Résumé

Le contexte de cette thèse est celui des corps de fonctions en caractéristique $p > 0$ et plus précisément celui des $\mathbb{Z}_p$-extensions géométriques de tels corps ; son but, l'obtention d'un critère alternatif (formulé en terme de semi-simplicité) à celui proposé par Villa-Salvador et Madan relativement à une formulation d'une conjecture de Gross dont on rappelle l'énoncé ci-après.

On se donne F un corps fini à q éléments ($q = p^r$ si p est un nombre premier $\neq 2$) et l'on désigne par K un corps de fonctions algébriques d'une variable de corps des constantes F. Soient K_∞/K une $\mathbb{Z}_p$-extension de groupe de Galois associé $\Gamma \simeq \mathbb{Z}_p$ et S l'ensemble, supposé *fini*, des places de K qui se ramifient (sauvagement) dans K_∞. Si l'on désigne par $\mathcal{C}_{\infty,S}(p)$ la p-partie du groupe des S-classes d'idéaux de K_∞ et que l'on considère l'action naturelle du groupe topologique Γ sur cette dernière, on peut se demander si le groupe des invariants pour cette action (vu comme sous-groupe de $\mathcal{C}_{\infty,S}(p)$), à savoir $\mathcal{C}_{\infty,S}(p)^\Gamma$, est d'ordre *fini*. C'est l'intitulé auquel nous nous intéressons.

Dans le *premier chapitre*, on se propose de revenir sur quelques-uns des résultats majeurs de la théorie d'Artin-Schreier-Witt dont l'objet est d'offrir une description explicite en caractéristique $p > 0$ des extensions cycliques de degré une puissance de p.

Le *chapitre* 2 présente une traduction dans le contexte des corps de fonctions de certains résultats fondamentaux de la théorie d'Iwasawa ainsi qu'une invitation, au travers d'une brève incursion au coeur de la théorie des modules de Carlitz, au pendant de la théorie cyclotomique. Ceci nous donnera en particulier l'occasion de nous attarder sur un candidat particulièrement séduisant pour jouer le rôle d'analogue de la $\mathbb{Z}_p$-extension cyclotomique des corps de nombres.

Au chapitre 3, nous présentons en détail le contenu de l'article de Villa et Madan cité plus haut et suggérons, au travers d'exemples, que si le critère exhibé est original et astucieux, il peut malgré tout se révéler difficile d'application au point peut-être de nécessiter une reformulation .

Enfin le *dernier chapitre* propose de plonger la situation initiale dans un cadre métabélien et, à la lumière d'un article de Greenberg, d'établir un critère suffisant de non-semi-simplicité découlant de la comparaison "à la limite" des comportements des suites exactes des classes ambiges et des genres que l'on aura eu soin auparavant d'établir.

Mots-clés : Corps de fonctions, $\mathbb{Z}_p$-extensions géométriques, Conjecture de Gross, Théorie d'Iwasawa, Semi-simplicité.

Abstract

Suppose K to be a congruence function field and denote by $\mathbb{K}_\infty/K$ a geometric $\mathbb{Z}_p$-extension. Villa-Salvador and Madan, using Artin-Schreier-Witt theory, give a necessary and sufficient condition for the finiteness of the p-part $\mathcal{C}_{\infty,S}(p)^\Gamma$ wich is not more than the formulation of the analogue of a conjecture of Gross in the function field case.

Now, considering the metabelian case, we use Greenberg's works on p-adic representation and the theory of characters to obtain another criterion for the finiteness of $\mathcal{C}_{\infty,S}(p)^\Gamma$ in terms of semi-simplicity.

Keywords : Function fields theory, Geometric $\mathbb{Z}_p$-extensions, Gross conjecture, Iwasawa theory, Semi-simplicity.

Karen BRANDIN **Autour d'une conjecture de Gross pour les corps de fonctions** **2006**

$N°$ d'ordre : 3159

THÈSE

présentée à

L'UNIVERSITÉ BORDEAUX I

ÉCOLE DOCTORALE DE MATHÉMATIQUES ET INFORMATIQUE

par **Karen BRANDIN**

POUR OBTENIR LE GRADE DE

DOCTEUR

SPÉCIALITÉ : **Mathématiques Pures**

****

Autour d'une conjecture de Gross pour les corps de fonctions

****

Soutenue le 26 Juin 2006 à l'Institut de Mathématiques de Bordeaux

Après avis de :

B. ANGLES	Professeur, Université de Caen	**Rapporteur**
C. MAIRE	Professeur, Université Toulouse 2	**Rapporteur**

Devant la commission d'examen composée de :

B. ANGLES	Professeur, Université de Caen	
J.F. JAULENT	Professeur, Université Bordeaux I	**Directeur**
C. MAIRE	Professeur, Université Toulouse 2	
J. QUEYRUT	Professeur, Université Bordeaux I	
F. SORIANO-GAFIUK	Maître de Conférences, Université Paul Verlaine (Metz)	
A. THIERY	Maître de Conférences, Université Bordeaux I	

- 2006 -

Remerciements ...

Je remercie *Jean-François Jaulent* de m'avoir permis de poursuivre en thèse me permettant ainsi de réaliser un rêve et d'avoir attiré mon attention sur un travail rédigé en collaboration avec J. Sands grâce auquel j'ai pu remonter le fil de la semi-simplicité découvrant par là-même certains articles particulièrement éclairants de Caroll et Kisilevsky.

Je remercie vivement mes rapporteurs *Bruno Anglès* et *Christian Maire* qui ont accepté sans hésitation ni mouvement d'humeur de remplir le tour de force qui consistait à construire un rapport en un temps record. J'ai été tout au long de ma thèse sensible à la bienveillance que m'a manifestée B. Anglès, rompant mon isolement en me permettant de suivre l'évolution de son travail et de ses centres d'intérêts qui sont pour moi autant de sources d'inspiration.
Christian Maire, par sa curiosité, sa gentillesse mais aussi ses nombreuses questions, remarques et commentaires aura largement contribué à l'amélioration de la rédaction de cette thèse quand le courage me manquait de modifier les choses.

Je remercie *Jacques Queyrut* (aujourd'hui conscient du danger d'être matinal ...), *Florence Soriano-Gafiuk* et *Alain Thiéry* (dont j'avais eu le plaisir de suivre les travaux dirigés à l'occasion d'un module de maîtrise) d'avoir rendu cette soutenance de thèse possible en acceptant de participer à mon Jury et en lui donnant une tonalité dynamique et chaleureuse.

Les mots me manquent décidemment pour exprimer sans rien omettre tout ce que *Philippe Cassou-Noguès* apporte de richesse aux étudiants qui comme moi ont eu la chance de croiser sa route avant de la suivre. Si je me fais toute petite devant un chercheur passionné et passionnant dont je ne fais malheureusement que soupçonner l'étendue, l'originalité et la diversité des travaux, je souhaite ici rendre un hommage appuyé et ému à l'être humain, ce pédagogue talentueux et humble qui ne semble jamais chercher à emprunter d'autres voies pour convaincre son auditoire que celle sur laquelle le plus grand nombre pourra l'accompagner.

La marche du temps n'y fait rien, je me souviens aujourd'hui encore de mon premier cours avec *Alain Hénaut*, de l'énergie débordante et revigorante qui émanait de sa personne qu'il n'essayait en aucun cas de ménager, de cette volonté de convaincre, d'éveiller la curiosité qui je crois ne l'a jamais quitté. Même si la vie n'est pas toujours juste et que le retour se fait parfois longtemps attendre, je voudrais lui dire, je voudrais vous dire Mr Hénaut que "nous" (Martin, Olivier et moi) sommes toujours là, prêts à défendre la Géométrie sous tous ses aspects, dans tous ses états, comme vous avez été auprès de nous durant toutes ces années, attentif et bienveillant, encourageant mais lucide et à bien des égards soulageant car luttant sans cesse par le biais de *l'Atelier* en particulier contre la solitude qui menaçait de nous engloutir.

Un second Alain vient conclure cette liste ...
Toujours prêt à vous encourager, d'une bienveillance rare et d'une humilité troublante, *Alain Yger* est l'une des seules personnes, qu'en dépit d'une handicapante timidité, je n'ai jamais hésité à solliciter peut-être parce que qui que vous soyez et d'où que vous veniez, il fait partie de ces êtres pour lesquels les "à priori" n'ont pas droit d'asile et qui vous considère d'instinct comme quelqu'un de capable et de digne d'intérêt. D'une gentillesse qui n'a d'égale que sa passion pour tous les domaines qui touchent les Mathématiques, je tiens à le remercier très chaleureusement pour l'aide qu'à chaque étape de mon cursus universitaire il a bien voulu m'apporter et l'estime dont il m'a gratifiée et à laquelle je ne m'attendais pas.

Une pensée pour *Boas Erez*, *Gérard Galusinski* et *Jacques Martinet* qui chacun à leur manière et en ayant toujours fait montre d'une grande pudeur ont su je crois comprendre l'étendue de mes doutes.

Je voudrais enfin dire à *Yuri Bilu* , *François Levron* et *Michel Matignon* combien leur enthousiasme est communicatif, leur bonne humeur et leur simplicité encourageantes au sein d'un milieu somme tout délicat à appréhender ; et si je suis heureuse d'une chose, c'est que les étudiants ne s'y soient pas trompés.
Merci aussi à *Pierre Parent* et *Eric Charpentier* qui ne se sont jamais arrêtés à mon statut d'étudiante et m'ont manifestée, comme aux "Grands", confiance et bienveillance.

Vient le moment de remercier les quelques doctorants ou jeunes docteurs qui m'ont accompagnée durant ces années passées au sein de l'IMB.
Nabil tout d'abord dont le rire était un soulagement et la présence un soutien ; Matthieu ensuite dont les conversations matinales ressemblent en tous points au jus d'orange : vitaminées et acides. Un regret pourtant, celui ne pas être parvenu à exaucer son rêve de publier dans le *Journal de Théorie des Nombres de Bordeaux* (console-toi Matthieu car tu n'es pas le seul).
Merci aussi à Romain, Florent, Mourad, Martin, Catalina sur le point de rejoindre son Canada natal, Réda, Baptiste, Walter notre insatiable mangeur de carottes tout droit venu de Augsburg, Lara de Toulouse, Montse pour son coup de soleil, Eric, mes anciens co-bureaux Aurélien et Bertrand, Sébastien, Zohra avec laquelle je partage depuis peu et pour quelques jours encore le bureau 158 etc ... ; avec une mention spéciale aux nouveaux arrivants (Mike, Magali, Fabien, Bertrand, Jean ...) dont le dynamisme me rajeunit, me rassure peut-être aussi et auxquels je souhaite "*Bonne Chance*".

Enfin parce que la décision de poursuivre en thèse est difficile et ne se prend jamais seul(e), je remercie très sincèrement mes parents d'avoir accepter de me suivre dans cette aventure à laquelle je n'ai pas toujours pu ou su les associer autrement que de très loin, ma soeur Gaëlle pour beaucoup dans mon caractère atypique et mon petit frère Benoît qui fera mieux que moi j'en suis sûre.

Sans oublier UN GRAND MERCI à l'équipe de la Cellule Informatique qui m'aura, par sa gentillesse et son humanité, réconciliée avec les ordinateurs ainsi qu'à Chantal Bon-Saint-Côme, Marion Cazeaux, Cyril Mauvillain, Christine Parison et Véronique Saint-Martin dont l'efficacité, la disponibilité souriante aura été

un grand soulagement.

On fait la Science avec des faits comme une maison avec des pierres ; mais une accumulation de faits n'est pas plus une science qu'un tas de pierres n'est une maison.
Henri Poincaré

Introduction

Le contexte de cette thèse est celui des corps de fonctions, néammoins notre intérêt étant centré autour de considérations arithmétiques au détriment de l'interprétation géométrique sous-jacente, nous aurons à coeur à chaque fois que cela sera possible d'établir un parallèle avec la situation, de ce point de vue peut-être plus familière, des corps de nombres espérant ainsi mettre en exergue qu'en dépit de l'appartenance à la famille plus générale des corps globaux (caractérisés par l'existence d'une formule du produit), il subsiste entre corps de nombres et corps de fonctions certaines différences fondamentales, comme une dissymétrie de comportement, rendue d'autant plus frappante lorsque l'on se focalise sur la classe des $\mathbb{Z}_p$-extensions.

Le chapitre 1, après une rapide présentation des principaux protagonistes peuplant l'univers des corps de fonctions, se veut un hymne à la théorie d'Artin-Schreier-Witt dont on ne connait bien souvent que le cas particulier des extensions d'Artin-Schreier et dont l'objet est la description en caractéristique $p > 0$ des extensions de degré une puissance de p. A cet égard, nous rappelons que la construction de l'anneau des vecteurs de Witt trouve son origine dans la volonté d'établir dans le cadre de la caractéristique positive, les énoncés d'une théorie du corps de classes ; ainsi nous rappelons comment toute extension K_n/K de degré p^n peut être paramétrée par un vecteur de Witt de longueur n appelé "générateur d'Artin-Schreier-Witt" et dont la forme renferme la totalité de l'information relative à la ramification de cette dernière. En vertu de l'isomorphisme $\mathbb{Z}_p \simeq W(\mathbb{F}_p) = \varprojlim_n W_n(\mathbb{F}_p)$, on associera plus généralement à une $\mathbb{Z}_p$-extension un vecteur de Witt de longueur infinie ; cette description se révèlera le point de départ de l'article de Villa-Madan dont l'étude détaillée sera l'objet du chapitre 3.

Le chapitre 2 propose de traduire dans le contexte des corps de fonctions quelques résultats fondamentaux de la théorie d'Iwasawa et pour ce faire, nécessite de distinguer deux grandes familles d'extensions : d'une part celles, non-ramifiées, que l'on dit *"arithmétiques"* (c'est-à-dire obtenues par compositum du corps de base - par exemple le corps des fonctions rationnelles - avec une extension du corps des constantes, par exemple $\mathbb{F}_q$) et d'autre

part, celles que l'on dit *"géométriques"* où à l'inverse le corps de constantes est invariant par extension. Ce sont ces dernières qui retiendront toute notre attention par la suite du fait de la relative parité entre le comportement de leurs $\mathbb{Z}_p$-extensions et celui des pro-p-extensions de corps de nombres. En particulier et conformément aux travaux menés par Aiba en 2003, elles nous fourniront un contexte sinon favorable du moins encourageant quant à la recherche d'un candidat raisonnable (et ce faisant "non historique") pour assurer le rôle d'analogue de la $\mathbb{Z}_p$-extension cyclotomique des corps de nombres. Pour ce faire, un petit détour par les modules de Carlitz sera nécessaire et avec eux la mise en place d'une théorie cyclotomique dans le cadre des corps de fonctions. On disposera à ce stade des notions requises pour procéder à l'étude d'un article de Li et Zhao [41] où il est proposé un modèle de construction d'une $\mathbb{Z}_p$-extension du corps K des fonctions rationnelles en tout point inspirée de celle de $\mathbb{Q}_\infty$, la $\mathbb{Z}_p$-extension cyclotomique de $\mathbb{Q}$, c'est-à-dire obtenue par "troncature" le long de la tour d'extensions correspondante, du groupe de Galois $Gal(K(\Lambda_M)/K)$ d'ordre $\Phi(M)$ associé au M-ième corps cyclotomique $K(\Lambda_M)$.

Au chapitre 3, nous présentons en détail le contenu de l'article de Villa et Madan [42] à l'origine de ce travail de thèse, revenant dans un premier temps sur les travaux d'Iwasawa réalisés dans le contexte des corps de nombres pour justifier, en vertu d'un dictionnaire souvent évoqué, la formulation de la conjecture de Gross sur laquelle les auteurs se sont interrogés. On rappelle à cet effet qu'étant donnés K un corps de nombres et K_∞/K une $\mathbb{Z}_p$-extension de type CM, la conjecture de Gross statue que si S désigne exactement l'ensemble des places ramifiées (qui sont donc des p-places) alors $(\mathcal{C}_{\infty,S}(p)^-)^\Gamma$ est un groupe d'ordre fini.
Revenant au contexte des corps de fonctions, on se donne F un corps fini à q éléments ($q = p^r$ si p est un nombre premier $\neq 2$) et l'on désigne par K un corps de fonctions algébriques d'une variable de corps des constantes F. Soient K_∞/K une $\mathbb{Z}_p$-extension de groupe de Galois associé $\Gamma \simeq \mathbb{Z}_p$ et S l'ensemble, supposé *fini*, des places de K qui se ramifient (sauvagement) dans K_∞. Si l'on désigne par $\mathcal{C}_{\infty,S}(p)$ la p-partie du groupe des S-classes d'idéaux de K_∞ et que l'on considère l'action naturelle du groupe topologique Γ sur cette dernière, on peut se demander si le groupe des invariants pour cette action (vu comme sous-groupe de $\mathcal{C}_{\infty,S}(p)$), à savoir $\mathcal{C}_{\infty,S}(p)^\Gamma$, est d'ordre *fini*.
Dans le cas d'une $\mathbb{Z}_p$-extension arithmétique, la finitude du groupe $\mathcal{C}_{\infty,S}(p)^\Gamma$ découle de la théorie des modules noethériens aussi les auteurs concentrent-ils leur attention sur le cas des $\mathbb{Z}_p$-extensions géométriques. Partant de la description d'Artin-Schreier-Witt rappelée au chapitre 1 et après avoir établi une formule des classes ambiges, ils donnent une condition nécessaire formulée en termes de normes de S-unités garantissant la finitude du groupe $\mathcal{C}_{\infty,S}(p)^\Gamma$. Ainsi on est amené à associer à chaque étage n de la tour d'exten-

sions géométriques sous-jacente, une matrice carrée $\mathcal{M}_n \in M_{|S|-1}(\mathbb{Z}_p)$ qui concentre l'ensemble des conditions normiques ; on définit alors la matrice $\mathcal{M}$ associée à la $\mathbb{Z}_p$-extension K_∞/K comme la limite des $\mathcal{M}_n$ (dans un sens à préciser) et l'on montre que le caractère inversible de cette dernière assure la finitude de $\mathcal{C}_{\infty,S}(p)^\Gamma$; la réciproque sera assurée dès lors que $\mathcal{M} \in M_{|S|-1}(\mathbb{Q})$. Deux exemples viendront illustrer notre propos, exemples qui bien que choisis élémentaires, nous convaincrons du caractère un petit peu laborieux de la méthode proposée. Nous conclurons par une brève incursion en théorie des genres, comme un écho à l'aspect "*ambige*" jusqu'alors prédominant.

Partant d'un résultat de Greenberg énoncé en terme de semi-simplicité[1] et adoptant pour base de réflexion l'énoncé de la *conjecture de Gross généralisée* proposé par J.F. Jaulent en 1985 [33] qui prédit en substance, pour la $\mathbb{Z}_p$-extension cyclotomique d'un corps de nombres K et S l'ensemble des places (p-places) ramifiées, que l'ordre du groupe $(Cl^S_{K_n})^{\Gamma_n}$ est borné pour $(Cl^S_{K_n}) := \mathcal{C}l_{K_n}/\mathcal{C}l_{K_n}(S)$, nous nous proposons dans le dernier chapitre d'élargir le contexte considéré par Villa et Madan à un cadre *métabélien* avec l'idée qu'en rigidifiant un tant soit peu la situation initiale (en l'occurrence, par l'adjonction d'une action de groupe), on augmente d'autant nos chances d'obtenir, pour l'analogue de la conjecture de Gross considéré, un critère d'application plus aisée que le caractère inversible de la matrice $\mathcal{M}$ évoquée plus haut (somme toute assez pénible à établir dès lors que $|S| > 2$).
Soit donc K un corps de fonctions sur $\mathbb{F}_q$ (où $q = p^\alpha$). Pour chaque entier naturel n, on définit K_n comme une extension cyclique de degré p^n de $K = K_0$ telle que :
(i) $\forall\, n \in \mathbb{N}$, $K_n \subset K_{n+1}$ avec $[K_{n+1} : K_n] = p$.
(ii) Le corps des constantes de K_n est $k = \mathbb{F}_q$.
(iii) $K_\infty = \bigcup_n K_n$.
En d'autre termes, K_∞/K est un $\mathbb{Z}_p$ - extension géométrique.
On se donne enfin S un ensemble fini de places ramifiées (on fera l'hypothèse par la suite que ces dernières le sont totalement) et l'on désigne par $Cl^S_{K_n}$ le groupe des S-classes de diviseurs de K_n. Se placer dans le cadre métabélien signifie adjoindre à K_∞/K une composante *horizontale* sous la forme d'une extension K/F de degré d premier à p de groupe de Galois Δ supposé abélien et telle que l'extension K_∞/F soit galoisienne (nous tenons à travailler dans un cadre *semi-simple* de sorte de retirer le maximum d'informations de l'étude des φ-composantes à laquelle nous nous ramènerons). Si l'on note G le groupe de Galois de K_∞/F et $\Gamma = \gamma^{\mathbb{Z}_p}$ celui associé à K_∞/K, on s'autorisera l'abus de langage qui consiste à désigner par Δ un relèvement de $Gal(K/F)$ dans G. Ceci précisé, le groupe G s'écrit alors comme le produit

[1] On a certain l-Adic Representation, Invent. Math. **21**, p 117-124 (1973)

semi-direct $\Gamma \rtimes \Delta$. L'application,

$$\begin{array}{rcl} \kappa : \Delta \times \Gamma & \to & \Gamma \\ (\tau, \gamma) & \mapsto & \tau.\gamma = \tilde{\tau}\gamma\tilde{\tau}^{-1} \end{array}$$

qui définit ce dernier se factorise par un caractère p-adique ω de Δ selon :

$$\tau.\gamma.\tau^{-1} = \gamma^{\omega(\tau)},\ \forall\ \tau \in Gal(K_\infty/F_\infty) \simeq \Delta.$$

Ainsi donc, Γ et plus généralement les objets à considérer sont dotés d'une structure de $\mathbb{Z}_p[\Delta]$-module où $\mathbb{Z}_p[\Delta]$ est une algèbre galoisienne semi-locale ; c'est en particulier le cas pour le groupe de classes $Cl^S_{K_n}$ qui retient notre attention et qui posséde de ce fait une structure de $\mathbb{Z}_p[\Delta]$-module et conjointement une structure de Λ-module. La nécessité, pour ne rien perdre de la richesse du contexte métabélien, de tenir compte de cette mixité structurelle, nous engage à introduire l'algèbre gauche dite d'*Iwasawa généralisée* :

$$\Lambda[\Delta] = \mathbb{Z}_p[\Delta][[\theta]] \simeq \mathbb{Z}_p[[\theta]][\Delta]$$

qui n'est autre que l'algèbre du groupe Δ à coefficient dans Λ "tordue" par la relation :

$$\tau\gamma\tau^{-1} = \omega(\tau)\theta, \quad \forall\ \tau \in \hat{\Delta}$$

où,

$$\theta = \frac{1}{d}\sum_{\tau\in\Delta} \omega(\tau^{-1})(\gamma^{\omega(\tau)} - 1)$$

sachant que θ satisfait la congruence :

$$\theta \equiv \gamma - 1[(\gamma - 1)^2]$$

et engendre en tant que tel l'idéal $(\gamma - 1)\mathbb{Z}_p[[(\gamma - 1)^2]]$ de l'algèbre $\Lambda = \mathbb{Z}_p[[(\gamma - 1)^2]]$. La résolvante θ possède en outre cette propriété intéressante que son action "décale les φ composantes" (c'est-à-dire les composantes associées à un idempotent e_φ pour φ un caractère irréductible de Δ) au sens où l'on dispose de l'identité :

$$\theta e_\varphi = e_{\varphi\omega}\theta,$$

propriété qui se transmet aux suites exactes selon le modèle :

$$1 \to (Cl^S_{K_n})^{\Gamma_n}_\varphi \hookrightarrow \left(Cl^S_{K_n}\right)_\varphi \xrightarrow{\theta} \left(Cl^s_{K_n}\right)_{\omega\varphi} \to^{\Gamma_n} (Cl^S_{K_n})_{\omega\varphi} \to 1$$

Après avoir établi à un niveau fini et dans le contexte particulier où S désigne l'ensemble des places ramifiées, une formule des classes ambiges et une formule des genres, l'examen asymptotique du quotient

$$Z := \frac{|(Cl^S_{K_n})^{\Gamma_n}_\varphi|}{|^{\Gamma_n}\left(Cl^S_{K_n}\right)_{\omega\varphi}|}$$

permet d'obtenir des critères suffisants de non-semi-simplicité (on rappelle que dans le cas "semi-simple", quotient des genres et classes ambiges sont régis par le même caractère) ainsi que des critères suffisants de non trivialité pour l'invariant d'Iwasawa généralisé λ^S.

