, i.e. $\text{rank}_{O_K}\mathfrak{m}_A^2 = \text{rank}_{O_K}\mathfrak{m}_A = p$.
La méthode qui suit permet alors de construire une base sur O_K pour $\mathfrak{m}_A^2$ en partant de la O_K-base de $\mathfrak{m}_A$ donnée plus haut. D'abord, on prend T^2 et on le complète en une base de $\mathfrak{m}_A^2$ de la façon suivante. Pour chaque i, i allant de 1 à $p-1$, si i est un point spécial, on complète avec $T\dfrac{X^i}{T^{m_i}}$, sinon avec $\dfrac{X^i}{T^{m_i}}$. Montrons qu'ainsi on obtient bien une O_K-base de $\mathfrak{m}_A^2$, c'est-à-dire que $\mathfrak{m}_A^2$ est précisément le module M libre sur O_K défini par :

$$M := T^2O_K \oplus \bigoplus_{i\notin\mathcal{S}} \frac{X^i}{T^{m_i}} \oplus \bigoplus_{i\in\mathcal{S}} T\frac{X^i}{T^{m_i}}.$$

D'abord, il est facile de voir que T^2 ainsi que les $T\dfrac{X^i}{T^{m_i}}$, pour $i \in \mathcal{S}$, sont dans $\mathfrak{m}_A^2$. De plus, si i n'est pas un point spécial, il existe $j < i$ tel que $m_i = m_j + m_{i-j}$ et donc $\dfrac{X^i}{T^{m_i}} = \dfrac{X^j}{T^{m_j}}\dfrac{X^{i-j}}{T^{m_{i-j}}}$ appartient aussi à $\mathfrak{m}_A^2$. D'où l'inclusion $M \subset \mathfrak{m}_A^2$.

Pour l'inclusion inverse, cela revient à montrer que tous les produits $\dfrac{X^i}{T^{m_i}}\dfrac{X^j}{T^{m_j}}$ sont dans M. A partir de l'écriture :

$$\frac{X^i}{T^{m_i}}\frac{X^j}{T^{m_j}} = \frac{X^{i+j}}{T^{m_i+m_j}},$$

on distingue alors deux cas :

- soit $m_{i+j} = m_i + m_j$, i.e. $i+j$ n'est pas un point spécial et donc $\dfrac{X^{i+j}}{T^{m_i+m_j}}$ est dans la O_K-base de M.

- soit $m_{i+j} > m_i + m_j$, i.e. $\dfrac{X^{i+j}}{T^{m_i+m_j}}$ est vu comme élément de $O_K.T\dfrac{X^{i+j}}{T^{m_{i+j}}}$ qui est encore inclus dans M, que $i+j$ soit ou non un point spécial.

Enfin, il est clair que les éléments T^2, $\dfrac{X^i}{T^{m_i}}$ pour $i \notin \mathcal{S}$ et $T\dfrac{X^i}{T^{m_i}}$ pour $i \in \mathcal{S}$, sont linéairement indépendants sur O_K. Ils forment donc une base de $\mathfrak{m}_A^2$ sur O_K et l'on a bien $\mathfrak{m}_A^2 = M$.

En conséquence, on a l'égalité :

$$\mathfrak{m}_A/\mathfrak{m}_A^2 = \kappa \oplus \bigoplus_{i\in\mathcal{S}} \kappa$$

d'où :

$$\dim_\kappa \mathfrak{m}_A/\mathfrak{m}_A^2 = 1 + \text{card } \mathcal{S},$$

ce qui montre la proposition. ◇

5.6.3 L'équivalence $(i) \Leftrightarrow (iv)$

La proposition 5.23 précédente est la traduction de la notion algébrique d'embedding dimension pour l'ordre A dans le langage purement combinatoire des points spéciaux. Cela nous permet de montrer la proposition 5.16 en dénombrant simplement les points spéciaux de la suite ϵ.