Table des matières

Chapitre 1

Des vecteurs et des corps ...

1.1 Introduction

L'objet de ce chapitre n'est pas de relater en détail la construction un peu laborieuse de l'anneau des vecteurs de Witt mais bien davantage de mettre en lumière ce qui a justifié sa genèse en rappelant l'origine du problème mathématique qu'E. Witt se proposait alors de résoudre. En effet, on pense généralement aux vecteurs de Witt comme à l'outil permettant de décrire la structure des anneaux locaux noethériens complets ou, plus simplement, au moyen de traiter le cas *"d'inégale caractéristique"*. Ainsi, les anneaux de valuation discrète sont de deux types suivant que leur corps résiduel k et leur corps de fractions K ont même caractéristique ou que k soit de caractéristique $p > 0$ quand K est de caractéristique 0 (un exemple classique est donné par l'anneau des entiers p-adiques $\mathbb{Z}_p$ de corps résiduel $\mathbb{F}_p$). On peut alors montrer que pour tout corps k de caractéristique $p > 0$, il existe un anneau de valuation complet W_k (appelé anneau des vecteurs de Witt sur k) dont le corps de fractions est de caractéristique 0, le corps résiduel est isomorphe à k et dont p est une uniformisante (par exemple, si l'on prend $k = \mathbb{F}_p$, W_k est isomorphe à $\mathbb{Q}_p$ qui n'est autre que le corps de fractions de l'anneau des entiers p-adiques). On dispose alors d'un théorème général de structure pour un anneau local noethérien complet A quelconque de corps résiduel k dont on rappelle l'énoncé ci-dessous :

Théorème 1.1.1. *Si A contient un corps isomorphe à k, ou bien il est isomorphe à un quotient d'un anneau de séries formelles $k[[T_1, T_2, \ldots, T_n]]$ ou sinon à un quotient de $W_k[[T_1, T_2, \ldots, T_n]]$.*

1. On distingue deux cas particuliers :
   - Si A est intègre, c'est une B-algèbre finie où B est de la forme soit $k[[T_1, T_2, \ldots, T_n]]$, soit $W_k[[T_1, T_2, \ldots, T_n]]$ (théorème de I. Cohen).
   - Si en outre l'anneau A est régulier et contient un corps isomorphe à k, il est lui-même isomorphe à $k[[T_1, \cdots, T_n]]$. Géométriquement, on

peut dire que les complétés des anneaux locaux de toutes les variétés algébriques sur k en des points "simples" sont isomorphes (ce qui est loin d'être le cas pour les anneaux locaux).

Reste que la question qui retenait l'attention d'E. Witt n'était pas tant la construction d'anneaux de valuation discrète complets que la généralisation aux extensions cycliques de degré p^n en caractéristique $p > 0$ de la théorie d'Artin-Schreier et ce sont les différentes étapes qui ont permis d'aboutir à cette dernière sur lesquelles nous souhaiterions nous attarder...

1.2 A propos des corps de fonctions...

1.2.1 Rappels concernant les anneaux de valuation

Définition 1.2.1. *Étant donné un corps commutatif K, on appelle "Valeur absolue" sur K toute application $\varphi : K \to \mathbb{R}^+$ satisfaisant aux propriétés suivantes :*

1. *Pour tout $x \in K, \varphi(x) = 0 \Leftrightarrow x = 0$*
2. *$\forall (x, y) \in K^2,\ \varphi(xy) = \varphi(x).\varphi(y)$*
3. *Il existe un nombre réel positif C tel que :*

$$\forall\ (x, y) \in K^2,\ \ \varphi(x + y) \leq C\ Sup\ \{\varphi(x), \varphi(y)\}$$

Remarque : Les conditions *1* et *3* entrainent que la restriction de φ au groupe multiplicatif $K^\times$ est un morphisme à valeurs dans $\mathbb{R}_+^\times$. En particulier, $\varphi(-1) = \varphi(1) = 1$.

On peut définir sur l'ensemble des valeurs absolues une relation d'équivalence "$\sim$" via :

$$\varphi_1 \sim \varphi_2 \Leftrightarrow \text{il existe } s \in \mathbb{R}_+^\times \text{ tel que } \varphi_2 = \varphi_1^s$$

ainsi qu'une constante réelle positive C_φ, appelée quelquefois *coefficient de* φ, donnée par :

$$C_\varphi = \text{Sup}_{\varphi(x)\leq 1}\{\varphi(1 + x)\}$$

Il s'agit de la plus petite constante possible dans *3* (c'est-à-dire celle qui donne l'inégalité la plus fine). En particulier, $C_\varphi \geq 1$.
Lorsque $C_\varphi = 1$, on qualifie la valeur absolue associée que l'on dit alors *non-archimédienne* ou encore *ultramétrique*, au sens où elle satisfait une "ultra" inégalité triangulaire. Dans tous les autres cas, on parle de valeur absolue *archimédienne* l'exemple le plus familier étant sans doute la valeur absolue usuelle $|.|$ définie sur $\mathbb{R}$ dite *"à l'infini"*. En particulier, deux valeurs absolues équivalentes sont simultanément ultramétriques ou archimédiennes . Dans le cas des corps de fonctions, qui est le contexte que nous privilégierons par la

suite, toutes les valeurs absolues ont le même statut et sont ultramétriques ; de cet état de fait, on pourrait conclure à une certaine simplicité du comportement de cette famille de corps globaux en comparaison à celui, à cet égard pathologique, des corps de nombres mais nous verrons à l'occasion du chapitre 2 que cet enthousiasme convient d'être modéré ...

Intrinsèquement, la notion de valeur absolue porte en elle une information "métrique", reste à justifier comment elle peut permettre de définir une topologie.

Définition 1.2.2. *Soit φ une valeur absolue sur K ; on appelle* pseudo-boule de centre a et de rayon ρ, *l'ensemble $\mathcal{B}(a,\rho) = \{x \in K / \varphi(a-x) < \rho\}$ et* topologie définie par φ, *la topologie pour laquelle les ouverts sont les réunions quelconques de pseudo-boules.*

Remarques-Conséquences :
- Deux valeurs abolues équivalentes (au sens précédent) définissent la même topologie (c'est-à-dire les mêmes ouverts...).
- Lorsque la valeur absolue φ (comprendre : "un représentant de la classe d'équivalence associée") est ultramétrique, on attribue à la topologie induite le même qualificatif. Cette dernière a ceci de particulièrement agréable qu'elle rend équivalent la convergence d'une série avec celle de son terme général vers 0. On en rêvait ...

Dans toute la suite, φ désignera invariablement une valeur absolue *ultramétrique.*

Définition 1.2.3. *On appelle valuation réelle sur un corps commutatif K toute application $v : K \to \mathbb{R} \cup \{\infty\}$ telle que :*

1. *Pour tout $x \in K, v(x) = +\infty \Leftrightarrow x = 0$*
2. $\forall\ (x,y) \in K^2, v(xy) = v(x) + v(y)$,
   avec les conventions : $\forall\ r \in \mathbb{R} \cup \{\infty\}, r + (\infty) = \infty + r = \infty$
3. $\forall\ (x,y) \in K^2, v(x+y) \geq Inf\{v(x), v(y)\}$,
   avec la convention : $r < \infty\ \forall\ r \in \mathbb{R}$.

On remarque qu'il s'agit là essentiellement du pendant "additif" de la liste de propriétés caractérisant une valeur absolue ce que l'on formalise en disant que φ et v *sont associées* s'il existe $0 < a < 1$ tel que $v = \log_a \varphi$ (ou de manière équivalente $a^v = \varphi$). En particulier, les diverses valeurs absolues associées à une même valuation sont équivalentes entre-elles.

Raffinement :

Définition 1.2.4. *On appelle* valuation discrète *(resp.*discrète normalisée*) sur un corps K, toute valuation v telle que $v(K^\times)$ soit un sous-groupe additif de $\mathbb{R}$ isomorphe (resp. égal) à $\mathbb{Z}$. On appelle alors* uniformisante *d'une*

valuation discrète, tout élément $\pi \in K$ tel que $v(\pi)$ soit le générateur positif de $v(K^\times)$.

Exemple : Soient k un corps commutatif et $k(T)$ le corps des fractions rationnelles associé *ie* $k(T) \simeq (k[T]-\{0\})^{-1} \times k[T]$. Tout élément P de $k(T)$ admet une unique décomposition sous la forme : $P = T^e Q$ où e est un entier, Q un quotient de polynômes $\in k[T]$ non-factorisables par T.
En posant, $v(0) = \infty$ et $v(P) = e$ pour $P \neq 0$, on obtient une valuation sur le corps $k(T)$ telle que $v(T) = 1$ sachant que l'on pourrait substituer à T un polynôme irréductible $f(T)$ et définir selon le même principe une valuation v sur $k(T)$ telle que $v(f) = 1$...
La définition à venir introduit des objets propres aux valeurs absolues ultramétriques qui seront omniprésents dans la suite de la discussion :

Définition 1.2.5. *Soit v une valuation sur K associée à une valeur absolue φ. On appelle respectivement : anneau, idéal et groupe des unités de v les ensembles :*

$$A_v = v^{-1}([0, +\infty]) = \varphi^{-1}([0, 1])$$

$$M_v = v^{-1}(]0, +\infty]) = \varphi^{-1}(]0, 1])$$

$$E_v = v^{-1}(0) = \varphi^{-1}(1) = A_v^\times$$

et l'on a le théorème :

Théorème 1.2.6. *A_v est un anneau* local *d'unique idéal maximal M_v et de corps des fractions $K = Frac(A_v)$. En outre, si $x \in K \setminus A_v$ alors $x^{-1} \in A_v$.*

Lorsque v est discrète, on parle d'anneau de valuation *discrète* et l'on dispose de la caractérisation suivante qui rappelle qu'il s'agit là d'une propriété forte :

Proposition 1.2.7. *Soit A un anneau intègre local noethérien de dimension 1 (au sens de Krull) et $\mathfrak{P}$ son unique idéal maximal. Si l'on note $k = A/\mathfrak{P}$ le corps résiduel associé, les assertions suivantes sont équivalentes :*

1. *A est un anneau de valuation discrète*
2. *A est intégralement clos dans son corps de fractions*
3. *$\mathfrak{P}$ est principal*
4. *$dim_k(\mathfrak{P}/\mathfrak{P}^2) = 1$*
5. *tout idéal non nul est une puissance de $\mathfrak{P}$*
6. *il existe $t \in A$ tel que tout idéal non-nul soit de la forme t^m pour $m \in \mathbb{Z}$*

Le cas des corps de fonctions :

Définition 1.2.8. *Etant donné un corps commutatif k quelconque, on appelle corps de fonctions algébriques en une variable sur k une extension L/k avec L une extension finie de $k(x)$* (ie $[L : k(x)] < \infty$) *pour $x \in L$ transcendant sur k.*

On parle pour k de *corps de base* de L/k (que l'on prendra souvent égal à $k = \mathbb{F}_q$, le corps fini à q éléments) et pour l'ensemble

$$\tilde{k} = \{z \in L |\ z \text{ algébrique sur } k\}$$

du *corps des constantes* de L/k. Le comportement de ce dernier sera particulièrement important lorsque l'on considèrera des tours d'extensions comme le suggère la définition suivante :

Définition 1.2.9. *Soit L/k un corps de fonctions de corps des constantes k. On dit que L'/k' est une* extension algébrique *de L/k si :*

1. *L'/L est un extension algébrique (au sens usuel)*
2. *on a l'inclusion : $k \subseteq k'$*

En particulier, on dit que l'extension algébrique L'/k' de L/k est finie *si le degré $[L' : L]$ est fini.*

Exemple : Même si cela peut sembler un petit peu prématuré, on donne l'exemple important suivant sur lequel nous serons amenés à revenir... Étant donnée L/k une extension de corps de fonctions de corps des constantes k, on appelle *Corps de classes de Hilbert* de L (au sens de Rosen) et l'on note H_L l'extension abélienne maximale de L qui est non-ramifiée aux places finies et dans laquelle toute place à l'infini se décompose totalement.

Remarque :
Si L est une extension monogène de $k(x)$ de degré n, ce qui vrai par exemple lorsque le corps k est parfait[1], il existe y algébrique sur $k(x)$ tel que
$L = k(x, y)$ et si l'on désigne par $P(x, Y)$ le polynôme minimal de y sur $k(x)$, alors ce dernier est de degré n.

Places d'un corps de fonctions :

Définition 1.2.10. *Une place $\mathfrak{P}$ d'un corps de fonctions L/k est l'idéal maximal associé à un anneau de valuation de L/k. Il existe une bijection entre l'ensemble des places de L/k et les valuations discrètes de L qui sont triviales sur k. On note $\mathcal{P}_{L/k}$ l'ensemble des places de L/k dont on admet qu'il est non-vide.*

[1] On rappelle qu'un corps k est dit *parfait* si toute extension algébrique L/K est séparable (en particulier les corps finis sont parfaits).

Définition 1.2.11. *1. Soit $\mathfrak{P}$ une place de L/k ; on appelle "corps résiduel" en $\mathfrak{P}$ le quotient $\mathcal{L}_{\mathfrak{P}} := A_{\mathfrak{P}}/\mathfrak{P}$ et l'on peut définir une application :*

$$\vartheta_{\mathfrak{P}} : L \to \mathcal{L}_{\mathfrak{P}} \cup \{\infty\}$$
$$u \mapsto u(\mathfrak{P})$$

telle que :
$u(\mathfrak{P}) := \overline{u} \in A_{\mathfrak{P}}/\mathfrak{P}$ si $u \in A_{\mathfrak{P}}$ et ∞ sinon.

- *En outre, si $u \in \mathfrak{P}$, $\vartheta_{\mathfrak{P}}(u) = 0$.*

2. $\mathcal{L}_{\mathfrak{P}}$ étant naturellement doté d'une structure de k-espace vectoriel, on appelle degré de la place $\mathfrak{P}$, *le degré de l'extension $[\mathcal{L}_{\mathfrak{P}} : k]$ et l'on note $\mathcal{P}^n_{L/k}$ l'ensemble des places de L/k de degré n.*

Exemple du corps des fonctions rationnelles :

En général ...	Cas du corps rationnel $K(x)$
On définit *l'anneau de valuation* en P : $$\mathcal{O}_P = \{x \in L, v_P(x) \geq 0\}$$ *d'unique idéal maximal* de $\mathcal{O}_P$: $$P = \{x \in L, v_P(x) > 0\}$$ Et enfin, *le groupe des inversibles* de l'anneau $\mathcal{O}_P$: $$\mathcal{O}_P^{\times} = \{x \in L, v_P(x) = 0\}$$ *Définition* : Soient $u \in L^{\times}$ et P une place de L. On dit que P est un zéro d'ordre n de u si $v_P(u) = n > 0$. On dit que P est un pôle d'ordre n de u si $v_P(u) = -n < 0$. Ainsi, si $u \in L^{\times}$ on dispose de la caractérisation suivante : 1. P est un zéro de $u \Leftrightarrow u \in P$ 2. P est un pôle de $u \Leftrightarrow 1/u \in P$	Soit $P(x) \in K[x]$ un polynôme unitaire irréductible. On pose : $$\mathcal{O}_P = \{\frac{f(x)}{g(x)} \text{tel que} (f,g) = 1 \text{ et } (P,g) = 1\}$$ Il s'agit d'un anneau de valuation de $K(x)$ d'idéal maximal : $$P = \{\frac{f(x)}{g(x)} \in \mathcal{O}_P \text{ avec } P(x) \mid f(x)\}$$ où $\deg(P) = \deg(P(x))$. De la même façon, on peut définir : $$\mathcal{O}_\infty = \{\frac{f(x)}{g(x)} \text{ tel que } deg(f(x)) < deg(g(x))\}$$ l'anneau de valuation discrète de $K(x)/K$ d'idéal maximal : $$P_\infty = \{\frac{f(x)}{g(x)} \in \mathcal{O}_\infty, \deg(f(x)) < \deg(h(x))\}$$ où par convention $\deg(\infty) = 1$. On peut énoncer pour le corps rationnel $K(x)$ un théorème du type "Ostrowski". ***Théorème*** : Les seules places de $K(x)/K$ sont de la forme $P = (P(x))$ où $P(x) \in K[x]$ est un polynôme unitaire irréductible (on parle alors de *places finies*) ou la place à l'infini notée ∞. Comme conséquence de la caractérisation des places de $K(x)$, on a la relation suivante : $$\bigcap_{P \neq \infty} \mathcal{O}_P = K[x].$$

Remarque : Pour $K = k(X)$ le corps des fractions rationnelles en une variable sur le corps k (supposé fini de cardinal q) et F un élément non-nul de $k(X)$, on considère l'application $|.|$ définie comme suit :

$$\begin{array}{rcl} |.| : k[X] & \rightarrow & \mathbb{N} \\ F & \mapsto & |F| = q^{deg(F)} \\ 0 & \mapsto & 0 \end{array}$$

En prolongeant cette application de façon naturelle à $k(X)$ (à valeur dans $\mathbb{Z}$), on obtient une valeur absolue sur $K(X)$ qui est ultramétrique et que l'on note $|.|_\infty$.

Soit maintenant P un polynôme irréductible unitaire de $k[X]$ de degré n. Pour F un élément non-nul de k(X), on note $v_P(F)$ l'exposant de P dans la décomposition

de F en produits de polynômes irréductibles sur k et l'on pose :

$$\begin{array}{rcl} |.|_P : k[X] & \to & \mathbb{N} \\ F & \mapsto & |F|_P = q^{-n\, v_P(F)} \\ 0 & \mapsto & 0 \end{array}$$

Ce faisant, on obtient une autre valeur absolue ultramétrique sur $k(X)$ et comme dans le cas du corps $\mathbb{Q}$ des rationnels, on dispose d'une formule du produit :

$$|F|_\infty \prod_P |F|_P = 1 \quad \forall \ F \in \ k(X)^\times$$

Classification des corps locaux :
Si l'on désigne par *corps local*, tout corps muni d'une valuation discrète et complet pour les valeurs absolues qui lui sont associées, on a la proposition suivante :

Proposition 1.2.12. *Les corps locaux sont soit des extensions finies du corps p-adique $\mathbb{Q}_p$ soit des extensions finies du corps de séries formelles $\mathbb{F}_p((T))$.*

Dans le cas particulier où K désigne un corps de fonctions de corps des constantes k et $K_\mathfrak{p}$ son complété en une place $\mathfrak{p}$ (nécessairement non-archimédienne) d'uniformisante associée π satisfaisant $v_\mathfrak{p}(\pi) = 1$, la structure du corps local $K_\mathfrak{p}$ peut être décrite comme suit :

$$K_\mathfrak{p} = \mathcal{K}((\pi)) = \{ \sum_{n=m}^{\infty} \alpha_n \pi^n / \ m \in \mathbb{Z} \text{ et } \alpha_n \in \mathcal{K} \ \forall \ n\}$$

où $\mathcal{K} \supset k$ désigne le corps résiduel associé à la place $\mathfrak{p}$ de degré $\deg \mathfrak{p}$ sur $\mathbb{F}_q$.

Exemple : On prend pour K le corps des fonctions rationnelles $\mathbb{F}_q(T)$ et l'on considère la place à l'infini (de degré 1) d'uniformisante associée $\frac{1}{T}$. Le complété $K_{\frac{1}{T}}$ est alors isomorphe au corps de séries formelles $\mathbb{F}_q((\frac{1}{T}))$ qui joue, dans le contexte des corps de fonctions, le rôle de $\mathbb{R}$ pour les corps de nombres. En outre, pour $\mathfrak{p} \in Pl_K$ d'uniformisante associée $\pi := \pi_\mathfrak{p}$, on est amené à distinguer certains sous-groupes de $K_\mathfrak{p}^\times$ intervenant sans cesse en Théorie des Nombres et en particulier en théorie du corps de classes. Ainsi, on pose :

$$U_\mathfrak{p}^{(n)} := 1 + \mathfrak{p}^n = \{1 + \alpha_n \pi^n + \alpha_{n+1} \pi^{n+1} |\ \alpha_n, \alpha_{n+1}, \cdots \in \mathbb{F}_\mathfrak{p}\}$$

Pour $n = 1$, on parle du *groupe des unités principales* et l'on a l'isomorphisme $\mathbb{F}_\mathfrak{p}^\times \simeq U_\mathfrak{p}/U_\mathfrak{p}^{(1)}$.

1.2.2 Anneaux d'entiers

On se propose de préciser en quelques mots et dans un cadre orienté vers "les corps de fonctions" les définitions d'outils de base que nous serons amenés, quitte à les raffiner un petit peu, à évoquer (et invoquer...) dans toute la suite.