On a de plus, la simplification suivante. Notons en effet l'égalité $\dim A = \dim A_{red}$ puisque la dimension d'un anneau n'est pas affectée par les nilpotents. Alors, d'après la proposition 5.10, $\dim A = \dim O_K = 1$, car O_K est principal. Cela signifie que la seule chaîne d'idéaux premiers dans A est $\sqrt{0} \subset \mathfrak{m}_A$, où $\sqrt{0} = \text{nil}(A)$ est le nilradical de A. En particulier, embed$(A) \geq 1$.

Or, embed(A) ne peut valoir 1 car sinon A serait régulier, ce qui est impossible. L'embedding dimension de A est donc supérieure ou égale à 2 et la proposition 5.16 revient à montrer que O_L est libre sur A si et seulement si embed(A) vaut 2 ou 3. Voici sa preuve. Là encore, l'argument utilisé est purement combinatoire :

Preuve : Supposons d'abord que O_L est libre sur A.Soit donc l la longueur constante de chaque bloc de 0 dans la suite ϵ (cf. sous-paragraphe 5.4.3). Si $l = 0$, tous les ϵ_i valent 1 et l'on sait qu'alors $i = 1$ est le seul point spécial associé à la suite, d'où embed$A = 2$.

Maintenant, si $l \geq 1$, alors 1 et $l+1$ sont les deux premiers points spéciaux, correspondant aux minima $m_1 = ... = m_l = 0$ et $m_{l+1} = 1$. Quant aux autres m_i, puisque chaque indice i s'écrit $i = k(l+1)+r$ avec $k \geq 0$ et $0 \leq r \leq l$, grâce à la division euclidienne par $l+1$, on a $m_i = m_{k(l+1)+r} = m_{k(l+1)} + m_r = k$ puisque la suite ϵ est du type $(10...0)^s$ avec précisément l termes 0 entre deux 1 consécutifs. Alors, si $r \neq 0$, l'indice i n'est pas un point spécial puisque $m_i = m_r + m_{k(l+1)}$. Si $r = 0$ avec $k > 1$, i n'en est pas un non plus puisque cette fois $m_i = 1 + (k-1) = m_{l+1} + m_{(k-1)(l+1)}$. Ainsi, 1 et $l+1$ sont les deux seuls points spéciaux de la suite ϵ, d'où card $\mathcal{S} = 2$, i.e. embed $A = 3$.

Réciproquement, si embed $A = 2$, cela signifie qu'il n'y a qu'un seul point spécial et donc que tous les ϵ_i valent 1. L'anneau O_L est donc libre sur A d'après la proposition 5.14.

Enfin, si embed $A = 3$, notons l la longueur du plus grand bloc de 0 dans la suite ϵ. Par la proposition 5.23, il y a exactement deux points spéciaux qui sont 1 et $l+1$, avec $m_1 = ... = m_l = 0$ et $m_{l+1} = 1$. Montrons alors que pour tout i on a $m_i = k_i$ où k_i est le quotient dans la division euclidienne de i par $(l+1)$. Cette égalité est évidente pour $i \leq l+1$. Si $i > l+1$, on écrit $i = k_i(l+1)+r$, avec $k_i \geq 1$ et $0 \leq r \leq l$. D'une part, on a $m_i \geq k_i m_{l+1} + m_r = k_i$ par minimalité des m_i. D'autre part, d'après la proposition 5.22, il existe deux entiers positifs ω et ζ tels que $\overrightarrow{OP_i} = \omega\overrightarrow{OP_1} + \zeta\overrightarrow{OP_{l+1}}$, avec $\omega + \zeta(l+1) = k(l+1) + r$. Cela entraîne respectivement que $m_i = \beta$ et $\beta \leq k_i$, d'où $m_i = k_i$.

En particulier, $m_i \neq m_{i+1}$ si et seulement si $(l+1)$ divise $i+1$.

Or, $m_{p-1} = s$ puisque la suite ϵ contient exactement s termes 1. On a aussi $m_{p-2} = s-1$ car $\epsilon_1 = 1$. Alors $(l+1)$ divise $p-1$ et d'après ce qui précède $p-1 = s(l+1)$, donc O_L est encore libre sur A par la proposition 5.15. ◇

Bibliographie

[1] A. Aiba, *Carlitz modules and Galois module structure*, J. Number Theory **62** (1997), 213-219.

[2] A. Aiba, *Carlitz modules and Galois module structure II*, J. Number Theory **68** (1998), 29-35.

[3] A. Aiba, *Artin-Schreier extensions and Galois module structure*, J. Number Theory, **102** (2003), 118-124.

[4] A.A. Albert, *Cyclic fields of degree p^n over F of characteristic p*, Bull. Am. Math. Soc., **40** (1934), 625-631.

[5] E. Artin, *Kennzeichnung des Körpers der reellen algebraischen Zahlen*, Abh. Math. Sem. Hamburg, **3** (1924), 319-323.

[6] E. Artin, *Beweis des allgemeinen Reziprozitätsgesetzes*, Abh. Math. Sem. Hamburg **5** (1927), $353 - 363$.

[7] E. Artin, O.Schreier, *Eine Kennzeichnung der reell algeschlossenen Körper*, Abh. Math. Sem. Hamburg **5** (1927), $225 - 231$.

[8] E. Artin, J.Tate, *Class field theory*, New York - Amsterdam (1968).

[9] M.F. Atiyah, I.G. Macdonald, *Introduction to Commutative Algebra*, Addison-Wesley (1969).

[10] A.M. Bergé, *Arithmétique d'une extension galoisienne à groupe d'inertie cyclique*, Ann. Inst. Fourier, **28**.4, Grenoble (1978), 17-44.

[11] F. Bertrandias, *Sur les extensions cycliques de degré p^n d'un corps local*, Acta Arithmetica, **34** (1979)

[12] F. Bertrandias, M.-J. Ferton, *Sur l'anneau des entiers d'une extension cyclique de degré premier d'un corps local*, C. R. Acad. Sci. Paris Sér. A **274** (1972), 1330-1333.

[13] F. Bertrandias, J.-P. Bertrandias, M.-J. Ferton, *Sur l'anneau des entiers d'une extension cyclique de degré premier d'un corps local*, C. R. Acad. Sci. Paris Sér. A **274** (1972), 1388-1391.

[14] J. Borger, *Conductors and the moduli of residual perfection*, Mathematische Annalen, **329**.1 (2004), 1-30.

[15] N. Bourbaki, *General Topology*, Springer (1989).

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

[17] N.P. Byott, *Some self-dual local rings of integers not free over their associated orders*, Math. Proc. Cambridge Philos. Soc. **110** (1991), 5-10.

[18] P. Cassou-Noguès, M.J. Taylor, *Elliptic Functions and Rings of Integers*, Progress in Mathematics, **66**, Birkhäuser (1987).

[19] B. Deschamps, *Théorie de Galois et groupes profinis*, lecture given at the University of Lyon (France) (2000).

[20] D. Eisenbud, *Commutative Algebra with a view toward algebraic geometry*, Graduate Texts in Mathematics **150**, Springer (1995).

[21] G.G. Elder, *Galois module structure of ideals in widly ramified cyclic extensions of degree p^2*, Ann. Inst. Fourier, **45**.3, Grenoble (1995), 625-647, Corrigendum, Ann. Inst. Fourier, **48**.2, Grenoble (1998), 23-38..

[22] I.B. Fesenko, S.V. Vostokov, *Local Fields and Their Extensions*, Translation of Mathematical Monographs **121**, Amer. Math. Soc. (1993).

[23] M. Garuti, *Linear sytems attached to cyclic inertia* (Berkeley, CA, 1999), 377-386, Proc. Sympos. Pure Math., **70**, Amer. Math. Soc., Providence, RI (2002).

[24] G. Gras, *Class Field Theory, From theory to practice*, Springer Monographs in Mathematics, Springer-Verlag (2003).