Définition 1.2.13. *Soient R un anneau avec $f \in R$ supposé non-nul et A un sous-anneau de R non-trivial. On dit que l'élément f est entier sur A si et seulement s'il est solution d'un polynôme unitaire à coefficients dans A.*

Définition 1.2.14. *On considère $\mathfrak{p}$ une place de $k(x)$ et $\mathcal{O}_\mathfrak{p}$ son anneau de valuation associé. Une fonction f de R est dite entière en $\mathfrak{p}$ si elle est entière sur $\mathcal{O}_\mathfrak{p}$.*

La proposition suivante permet de lier "éléments entiers" et la notion d'anneaux de valuation discutée précédemment :

Proposition 1.2.15. *Soit A un anneau contenu dans un* corps *R. Un élément f est entier sur A (au sens précédent) si et seulement s'il appartient à tous les anneaux de valuation de R contenant A.*

En particulier, si R est une extension finie de $k(x)$ et si l'on désigne par $\mathfrak{p}$ une place de ce dernier, les fonctions de R entières en $\mathfrak{p}$ sont exactement les fonctions n'admettant pas de pôle en $\mathfrak{P}$ pour toute place $\mathfrak{P}$ de R telle que $\mathfrak{P}|\mathfrak{p}$. Soit $\mathcal{O}_\mathfrak{P}$ l'ensemble de ces fonctions ; on vérifie assez facilement en utilisant les propiétés des valuations qu'il s'agit d'un anneau et plus encore, à savoir la clôture intégrale de $k[x]$ dans R. En particulier, $\mathcal{O}_\mathfrak{P}$ est un $\mathcal{O}_\mathfrak{p}$-module libre de rang $[R : k(x)] = n$. On baptise *"base entière"* en $\mathfrak{p}$ (ou base entière *locale*) une base de $\mathcal{O}_\mathfrak{P}$ sur $\mathcal{O}_\mathfrak{p}$.

Définition 1.2.16. *Étant donnée L une extension algébrique finie de $k(x)$, on appelle* anneau des entiers de L *l'ensemble des éléments de L solutions d'un polynôme unitaire à coefficients dans $k[x]$. Soit $\mathcal{O}_L$ ce dernier.*

Remarque : Contrairement à ce qui se passe pour les corps de nombres, le concept d'anneau des entiers d'un corps de fonctions n'est pas canonique au sens où il dépend fondamentalement du choix de l'élément transcendant x.

Proposition 1.2.17. *$\mathcal{O}_L$ est exactement décrit par l'ensemble des fonctions de L sans pôle en les places finies (i.e. en les places $\mathfrak{P}$ de $\mathcal{O}_L$ telles que : $\mathfrak{P} \nmid \infty$.)*

Preuve : On commence par remarquer que x appartient à tous les anneaux de valuation attachés à $k(x)$ sauf celui associé à la place à l'infini. Par conséquent, x appartient à tous les anneaux de valuation de L exceptés

ceux provenant d'une place au-dessus de l'∞. Il en est de même pour $k[x]$ puisque k est inclus dans tous les anneaux de valuation de L. Ainsi, par la proposition précédente les éléments de L entiers sur $k[x]$ sont les fonctions éléments de L appartenant à tous les anneaux de valuation contenant $k[x]$. Il s'agit donc des fonctions n'admettant (éventuellement) de pôles qu'en les places au-dessus de l'∞.

Conséquence (qui est un corollaire immédiat) : on dispose de la description suivante pour $\mathcal{O}_L$:

$$\mathcal{O}_L = \bigcap_{\mathfrak{P}\nmid\infty} \mathcal{O}_{\mathfrak{P}}$$

et du théorème de structure :

Proposition 1.2.18. *Si $L/k(x)$ est une extension de corps de fonctions de degré n fini, l'anneau des entiers $\mathcal{O}_L$ est un $k[x]$-module libre de rang n. On appelle* base entière globale *une base de $\mathcal{O}_L$ sur $k[x]$.*

Enfin, on énonce :

Proposition 1.2.19. *Une famille de L libre sur $k[x]$ l'est encore sur $k(x)$ et sur $\mathcal{O}_{\mathfrak{p}}$ pour toute place $\mathfrak{p}$.*

Idée de la preuve : Une combinaison linéaire nulle sur $k(x)$ peut se ramener par réduction au même dénominateur, en une combinaison linéaire nulle sur $k[x]$ et donc sur $\mathcal{O}_{\mathfrak{p}}$ pour tout $\mathfrak{p}$.
Conséquence : Une famille de L de dimension n libre sur $k[x]$ ou sur $\mathcal{O}_{\mathfrak{p}}$ pour une place quelconque, est une base de L sur $k(x)$.

1.2.3 Notions de Diviseurs

Si l'on propose une présentation très algébrique et donc essentiellement formelle du groupe des diviseurs d'un corps de fonctions, on précise que cette notion trouve son origine en géométrie et fut introduite par Riemann.

Dans toute la suite, on désignera par L/k un corps de fonctions de corps des constantes k.

Définition 1.2.20. *Un diviseur de L/k est un élément du groupe abélien libre engendré par les places de L/k. L'ensemble des diviseurs est noté $\mathcal{D}_{L/k}$ et l'on a pour $D \in \mathcal{D}_{L/k}$:*

$$D = \sum_{P \in Pl_L} n_P P$$

avec $n_P \in \mathbb{Z}$ et n_P nul pour presque toute place P de L.

On rencontre souvent l'abus de notation qui consiste à l'identification : $n_P := v_P(D)$. On définit maintenant le support du diviseur D comme l'ensemble :

$$\mathrm{Supp}(D) := \{P \in Pl_L / v_P(D) \neq 0\}$$

et son degré (par linéarité) via l'introduction d'un homomorphisme "deg" :

$$\begin{array}{rcl} \deg : \mathcal{D}_{L/k} & \to & \mathbb{Z} \\ D & \mapsto & \deg(D) := \sum_{P \in Pl_L} v_P(D) \deg P \end{array}$$

où $\deg P := [\mathcal{O}_P/P : k]$. On note généralement $\mathcal{D}^n_{L/k}$ l'ensemble des diviseurs de degré n.

Cette notion ne serait pas d'un grand intérêt si l'on n'avait la proposition suivante :

Proposition 1.2.21. *L'ensemble $\mathcal{D}_{L/k}$ est muni d'une structure de groupe abélien pour l'addition via :*

$$D_1 + D_2 = \sum_{P \in Pl_{L/k}} (v_{P_1}(D) + v_{P_2}(D))P$$

d'élément neutre $0 = \sum_{P \in Pl_{L/K}} 0.P$.

Remarque : Le groupe $\mathcal{D}^0_{L/k}$ des diviseurs de degré 0 est un sous-groupe de $\mathcal{D}_{L/k}$ d'autant plus important qu'il joue dans le contexte des corps de fonctions le rôle du groupe des idéaux fractionnaires pour les corps de nombres mais nous y reviendrons.

Définition 1.2.22. *Soient z un élément du corps de fonctions L et $\mathfrak{P}$ une place de ce dernier .*

- *On dit que $\mathfrak{P}$ est un zéro de z si et seulement si $v_{\mathfrak{P}}(z) > 0$.*
- *On dit que $\mathfrak{P}$ est un pôle de z si et seulement si $v_{\mathfrak{P}}(z) < 0$.*

Conséquences :

1. Si $v_{\mathfrak{P}}(z) = m > 0$, alors $\mathfrak{P}$ est un zéro de z d'ordre m.
2. Si $v_{\mathfrak{P}}(z) = -m < 0$, alors $\mathfrak{P}$ est un pôle d'ordre m pour z.

Cas particulier : Soit $u \in L^\times$. On note $\mathcal{Z}_u$ (resp. $\mathcal{N}_u$) l'ensemble (fini) de ses zéros (resp. de ses pôles). On a la définition suivante :

Définition 1.2.23. *Le diviseur des zéros d'un élément $u \in L^\times$ est :*

$$(u)_0 := \sum_{P \in \mathcal{Z}_u} v_P(u)P.$$

De la même façon, on pose pour le diviseur des pôles :

$$(u)_\infty := -\sum_{P\in\mathcal{N}_u} v_P(u)P.$$

Ainsi le diviseur principal associé à u s'écrit :

$$\begin{aligned}(u) &= \sum_{P\in Pl_{L/K}} v_P(u)P \\ &= (u)_0 - (u)_\infty\end{aligned}$$

Remarques :

1. Étant donné le corps des constantes k, on a $x \in k^\times \Leftrightarrow (x) = 0$ (ce qui peut éclairer sur la dénomination, à savoir qu'il s'agit de fonctions qui n'ont ni pôle ni zéro et donc qui sont constantes...)
2. On note $\mathcal{P}_{L/k}$ l'ensemble des diviseurs principaux de L/k.

Définition 1.2.24. *Sur $\mathcal{D}_{L/k}$, on définit une relation d'équivalence en posant :*

$$D_1 \sim D_2 \Leftrightarrow \textit{il existe } u \in L^\times, D_1 - D_2 = (u) \in \mathcal{P}_{L/k}.$$

Le groupe quotient associé $\dfrac{\mathcal{D}_{L/k}}{\mathcal{P}_{L/k}}$ *est appelé* groupe de Picard *et noté* $Pic_{L/k}$.

Remarque : L'application "degré" définit précédemment passe au quotient, c'est-à-dire que si l'on note $\overline{D}$ la classe d'un diviseur D, l'application $\overline{D} \mapsto \deg(D)$ est un morphisme de groupes.

La tentation est grande alors de voir le groupe de Picard (ou groupe des classes de diviseurs) comme l'analogue du groupe des classes d'idéaux d'un corps de nombres *mais* contrairement à ce dernier $\mathrm{Pic}_{L/k}$ n'est pas fini ... Du théorème suivant va émerger le "bon candidat" pour poursuivre l'analogie :

Théorème 1.2.25. *(analogue additif de la formule du produit) Soit L/k un corps de fonctions de corps des constantes k. On a que tout diviseur principal est de degré zéro i.e. :*

$$\forall u \in L^\times, deg((u)) = \sum_{P\in Pl_{L/k}} v_P(u)deg(P) = 0.$$

Plus précisément :

$$\forall u \in L \setminus k, deg(x)_0 = deg(x)_\infty = [L : k(x)]$$

Interprétation :

1. Une fonction algébrique (non-constante) admet autant de pôles que de zéros comptés avec leur multiplicité.

2. On déduit de ce théorème que $\mathcal{P}_{L/k}$ est un *sous-groupe* de $\mathcal{D}^0_{L/k}$. On peut donc considérer le groupe des classes de diviseurs de degré 0 : $\mathrm{Pic}^0_{L/k} = \dfrac{\mathcal{D}^0_{L/k}}{\mathcal{P}_{L/k}}$. Il s'agit de la Jacobienne associée à l'extension L/k (ou plus exactement, à la courbe algébrique sous-jacente) que l'on peut doter d'une structure de variété abélienne.

Dans le cas où $k = \mathbb{F}_q$, $\mathrm{Pic}^0_{L/k}$ est un groupe FINI qui servira d'analogue au groupe des classes d'idéaux d'un corps de nombres. On dispose de la suite exacte :

$$1 \to k^\times \hookrightarrow L^\times \to \mathcal{D}^0_{L/k} \twoheadrightarrow \mathrm{Pic}^0_{L/k} \to 0$$

qui est l'analogue dans les corps de nombres de :

$$1 \to \mathcal{O}_L^\times \hookrightarrow L^\times \to I_L \twoheadrightarrow \mathcal{C}_L \to 1.$$

1.3 Les travaux d'Artin et Schreier

Aux environs de 1926, Artin[2] et Schreier[3] ont cherché à caractériser la famille des corps K qui admettaient une extension quadratique (i.e. de degré 2 premier ...) algébriquement close comme c'est le cas pour le couple $(\mathbb{R}, \mathbb{C})$ où $\mathbb{C} \simeq \mathbb{R}(i)$ et $\mathbb{C}$. Ils ont ainsi obtenu un critère selon lequel de tels corps sont obtenus par adjonction de l'élément $\sqrt{-1}$. La brèche était alors ouverte et l'étape suivante a consisté à s'intéresser à des extensions de degré un nombre premier $p > 2$ et à se demander si, de la même façon, il existait des corps K tel que le groupe de Galois $Gal(\overline{K}/K)$ soit cyclique d'ordre p (ceci impose en particulier que K soit de caractéritique p). Une question "duale" et tout aussi naturelle consiste, étant donnée une extension L/K cyclique de degré p à se demander si L peut être algébriquement clos. C'est par la négative qu'A. et S. répondent à ce problème avant d'en formuler un suivant. On suppose donnée une extension cyclique K_1/K de degré p, existe-t-il toujours une tour de corps

$$K \subseteq K_1 \subseteq K_2 \subseteq \cdots K_n \subseteq \cdots$$

telle que K_n/K soit cyclique de degré p^n et si oui comment la construire ? Le premier étage de cette tour, à savoir le corps K_1, est, ce qu'en hommage aux travaux des mathématiciens précédemment cités, on convient d'appeler une extension d'*"Artin-Schreier"* ; avant d'y revenir plus avant, nous rappelons brièvement qu'elle est engendrée par une équation du type $x^p - x = a$ avec a convenable. On remarque par la suite que l'on peut plonger cette dernière dans une extension cyclique de degré p^2 en cherchant à déterminer
$P(X) \in K[X]$ de degré $< p$ tel que l'équation $y^p - y = P(x)$ définisse une

[2] Emil Artin (1898-1962)
[3] Otto Schreier (1901-1929)

extension p^2-cyclique de K. C'est le mathématicien français Albert [4] qui le premier va tenter de construire les étages supérieurs de cette tour mais la profusion des relations et leur complexité l'induiront en erreur et ne lui permettront pas de mener ce travail à son terme. Le flambeau est alors repris par L. Schmid avec plus de succès cette fois quand bien même les techniques employées restent lourdes et fastidieuses. Il faudra donc attendre l'intervention d'E. Witt en 1936 pour construire un outil adapter à la résolution de ce problème : l'anneau des vecteurs de Witt qui va permettre dans le même temps de paramétrer de manière agréable les p-extensions cycliques en caractéristique $p > 0$ et de donner, pour les corps de fonction une traduction complète de la Théorie du Corps de Classes, formules de Réciprocité comprises.

1.4 Quelques propriétés de l'anneau des vecteurs de Witt

1.4.1 Historique

C'est en 1937, dans le cadre du prestigieux Göttingen Arbeitsgemeinschaft qu'il dirigeait que paraît le papier d'E. Witt (1911-1991) intitulé : *Zyklische Körper und Algebren der Charakteristik p vom Grad* p^n dans lequel il introduit l'anneau des vecteurs qui portent aujourd'hui son nom. Dans l'esprit du mathématicien allemand le concept envisagé devait être *fonctoriel*, ce qui signifie qu'étant donné un morphisme $K \hookrightarrow L$ (nécessairement injectif puisque K et L sont des corps), on doit pouvoir déduire un plongement $W(K) \hookrightarrow W(L)$. On suppose pour un instant être dans le cas particulier où $K := \mathbb{F}_{p^n}$. Soit $\mathbb{Q}_p$ le corps des nombres p-adiques. On considère l'anneau des entiers $\mathcal{O}_{p,n}$ associé à l'unique extension non-ramifiée de $\mathbb{Q}_p$ de degré n. Ce dernier est un anneau de valuation discrète, complet, d'idéal maximal engendré par p et de corps résiduel isomorphe à $\mathbb{F}_{p^n}$. On en déduit en particulier qu'il est déterminé à isomorphisme près. L'idée de Witt a consisté à construire l'anneau $W(\mathbb{F}_{p^n})$ de sorte de le rendre isomorphe à $\mathcal{O}_{p,n}$ (en d'autres termes, il a souhaité reconstruire l'anneau $\mathcal{O}_{p,n}$ à partir de son corps résiduel associé).

1.4.2 Description et propriétés essentielles

Définition 1.4.1. *Étant donné un anneau commutatif R, on appelle vecteur de Witt à coefficients dans R une suite infinie $a = (a_0, a_1, a_2, \cdots, a_n, \cdots)$ avec $a_i \in R \ \forall\, i \geqslant 0$.*

La structure d'anneau est donnée comme suit : étant donnés deux vecteurs de Witt a et b à coefficients dans R, on pose :

$$a + b = (S_0(a,b), S_1(a,b), \cdots, S_n(a,b), \cdots)$$

[4] A. Adrian Albert (1905-1972)

$$a * b = (P_0(a,b), P_1(a,b), \cdots, P_n(a,b), \cdots)$$

où pour $i, j \geqslant 0$ S_i *et* P_j sont des éléments de $\mathbb{Z}[X_0, X_1, \cdots; Y_0, Y_1, \cdots]$. Bien entendu, il existe des formules explicites permettant de donner les expressions des S_i et P_j mais ces dernières -très compliquées- ne présentent que peu d'intérêt aussi nous prenons le parti de les passer sous silence (pour plus de détails, voir par exemple [36],[44]).

Définition 1.4.2. *Muni de ces opérations, l'ensemble des vecteurs est doté d'une structure d'anneau intègre, commutatif et unitaire d'élément unité* $\mathbf{1} = (1, 0, \cdots, 0, \cdots)$ *appelé anneau des vecteurs de Witt à coefficients dans* R.

L'anneau des vecteurs de Witt en tant qu'anneau de valuation :

Soit k un corps parfait de caractéristique p. Étant donné $x = (x_0, x_1, \cdots)$ un vecteur de Witt à coefficients dans k, on pose :

$$v(x) = min\{i, x_i \neq 0\} \ \ si \ \ x \neq 0$$

et

$$v(0) = \infty$$

Soit maintenant K le corps de fractions de $W(k)$ et

$$v : K \to \mathbb{Z} \cup \{\infty\}$$

le prolongement de v à K via :

$$v(xy^{-1}) = v(x) - v(y) \ \ \forall\, x, y \in W(k).$$

On vérifie alors que v ainsi définie est une valuation discrète sur K et dote ainsi ce dernier d'une structure de corps de valuation discrète (i.e. complet pour la topologie assiociée à v) de caractéristique nulle admettant pour anneau des entiers (ou anneau de valuation) $W(k)$ et pour corps résiduel un corps isomorphe à k. On énonce :

Théorème 1.4.3. *On suppose que* R *est un corps de caractéristique* p *et l'on pose* $I := (0, x_1, x_2, \cdots) \in W(R)$ *avec* $x_i \in R$.

1. $W(R)$ *est un anneau intègre, de caractéristique nulle, local, d'unique idéal maximal* I *tel que* $\dfrac{W(R)}{I} \simeq R$.
2. *Si* R *est parfait alors tout élément non-nul de* $W(R)$ *s'écrit de manière unique sous la forme* $p^k c$ *avec* $k \geq 0$ *et* $c \notin I$.

Suivant le même modèle, on peut décider de tronquer les suites infinies ci-dessus à partir d'un rang n et définir ainsi *l'anneau des vecteurs de Witt tronqués de longueur* n *à coefficients dans* R noté $W_n(R)$ (en particulier,

$W_1(R) \simeq R$). Il s'agit d'un anneau commutatif unitaire d'élément unité le n-uplet $(1, 0, \cdots, 0)$. Les applications suivantes de projection interviennent alors tout naturellement :

$$\begin{array}{rcl} \sigma_n : W(R) & \to & W_n(R) \\ (a_i) & \mapsto & (a_0, \cdots, a_{n-1}) \end{array}$$

et

$$\begin{array}{rcl} f_{mn} : W_n(R) & \to & W_m(R) \\ (a_0, a_1, \cdots, a_{n-1}) & \mapsto & (a_0, \cdots, a_{m-1}) \end{array}$$

pour $m \leqslant n$. Les propriétés suivantes sont immédiates :

1. $Ker\sigma_1 \supset Ker\sigma_2 \supset \cdots Ker\sigma_n \supset \cdots$
2. $\bigcap_{i=1}^{\infty} Ker\sigma_i = \{0\}$

Il est commode d'introduire aussi certaines applications caractéristiques qui, de par leurs propriétés, sont amenées à intervenir régulièrement dans les démonstrations.

1. *L'application de plongement*

$$\begin{array}{rcl} r_0 : R & \to & W(R) \\ a & \mapsto & (a, 0, \cdots, 0, \cdots) \end{array}$$

Elle satisfait :
– $r_0(ab) = r_0(a)\, r_0(b) \quad \forall a, b \in R$
– $r_0(a) * (x_0, x_1, \cdots) = (ax_0, a^p x_1, \cdots) \quad \forall a \in R$ et $x \in W(R)$
Dans le cas particulier où l'on prend pour R un corps K de caractéristique p, on parle pour $r_0 = T$ de l'application de Teichmüller.

2. *L'application de "décalage" ou "Verschiebung"*

$$\begin{array}{rcl} V : W(R) & \to & W(R) \\ (x_0, x_1, \cdots) & \mapsto & (0, x_0, x_1, \cdots) \end{array}$$

Elle satisfait :
– $V(x+y) = V(x)+V(y) \quad \forall \; x, y \in W(R)$

– et donne lieu à la suite exacte :

$$0 \to W_n(R) \overset{V}{\hookrightarrow} W_{n+1}(R) \twoheadrightarrow R \to 0$$

3. *L'application "Frobenius"*

$$\begin{aligned} \mathbf{F} : W(R) &\to W(R) \\ (x_0, x_1, \cdots) &\mapsto (x_0^p, x_1^p, \cdots) \end{aligned}$$

Elle commute avec le "Verschiebung" selon :
– $V\mathbf{F}(x) = \mathbf{F}V(x) = px$

Lorsque $R = K$ désigne un corps de caractéristique p, les applications $\mathbf{F}$ et V sont injectives ; si en outre K est un corps parfait de caractéristique p (typiquement un corps fini) alors $\mathbf{F}$ est un *automorphisme* de $W(K)$.
Remarque : On peut construire l'anneau des vecteurs de Witt de longueur n comme suit :

$$W_n(\mathbb{F}_p) \simeq \frac{W(\mathbb{F}_p)}{V^n W(\mathbb{F}_p)}.$$

Théorème 1.4.4. *Soient R un anneau commutatif arbitraire de caractéristique p et $n \geq 1$ un entier. Si l'on désigne par $\boldsymbol{F}_n$ la restriction de $\boldsymbol{F}$ à $W_n(R)$ alors les applications $\boldsymbol{F}$ et $\boldsymbol{F}_n$ sont des homomorphismes d'anneaux.*
On a l'isomorphisme : $W_n(\mathbb{F}_p) \simeq \dfrac{\mathbb{Z}}{p^n\mathbb{Z}}$ donné par :

$$\begin{aligned} W_n(\mathbb{F}_p) &\to \frac{\mathbb{Z}}{p^n\mathbb{Z}} \\ (x_0, x_1, \cdots, x_{n-1}) &\mapsto (\overline{x}_0 + \overline{x}_1 p + \cdots + \overline{x}_{n-1} p^{n-1})\ [p^n] \end{aligned}$$

où $\overline{x}_i \in \mathbb{Z}$ désigne l'unique représentant de x_i tel que $0 \leq x_i < p$.
En outre, $W_n(\mathbb{F}_p)$ est le sous-anneau premier de $W_n(R)$ qui est ainsi de caractéristique positive.

Théorème 1.4.5. *Étant donnés R un anneau commutatif de caractéristique p et n un entier naturel ≥ 1, l'application :*

$$\begin{aligned} W_n(R) &\to R \\ (x_0, x_1, \cdots, x_{n-1}) &\mapsto x_0 \end{aligned}$$

est un homomorphisme d'anneaux surjectif dont le noyau J est un idéal nilpotent.

Proposition 1.4.6. *Soit R un anneau commutatif de caractéristique p, alors pour tout n, un élément $(x_0, x_1, \cdots, x_{n-1})$ est une unité de $W_n(R)$ si et seulement si x_0 est une unité de R.*

Corollaire 1.4.7. *Soit R un anneau commutatif de caractéristique p alors un élément $x = (x_0, x_1, \cdots)$ est une unité de $W(R)$ si et seulement si x_0 est une unité de R.*

Preuve : On utilise d'une part le fait que $\{W_n(R),\ f_{mn}$ avec $n, m \in \mathbb{N},\ m \leq n\}$ est un système projectif d'anneaux et en outre que l'application

$$W(R) \to \varprojlim_n W_n(R)$$

$$x \mapsto (\sigma_n(x))$$

est isomorphisme d'anneaux. Ainsi donc, x est une unité de $W(R)$ si et seulement si $\forall\ n \geq 1\ , \sigma_n(x_0, x_1, \cdots, x_{n-1})$ est une unité de l'anneau des vecteurs de Witt tronqués $W_n(R)$. On conclut grâce à la proposition précédente.

Définition 1.4.8. *Soit E/F une extension galoisienne de groupe de Galois G où F est un corps de caractéristique $p > 0$. Pour tout entier positif n, on a que l'anneau $W_n(F)$ peut être identifié à un sous-anneau de $W_n(E)$. En particulier, l'action naturelle de G sur E peut être étendue en une action de G sur $W_n(E)$ en posant :*

$$g(a_0, a_1, \cdots, a_{n-1}) = (g(a_0), (g(a_1), \cdots, g(a_{n-1}))$$

pour $g \in G$ et $a_i \in E$. On peut alors caractériser $W_n(F)$ comme le sous-anneau de $W_n(E)$ fixé par G i.e. :

$$W_n(F) = \{a \in\ W_n(E) | ga = a\ \forall\ g \in\ G\}.$$

Proposition 1.4.9. *(Théorème 90 de Hilbert)*
Soit E/F une extension cyclique de degré n et de groupe de Galois G engendré par σ. Alors pour tout $x \in E$, on a l'équivalence :

$$N_{E/F}(x) = 1 \Leftrightarrow\ \exists\ y \in\ E^{\times}\ \textit{tel que} : x = y\sigma(y^{-1})$$

si $y \in E$ et $y \neq 0$.

Théorème 1.4.10. *Soit E/F une extension galoisienne finie de groupe de Galois G. On suppose que l'action de ce dernier sur le groupe additif de $W_n(E)$ est donnée comme ci-dessus alors :*

$$H^1(G, W_n(E)) = 0.$$

1.4.3 Les extensions d'Artin-Schreier

Le rôle joué par les extensions d'Artin-Schreier dans l'étude des extensions cycliques de degré égal à la caractéristique peut être vu comme un analogue de celui joué par les extensions de Kummer relativement à la description des extensions cycliques d'un corps global contenant les racines de l'unité et d'ordre son degré. Dans toute la suite, on se place donc dans le cas particulier où E/F est une extension cyclique de degré p en caractéristique

$p > 0$ (situation qui correspond à la construction du premier étage K_1/K_0 de notre tour d'extensions précédemment évoquée). C'est donc aux travaux d'A. et S. que nous devons la description complète de ce type d'extension, description que nous nous contenterons de rappeler dans ses grandes lignes avant de concentrer notre attention sur le cadre plus général des extensions dites "d'Artin-Schreier-Witt" de degré p^n pour $n > 1$.

Etant donnée $\overline{F}$ une clôture algébrique supposée fixée de F, on désigne par $\wp : \overline{F} \to \overline{F}$ l'opérateur défini comme suit et qui n'est autre, en théorie de Kummer, que le pendant de l'opérateur $x \mapsto x^p$:

$$\begin{array}{rcl} \wp : \overline{F} & \to & \overline{F} \\ x & \mapsto & x^p - x \end{array}$$

On peut alors énoncer le théorème de structure suivant :

Théorème 1.4.11. *Les assertions suivantes sont équivalentes :*

1. *E/F est une extension cyclique de degré p (donc galoisienne)*
2. *$E = F(y)$ avec $\wp(y) = y^p - y = u$ où $u \in F$ et $u \neq \alpha^p - \alpha, \forall\, \alpha \in F$*

Une extension ainsi générée est appelée *extension d'Artin-Schreier* et l'élément y un générateur d'Artin-Schreier de E/F. On connaît une description explicite de son groupe de Galois $Gal(E/F)$ via :

$$\sigma(y) = y + \nu,\ \nu \in \mathbb{F}_p \text{ avec } \sigma \in Gal(E/F)$$

En outre, il est possible étant donnée une extension d'Artin-Schreier fixée de caractériser les générateurs de cette dernière ; en effet, ils répondent au critère suivant :

Critère de génération : Si E/F désigne une extension d'A.S, alors $y' \in E$ engendre E si et seulement s'il existe $\mu \in \mathbb{F}_p \subset F$ et $\zeta \in F$ tels que :

$$y' = \mu y + \zeta$$

et

$$y'^p - y' = u' = \mu u + (\zeta^p - \zeta)$$

i.e. si et seulement si $y' \in \wp^{-1}(u')$ avec $u' \in F$ et $u' - \mu u \in \wp(F)$ pour $\mu \in \mathbb{F}_p$. Dans ce cas, le polynôme minimal de y' sur F est donné par $f(T) = T^p - T - u' \in F[T]$.
Reste qu'outre la manière de générer des extensions d'A.-S., nous voudrions connaître leur comportement du point de vue de la ramification et savoir en particulier si ce dernier peut se lire assez simplement. Avant d'énoncer la proposition qui nous renseignera à ce propos on introduit la définition suivante ...

Définition 1.4.12. *Soient F/k un corps de fonctions de caractéristique $p > 0$ de corps des constantes k suposé parfait et $\mathfrak{p}$ une place de F* (dont on rappelle qu'elles sont toutes ultramétriques). *Pour chaque élément $u \in F$, on définit l'entier $\lambda_{\mathfrak{p}}(u)$ égal à :*

- λ *s'il existe un élément* $\zeta := \zeta(\mathfrak{p}, u) \in F$ *tel que :*

$$v_{\mathfrak{p}}(u - (\zeta^p - \zeta)) = -\lambda < 0 \quad avec \quad \lambda \not\equiv 0\ [p]$$

- 0 *s'il existe un élément* $\zeta := \zeta(\mathfrak{p}, u) \in F$ *avec* $v_{\mathfrak{p}}(u - (\zeta^p - \zeta)) \geqslant 0$

Remarques :

1. S'il existe ζ_1 et $\zeta_2 \in F$ avec $\lambda_1 := v_{\mathfrak{p}}(u + (\zeta_1^p - \zeta_1))$ et $\lambda_2 := v_{\mathfrak{p}}(u + (\zeta_2^p - \zeta_2))$ non-congrus à 0 modulo p alors $\lambda_1 = \lambda_2$. L'entier λ défini plus haut associé à une place $\mathfrak{p}$ fixée est donc unique et c'est de lui que l'on va tirer tous les renseignements concernant les places susceptibles de se ramifier dans une extension d'A.-S.
2. Si y' désigne un autre générateur d'Artin-Schreier de E/F tel que $\wp(y') = u'$ alors $\lambda_{\mathfrak{p}}(u) = \lambda_{\mathfrak{p}}(u')$.

Proposition 1.4.13. *Étant donnée une extension d'Artin-Schreier E/F de générateur y tel que $\wp(y) = u \in F$ alors :*
- $\mathfrak{p}$ *est non-ramifiée dans E si et seulement si* $\lambda_{\mathfrak{p}}(u) = 0$
- $\mathfrak{p}$ *est totalement ramifiée dans E si et seulement si* $\lambda_{\mathfrak{p}}(u) > 0$

L'énoncé ci-dessus montre combien il est primordial, pour maîtriser le comportement de la ramification dans une extension du type E/F d'être en mesure de déterminer explicitement l'entier $\lambda_{\mathfrak{p}}(u)$ associé à une place $\mathfrak{p}$; aussi nous signalons qu'il existe un algorithme assez simple qui permet d'effectuer cette détermination (voir à ce propos [16]).
Après ce bref rappel, comme un échauffement avant d'entreprendre la vertigineuse ascension de la tour, nous en arrivons à dresser le plan de la construction des étages supérieurs en introduisant les extensions d'Artin-Schreier-Witt ...

1.4.4 Les extensions d'Artin-Schreier-Witt : une description explicite

On supposera fixés dans toute la suite un entier naturel n et une clôture algébrique $\overline{F}$ d'un corps de fonctions F (typiquement $\mathbb{F}_p[T]$). On note A le groupe additif associé à l'anneau des vecteurs de Witt de longueur n $W_n(\overline{F})$. On dote A d'une structure additive de G-module via :
- $\mathrm{id}(a) = a$, $a \in A$

- $\sigma(a+b) = \sigma(a) + \sigma(b)$ si $a, b \in A$
- $\sigma(\tau(a)) = (\sigma\tau)(a)$ si $\sigma, \tau \in G$

Pour tout corps intermédiaire $F \subseteq E \subseteq \overline{F}$, on a :

$$A \cap E^n = W_n(E)$$

On définit alors l'homorphisme suivant dont le rôle sera essentiel dans toute la suite.

Proposition 1.4.14. *L'homomorphisme*

$$\begin{array}{rcl} \wp : W_n(\overline{F}) & \to & W_n(\overline{F}) \\ (x_1, x_2, \cdots, x_n) & \mapsto & (x_1^p, x_2^p, \cdots, x_n^p) - (x_1, x_2, \cdots, x_n) \end{array}$$

(où le signe $-$ est à prendre au sens du calcul instauré par Witt pour définir la structure d'anneau) satisfait aux propriétés suivantes :

1. *$\wp$ est G-linéaire*
2. *$\wp$ est surjectif*
3. *Le noyau $\mu_\wp$ de $\wp$ est fini, cyclique, d'ordre p^n. Plus précisément, on a l'isomorphisme :*

$$\mu_\wp = W_n(\mathbb{F}_p) \simeq \frac{\mathbb{Z}}{p^n\mathbb{Z}}$$

Preuve : Elle ne présente pas de réel intérêt si ce n'est d'illustrer un certain type de raisonnement par récurrence très prisé dans le contexte des vecteurs de Witt.

1. La première assertion se vérifie immédiatement.
2. Montrer la surjectivité de $\wp$, cela signifie étant donné $(b_1, b_2, \cdots, b_n) \in W_n(\overline{F})$, exhiber $(a_1, a_2, \cdots, a_n) \in W_n(\overline{F})$ tel que :

$$\wp((a_1, a_2, \cdots, a_n)) = ((b_1, b_2, \cdots, b_n)).$$

Le polynôme $T^p - T - b_1 \in \overline{F}[T]$ étant séparable, il existe $a_1 \in \overline{F}$ tel que $a_1^p - a_1 = b_1$. On suppose déterminés $d_2, \cdots, d_n$ réalisant :

$$\begin{array}{rcl} \wp((0, d_2, \cdots, d_n)) & = & (b_1, b_2, \cdots, b_n) - \wp((a_1, 0, \cdots, 0)) \\ & := & (0, b_2', \cdots, b_n'), \end{array}$$

ainsi donc on aurait :

$$\begin{array}{rcl} \wp((a_1, d_2, \cdots, d_n)) & = & \wp((0, d_2, \cdots, d_n)) + \wp((a_1, 0, \cdots, 0)) \\ & = & (b_1, b_2, \cdots, b_n) \end{array}$$

et le résultat serait acquis. Reste à remarquer que

$$\wp((0, d_2, \cdots, d_n)) = (0, b_2', \cdots, b_n') \in W_n(\overline{F})$$

si et seulement si

$$\wp((d_2, \cdots, d_n)) = (b'_2, \cdots, b'_n) \in W_{n-1}(\overline{F}),$$

ainsi donc on construit le candidat $(a_1, a_2, \cdots, a_n)$ par récurrence.

3. On vérifie simplement que :

$$\begin{aligned}
\mu_\wp &= \{x \in W_n(\overline{F}) |\ \wp(x) = 0\} \\
&= \{x \in W_n(\overline{F}) |\ \mathbf{F}(x) - x = 0\} \\
&= \{x = (x_1, x_2, \cdots, x_n) \in W_n(\overline{F}) | (x_1^p, x_2^p, \cdots, x_n^p) = (x_1, x_2, \cdots, x_n)\} \\
&= \{x = (x_1, x_2, \cdots, x_n) \in W_n(\overline{F}) |\ x_i \in \mathbb{F}_p\}
\end{aligned}$$

d'où le résultat.

Remarques :

- Si R est un anneau de caractéristique p (ie tel que $pR = 0$), on a la suite exacte :
$$0 \to W_n(\mathbb{F}_p) \hookrightarrow W_n(R) \xrightarrow{\wp} W_n(R)$$
- Pour rendre le plus naturel possible l'intervention de l'opérateur $\wp$ et faire le parallèle avec les outils que l'on manipule habituellement, on consigne dans le tableau suivant quelques rappels concernant la théorie de Kummer dans toute sa généralité telle qu'elle est exposée par exemple dans [48].

Dualité de Kummer classique	Dualité d'Artin-Schreier
Soient n un entier positif et K un corps global contenant les racines n-ième de l'unité (on notera le groupe associé μ_n). La dualité de Kummer a pour objet la description des extensions abéliennes d'exposant n de K au moyen du groupe $\dfrac{K^\times}{(K^\times)^n}$	Étant donné un corps F de caractéristique $p > 0$, la théorie d'Artin-Schreier s'intéresse à la description des extensions E de F d'exposant p^n.
On considère le groupe μ_n comme le noyau de l'opérateur : $$\wp : \overline{K} \to \overline{K}$$ $$x \mapsto x^n;$$ ce faisant, $(K^\times)^n$ n'est autre que l'image du groupe multiplicatif $K^\times$ par ce dernier.	Étant supposée fixée $\overline{F}$ une clôture algébrique de F on considère l'opérateur dit "d'Artin-Schreier" $$\wp : W_n(\overline{F}) \to W_n(\overline{F})$$ $$x \mapsto x^p - x.$$ On introduit, $$Ker\ \wp = \{x \in W_n(\overline{F}) \text{tels que } x^p = x\}$$ (égalité au sens des vecteurs de Witt)
Soit Δ un sous groupe *multiplicatif* de $\dfrac{K^\times}{(K^\times)^n}$(i.e. un sous-groupe de $K^\times$ contenant $(K^\times)^n$.) L'extension $L = K(\Delta^{1/n})$ est bien définie et est galoisienne sur K. On considère l'accouplement de Kummer : $$Gal(L/K) \times \Delta \to \mu_n$$ $$(\sigma, \alpha) \mapsto \frac{\sigma(\alpha^{1/n})}{\alpha^{1/n}}$$ dont on montre qu'il est *non-dégénéré* .	On se donne Δ un sous-groupe *additif* de $W_n(F)$ tel que $\wp(W_n(F)) \subseteq \Delta$. L'extension $E = F(\wp^{-1}(\Delta))$ est bien définie et est galoisienne sur F. On considère l'accouplement *non-dégénéré* d'Artin-Schreier : $$Gal(E/F) \times \Delta \to Ker(\wp)$$ $$(\sigma, u) \mapsto \sigma(\wp^{-1}(u)) - \wp^{-1}(u)$$
On dispose alors des résultats suivants : – $Gal(L/K)$ est fini si et seulement si $\dfrac{\Delta}{(K^\times)^n}$ est fini. – Si $Gal(L/K)$ est fini, l'accouplement ψ induit la suite d'isomorphismes : $$Gal(L/K) \simeq \text{Hom}(\frac{\Delta}{(K^\times)^n}, \mu_n)$$ $$\overset{n.c.}{\simeq} \frac{\Delta}{(K^\times)^n}$$	On a les assertions suivantes : – $Gal(E/F)$ est fini si et seulement si $\dfrac{\Delta}{\wp(W_n(F))}$ est fini. – Si $Gal(E/F)$ est fini, alors l'accouplement ψ induit les isomorphismes suivants : $$Gal(E/F) \simeq \text{Hom}(\frac{\Delta}{\wp(W_n(F))}, Ker(\wp))$$ $$\overset{n.c.}{\simeq} \frac{\Delta}{\wp(W_n(F))}$$

et

$$\frac{\Delta}{(K^\times)^n} \simeq \text{Hom}(Gal(L/K), \mu_n) \overset{n.c.}{\simeq} Gal(L/K).$$

En particulier,

$$[L:K] = |\frac{\Delta}{(K^\times)^n}| = (\Delta : (K^\times)^n)$$

et

$$\frac{\Delta}{\wp(W_n(F))} \simeq \text{Hom}(Gal(E/F), Ker(\wp)) \overset{n.c.}{\simeq} Gal(E/F).$$

En particulier,

$$[E:F] = |\frac{\Delta}{\wp(W_n(F))}| = (\Delta : (\wp(W_n(F)))$$

On peut énoncer le lemme suivant :

Lemme 1.4.15. *Soit Δ un sous-groupe additif de $W_n(F)$ tel que $\wp(W_n(F)) \subseteq \Delta$. Les assertions suivantes sont équivalentes :*

1. $\frac{\Delta}{\wp(W_n(F))} \simeq \frac{\mathbb{Z}}{p^n\mathbb{Z}}$
2. $\Delta = \Delta_u$ *pour* $u = (u_1, u_2, \cdots, u_n) \in W_n(F)$ *avec* $u_1 \neq \alpha^p - \alpha, \forall\ \alpha \in F$

Comme conséquence de ce qui précède, on a la description des extensions d'Artin-Schreier-Witt suivante :

Théorème 1.4.16. *Les assertions suivantes sont équivalentes* [5] *:*

1. *E/F est une extension d'Artin-Schreier-Witt cyclique de degré p^n*
2. *$E = F(y) = F(\wp^{-1}(u))$ où $\wp(y) = u \in W_n(F)$ et $p^i u \notin \wp(W_n(F)$ $\forall\ 1 \leq i < n$, i.e. $\overline{\Delta} := \frac{\Delta_u}{\wp(W_n(F))}$ est cyclique d'ordre p^n.*
3. *$E = F(y) = F(\wp^{-1}(u))$ où $u = (u_1, u_2, \cdots, u_n) \in W_n(F)$ avec $\wp(y) = u$ et $u_1 \neq \alpha^p - \alpha\ \forall\ \alpha \in F$*

Soit maintenant E/F une extension d'A.-S.-W. de degré p^n ; par application du théorème ci-dessus, on peut la paramétrer selon $E = F(y_1, y_2, \cdots, y_n)$ avec les conditions rappelées plus haut.
On pose alors :

$E_0 = F,\ E_n := E$ et $E_i := F(y_1, y_2, \cdots, y_i)$ le i-ème corps intermédiaire entre E et F. On remarque alors que E_i/F est cyclique et admet pour uniques sous-corps intermédiaires la famille $\{F, E_1, E_2, \cdots, E_{i-1}\}$ si bien que l'on a :

$$E_i = F(y_1, \cdots, y_i) = F_{i-1}(y_i)$$

[5] La notation $\wp^{-1}$ peut sembler abusive dès lors que l'homorphisme $\wp$ est simplement surjectif, néammoins cette dernière étant communément admise par les spécialistes, nous nous y conformons.

En particulier, chaque extension E_i/E_{i-1} est une extension d'Artin-Schreier de générateur y_i.

Description du groupe de Galois $Gal(E/F)$:

Soit σ un élément de $Gal(E/F)$; on vérifie que l'application

$$\begin{array}{rccc} \psi : Gal(E/F) & \to & \mu_\wp \\ \sigma & \mapsto & \sigma(y) - y \end{array}$$

est un isomorphisme et par conséquent si y désigne un générateur d'Artin-Schreier-Witt de E, on a $\sigma(y) = y + \alpha$ où α est un générateur de $\mu_\wp = W_n(\mathbb{F}_p) \simeq \dfrac{\mathbb{Z}}{p^n\mathbb{Z}}$. On en déduit par conséquent que pour $k \in \mathbb{N}$, les itérés $\sigma^k(y) = y + k\alpha$. En d'autres termes, les éléments de $Gal(E/F)$ sont donnés par :

$$\sigma^k(y_i) = (y + k\alpha)_i,\ 1 \leqslant i \leqslant n \text{ et } 1 \leqslant k \leqslant p^n.$$

Remarque : On a $\sigma(y) = y + \alpha = (y_1 + c_0, \cdots, y_n + c_{n-1})$ avec $c_i \in E_i$ ie $\sigma_i(y_j) = y_j + c_{j-1}$ pour $1 \leq j \leq i \leq n$ où est un générateur du groupe de Galois de l'extension intermédiaire E_i/F tel que $\sigma_i|_{E_j} = \sigma_j$.

Définition 1.4.17.

- *Tout élément* $y' = (y'_1, \cdots, y'_n) \in \wp^{-1}(W_n(F))$ *tel que* $E := E_n = F(y'_1, \cdots, y'_n)$ *est appelé générateur d'Artin-Schreier-Witt de* E/F .
- *Si* y' *est un générateur d'Artin-Schreier-Witt de* E/F *alors pour chaque entier naturel* i, $1 \leq i \leq n$, $(y'_1, \cdots, y'_i)$ *est un générateur d'A.S.W. de* E_i/F.

Etant donnée une extension E/F fixée, la proposition suivante fournit une caractérisation de l'ensemble de ses générateurs :

Proposition 1.4.18. *Soit* E/F *une extension d'A.S.W. de degré* p^n *i.e. telle que* $E = F(y_1, \cdots, y_n)$ *avec* $y = (y_1, \cdots, y_n) \in \wp^{-1}(u)$ *pour* $u \in W_n(F)$ *et* $u_1 \neq \alpha^p - \alpha\ \forall\ \alpha\ \in F$, *alors pour* $y' \in W_n(\overline{F})$ *les assertions suivantes sont équivalentes :*

1. y' *est un générateur d'A.S.W. de* E/F
2. $y' \in \wp^{-1}(u')$ *pour* $u' \in W_n(F)$ ***et*** $u' - \lambda u \in \wp(W_n(F))$ *avec* $\lambda \in (\dfrac{\mathbb{Z}}{p^n\mathbb{Z}})^\times$
3. $y' = \lambda y + \zeta$ *pour* $\lambda \in (\dfrac{\mathbb{Z}}{p^n\mathbb{Z}})^\times$ *et* $\zeta \in W_n(F)$

Preuve :$1 \Leftrightarrow 2$.

$$\begin{aligned} F(y) = F(y') &\Leftrightarrow F(\wp^{-1}(\Delta_u) = F(\wp^{-1}(\Delta_{u'}) \\ &\Leftrightarrow \Delta_u = \Delta_{u'} \\ &\Leftrightarrow \overline{\Delta_u} = \overline{\Delta_{u'}} \\ &\Leftrightarrow \exists\, \lambda \in (\frac{\mathbb{Z}}{p^n\mathbb{Z}})^\times \end{aligned}$$

avec $u' - \lambda u \in \wp(W_n(F))$.