[25] H. Hasse, *Theorie der relativ-zyklischen algebraischen Funktionenkörper, insbesondere bei endlichem Konstantenkörper*, J. Reine Angew. Math. **172** (1934), 37-54.

[26] M. Hazewinkel, *Abelian extensions of local fields*, *Ph.D. thesis*, Universiteit Nijmegen, Holland (1969).

[27] H. Helmut, E. Witt, *Zyklische unverzweigte erweiterungskorper von primzahlgrad p über einen algebraischen funktionkörper der characteristic p*, Monatsh. Math, **43** (1936), 477-492.

[28] L. Hesselholt, *Galois cohomology of Witt vectors of algebraic integers*, Math.Proc.Camb.Phil.Soc., **137** (2004), 551-557.

[29] M.Honsbeek, *Radical extensions and Galois groups*, Ph.D. thesis, Radboud Universiteit Nijmegen, Holland (2005).

[30] H. Ichimura, *On normal integral bases of unramified abelian p-extensions over a global function field of characteristic p*, Finite Fields and Their Applications, **10** (2004), 432-437.

[31] K. Iwasawa, *Local Class Field Theory*, Oxford Mathematical Monographs, Oxford Science Publications (1986).

[32] K. Kato, *Swan Conductors with Differential Values*, Advanced Studies in Pure Mathematics **12** (1987), Galois Representations and Arithmetic Algebraic Geometry, 315-342.

[33] K. Kato, *Swan Conductors for characters of degree one in the imperfect residue field case*, Algebraic K-theory and algebraic number theory, ed. M. Stein and R.K. Dennis, Contemp. Math., **83**, Amer. Math. Soc., Providence (1989), 101-131.

[34] H. Koch, *Galois theory of p-extensions*, Springer Monographs in Mathematics, Springer (2002).

[35] S. Lang, *Algebra*, Addison-Wesley, third edition (1993).

[36] H.W. Lenstra, *Galois Theory for schemes*, University of California, second printing (1997).

[37] G. Lettl, *Note on a theorem of A.Aiba*, Journal of Number Theory, to appear.

[38] D.J. Madden, *Arithmetic in Generalized Artin-Schreier Extensions of $k(x)$*, Journal of Number Theory, **10** (1978), 303-323.

[39] R. MacKenzie, G. Whaples, *Artin-Schreier equations in characteristic zero*, Am. J. Math. **78** (1952), 348-366.

[40] M.A. Marshall, *Ramification Groups of Abelian Local Field Extensions*, Can. J. Math. **23**, No. **2**, (1971), 271-281.

[41] J. Martinet, *Sur l'arithmétique des extensions galoisiennes à groupe de Galois diedral d'ordre $2p$*, Ann. Inst. Fourier, Grenoble, **19**,1 (1969), 1-80.

[42] J. Martinet, *Anneau des entiers d'une extension galoisienne considéré comme module sur l'algèbre du groupe de Galois*, Bull. Soc. Math. Fr., Mémoire **25**, (1971), 123-126.

[43] S. Matsuda, *On the Swan conductor in positive characteristic*, American Journal of Mathematics, **119** (19997), 705-739.

[44] H. Matsumura, *Commutative algebra*, Benjamin, New-York (1970).

[45] E. Maus, *Arithmetisch disjunkte Korper*, J. Reine. Angew. Math. **226** (1967), 184-203.

[46] E. Maus, *Die Gruppentheoretische Struktur der Verzweigungsgruppenreihen*, J. Reine. Angew. Math. 230 (1968), 1-28.

[47] E. Maus, *On the jumps in the series of ramification groups*, Bull. Soc. Math. France, Mémoire **25** (1971), 127-133.

[48] J. Neukirch, *Algebraic Number Theory*, Grundlehren **322**, Springer-Verlag (1999).

[49] J. Neukirch, A. Schmidt, K. Wingberg, *Galois cohomology of number fields*, Grundlehren **323**, Springer-Verlag (2000).