$2 \Rightarrow 3$: Soit $u' \equiv \lambda u \; mod \; (\wp(W_n(F))$ pour $\lambda \in (\frac{\mathbb{Z}}{p^n\mathbb{Z}})^\times$ *i.e.* $u' = \lambda u + \wp(\theta)$ avec $\theta \in W_n(F)$. Si $y' \in \wp^{-1}(u')$ alors on a $y' = \lambda y + \theta + \theta'$ avec $\theta' \in Ker(\wp) \subset W_n(F)$.
$3 \Rightarrow 2$: Si $y' = \lambda y + \zeta$ pour $\lambda \in (\frac{\mathbb{Z}}{p^n\mathbb{Z}})^\times$ et $\zeta, \in W_n(F)$ alors $\wp(y') = \lambda u + \wp(\zeta) := u' \in W_n(F)$ et $u - u' = \wp(\zeta) \in \wp(W_n(F)$.

1.4.5 Les extensions d'Artin-Schreier-Witt du point de vue de la ramification

Je tiens à exprimer toute ma reconnaissance à Peter Roquette pour sa précieuse aide dans la traduction des articles fondateurs de H.L.Schmid et E. Wittt [6] dont le contenu est repris ci-après.

Dans [58], H.L. Schmid se place dans le contexte suivant que nous observerons dans toute la suite :

- k est un corps fini de caractéristique p
- F est un corps de fonctions d'une variable de corps des constantes k
- E/F est une extension cyclique de degré p^n de groupe de Galois G ; en particulier, $E = F(y)$ avec $\wp(y) = u$ pour y et u deux vecteurs de Witt de longueur n convenables (on rappelle en particulier que la condition $u_1 \notin \wp(F)$ est nécessaire et suffisante pour que l'équation $\wp(y) = u$ soit irréductible et définisse ainsi une extension de degré exactement p^n sur F).

On considère la tour de corps suivante :

$$F := E_0 \subseteq E_1 \subseteq \cdots \subseteq E_n = E$$

telle que $E_i = E_{i-1}(y_i)$ avec $\wp(y_i) \in E_{i-1}$ et $[E_i : E_{i-1}] = p$. . Soit σ un élément du groupe de Galois de E/F ; on a vu qu'il opérait sur les vecteurs

[6] [57], [58], [59], [60] et [70]

de Witt "composante par composante" et puisque y^σ est aussi une solution de l'équation $\wp(y) = u$, on a :

$$y^\sigma = y + \chi(\sigma)$$

avec $\chi(\sigma)_; \in W_n(\mathbb{F}_p)$.
On rappelle que l'application :

$$\chi : G \to W_n(\mathbb{F}_p) \simeq (\frac{\mathbb{Z}}{p^n\mathbb{Z}}, +)$$

est un isomorphisme ; par conséquent il existe un unique $\sigma_0 \in G$ tel que $\chi(\sigma_0) = \mathbf{1} := (1, 0, \cdots, 0)$ et qui engendre le groupe de Galois G.
Soit maintenant $\mathfrak{p}$ une place de F et $v_\mathfrak{p}$ la valuation $\mathfrak{p}$-adique associée. On introduit la définition suivante qui est à rapprocher de l'élément λ que l'on avait défini dans le cas "élémentaire" des extensions d'Artin-Schreier.

Définition 1.4.19. *On dira d'un élément $a \in F$ qu'il est $\mathfrak{p}$-normalisé si $v_\mathfrak{p}(a) \geq 0$ ou bien si $v_\mathfrak{p}(a) \not\equiv 0\ [p]$. Plus généralement, on dira qu'un vecteur $a \in W_n$ est $\mathfrak{p}$-normalisé si chacune de ses composantes a_i est $\mathfrak{p}$-normalisée.*

Remarque : Cette définition se justifie car on peut montrer par récurrence sur n que l'on peut toujours trouver un vecteur $c \in W_n(F)$ tel que $a + \wp(c)$ soit $\mathfrak{p}$-normalisé (le cas $n = 1$ a été démontré par Hasse dans [26]). Ainsi donc, quitte à remplacer u par $u+\wp(c)$, on peut toujours supposer u **$\mathfrak{p}$-normalisé** .

H.L. Schmid définit ensuite le vecteur $\lambda = (\lambda_1, \cdots, \lambda_n)$ via ses composantes selon :

$$\lambda_i = 0 \quad \text{si } v_\mathfrak{p}(a_i) \geq 0$$

et

$$\lambda_i = -v_\mathfrak{p}(a_i) \quad \text{si } v_\mathfrak{p}(a_i) < 0.$$

En d'autres termes, λ_i désigne l'ordre du pôle (s'il existe) de a_i en $\mathfrak{p}$. *En particulier, le vecteur λ ainsi construit n'est pas un vecteur de Witt* mais simplement un n-uplet dont les composantes sont des nombres naturels positifs ou nuls. En fait, et pour être tout à fait rigoureux, on devrait noter ce dernier $\lambda(\mathfrak{p})$ pour marquer la dépendance de ce vecteur vis à vis de la place $\mathfrak{p}$ ce dont on se dispensera en l'absence d'ambigüité.
Reste que c'est la forme de ce vecteur qui va permettre de coder la ramification de la place $\mathfrak{p}$ au sein de la tour d'extension via le théorème suivant :

Théorème 1.4.20. *La place $\mathfrak{p}$ est ramifiée dans E si et seulement si le vecteur $\lambda := \lambda(\mathfrak{p})$ n'est pas le vecteur nul. En outre, si $\lambda_i > 0$ désigne la première composante non-nulle de λ alors $\mathfrak{p}$ est ramifiée dans E/E_{i-1}*

Exemple : Si l'on suppose que $\lambda_1 > 0$ alors $\mathfrak{p}$ est ramifiée dans E/F. De même, la place de F est non ramifiée dans E si et seulement si $\lambda = 0$.

Voyons maintenant comment le formalisme de Witt permet de construire *un critère normique* adapté au cas des extensions cycliques en caractéristique p. La question est la suivante :

Étant donnée une extension cyclique E/F de degré p^n paramétrée par un vecteur de Witt de longueur n, quand peut-on dire qu'un élément $\alpha \in F$, $\alpha \neq 0$ est la norme d'un élément de E ?
On commence de prime abord par se remémorer le "Principe Local-Global" de Hasse, outil majeur de la théorie du corps de classes, celle-là même qui est à l'origine de l'élaboration de la théorie d'Artin-Schreier-Witt.

Théorème 1.4.21. *(*Hasse 1930*) Étant donnée une extension algébrique de corps globaux, un élément α est une norme de E/F si et seulement s'il s'agit d'une norme de $E_\mathfrak{p}/F_\mathfrak{p}$ pour chaque place $\mathfrak{p}$ de F (par abus de langage, on note encore $\mathfrak{p}$ une place de E au-dessus de $\mathfrak{p}$).*

Autrement dit, α est une norme dans l'extension globale si et seulement s'il s'agit d'une norme "localement partout". Ainsi donc, il suffirait pour répondre à notre interrogation d'établir un critère permettant de déterminer sous quelle(s) condition(s) un élément est une norme locale.
On peut en outre opérer une seconde réduction car dans le cas où l'extension locale $E_\mathfrak{p}/F_\mathfrak{p}$ (que pour simplifier, la place étant supposée fixée, l'on continuera de noter E/F) est *non-ramifiée*, la condition pour que α soit norme est bien connue : on doit voir satisfaite la congruence,

$$v_\mathfrak{p}(\alpha) \equiv 0 \ [p^{n_\mathfrak{p}}]$$

où $p^{n_\mathfrak{p}} = [E_\mathfrak{p} : F_\mathfrak{p}]$. En particulier, si $v_\mathfrak{p}(\alpha) = 0$ (ce qui est le cas pour presque tout $\mathfrak{p}$ par la forme additive de la formule du produit) alors α est une norme locale en $\mathfrak{p}$. On est donc ramené à considérer le cas où $\mathfrak{p}$ se ramifie.

On se place dorénavant dans le contexte suivant :

- On suppose que E est un corps local (i.e. muni d'une valuation discrète et complet pour cette dernière), typiquement un corps de séries formelles sur $k = \mathbb{F}_q$ supposé fini.
- Soit $\mathfrak{p}$ une place de F *fixée* (ce qui nous permettra d'oublier la dépendance).
- E/F une extension cyclique de corps locaux de degré p^n

Remarque : Localement, on a comme pour les extensions globales $E_\mathfrak{p} = F_\mathfrak{p}(y_\mathfrak{p})$ où $y_\mathfrak{p}$ est un vecteur de Witt de longueur $n_\mathfrak{p}$ et $F_\mathfrak{p}$ est un corps de

séries formelles d'une variable (typiquement $\mathbb{F}_q((T))$).

Etant donné $\alpha \in F(\alpha \neq 0)$, Witt, pour établir son critère normique, raisonne en terme d'*algèbres* si bien que l'on débute par un bref rappel concernant la notion d'algèbre centrale simple :

Rappel : On commence par énoncer le critère suivant dont on se servira comme d'une définition [7].

Définition 1.4.22. *Etant donné un corps K, on considère A une K-algèbre de dimension finie. On dit de cette dernière est* centrale simple *si et seulement s'il existe une extension galoisienne finie L de K telle que $A_L = A \otimes_K L$ soit isomorphe à une algèbre de matrices $\mathcal{M}_n(L)$.*

Définition 1.4.23. *On considère A une K-algèbre de dimension finie supposée centrale simple. On dit de A* qu'elle se décompose *sur l'extension galoisienne L/K (ou encore que L est le corps de décomposition de A) si l'on dispose d'un isomorphisme $A_L = A \otimes_K L \simeq M_n(L)$ pour un certain n.*

Cas Particulier : L'algèbre A est dite cyclique si son corps de décomposition L/K est une extension cyclique de degré $\sqrt{\dim_K(A)}$.

Définition 1.4.24. *On dit de deux K-algèbres centrales simples (de dimension finie) qu'elles sont équivalentes s'il existe des entiers r et s tels que :*

$$A \otimes_K M_r(K) \simeq B \otimes_K M_s(K)$$

On écrit alors : $A \sim B$. On appelle "groupe de Brauer" d'un corps K et l'on note $Br(K)$ l'ensemble des classes de similarité $[A]$ de la K-algèbre centrale simple A [8] ; muni de la multiplication induite par le produit tensoriel et définie par :

$$[A][B] = [A \otimes_K B],$$

ce dernier est doté d'une structure de groupe abélien.

Après ce court intermède, revenons à notre problème ...

Soit donc à considérer pour α $(\neq 0) \in F$ et $\beta = (\beta_0, \beta_1, \cdots, \beta_{n-1})$ un vecteur de Witt de longueur n, l'algèbre cyclique $(\alpha|\beta]$ définie par les générateurs $u, y_0, y_1, \cdots, y_{n-1}$ où les y_i commutent entre eux et où l'on dispose des relations :

$$u^{p^n} = \alpha, \;\; y^p - y = \beta \;, \;\; uyu^{-1} = y + \mathbf{1}$$

[7] voir par exemple [23] ou [48] pour des informations complémentaires

[8] Merkuriev et Suslin ont démontré que toute classe de similarité d'algèbres centrales simples contient un produit tensoriel de produits croisés. On peut même préciser qu'il s'agit de produits croisés d'algèbres cycliques.

si **1** désigne l'élément unité $(1, 0, \cdots, 0)$ et uyu^{-1} signifie $(uy_0u^{-1}, \cdots, uy_{n-1}u^{-1})$.

On rappelle que cette dernière se décompose *si et seulement si* α est une norme dans E. On est donc ramené à définir des conditions garantissant que l'algèbre $(\alpha|\beta]$ se décompose. Pour ce faire, on considère l'unique extension non-ramifiée de $\mathbb{Q}_p$ de corps résiduel fini k (le corps des constantes associé à F) que l'on note K'.
La série formelle

$$\alpha = a_m T^m + a_{m-1}T^{m-1} + \cdots \text{avec } a_i \in \mathbb{F}_q \text{ et } a_m \neq 0$$

peut se relever en une série formelle à coefficients dans K' :

$$A = A_m T^m + A_{m-1}T^{m-1} + \cdots$$

où $a_i \equiv A_i\ [p]$. De la même façon, les composantes β_i du vecteur de Witt β peuvent être relevées en séries formelles à coefficients dans K'. On obtient alors un vecteur $B = (B_0, B_1, \cdots, B_{n-1})$ de longueur n en caractéristique 0 auquel on associe sa n-i-ème "composante fantôme" [9] :

$$B^{(n-1)} = B_0^{p^{n-1}} + pB_1^{p^{n-2}} + \cdots + p^{n-1}B_{n-1}$$

qui est une série formelle sur K'.
On considère la différentielle $\frac{dA}{A}.B^{(n-1)}$ (où $\frac{dA}{A}$ désigne la dérivée logarithmique) et le résidu associé $\text{Res}(\frac{dA}{A}.B^{(n-1)})$ qui, par définition, n'est autre que le coefficient de T^{-1} dans le développement en puissances de T. Ce dernier est un élément du corps résiduel (en fait de l'anneau de valuation associé) et si l'on note S (pour "Spur") la fonction "Trace" de K' dans $\mathbb{Q}_p$, alors $\gamma := S(\text{Res}(\frac{dA}{A}.B^{(n-1)}))$ est un élément du corps des nombres p-adiques. On peut en fait montrer que $v_p(\gamma) \geq 0$ et que par conséquent $\gamma \in \mathbb{Z}_p (:= \varprojlim_n (\frac{\mathbb{Z}}{p^n\mathbb{Z}}))$ ce qui nous permet d'introduire une application :

$$(\alpha, \beta] \mapsto S(\text{Res}(\frac{dA}{A}.B^{(n-1)})) \in \frac{\mathbb{Z}}{p^n\mathbb{Z}}$$

Witt a montré que cette application est bien définie (au sens où elle ne dépend pas du choix des relèvements A et B de α et β).
On peut alors énoncer le critère suivant qu'utiliseront dans leur article Villa et Madan :

[9] voir annexes p 43

Théorème 1.4.25. *(Critère normique de Witt* [10]*) L'algèbre* $(\alpha, \beta]$ *se décompose si et seulement si :*

$$S(Res\ (\frac{dA}{A}B^{(n-1)})) \equiv 0\ [p^n]$$

Remarque : Pour être tout à fait exact, Witt montre que l'invariant de Hasse associé à l'algèbre $(\alpha, \beta]$ est congru à $\frac{1}{p^n}S(\mathrm{Res}(\frac{dA}{A})B^{(n-1)})$ mod 1 ce qui implique l'énoncé ci-dessus.

1.4.6 La loi de Réciprocité : survol

On suppose que le corps des constantes k est le corps fini $\mathbb{F}_q$ à q éléments. Si l'on note comme ci-dessus G le groupe de Galois de l'extension E/F, alors on a que toute place $\mathfrak{p}$ de F non-ramifiée dans E définit un automorphisme de Frobenius $\sigma_\mathfrak{p}$ tel que :

$$z^{\sigma_\mathfrak{p}} \equiv\ z^q \bmod \mathfrak{p}.$$

L'isomorphisme χ introduit plus haut permet de construire un symbole

$$\chi(\sigma_\mathfrak{p}) := \{\frac{a}{\mathfrak{p}}\}\ \in\ W_n(\mathbb{F}_p)$$

pour lequel H.L. Schmid a montré qu'il satisfaisait la relation :

$$\{\frac{a}{\mathfrak{p}}\} \equiv\ \Psi S_\mathfrak{p}(a) \bmod\ \mathfrak{p}$$

où $S_\mathfrak{p}$ désigne la fonction "Trace"

$$\begin{array}{rcl} S_\mathfrak{p} : W_n(\mathcal{F}) & \to & W_n(k) \\ \overline{a} & \mapsto & \overline{a} + \overline{a}^q + \cdots + \overline{a}^{q^{d-1}} \end{array}$$

avec $d = [\mathcal{F} : k]$ si $\mathcal{F}$ désigne le corps résiduel associé à F et

$$\Psi : W_n(k) \to W_n(\mathbb{F}_p)$$

la fonction "Trace" absolue i.e. relative aux sous-corps premiers. Étant donné un diviseur arbitraire (supposé premier avec le diviseur discriminant), il est maintenant facile de définir par linéarité le symbole $\{\}$ associé ; on est alors en mesure d'énoncer l'un des résultats majeurs relatif à l'obtention de la Loi de Réciprocité et dont Schmid n'avait pas fourni de preuve :

Théorème 1.4.26. *On a que :*

$$\{\frac{a}{\mathfrak{b}}\} = 0$$

(i.e. le vecteur de Witt identiquement nul *) si* $\mathfrak{b}$ *modulo les normes (de* E*) est le diviseur d'un élément* $b \equiv 1$ *modulo le conducteur* $\mathfrak{f}$ *de l'extension* E/F*.*

[10] Je remercie C. Maire pour m'avoir fait remarquer que l'on doit l'énoncé et la démonstration de ce critère généralement attribué à Witt à O. Teichmüller [66].

Annexes [11]

1.5 Quelques mots de la dualité de Pontryagin.

Puisqu'elle sera amenée à intervenir par la suite et permet en particulier d'obtenir pour les corps de nombres une expression cohomologique de la conjecture de Leopoldt (voir p104) , on se propose en quelques lignes d'introduire une dualité (au sens des catégories) particulière dite "de Pontryagin".

Pour ce faire, on considère le groupe topologique $\mathbb{R}/\mathbb{Z}$ muni de la topologie-quotient (à savoir la plus fine pour laquelle l'application de projection $\mathbb{R} \twoheadrightarrow \mathbb{R}/\mathbb{Z}$ est continue) héritée de celle de $\mathbb{R}$.
On se donne A un groupe topologique, abélien, séparé et localement compact ; on introduit alors la définition suivante :

Définition 1.5.1. *On appelle* dual de Pontryagin *de A, le groupe*

$$A^\vee := \mathrm{Hom}_{cont}(A, \mathbb{R}/\mathbb{Z}).$$

Reste avant d'énoncer le théorème de dualité dû à L.S. Pontryagin (1933)[12] à préciser qu'étant donnée deux espaces topologiques localement compacts X et Y, l'ensemble $Map_{cont}(X,Y)$ des applications continues est doté d'une topologie naturelle (qu'en anglais l'on qualifie de "compact-open topology") dont une base est donnée via :

$$\mathcal{U}_{V,U} = \{f \in Map_{cont}(X,Y) \mid f(V) \subseteq U\}$$

où V parcourt les sous-ensembles compacts de X et U les sous-ensembles ouverts de Y.

Théorème 1.5.2. *(dit "de dualité")*

- *Si A est un groupe topologique abélien, séparé et localement compact alors le dual de Pontryagin de A hérite, pour la topologie définie ci-dessus, des mêmes propriétés (à savoir $A^\vee$ est abélien, séparé et localement compact).*
- *L'homomorphisme canonique :*

$$A \xrightarrow[\sim]{\phi} (A^\vee)^\vee := \mathrm{Hom}_{cont}(A^\vee, \mathbb{R}/\mathbb{Z})$$

$$a \longmapsto \phi(a) : A^\vee \longrightarrow \mathbb{R}/\mathbb{Z}$$

$$\rho \longmapsto \rho(a) := \phi(a)(\rho)$$

[11] [48],[31]
[12] $(1908 - 1988)$

est un isomorphisme de groupes topologiques.

Conséquences :

1. "$^\vee$" définit un (auto)-foncteur *involutif* (via ϕ), *contravariant* (pour la catégorie des groupes topologiques abéliens séparés localement compacts) qui de plus, commute avec le passage à la limite (i.e. $\lim(A^\vee) = (\lim A)^\vee$).
2. "$^\vee$" induit une équivalence de catégories entre les catégories suivantes :

$$\begin{array}{rcl} \text{groupes abéliens compacts} & \overset{\vee}{\Leftrightarrow} & \text{groupes abéliens discrets} \\ \text{groupes abéliens profinis} & \overset{\vee}{\Leftrightarrow} & \text{groupes abéliens discret de torsion} \end{array}$$

Remarque : Sous certaines hypothèses sur le groupe abélien A (groupe discret de torsion ou profini), on dispose d'un isomorphisme : $A^* \simeq A^\vee$ où $A^* := \mathrm{Hom}(A, \mathbb{Q}/\mathbb{Z})$ pour la topologie définie précédemment.

1.6 Compléments

Une classe de corps particulière ...

Définition 1.6.1. *On dit d'un corps L qu'il est p-clos s'il n'admet pas d'extension galoisienne de degré p.*

Exemple : La p-extension maximale $K(p)/K$ (i.e. le compositum de toutes les extensions galoisiennes d'ordre une puissance de p) est p-clos.

Conséquence : On suppose $Car(K) = p > 0$. Si L est un corps p-clos alors il possède cette propriété intéressante que l'homomorphisme

$$\begin{array}{rcl} \wp : L & \to & L \\ x & \mapsto & x^p - x \end{array}$$

est *surjectif* ; en effet, étant donné $a \in L$, on considère le polynôme séparable $f(x) = x^p - x - a$. Si maintenant α est une racine de f alors les autres racines sont de la forme : $\{\alpha+1, \cdots, \alpha+p-1\}$ ainsi si $a \notin \wp(L)$ alors le corps de décomposition du polynôme f serait une extension de L de degré p ce qui est impossible puisque par hypothèse L est supposé p-clos. Dans ce cas, on obtient la suite exacte :

$$0 \to \mathbb{Z}/p\mathbb{Z} \hookrightarrow L \overset{\wp}{\twoheadrightarrow} L \to 0$$

La suite exacte longue de cohomologie associée permet d'énoncer :

Corollaire 1.6.2. *Soit $p = Car(K) > 0$; si L/K est p-clos alors :*

$$H^n(Gal(L/K)) = \begin{cases} K/\wp K & pour\ n = 1 \\ 0 & si\ n \geq 2 \end{cases}$$

En particulier, la p-dimension cohomologique $cd_p Gal(L/K) \leq 1$.

Remarque : Outre la suite exacte précédente, on utilise pour prouver le corollaire ci-dessus le résultat majeur suivant de cohomologie galoisienne (conséquence dans le cas fini de l'existence d'une base normale) :

"Étant donnée L/K une extension galoisienne arbitraire de groupe de Galois G alors $H^n(G, L) = 0 \ \forall\, n \geq 1$."

De cela découle le théorème caractérisant les extensions galoisiennes de K de degré une puissance de p.

Théorème 1.6.3. *Si $p = Car(K) > 0$ alors le groupe de Galois $\mathcal{G}$ de la p-extension abélienne maximale $K(p)/K$ est un pro-p-groupe libre de rang $dim_{\mathbb{F}_p}(K/\wp K)$.*

Cas des extensions du type "Artin-Schreier" :

Si maintenant l'on note K_p/K l'extension *abélienne* maximale d'exposant $p = Car(K)$ (à savoir le compositum de toutes les extensions cycliques de degré p) alors le groupe de Galois est décrit par :

$$Gal(K_p/K) = \mathcal{G}/\mathcal{G}^p[\mathcal{G}, \mathcal{G}]$$

où $[\mathcal{G}, \mathcal{G}]$ désigne l'adhérence (théorie de Galois infinie) du groupe des commutateur de $\mathcal{G} = Gal(K(p)/K)$.

La dualité de Pontryagin induit un isomorphisme :

$$Gal(K_p/K)^\vee \simeq H^1(\mathcal{G}, \mathbb{Z}/p\mathbb{Z}) \underset{cor}{\simeq} K/\wp K$$

qui à $a \in K$ associe un caractère χ_a tel que :

$$\begin{array}{rccc} \chi_a : Gal(K_p/K) & \to & \mathbb{F}_p \\ \sigma & \mapsto & \sigma(\alpha) - \alpha \end{array}$$

où α est une racine de $x^p - x = a$. On parle quelquefois pour χ_a du *caractère d'Artin-Schreier* associé à a (voir par exemple [31]). Par dualité, on obtient l'isomorphisme d'Artin-Schreier :

$$Gal(K_p/K) \simeq Hom(K/\wp K, \mathbb{Q}/\mathbb{Z})$$

Cas des extensions du type "Artin-Schreier-Witt" :

On peut généraliser les résultats précédents à l'extension abélienne maximale K_{p^n}/K d'exposant p^n dont on possède du groupe de Galois la description suivante :

$$Gal(K_{p^n}/K) = \mathcal{G}/\mathcal{G}^{p^n}[\mathcal{G},\mathcal{G}]$$

Quel que soit $n \geq 1$, il existe un unique foncteur de la catégorie des anneaux dans elle-même tel que pour tout anneau commutatif unitaire R de caractéristique nulle l'application :

$$\begin{array}{rcl} gh : W_n(R) & \to & R^n \\ (a_0, a_1, \cdots, a_{n-1}) & \mapsto & (a_0, a_0^p + pa_1, \cdots, a_0^{p^{n-1}} + pa_1^{p^{n-2}} + \cdots + p^{n-1}a_{n-1}) \end{array}$$

soit un homomorphisme d'anneaux.

Remarque : Les éléments $\{a_0, a_0^p + pa_1, \cdots, a_0^{p^{n-1}} + pa_1^{p^{n-2}} + \cdots + p^{n-1}a_{n-1}\}$ sont appelés les *composantes fantômes* ("Nebenkomponenten" en allemand) associées au vecteur de Witt a de longueur n.
Si l'on note $x^{(n)} = x_0^{p^n} + px_1^{p^{n-1}} + \cdots + p^n x_n$ la n-ième composante fantôme de x alors on peut exprimer la somme et le produit de deux vecteurs de Witt de longueur n via :

$$\begin{array}{rcl} x + y & = & (x^{(0)} + y^{(0)}, \cdots, x^{(n)} + y^{(n)}) \\ x * y & = & (x^{(0)} * y^{(0)}, \cdots, x^{(n)} * y^{(n)}) \end{array}$$

En outre, $(Vx)^{(n)} = px^{(n-1)}$ et $x^{(n)} = (Fx)^{(n)} + p^n x_n$.
Cas particulier : Le lien entre composantes "fantômes" et composantes dites "principales" se définit en caractéristique 0, ainsi lorsque l'on est amené à considérer les composantes fantômes d'un vecteur de Witt à coefficients dans un corps de caractéristique p, on perçoit implicitement ce dernier comme le corps résiduel associé à un anneau intègre de caractéristique nulle (ce qui permet de considérer les pré-images des composantes fantômes et lève ainsi toute ambigüité).

On énonce :

Théorème 1.6.4. *(Artin-Schreier-Witt) Soit K un corps de caractéristique $p > 0$ alors le groupe de Galois de l'extension abélienne maximale K_{p^n}/K d'exposant p^n est tel que :*

$$Gal(K_{p^n}/K) \simeq Hom(W_n(K)/\wp W_n(K), \mathbb{Q}/\mathbb{Z})$$

Preuve : (idée)

On désigne par $\overline{K}$ la clôture séparable de K et l'on considère la suite exacte de $G_K := Gal(\overline{K}/K)$-modules :

$$0 \to \mathbb{Z}/p^n\mathbb{Z} \hookrightarrow W_n(\overline{K}) \overset{\wp}{\twoheadrightarrow} W_n(\overline{K}) \to 0 \quad (*)$$

La suite exacte (voir p 25) :

$$0 \to W_n(\overline{K}) \overset{V}{\hookrightarrow} W_{n+1}(\overline{K}) \twoheadrightarrow \overline{K} \to 0$$

permet de prouver par récurrence sur n que le G_K-module $W_n(\overline{K})$ est cohomologiquement trivial puisque $\overline{K}$ l'est.
Reste à associer par un procédé classique à $(*)$ sa suite exacte longue de cohomologie qui en vertu du théorème 90 de Hilbert devient :

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z}/p^n\mathbb{Z} & \hookrightarrow & W_n(K) & \overset{\vartheta}{\twoheadrightarrow} & H^1(G_K, \mathbb{Z}/p^n\mathbb{Z}) & \longrightarrow & 0 \\ & & & & \downarrow & \overset{\sim}{\nearrow} & & & \\ & & & & W_n(K)/Ker(\vartheta) & & & & \end{array}$$

avec $Ker(\vartheta) = Im(\wp)$; d'où l'isomorphisme :

$$\begin{aligned} H^1(G_K, \mathbb{Z}/p^n\mathbb{Z}) &= Hom(Gal(K_{p^n}/K), \mathbb{Q}/\mathbb{Z}) \\ &\simeq W_n(K)/\wp(W_n(K)) \end{aligned}$$

et par dualité "$(.)^\vee$" :

$$Gal(K_{p^n}/K) \simeq Hom(W_n(K)/\wp(W_n(K), \mathbb{Q}/\mathbb{Z}),$$

ce que l'on voulait.

1.7 Invitation à la Théorie du Corps de Classes en caractéristique $p > 0$

Sans prétendre à aucune exhaustivité, on se propose de retracer en quelques lignes un début de chronologie relativement à un pan de la théorie des nombres souvent méconnu quoique fascinant à savoir la génèse, au travers des lois de Réciprocité et du théorème d'Existence, de la théorie du corps de classes en caractéristique positive.
Le lecteur curieux et/ou intéressé pourra pour de plus amples informations se référer par exemple à [14], [44], [51] ou encore à l'ouvrage de Shatz [63] dont on ne saurait que trop recommander la lecture, sans compter les articles fondateurs des grands acteurs de cette aventure mathématique majeure. On signale simplement que les articles de Witt (et plus généralement de *l'Ecole* d'E. Noether) utilisent fondamentalement le point de vue *des algèbres* aujourd'hui un peu vieilli, aussi on aura soin au fur et à mesure de l'exposé de suggérer le parallèle entre cette version "empirique" et la formulation en terme d'accouplement qui prévaut dans (entre autres) [14] et [63].

1.7.1 Les Formules de Réciprocité

Dans un papier daté de 1934 [26], Hasse propose dans le cas d'une extension cyclique finie E/F de degré n du corps des fonctions rationnelles une preuve alternative de la loi de Réciprocité d'Artin indépendante cette fois du théorème de Tsen et qualifiée d'élémentaire au sens où elle ne fait appel qu'à des manipulations sur des objets relativement concrets à savoir des polynômes et des fonctions rationnelles. Encouragé par cette avancée, Hasse propose alors à son étudiant, H.L. Schmid, d'essayer de généraliser ce résultat au cas où le corps de base est un corps de fonctions quelconque ce qui donna lieu à une publication extraite de la thèse de Schmid et intitulée : "Sur la loi de Réciprocité dans un corps de fonctions cyclique de corps des constantes fini". Il s'agit d'un travail effectué dans la lignée de celui de son inspirateur mais qui s'en distingue néammoins par le fait que S. propose des formules explicites pour les symboles normiques *locaux*. Comme l'avait remarqué Hasse, on est amené à distinguer deux cas selon que n est ou pas congru à 0 modulo p.

Le cas $n \not\equiv 0[p]$ relève de la t*héorie de Kummer* et fait intervenir le symbole de Hilbert dont on rappelle ci-dessous une définition [13].
Soit F un corps local (i.e. complet pour un valuation discrète) de corps résiduel supposé fini (typiquement $\mathbb{F}_q((T))$), on pose :

$$\begin{aligned}(.,.)_n : F^\times \times F^\times &\to \mu_n \\ (\alpha, \beta) &\mapsto \gamma^{-1}\psi_F(\alpha)(\gamma)\end{aligned}$$

où :

- μ_n désigne le groupe des racines de l'unité dans F^{sep}.
- $\gamma^n = \beta,\ \gamma \in\ F^{sep}$
- ψ_F désigne l'application de Réciprocité :

$$\psi_F : F^\times \to Gal(F^{ab}/F)$$

où l'on a noté F^{ab} l'extension abélienne maximale de F dans F^{sep}

On énonce quelques-unes de ses propriétés majeures dans le but de mettre en évidence le caractère "multiplicatif" sous-jacent contre celui additif de la théorie d'Artin-Schreier et des symboles qui s'y rapportent.

Proposition 1.7.1.

1. $(.,.)_n$ *est une application bilinéaire pour la structure multiplicative i.e. :* $(\alpha, \beta_1\beta_2)_n = (\alpha, \beta_1)_n(\alpha, \beta_2)_n$
2. $(-\alpha, \alpha)_n = 1 \quad si\, \alpha\ \in\ F^\times$
3. $(\alpha, \beta)_n = 1$ *si et seulement si* $\alpha \in N_{F(\beta^{1/n})/F}(F(\beta^{1/n})^\times)$ *et si et seulement si* $\beta \in N_{F(\alpha^{1/n})/F}(F(\alpha^{1/n})^\times)$

[13] voir [14]

Cependant le cas le plus intéressant reste celui où $p = n$ qui est cette fois du ressort de la *théorie d'Artin-Schreier*. Soit donc E/F une extension de corps de fonctions de degré p (p =Car(F)). On connaît via les travaux d'Artin et Schreier une description de cette dernière selon :

$$E = F(y) \text{ où } y^p - y = \beta, \ \beta \in F$$

$\forall\, \alpha \in F^\times$ et $\forall\, \mathfrak{p}$ une place de F (i.e. un idéal premier), Schmid considère le symbole normique local [14] ("en $\mathfrak{p}$") $(\frac{\alpha, E/F}{\mathfrak{p}}) \in Gal(E/F)$ que pour des raisons d'ordre pratique l'on va abandonner pour lui préférer l'élément $\{\frac{\alpha,\beta}{\mathfrak{p}}\}$ de $\mathbb{F}_p$ défini comme suit :

$$\begin{array}{rcl} G \times E & \to & E \\ ((\dfrac{\alpha, E/F}{\mathfrak{p}}), y) & \mapsto & y^{(\frac{\alpha, E/F}{\mathfrak{p}})} = y + c \end{array}$$

où l'on pose $c := \{\frac{\alpha,\beta}{\mathfrak{p}}\} \in \mathbb{F}_p$; on vérifie alors que ce symbole est assymétrique au sens où il est multiplicatif en la première variable et additif en la seconde. Les travaux de Schmid ont ceci de remarquable qu'ils proposent une description explicite de ce dernier selon :

$$\{\frac{\alpha, \beta}{\mathfrak{p}}\} = \Psi Sp_{\mathfrak{p}} res_{\mathfrak{p}}(\beta \frac{d\alpha}{\alpha}) \tag{1.1}$$

avec :
- $res_{\mathfrak{p}}(\cdots)$ désigne le résidu en $\mathfrak{p}$ (i.e. en π si π désigne une uniformisante en $\mathfrak{p}$).
- $Sp_{\mathfrak{p}} : \mathcal{K}_{\mathfrak{p}} \to k$, k corps des constantes, $\mathcal{K}_{\mathfrak{p}}$ corps résiduel en $\mathfrak{p}$ (ici le corps fini $\mathbb{F}_{p^f}$ si $f = \deg(\mathfrak{p})$
- $\Psi : k \to \frac{\mathbb{Z}}{p\mathbb{Z}}$ la fonction "Trace Absolue"

En particulier,

α est une norme dans le localisé $E_{\mathfrak{p}}$ *si et seulement si* $\{\frac{\alpha,\beta}{\mathfrak{p}}\} = 0$

L'importance de cette formule est *triple* :

1. Elle permet une formulation du théorème ("additif") des résidus dans le cadre des corps de fonctions :

$$\sum_{\mathfrak{p}} Sp_{\mathfrak{p}} res_{\mathfrak{p}}(\beta \frac{d\alpha}{\alpha}) = 0$$

d'où l'on déduit :

$$\sum_{\mathfrak{p}} \{\frac{\alpha, \beta}{\mathfrak{p}}\} = 0$$

[14] L'hypothèse de cyclicité est ici essentielle

2. La relation (1) donne la multiplicité de l'idéal $\mathfrak{p}$ dans le conducteur de l'extension E/F.
3. Enfin la formule (1) introduit ("au rang 1") un formalisme relatif aux p-algèbres sur des corps arbitraires de caractéristique p qui sera repris par la suite et largement exploité par Witt.

1.7.2 Le Théorème d'existence

Les extensions cycliques d'exposant p

Si les travaux de Schmid règle la question en matière de lois de Réciprocité, ils ne permettent pas de prouver le théorème d'existence de la théorie du corps de classes dans le cadre des corps de fonctions et c'est à Witt que l'on doit l'avancée majeure dans cette direction, avancée d'autant plus remarquable que le cas $n = p$ n'avaient jamais été envisagé auparavant (cf. les travaux d'Herbrand et Chevalley dans le cas des corps de nombres). Dans un premier temps, Witt a su estimer le conducteur d'une extension abélienne d'exposant p et a fourni de la formule de Schmid la généralisation suivante :

Étant donnés $\alpha \neq 0$ et $\beta \in F$, Witt définit sur F l'algèbre $(\alpha, \beta]$ via ses générateurs u et y tels que :

$$u^p = \alpha, \quad y^p - y = \beta, \quad u^{-1} y u = y + \mathbf{1}$$

Étant donné $\mathfrak{p}$ un idéal premier du corps de fonctions F, on désigne par $F_{\mathfrak{p}}$ le résultat de sa complétion $\mathfrak{p}$-adique, ainsi on définit l'algèbre "locale" :

$$\begin{array}{rcl} F & \overset{\mathfrak{p}}{\rightsquigarrow} & F_{\mathfrak{p}} \\ (\alpha, \beta] & \rightsquigarrow & (\dfrac{\alpha, \beta}{\mathfrak{p}}] \end{array}$$

Sur $F_{\mathfrak{p}}$, Witt énonce la relation :

$$(\frac{\alpha, \beta}{\mathfrak{p}}] \sim (\frac{\pi, res_{\mathfrak{p}}(\beta \frac{d\alpha}{\alpha})}{\mathfrak{p}}] \tag{1.2}$$

où $\sim$ désigne l'équivalence entre algèbres et π est une uniformisante associée à $\mathfrak{p}$.
On remarque que dans cette formule comme dans celle de Schmid apparaît la dérivée logarithmique. C'est d'ailleurs au papier de ce dernier que Witt renvoie pour la preuve quand bien même il existe entre les deux relations des différences fondamentales ; en particulier, (1.1) se rapporte aux invariants de Hasse des algèbres quand (1.2) vaut pour les algèbres elles-mêmes. En outre, la formule de Witt est plus générale car elle est valable pour un corps résiduel parfait quand celle de Schmid se limite au cas où le corps résiduel est fini.

Dans un langage plus moderne ... :

Pour F un corps local de caractéristique p et de corps résiduel fini $\mathbb{F}_q$ (pour $q = p^f$), on définit l'application :

$$\begin{aligned}(.,.] : F^\times \times F &\to (\mathbb{F}_p, +)\\ (\alpha, \beta) &\mapsto \psi_F(\alpha)(\gamma) - \gamma\end{aligned}$$

où γ est une racine du polynôme $X^p - X - \beta \quad (*)$ et ψ_F désigne l'application de Réciprocité :

$$\psi_F : F^\times \to Gal(F^{ab}/F)$$

On rappelle que si ς désigne une autre racine de $(*)$ alors la différence $\varsigma - \gamma \in \mathbb{F}_p$, ce qui montre que $(.,.]$ est bien défini.
En outre, cette application possède quelques propriétés remarquables dont nous rappelons les principales (au sens où nous retrouvons bien entendu celles du symbole construit par Witt) :

Proposition 1.7.2.

1. $(\alpha_1\alpha_2, \beta] = (\alpha_1, \beta] + (\alpha_2, \beta]$ *"multiplicativité en la première variable"*
2. $(\alpha, \beta_1 + \beta_2] = (\alpha, \beta_1] + (\alpha, \beta_2]$ *"additivité en la seconde variable"*
3. $(-\alpha, \alpha] = 0 \quad \forall\, \alpha \in F^\times$
4. $(\alpha, \beta] = 0$ *si et seulement si* $\alpha \in N_{F(\gamma)/F}F(\gamma)^\times$ *où* $\gamma^p - \gamma = \beta$

Dans [14], on donne une interprétation explicite de en montrant que cette dernière application coïncide avec celle notée d_π (pour π une uniformisante) et définie comme suit :

$$\begin{aligned}d_\pi : F^\times \times F &\to \mathbb{F}_p\\ (\alpha, \beta) &\mapsto Tr_{\mathbb{F}_q/\mathbb{F}_p} res_\pi(\beta\alpha^{-1}\frac{d\alpha}{d\pi})\end{aligned}$$

En particulier, d_π ne dépend pas du choix de l'élément uniformisant π.

On cite enfin le corollaire important suivant :

Corollaire 1.7.3. $(.,.]$ *induit un accouplement* non-dégénéré *:*

$$F^\times/F^{\times p} \times F/\wp(F) \to \mathbb{F}_p$$

Le cas des extensions cycliques d'exposant p^n

Les formules explicites de Réciprocité pour les extensions cycliques de degré une puissance de p (type $(*)$) ont été publiées par Witt et H.L. Schmid alors qu'ils étaient tous deux assistants de Hasse à Göttingen. Le problème était donc de généraliser les formules données par Schmid pour le symbole normique au cas des extensions de degré une puissance de p qui devaient permettre de présenter une théorie du corps de classes complète pour les corps de fonctions.
La première étape a consisté à généraliser la théorie d'Artin-Schreier de sorte d'obtenir une description (en terme de générateurs) des extensions du type $(*)$ à considérer. C'est à un trait de génie de Schmid que l'on doit la solution, solution pressentie quelques temps auparavant par Albert comme nous avons eu l'occasion de le préciser p 22. Le deuxième trait de génie (dû à Witt cette fois) a consisté à savoir exploiter la jungle de formules qui a résultée de ces investigations pour en extraire une structure, à savoir celle de *l'anneau des vecteurs de Witt*, qui devaient fournir une paramétrisation efficace des extensions appelées depuis : d'*Artin-Schreier-Witt*. Ainsi si E/F est du type $(*)$, on rappelle que l'on dispose du critère de génération suivant :

$$E = F(y) = F(y_0, y_1, \cdots, y_{n-1})$$

où $y \in W_n(E)$ et satisfait une équation de la forme $y^p - y = \beta$ avec $\beta = (\beta_0, \beta_1, \cdots, \beta_{n-1}) \in W_n(F)$.

En termes d'algèbres ...

Soient $\alpha \neq 0 \in F$ et $\beta = (\beta_0, \beta_1, \cdots, \beta_{n-1})$ un vecteur de Witt sur F de longueur n ; Witt considère l'algèbre $(\alpha|\beta]$ définie par les générateurs $u, y_0, y_1, \cdots, y_{n-1}$ où les y_i commutent entre eux et où l'on dispose des relations :

$$u^{p^n} = \alpha, \quad y^p - y = \beta \quad uyu^{-1} = y + \mathbf{1}$$

si $\mathbf{1}$ désigne l'élément unité $(1, 0, \cdots, 0)$ et uyu^{-1} signifie
$(uy_0u^{-1}, \cdots, uy_{n-1}u^{-1})$.
Ces relations permettent de définir une algèbre simple de centre F admettant pour corps de décomposition l'extension cyclique $E = F(y)$ qui est exactement de degré p^n dès lors que β n'est pas de la forme $b^p - b$, $b \in F$. Le symbole $(\alpha|\beta]$ considéré comme un élément du groupe de Brauer sur F est multiplicatif en la première variable et additif en la seconde. On remarque que l'algèbre $(\alpha|\beta]$ définie avec des vecteurs de Witt est une généralisation du candidat $(\alpha, \beta]$ évoqué plus haut alors défini pour des éléments du corps. Cela conduit naturellement à se demander si pour ces nouvelles algèbres, il n'existerait pas un analogue de la formule (1.2). Witt, de nouveau en utilisant des méthodes locales, répond par l'affirmative.

Ainsi si $\mathfrak{p}$ désigne un idéal premier de F, on peut considèrer sur la complétion $\mathfrak{p}$-adique $F_{\mathfrak{p}}$ (i.e. le corps des séries formelles à coefficients dans le corps résiduel $\mathcal{K}_{\mathfrak{p}}$) l'algèbre $(\frac{\alpha|\beta}{\mathfrak{p}}]$. L'opération se transporte sur les composantes fantômes $\beta^{(m)}$ et il en résulte un vecteur de Witt, qualifié de résiduel (car ses composantes appartiennent au corps résiduel), noté $(\alpha,\beta)_{\mathfrak{p}}$ qui permet d'énoncer :

$$(\frac{\alpha|\beta}{\mathfrak{p}}] \sim (\frac{\pi,(\alpha,\beta)_{\mathfrak{p}}}{\mathfrak{p}}]$$

Sans toutefois en fournir de preuve, Witt mentionne la relation :

$$\sum_{\mathfrak{p}} S_{\mathfrak{p}}(\alpha,\beta)_{\mathfrak{p}} = 0$$

vue comme une généralisation du théorème des résidus appliqués aux vecteurs résiduels (la trace $S_{\mathfrak{p}}$ est étendue aux vecteurs de Witt).
Par la suite H.L. Schmid publie un travail sur l'arithmétique des extensions cycliques E/F de degré une puissance de p en caractéristique p dans lequel il poursuit, cette fois avec à sa disposition le formalisme de Witt, ses investigations et établit des formules pour le conducteur, le discriminant et le genre de E en fonction de β si $E = F(y)$ et $y^p - y = \beta$.

Le point de vue moderne :

Étant donné F comme ci-dessus, on introduit l'application :

$$\begin{aligned} (.,.]_n : F^\times \times W_n(F) &\to W_n(\mathbb{F}_p) \simeq \mathbb{Z}/p^n\mathbb{Z} \\ (\alpha,\beta) &\mapsto \psi_F(\alpha)(z) - z \end{aligned}$$

où $z \in W_n(F^{sep})$ et $\wp(z) = \beta$.