[50] O. Ore, *Abriss einer arithmetischen Theorie der Galoisschen Körper*, Parts 1 and 2, Mathematische Annalen, **100** (1928), 650-673, and **102** (1930), 283-304.

[51] I. Reiner, *Maximal Orders*, London Mathematical Society Monographs, New series **28**, Oxford science publications (2003).

[52] P. Ribenboim, *L'arithmétique des corps*, Hermann (1972).

[53] L. Ribes and P. Zalesskii, *Profinite groups*, A series of Modern Surveys in Mathematics, Volume **40**, Springer (2000).

[54] P. Roquette, *Class Field Theory in characteristic p. Its origin and development*, K. Miyake (ed.), Class Field Theory- Its Centenary and Prospect, Advanced Studies In Pure Mathematics, vol. **30**, Tokyo (2000), 549-631.

[55] H.L. Schmid, *Über das Reziprozitätsgesetz in relativ-zyklischen algebraischen Funktionenkörpern mit endlichem Konstantenkörper*, Math. Zeitschr. **40** (1935), 91-106.

[56] H.L. Schmid, *Zyklischen algebraische Funktionkörper vom Grade p^n über endlichem Konstantenkörper der Charakteristik p*, J. Reine Angew. Math. **175**, (1936), 108-123.

[57] H.L. Schmid, *Zur Arithmetik der zyklischen p-Körper*, J. Reine Angew. Math. **176** (1937), 161-167

[58] J.-P. Serre, *Sur les corps locaux à corps résiduel algébriquement clos*, Bull. Soc. Math. France **89** (1961), 105-154.

[59] J.-P. Serre, *Groupes algébriques et corps de classes*, Hermann, Paris (1959).

[60] J.-P. Serre, *Corps Locaux*, Hermann, Paris (1962). [English translation : *Local Fields*, Graduate Texts in Math. **67**, Springer, New York (1979)].

[61] J.-P. Serre, *Galois Cohomology*, Springer-Verlag (1996).

[62] V. Shabat, *Curves with many points*, Ph.D. Thesis, Universiteit van Amsterdam, Holland (2001).

[63] R.T. Sharifi, *Ramification groups of nonabelian Kummer extensions*, J. Number Theory, **65** (1997), 105-115.

[64] R.T. Sharifi, *On norm residue symbols and conductors*, J. Number Theory, **86** (2001), 196-209.

[65] R.T. Sharifi, *Determination of conductors from Galois module structure*, Mathematische Zeitschrift, **241** (2002), 227-245.

[66] S.S. Shatz, *Profinite groups, arithmetic and geometry*, Princeton university press and university of Tokyo press (1972).

[67] B. de Smit, *Ramification groups of local fields with imperfect residue class fields*, J. Number Theory, **44** (1993), 353-365.

[68] B. de Smit, *The different and differentials of local fields with imperfect residue fields*, Proc. Edin. Math. Soc., **40** (1997), 353-365.

[69] L. Spriano, *Well ramified extensions of complete discrete valuation fields with Applications to the Kato Conductor*, Canad. J. Math. Vol., **52**.6 (2000), 1269-1309.

[70] H. Stichtenoth, *Algebraic function fields and codes*, Springer-Verlag (1991).

[71] D. Subrao, *The p-rank of Artin-Schreier curves*, Manuscripta Mathematica, **16** (1975).

[72] O. Teichmüller, *Zerfallende zyklische p-Algebren*, J. Reine Angew. Math., **174** (1936), 157-160.

[73] L. Thomas, *Galois theory of inifinite Artin-Schreier extensions*, mémoire de DEA sous la direction de Bart de Smit, Université Lyon I (2002).

[74] E. Weiss, *Algebraic Number Theory*, Chelsea Publishing Company, second edition (1963).

[75] E. Witt, *Der Existenzstaz für abelsche Funktionenkörper*, J. Reine Angew. Math., **173** (1935), 43-49.

[76] E. Witt, *Zyklische Körper und Algebren der Charakteristik vom Grad p^n*, J. Reine Angew. Math., **174** (1936), 126-140.