Remarque : En particulier, $(.,.]_1 = (.,.]$ et satisfait les mêmes propriétés que celles énoncées ci-dessus pour son analogue "au rang 1".

En outre, $(.,.]_n$ coïncide avec $d_{n,\pi}$ définie comme suit :

$$\begin{aligned} d_{n,\pi} : F^\times \times W_n(F) &\to W_n(\mathbb{F}_p) \\ (\alpha,\beta) &\mapsto (1 + \mathbf{F} + \mathbf{F}^2 + \cdots + \mathbf{F}^{f-1})y \end{aligned}$$

où :

1. $y(y^{(0)},\cdots,y^{(n-1)}) \in W_n(\mathbb{F}_q)$,
2. $y^{(m)} = res_\pi(\alpha^{-1}\frac{d\alpha}{d\pi}\beta^{(m)})$,
3. $\mathbf{F}$ désigne l'aplication "Frobenius" (voir p 25)

4. $\frac{d\alpha}{d\pi} := \frac{d\alpha(X)}{dX}]_{X=\pi}$

On a alors le corollaire suivant :

Corollaire 1.7.4. *L'application* $(.,.]_n$ *induit un accouplement non-dégénéré :*

$$F^\times/F^{\times p^n} \times W_n(F)/\wp(W_n(F)) \to W_n(\mathbb{F}_p)$$

Correspondances :

Suite exacte de Kummer :

$$1 \to \mu_n \hookrightarrow K^{sep} \overset{\wp}{\twoheadrightarrow} K^{sep} \to 1$$

où $\wp(x) = x^n$
Isogénie d'Artin-Schreier :

$$0 \to \mathbb{Z}/p\mathbb{Z} \hookrightarrow K^{sep} \overset{\wp}{\twoheadrightarrow} K^{sep} \to 0$$

où $\wp(x) = x^p - x$
Isogénie d'Artin-Schreier-Witt :

$$0 \to \mathbb{Z}/p^n\mathbb{Z} \hookrightarrow W_n(K^{sep}) \overset{\wp}{\twoheadrightarrow} W_n(K^{sep}) \to 0$$

On conclut cet aparté en signalant deux thèses de Troisième Cycle récemment soutenues et utilisant la théorie d'Artin-Schreier-Witt :

1. "*Computation of Maximal Orders of Cyclic Extensions of Function Fields*" par Robert Fraatz sous la direction de Rainer Wüst (2005) - Berlin
2. "*Arithmétique des extensions d'Artin-Schreier-Witt*" par Lara Thomas sous la direction de Christian Maire (2005) - Université Toulouse II le Mirail.

Chapitre 2

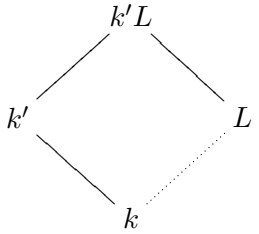
La théorie d'Iwasawa des corps globaux

2.1 Extensions de corps de fonctions : un panorama

On a vu dans la définition d'une extension algébrique de corps de fonctions qu'intervenait une condition sur le corps des constantes à savoir l'inclusion $k \subseteq k'$. Ceci va permettre d'introduire deux grands types d'extensions selon que $k \subsetneq k'$ ou que l'on ait l'égalité $k = k'$.

2.1.1 La catégorie des extensions de corps de fonctions dites *arithmétiques*

Il s'agit des extensions de corps de fonctions obtenues exclusivement par compositum du corps de fonctions de base (généralement le corps des fonctions rationnelles ou une extension finie de ce dernier) avec une extension non triviale du corps des constantes (généralement $\mathbb{F}_q$). Avant d'entrer plus avant dans le vif du sujet, on fait l'hypothèse (qui n'est pas restrictive dans notre contexte) que le corps des constantes k est *parfait* simplement pour éviter tout problème relatif à la séparabilité. On se place dans le schéma suivant :



Soit donc k' une extension algébrique stricte de k prise dans une clôture algébrique de k que l'on suppose fixée. Le compositum $L' := k'L$ est un corps de fonctions sur k' de corps des constantes une extension FINIE de ce dernier. On peut préciser via la proposition suivante :

Proposition 2.1.1. *Soit $L' := k'L$ une extension algébrique du corps L/k (de degré fini ou non). On a alors les assertions suivantes :*

1. *k' est le corps des constantes associé à L'*
2. *Tout sous-ensemble[1] de L linéairement indépendant sur k l'est encore sur k'*
3. *$[L : k(x)] = [L' : k'(x)] \; \forall \; x \; \in L \setminus k$*

On donne maintenant sous forme d'un théorème les principales propriétés des extensions arithmétiques de corps de fonctions :

Théorème 2.1.2. *Si $L' := k'L$ est une extension arithmétique de L/k, on dispose des propriétés suivantes :*

1. *L'/k' est une extension non-ramifiée*
2. *L'/k' a le même genre que l'extension originelle L/k*
3. *Le corps résiduel associé à une place P quelconque de L est isomorphe au compositum L de k' et du corps des classes résiduelles L_P où $P = P' \cap L$.*
4. *Si k'/k est de degré fini, toute base de cette dernière extension est une base entière de L'/L.*

Ce critère nous donne donc un moyen de dresser des tours d'extensions non-ramifiées, dont nous nous inspirerons dans la suite pour construire l'analogue suivant Iwasawa de la $\mathbb{Z}_p$-extension cyclotomique de corps de nombres. On remarque en particulier une première différence de comportement entre le corps des fonctions rationnelles et $\mathbb{Q}$ car si ce dernier n'admet pas d'extension non-ramifiée, d'après la construction précédente, son analogue en possède une infinité.

2.1.2 La catégorie des extensions de corps de fonctions dites *géométriques.*

Il s'agit là de la famille d'extensions qui va retenir notre attention dans toute la suite car elles sont à l'origine de l'article de Villa-Salvador et Madan. Pour éviter d'alourdir la rédaction, disons simplement que l'on appelle *extension géométrique* d'un corps de fonctions L une extension possédant le même corps des constantes que le corps dont elle provient. Un moyen simple d'en construire est donné par le lemme suivant :

Lemme 2.1.3. *Soit L/k un corps de fonctions de corps des constantes k. On désigne par L' une extension de degré n de L. S'il existe une place $\mathfrak{p}$ de L totalement ramifiée dans L' alors le corps des constantes de L'/L est égal à k (c'est-à-dire que l'extension L'/L est géométrique).*

[1] En toute rigueur, l'indépendance linéaire concerne les familles et non les parties.

On retiendra que si L/k est un corps de fonctions de corps des constantes k et L'/L un extension algébrique finie de L tel que k' soit la clôture algébrique de k dans L' alors L' est un corps de fonctions de corps des constantes k' et que l'on dispose d'une tour d'extensions $L \subseteq k'L \subseteq L'$ dont le premier étage est une extension aritmétique et le second étage une extension géométrique. En d'autres termes, il peut toujours se ramener à une extension géométrique quitte à "monter suffisamment haut" dans la tour.

Le moment semble donc bien choisi pour définir de manière un petit peu rigoureuse ce que l'on entend par "tour d'extensions" ...

Comme précédemment, on considère un corps de fonctions algébriques d'une variable L de corps des constantes le corps finis à q éléments $\mathbb{F}_q$.

Définition 2.1.4. *: Une tour de corps de fonctions sur $\mathbb{F}_q$ est une suite $(L_0, L_1, \cdots)$ de corps de fonctions $L_i/\mathbb{F}_q$ satisfaisant :*

1. $L_0 \subseteq L_1 \subseteq L_2 \subseteq \cdots$
2. *Pour chaque $n \geqslant 0$, l'extension L_{n+1}/L_n est séparable de degré ≥ 1*
3. $g(L_i) \geq 2$ *pour* $i \geq 0$ *(si $g(L_i)$ désigne le genre du corps L_i)*

En guise d'exemple, valable dans le contexte plus général des corps globaux, on peut s'arrêter quelques instants sur un cas particulièrement important de tour de corps que l'on connaît sous le terme générique de $\mathbb{Z}_l$-extensions et dont la richesse a été mise en exergue grâce aux travaux d'Iwasawa, ces mêmes travaux sur lesquels nous nous proposons de revenir dans ce chapitre.

Définition 2.1.5. *Une $\mathbb{Z}_l$-extension d'un corps global K est définie comme une extension galoisienne infinie généralement notée K_∞/K telle que $Gal(K_\infty/K) := \Gamma$ soit topologiquement isomorphe à $(\mathbb{Z}_l, +)$ le groupe additif associé à l'anneau des entiers l-adiques. En particulier, elle peut-être vue comme une tour infinie*

$$K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_n \subseteq \cdots \subseteq K_\infty = \bigcup_{i=0}^{\infty} K_i$$

avec à chaque étage n l'isomorphisme $Gal(K_n/K) \simeq \mathbb{Z}/l^n\mathbb{Z}$. On dit alors que K_n est le n-ième étage de la $\mathbb{Z}_l-$ extension K_∞/K.

Cas particuliers - Tours Ramifiées - Tours géométriques

Définition 2.1.6. *On dit qu'une tour F sur $\mathbb{F}_q$ est modérée si $\forall\ n \geq 0$ et pour toutes les places $\mathfrak{p}_n$ de L_n , l'indice de ramification $e(\mathfrak{p}_n)$ dans L_n/L_0 est premier avec la caractéristique p de $\mathbb{F}_q$ (on suppose $q = p^\alpha$). Si en revanche, il existe un indice de ramification dans la tour divisible par p, la tour F est qualifiée de* sauvage.

Le type de tours qui nous intéressera par la suite car il est à l'origine de l'article de Villa-Madan auquel nous consacrerons notre chapitre 3 est celui des tours d'extensions géométriques sauvages.
Ainsi, soit k un corps fini à q éléments où $q{=}p^{\alpha}$ pour p un nombre premier impair désignant la caractéristique du corps de base. On se donne K_0 un corps de fonctions de corps des constantes k et pour chaque entier naturel n, on note K_n/K_0 une extension cyclique de degré p^n telle que :

- Pour $n \geq 0$, $K_n \subset K_{n+1}$ et $K_{n+1}/K_n = p$
- Le corps des constantes de K_n est k (c'est à dire que chaque étage de la tour est une extension géométrique)
- $K_\infty = \bigcup K_n$

On obtient ainsi une $\mathbb{Z}_p$-extension géométrique ce qui nous permet de faire le lien avec le paragraphe suivant ...
La dualité que nous avons observé au niveau fini dans le cas des extensions de corps et qui provient de l'existence de deux familles aux comportements tout à fait différents va bien entendu se retrouver lorsque notre intérêt va se porter sur des tours infinies et plus particulièrement sur le cas des $\mathbb{Z}_p$-extensions.

2.2 A propos des $\mathbb{Z}_l$-extensions : différences et similitudes

2.2.1 Les $\mathbb{Z}_l$-extensions arithmétiques - lien avec la $\mathbb{Z}_l-$ extension cyclotomique des corps de nombres.

Étant donné un corps fini $\mathbb{F}$ à q éléments[2], on définit $\mathbb{F}_n$ comme l'unique sous-corps de la clôture algébrique $\overline{\mathbb{F}}$ supposée fixée tel que $[\mathbb{F}_n : \mathbb{F}] = n$. Dans le cas particulier où $n = l^m$ est une puissance d'un nombre premier l, on construit une tour d'extensions selon le procédé suivant :

$$\mathbb{F} \subseteq \mathbb{F}_l \subseteq \mathbb{F}_{l^2} \subseteq \cdots \subseteq \mathbb{F}_{l^m} \subseteq \cdots$$

et l'on pose : $\mathbb{F}_{l^\infty} := \cup_{m \geqslant 0} \mathbb{F}_{l^m}$. Il s'agit de la *l-extension maximale* de $\mathbb{F}$ dans $\overline{\mathbb{F}}$ au sens où pour toute extension finie $\mathbb{E}$ de $\mathbb{F}_{l^\infty}$, on a $[\mathbb{E} : \mathbb{F}_{l^\infty}]$ est premier avec l. C'est par "compositum" avec cette dernière qu'étant donné un corps de fonctions K nous allons construire la famille des $\mathbb{Z}_l$-extensions arithmétiques de ce dernier. Soit donc K un corps de fonctions de corps des constantes $\mathbb{F}$. A chaque étage fini n, on pose $K_n = K\mathbb{F}_n$ l'extension arithmétique résultant de la composition de sorte que comme ci-dessus on obtient une tour d'extensions :

$$K \subseteq K_l \subseteq K_{l^2} \subseteq \cdots \subseteq K_{l^m} \subseteq \cdots$$

[2] [55]

On pose alors $K_{l^\infty} = K\mathbb{F}_{l^\infty}$. Le recours à la théorie du corps de classes nous permet d'affirmer que lorsque le nombre premier l est égal à la caractéristique p du corps des constantes, il existe une infinité de $\mathbb{Z}_p$-extensions arithmétiques, en revanche lorsque l'on suppose l distinct de p, il existe pour un corps de fonctions K fixée une unique $\mathbb{Z}_l$-extension arithmétique, qui va servir de modèle à Iwasawa pour construire dans le cadre des corps de nombres la $\mathbb{Z}_l$-extension cyclotomique dont on appelle une construction ci-après. L'analogie utilisée consiste à faire jouer aux racines de l'unité dans les corps de nombres celui que remplissaient les éléments du corps des constantes dans le cas des corps de fonctions.
Soient donc l un nombre premier supposé impair et $n \geq 1$ un entier naturel. Si l'on note ζ_{l^n} une racine primitive l^n de l'unité, on a que le groupe de Galois associé à l'extension cyclotomique $\mathbb{Q}(\zeta_{l^n})/\mathbb{Q}$ est isomorphe à $\mathbb{Z}/(l-1)\mathbb{Z} \times \mathbb{Z}/l^{n-1}\mathbb{Z}$ via $\varphi(l^n) = l^{n-1}(l-1)$ si φ désigne l'indicatrice d'Euler. On désigne par $\mathbb{Q}_n$ le sous-corps de $\mathbb{Q}(\zeta_{l^n})$ fixé par le sous-groupe constitué des éléments d'ordre premier à p, ainsi donc $Gal(\mathbb{Q}_n/\mathbb{Q}) \simeq \mathbb{Z}/l^{n-1}\mathbb{Z}$ et $\cup_n \mathbb{Q}_n := \mathbb{Q}_\infty$ est une $\mathbb{Z}_l$-extension de $\mathbb{Q}$. Par compositum avec un corps de nombres K, on obtient que tout corps de nombres possède au moins une $\mathbb{Z}_l-$ extension $K_\infty = K\mathbb{Q}_\infty$ appelée *$\mathbb{Z}_l$-extension cyclotomique de K*. Il s'agit là de l'analogue de l'extension *non-ramifiée* $K_{l^\infty} = K\mathbb{F}_{l^\infty}$. Malheureusement ce dernier n'est que partiellement satisfaisant comme le montrent les propositions suivantes :

Proposition 2.2.1. *Soient K un corps de nombres et L/K une $\mathbb{Z}_l$-extension de K. Les seules places de K susceptibles de se ramifier dans L sont exactement celles au-dessus de l. On dit que les $\mathbb{Z}_l$-extensions de corps de nombres sont l-ramifiées.*

Conséquence : Étant donnés K un corps de nombres et L/K une $\mathbb{Z}_l$-extension de K, il n'existe qu'un nombre *fini* de places ramifiées.
En outre :

Proposition 2.2.2. *Étant donnée L/K une $\mathbb{Z}_l$-extension de corps de nombres alors il existe* au moins *une place ramifiée dans L et l'on peut trouver un entier n_0 à partir duquel toute place de K_{n_0} est totalement ramifiée dans L.*

2.3 Une brève incursion en Théorie d'Iwasawa

2.3.1 Un peu d'histoire

Rappels concernant la fonction Zêta associée à un corps de fonctions.

Etant donné un corps de fonctions K d'une variable de corps de constantes $\mathbb{F}_q$, on définit la fonction Zêta associée à K (ou plus précisément la fonction

Zêta attachée à la courbe propre lisse $C/\mathbb{F}_q$ de K) via :

$$\zeta_K(s) = \sum_{A \geq 0} NA^{-s}$$

où $A \in D_K$, le groupe des diviseurs de K et $NA = q^{deg(a)}$ désigne la norme du diviseur A. On peut alors montrer qu'il existe un polynôme $L_K(u)$ de $\mathbb{Z}[u]$ de degré $2g$ si g désigne le genre de K tel que :

$$\zeta_K(s) = \frac{L_K(q^{-s})}{(1-q^{-s})(1-q^{1-s})}$$

pour tout s tel que $Re(s) > 1$.

A l'origine de ce que l'on connait aujourd'hui sous le nom générique de théorie d'Iwasawa était une volonté de la part de ce dernier de traduire dans le contexte des corps de nombres un résultat particulièrement remarquable qu'avait obtenu Weil dans le cadre moins restrictif du fait de l'ubiquïté des objets étudiés des corps de fonctions. En quelques mots, la théorie développée par A. Weil permet de relier la fonction Zêta associée à un corps de fonctions et voici comment ...

Soit $\overline{\mathbb{F}}_q$ une clôture algébrique de $\mathbb{F}_q$ où comme précédemment $\mathbb{F}_q$ désigne le corps fini à $q = p^\alpha$ éléments. Étant donnée K/k une extension de corps de fonctions géométrique, on pose $\overline{k} = k\overline{\mathbb{F}}_q$ et $\overline{K} = K\overline{\mathbb{F}}_q$ et l'on a $K \cap \overline{k} = k$. Il suit que le groupe de Galois de $\overline{K}/k$ est le produit direct de $Gal(\overline{K}/\overline{k})$ avec $Gal(\overline{K}/K)$ et le rôle des extensions de type arithmétique devient alors apparent. De l'isomorphisme naturel $Gal(\overline{K}/\overline{k}) \simeq Gal(K/k) := G$, on considère les éléments de G comme des automorphismes de $\overline{K}$ laissant $\overline{k}$ fixe. Soit ϕ un automorphisme de $\overline{K}/K$ qui induit par restriction à $\overline{\mathbb{F}}_q$ l'automorphisme de Frobenius

$$\begin{array}{rccc} \phi_q : \overline{\mathbb{F}}_q & \rightarrow & \overline{\mathbb{F}}_q \\ \beta & \mapsto & \beta^q \end{array}$$

On parle pour ϕ_q du Frobenius *aritmétique* associé à l'extension $\overline{K}/K$, c'est-à-dire le générateur naturel du groupe de Galois $Gal(\overline{\mathbb{F}}_q/\mathbb{F}_q) \simeq \hat{\mathbb{Z}}$ où $\hat{\mathbb{Z}}$ désigne un groupe profini libre de rang 1. Si maintenant l'on note $J = Cl^0_K$, on a que ϕ agit sur le module de Tate de la variété Jacobienne J de $C/\mathbb{F}$ la courbe lisse et propre associée au corps K où ce dernier est défini comme la limite projective des groupes de points de l^n-torsion, si $l \neq p$. Plus précisément, on dispose pour les points de N-torsion de J d'ordre divisant N (avec p premier à N) du théorème de structure suivant :

$$J[N] \simeq \bigoplus_{i=1}^{2g} \mathbb{Z}/N\mathbb{Z}$$

On fixe l un nombre premier distinct de p et l'on considère la suite des groupes $J[l^n]$. On voit alors que pour chaque entier naturel $n \in \mathbb{N}$, la multiplication par l envoie $J[l^{n+1}]$ dans $J[l^n]$ et permet ainsi la définition d'un système projectif. On pose alors :

$$T_l(J) = \varprojlim_n J[l^n]$$

Les éléments du module de Tate ainsi défini peuvent être identifiés avec les suites infinies $(a_1, a_2, \cdots)$ où pour tout $n > 0$, a_n est un élément de $J[l^n]$ tel que $la_{n+1} = a_n$. Ce dernier agit sur l'anneau des entiers l-adiques comme suit :

$$\begin{array}{rcl} T_l(J) \times \mathbb{Z}_\ell & \to & \mathbb{Z}_\ell \\ ((a_1, a_2, \cdots), \delta) & \mapsto & \delta \star a := (\delta a_1, \delta a_2, \cdots) \end{array}$$

De la même façon, puisque G et ϕ agissent conjointement sur $J[l^n]$ pour tout n, ces actions peuvent être étendues par un procédé diagonal en une action sur $T_l(J)$ de sorte que l'on munit le module de Tate d'une structure de $\mathbb{Z}_\ell[G]$-module. En utilisant le théorème de structure relatif à $J[N]$, on peut alors montrer que $T_l(J)$ est un $\mathbb{Z}_l$-module libre de rang $2g$. On pose alors :

$$V_l = V_l(J) = \mathbb{Q}_\ell \bigotimes_{\mathbb{Z}_\ell} T_l(J)$$

Ce faisant V_l se voit doté d'une structure de $\mathbb{Q}_\ell$-espace vectoriel de dimension $2g$ et l'on est en mesure d'énoncer le résultat suivant dû à Weil :

Théorème 2.3.1. *Le déterminant de l'application* $1 - \phi u$ *est égal au numérateur de la fonction Zêta associé au corps de fonction* K.

Obtenir un résultat analogue dans le cadre des corps de nombres supposait pour Iwasawa de déterminer respectivement des analogues raisonnables pour d'une part la fonction Zêta associée à un corps de fonctions et d'autre part le groupe des classes de diviseurs. Le candidat pour la première analogie sera la fonction Zêta p-adique de Kubota-Leopold que nous ne ferons que citer et quant au second, c'est le module d'Iwasawa usuellement noté X ou X_∞ qui répondra à la question à savoir la limite projective des X_n (relativement aux applications norme) si X_n désigne la l-partie du groupe de classes relatif au n-ième étage de la $\mathbb{Z}_\ell$-extension cyclotomique dont on a rappelé une construction précédemment. En quelques mots, la conjecture principale pour les corps de nombres statue que les polynômes caractéristiques relatifs aux actions de $\Gamma = Gal(K_\infty/K)$ sur les divers groupes de Galois des extensions abéliennes de K_∞ sont reliés aux fonctions L l-adiques. Elle a été prouvée par Mazur et Wiles sous l'hypothèse que le corps de base était abélien sur $\mathbb{Q}$ puis par Wiles dans le cas des corps totalement réels.

2.3.2 Quelques résultats incontournables en théorie d'Iwasawa

Présentation de l'algèbre d'Iwasawa[3]

On considère $\mathcal{O}$ un anneau commutatif local noethérien d'idéal maximal pricipal (π). On suppose ce dernier complet pour la topologie π-adique associée et l'on note $\mathcal{K} := \frac{\mathcal{O}}{(\pi)}$ le corps résiduel correspondant (typiquement, $\mathcal{O} = \mathbb{Z}_p$, l'anneau des entiers p-adiques, d'idéal maximal (p) et de corps résiduel associé $\mathbb{F}_p$). Soit $\Lambda := \mathcal{O}[[T]]$ l'algèbre des séries formelles en une variable à coefficients dans $\mathcal{O}$. On appelle Λ *l'algèbre d'Iwasawa* ; il s'agit d'un anneau local d'unique idéal maximal engendré par (π, T), de corps résiduel $\mathcal{K}$. Muni de sa topologie (π, T)-adique, on vérifie que la famille $(\pi, T)^n$ constitue une base de voisinage de 0 et que Λ est complet et compact pour cette dernière. *Parce qu'il s'agira par la suite du cas qui retiendra toute notre attention, on suppose dorénavant que* : $\Lambda = \mathbb{Z}_p[[T]]$.

Définition 2.3.2. *Un polynôme* $P(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_1T + a_0$ *élément de* $\mathbb{Z}_p[T]$ *est dit* distingué *si* $a_i \equiv 0$ *mod* p *pour* $0 \leq i \leq n-1$ *(on parle quelquefois aussi de "polynôme de Weierstrass").*

Exemple : Les polynômes cyclotomiques : $\omega_n = (1+T)^{p^n} - 1$ sont des polynômes distingués dont le rôle est essentiel en théorie d'Iwasawa.
Ces derniers interviennent dans le théorème suivant qui renseigne sur la structure des éléments de l'algèbre $\mathbb{Z}_p[[T]]$:

Théorème 2.3.3. *(de préparation de Weierstrass) Soit*

$$f(T) = \Sigma_{i=0}^{\infty} a_i T^i \ \in \mathbb{Z}_p[[T]]$$

alors f *s'écrit de manière unique sous la forme*

$$f(T) \ = \ p^{\mu} U(T) P(T)$$

où $U(T) \in \ \mathbb{Z}_p[[T]]^{\times}$ *et* $P(T)$ *est un polynôme distingué.*

En outre, ils permettent de donner une description du spectre de l'algèbre Λ, en effet on a la proposition :

Proposition 2.3.4. *Les idéaux premiers de* Λ *sont exactement l'idéal trivial :* (0)*, l'idéal maximal* (p) *de* $\mathbb{Z}_p$*, les idéaux principaux de la forme* (f) *où* f *est un polynôme distingué irréductible et enfin l'idéal* (p, T)*. En outre ce dernier est l'unique idéal maximal de l'anneau noethérien* Λ*.*

[3] [48]

Structure des Λ-modules de type fini :

Une notion fondamentale est celle de *"pseudo-isomorphisme"* que l'on introduit en toute généralité avant de nous restreindre au cas particulier qui nous intéresse ...[4]

Définition 2.3.5. *Étant donné A un anneau commutatif noethérien intégralement clos,un morphisme $f : M \to N$ de A-modules de type fini est un pseudo-isomorphisme si $Ker(f)$ et $Coker(f)$ sont pseudo-nuls.*

Remarques :

- Dans le cas particulier où $A = \Lambda$, les modules pseudo-nuls sont exactement les modules finis.
- Usuellement, on note $M \sim N$ pour signifier que deux modules M et N sont pseudo-isomorphes. En général, $\sim$ n'est pas une relation d'équivalence mais elle le devient en revanche lorsque l'on considère des Λ-modules de torsion.
- Si l'on considère X_n et Y_n deux suites de groupes finis, alors on note $X_n \sim Y_n$ pour signifier qu'il existe des homomorphisme $\phi_n : X_n \to Y_n$ dont les noyaux et conoyaux ont des ordres bornés indépendamment de n. Une telle situation se présente tout naturellement dans le cas où $X = \varprojlim_n X_n$, $Y = \varprojlim_n Y_n$ et $X \sim Y$. Enfin, si $|X_n|$ et $|Y_n|$ désignent les ordres respectifs de X_n et Y_n, on écrit $|X_n| \sim |Y_n|$ pour traduire que les quotients $|X_n|/|Y_n|$ et $|Y_n|/|X_n|$ sont bornés indépendamment de n. Par exemple, si $X_n \sim Y_n$ alors $|X_n| \sim |Y_n|$.
- Enfin, dans le cas particulier où l'on note f et g deux polynômes de $\mathbb{Z}_p[T]$ premiers entre eux alors on a :

$$\Lambda/(fg) \sim \Lambda/(f) \oplus \Lambda/(g) \text{ et } \Lambda/(f) \oplus \Lambda/(g) \sim \Lambda/(fg)$$

On est en mesure d'énoncer le théorème de structure suivant, naturel si l'on remarque que l'anneau Λ est "presque" principal (c'est justement ce défaut de principalité que mesure la notion de pseudo-isomorphisme).

Théorème 2.3.6. *Soit M un $\Lambda = \mathbb{Z}_p[[T]]$-module de type fini. Alors il existe des entiers $r, m, s \geq 0$ et $m_i, n_i \geq 1$ tels que :*

$$M \sim \Lambda^r \oplus (\bigoplus_{i=1}^{s} \Lambda/p^{n_i}) \oplus (\bigoplus_{i=1}^{m} \Lambda/(f_i(T))^{m_i}$$

où les $f_i(T)$ sont des polynômes distingués irréductibles.

[4] La classification des modules pseudo-isomorphes a été développée par Iwasawa et Serre.

Ce dernier nous permet d'introduire les invariants d'Iwasawa dont le comportement au sein d'une tour d'extensions sera déterminant pour coder l'évolution du groupe des classes d'idéaux :

- $r := rg_\Lambda M$ le Λ-rang de M
- $\mu(M) := \Sigma_{i=1}^m n_i$ l'invariant μ de M.
- $\lambda(M) := \Sigma_{i=1}^m m_i \deg f_i$ l'invariant λ de M
- $f_M(T) := \Pi_{i=1}^m f_i(T)^{m_i}$ le polynôme caractéristique de M

Remarques :

1. Les invariants r, μ, λ dépendent uniquement de M.
2. Dans le cas particulier où M un Λ-module de torsion (ie $r = 0$) alors $\lambda = \dim_{\mathbb{Q}_p} \otimes_{\mathbb{Z}_p} M$ et le polynôme caractéristique de l'endomorphisme de $\mathbb{Q}_p \otimes M$ est donné par la multiplication par T.

Ils satisfont en outre la proposition suivante :

Proposition 2.3.7. *On se donne une suite exacte de modules de torsion noethériens :*

$$0 \to X \hookrightarrow Y \twoheadrightarrow Z \to 0$$

alors on a : $\lambda(Y) = \lambda(X) + \lambda(Z)$ *et* $\mu(Y) = \mu(X) + \mu(Z)$.

Reste à faire le lien entre la théorie des nombres et ce pan d'algèbre commutative, lien qui est assuré par le théorème de correspondance suivant :

Théorème 2.3.8. *On désigne par Γ un pro-p-groupe isomorphe au groupe additif $(\mathbb{Z}_p, +)$ dont on fixe un générateur topologique noté γ. L'application*

$$\begin{array}{rcl} \mathbb{Z}_p[[T]] & \to & \mathbb{Z}_p[[\Gamma]] \\ T & \mapsto & \gamma - 1 \end{array}$$

est un isomorphisme topologique de $\mathbb{Z}_p$-algèbres.

Définition 2.3.9. *Pour un Λ-module M, on note M^Γ le sous-module de M constitué des éléments invariants sous l'action de Γ et M_Γ (ou indifféremment ${}^\Gamma M$) les "co-invariants" pour cette action, à savoir le quotient $\dfrac{M}{(\gamma-1)M}$ où $\gamma - 1$ engendre l'idéal d'augmentation (il s'agit du plus grand quotient de M sur lequel Γ agit trivialement).*

Ils sont liés par la proposition suivante :

Proposition 2.3.10. *Soit M un Λ-module de type fini et de torsion. Les assertions suivantes sont équivalentes :*

1. M^Γ *est fini*
2. M_Γ *est fini*

Lemme 2.3.11. *Étant donnée* $0 \to M_1 \hookrightarrow M_2 \twoheadrightarrow M_3 \to 0$ *une suite exacte de* Λ*-modules, il existe une suite de* $\mathbb{Z}_p$*-modules :*

$$0 \to M_1^\Gamma \to M_2^\Gamma \to M_3^\Gamma \to (M_1)_\Gamma \to (M_2)_\Gamma \to (M_3)_\Gamma \to 0$$

Preuve : C'est une conséquence directe du Lemme du serpent puisque par définition les suites

$$0 \to M_i^\Gamma \to M_i \overset{\gamma-1}{\to} M_i \to (M_i)_\Gamma \to 0$$

sont exactes pour i $= 1, 2, 3$.

2.3.3 De l'algèbre commutative à la théorie des nombres...

Le cas des corps de nombres

Étant donnés un nombre premier l et un corps de nombres K, on note K_∞/K une $\mathbb{Z}_l$-extension de K de groupe de Galois $\Gamma = (\gamma)$. Si l'on désigne par K_n le n-ième étage de la tour de corps associée, ce dernier peut être vu comme le sous-corps de K_∞ fixé par γ^{l^n} tel que $Gal(K_n/K) \simeq \mathbb{Z}/l^n\mathbb{Z}$.
On note $X_n := \mathbb{Z}_l \otimes Cl_{K_n}$, la l-partie (conséquence de la tensorisation par $\mathbb{Z}_l$) de groupe de classes de K_n. Si maintenant l'on désigne par L_n la l-extension abélienne non-ramifiée maximale de K_n, on a l'isomorphisme : $X_n \simeq Gal(L_n/K_n)$. On pose alors $X_\infty := \varprojlim_n X_n$ relativement à l'application "norme" : N_{K_{n+1}/K_n}. On peut alors énoncer la proposition suivante :

Proposition 2.3.12.

1. *La réunion* $L = \cup_n L_n$ *est la pro-l-extension abélienne maximale de* K_∞.
2. *On a l'isomorphisme :* $X_\infty \simeq Gal(L/K_\infty)$
3. X_∞ *est un* $\mathbb{Z}_l[[\Gamma]]$*-module noethérien, de torsion avec* $\mathbb{Z}_l[[\Gamma]] = \varprojlim_n \mathbb{Z}_l[\Gamma_n]$

Théorème 2.3.13. *(Iwasawa) Soit* K *un corps de nombres algébriques et* l *un nombre premier. On note pour une* $\mathbb{Z}_l$*-extension* K_∞ *de* K, $e_n := ord_l h(K_{l^n})$ *la l-partie du nombre de classes de* K_{l^n}*. Il existe alors des entiers* λ_l, μ_l, ν_l *et un indice* n_0 *tels que* $\forall n \geq n_0$*, on ait la formule asymptotique :*

$$e_n = \lambda_l n + \mu_l l^n + \nu_l$$

On évoque en outre via la proposition suivante la généralisation d'un réultat démontré par Ph. Furtwängler et H. Weber dans le cas particulier du corps cyclotomique $k = \mathbb{Q}(\mu_p)$:

Proposition 2.3.14. *Soit K_∞/K une $\mathbb{Z}_l$-extension dans laquelle on suppose que seule une place se ramifie et qu'en outre, elle l'est totalement alors :*

$$e_0 = 0 \Rightarrow e_n = 0 \ \forall \ n \geq \ 0.$$

Remarques :
- Dans le cas particulier de la $\mathbb{Z}_l$-extension cyclotomique $\mathbb{Q}_\infty$ de $\mathbb{Q}$ on a : $\lambda_l = \mu_l = \nu_l = 0$.
- Iwasawa a conjecturé la nullité de μ_l pour la $\mathbb{Z}_l-$ extension cyclotomique. Dans le cas particulier où $K/\mathbb{Q}$ est abélienne, ce résultat a été démontré par Ferrero et Washington mais dans tous les autres cas le problème reste ouvert. Ce qui est acquis en revanche c'est que ce dernier n'est pas toujours nul ; Iwasawa a donné des exemples de $\mathbb{Z}_l-$ extensions pour lesquelles μ_l était arbitrairement grand.
- Si K_n/K désigne le n-ième étage de la $\mathbb{Z}_l$-extension alors on a :

$$\mu(K_\infty/K_n) = p^n \mu(K_\infty/K) \text{ et } \lambda(K_\infty/K_n) = \lambda(K_\infty/K).$$

Le cas des corps de fonctions : [5]
On a vu précédemment que l'origine de l'intérêt d'Iwasawa pour les $\mathbb{Z}_l-$ extensions de corps de nombres prenait sa source dans la théorie des corps de fonctions, aussi il est naturel de se demander si le résultat obtenu ci-dessus connait un analogue dans le contexte des corps de fonctions et si oui, quelle en est sa formulation. En ce qui concerne la famille des $\mathbb{Z}_l-$ extensions dites arithmétiques dont la construction a guidé celle de la $\mathbb{Z}_l-$ extension cyclotomique d'un corps de nombres, la formule asymptotique ci-dessus fait écho à un résultat obtenu antérieurement aux travaux d'Iwasawa et dont on rappelle l'énoncé ci-dessous. Soit K un corps de fonctions algébriques de corps des constantes le corps fini $\mathbb{F}_q$ à q éléments. Étant supposée fixée une clôture algébrique $\overline{\mathbb{F}}_q$ de $\mathbb{F}_q$, on désigne comme précédemment par $\mathbb{F}_n$ l'unique sous-corps de $\overline{\mathbb{F}}$ tel que $[\mathbb{F}_n : \mathbb{F}] = n$. Soit maintenant $K_n := K\mathbb{F}_n$, l'extension arithmétique de K de corps des constantes $\mathbb{F}_n$ dont on note h_{K_n} le nombre de classes, à savoir le cardinal du groupe $Cl^0_{K_n}$ des classes de diviseurs de degré nul que par référence à la nature géométrique des informations qu'il concentre l'on note aussi parfois $J(\mathbb{F}_n)$. La question qui nous intéresse serait de connaître le comportement de cet entier au sein de la l-tour :

$$K \subset K_l \subset K_{l^2} \subset K_{l^n} \subset \cdots$$

ou plus simplement l'évolution de l'ordre de la l-partie $J(\mathbb{F}_{l^n})(l)$ associée aux groupes abéliens $J(\mathbb{F}_{l^n})$ que l'on peut noter l^{e_n} pour $e_n = \text{ord}_l \ h(K_{l^n})$ où e_n dépend de l. On dispose alors du résultat fondamental suivant qui est à rapprocher de celui énoncer dans le contexte des corps de nombres à savoir :

[5] [40]

Théorème 2.3.15. *Il existe des constantes λ_l, ν_l et un entier positif n_0 tels que pour tout $n \geq n_0$, $e_n = \lambda_l n + \nu_l$. Autrement dit, les entiers e_n croissent linéairement avec n.*

On dispose en outre du théorème de structure suivant :

Proposition 2.3.16. *Sous les hypothèses et avec les notations précédentes, on a l'isomorphisme :*

$$J(\mathbb{F}_{l_\infty})(l) \simeq \bigoplus_{i=1}^{r_l} \mathbb{Q}_l/\mathbb{Z}_l$$

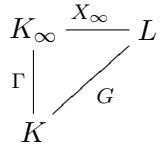
où r_l désigne la dimension sur $\mathbb{Z}/l\mathbb{Z}$ de $J[l] \cap J(F_{l_\infty})$.

Dans le cas des $\mathbb{Z}_p$-extensions géométriques[6] en revanche, le dictionnaire n'a été complété que plus tardivement car, certaines précautions sont à observer, certaines hypothèses à préciser de sorte de se placer dans un contexte favorable à la définition des invariants d'Iwasawa.
On commence par exploiter les travaux de Gold et Kisilevsky menés dans [21] pour mettre en lumière l'une des différences fondamentales régissant le comportement des $\mathbb{Z}_p$-extensions de corps globaux. Ainsi, si l'on note $\mathcal{G}$ le groupe de Galois associée à la p-extension maximale de K (où K désigne un corps de fonctions de corps des constantes $\mathbb{F}_q$) on peut montrer, en considérant la p-partie associée, l'isomorphisme $\mathcal{G}_p \simeq \mathbb{Z}_p^\infty$ qui apparaît de ce fait comme un pro-p-groupe libre de rang infini. Sachant qu'une $\mathbb{Z}_p$-extension est la donnée d'un homomorphisme $f : \mathcal{G}_p \to \mathbb{Z}_p$ et que les conditions de ramification sont données par l'équivalence : L/K est totalement ramifiée en $\mathfrak{p} \Leftrightarrow f(\prod U_\mathfrak{p}^1) = \mathbb{Z}_p$, on a une infinité de $\mathbb{Z}_p$-extension et en outre on peut choisir f tel que la $\mathbb{Z}_p$-extension associée soit ramifiée en une infinité de premiers.
La situation qui se présente à nous est donc bien différente et en un certain sens bien plus défavorable que celle qui prévaut dans les corps de nombres ; on rappelle à cette occasion que si l'on note $\hat{K}$ le compositum de toutes les $\mathbb{Z}_p$-extensions d'un corps de nombres K et que l'on suppose satisfaite la conjecture de Leopoldt (en p) usuellement notée $\mathcal{L}(K,p)$ alors $Gal(\hat{K}/K) \simeq \mathbb{Z}_p^{r_2+1}$ où r_2 désigne le nombre de plongements complexes.

Étant donné K un corps de fonctions que l'on peut, pour fixer les idées, supposer égal au corps des fonctions rationnelles $\mathbb{F}_q(T)$, on désigne par K_∞/K une $\mathbb{Z}_p$-extension géométrique provenant d'une p-tour d'extensions dont on baptisera K_n le n-ième étage (en particulier, $[K_n : K] = p^n$). Comme il est d'usage dans le cadre de la théorie d'Iwasawa, on note Γ le groupe de Galois $Gal(K_\infty/K) =< \gamma >$ et l'on considère L la p-extension abélienne

[6] On remarque qu'étant donné K un corps de fonctions de corps des constantes k fini isomorphe à $\mathbb{F}_q$ où $q = p^\alpha$, il n'existe pas de $\mathbb{Z}_l$-extension pour $l \neq p$.

non-ramifiée maximale de K_∞. Soient X_∞ et G les groupes de Galois de L/K_∞ et L/K respectivement selon le diagramme d'extensions :



En particulier, on a l'isomorphisme naturel $\Gamma \simeq G/X_\infty$ et l'on transporte l'action (par conjugaison) de G sur X_∞ en une action de Γ sur X_∞ lui conférant ainsi une structure de Γ-module. En effet, on considère la suite exacte courte (simple traduction de l'isomorphisme exhibé ci-dessus) :

$$0 \to X_\infty \hookrightarrow G \overset{\pi}{\twoheadrightarrow} \Gamma \to 0$$

Pour tout $x \in X_\infty$ et tout $r \in \Gamma$, on choisit via la surjectivité de l'application π, $g \in G$ tel que $\pi(g) = r$; on pose alors :

$$\Gamma \times X_\infty \to X_\infty$$

$$(r, x) \mapsto x^r := gxg^{-1}$$

dont on vérifie qu'elle est bien définie car si g_1 désigne un autre antécédent de r par π alors $g^{-1}.g_1 = x_0$ pour $x_0 \in X$. Or ce dernier étant abélien, on obtient immédiatement que :

$$x^r = gxg^{-1} = g_1 x_0^{-1} x x_0 g_1^{-1} = g_1 x g_1^{-1},$$

d'où le résultat. Si maintenant on note Λ l'algèbre de groupe complète (dite "Algèbre d'Iwasawa") $\mathbb{Z}_p[[\Gamma]]$ dont on rappelle qu'elle isomorphe à $\mathbb{Z}_p[[T]]$ via $\gamma - 1 \mapsto T$) ; X_∞ est alors muni d'une structure de Λ-module compact que l'on peut raffiner via la proposition suivante dûe à Gold et Kisilevsky et qui sera, en même temps qu'elle est propre au contexte des extensions géométriques des corps de fonctions, essentielle par la suite :

Proposition 2.3.17. *S'il existe un nombre fini de premiers de K qui se ramifient dans la $\mathbb{Z}_p$-extension K_∞/K alors le Λ-module X_∞ est noethérien et de torsion. En revanche, on perd le caractère noethérien dès lors qu'une infinité de places se ramifient.*

Conséquences :

- Notre but étant de développer une théorie d'Iwasawa des Z_p-extensions géométriques, ce qui suppose en particulier de définir les invariants que l'on a mis en évidence conjointement dans le cas des corps de nombres et celui des $\mathbb{Z}_l$-extensions arithmétiques de corps de fonctions, *nous serons sans cesse tenus* de nous placer sous l'hypothèse qu'il n'existe qu'un nombre fini de premiers potentiellement ramifiés dans K_∞ (hypothèse que Li et Zhao désignent de manière abrégée par le sigle : FRP pour "Finitely Ramified Primes ").
- Sous "FRP", on a que les groupes d'inertie associés aux premiers ramifiés sont des sous-groupes de $\mathbb{Z}_p$, à savoir de la forme $p^d\mathbb{Z}_p$ pour un certain d. En particulier, il existe un n_0 à partir duquel les places sont totalement ramifiées, aussi quitte à monter assez haut dans la tour, on peut toujours supposer, sans perte de généralité, que les premiers ramifiés dans K_∞/K le sont totalement.

Dorénavant, tous les résultats sont énoncés sous l'hypothèse F.R.P .

On commence par la proposition suivante qui nous donnerait envie de renverser le cours de l'histoire en rapprochant les $\mathbb{Z}_p$-extensions géométriques de celles des corps de nombres, à moins qu'il ne s'agisse là d'un premier avertissement que le miroir qui invite à une correspondance entre les deux grandes familles de corps globaux, reste déformant ...

Proposition 2.3.18. *Soient L la p-extension abélienne non-ramifiée maximale de K_∞ et K_0 la p-extension abélienne non-ramifiée maximale de K contenue dans L. Si l'on désigne par K_∞ une $\mathbb{Z}_p$-extension géométrique de K alors il existe au moins une place de K qui se ramifie dans K_∞.*

Preuve : On raisonne par l'absurde en supposant qu'il existe une $\mathbb{Z}_p$-extension géométrique K_∞/K non-ramifiée. Soit maintenant $\widetilde{K}$ la $\mathbb{Z}_p$-extension arithmétique de K (dont on rappelle qu'elle est non-ramifiée), alors le compositum $K_\infty\widetilde{K}$ est non-ramifée sur K de groupe de Galois isomorphe à $\mathbb{Z}_p \times \mathbb{Z}_p$. Or par la théorie du corps de classes, on a :

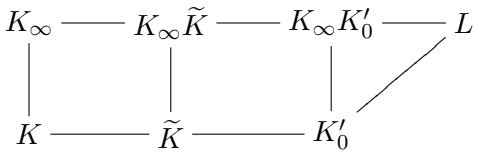
$$Gal(K_0/K) \simeq \mathbb{Z}_p \times Cl_0(K_n)$$

où $Cl_0(K_n)$ est fini quand on a l'inclusion $\tilde{K} \subseteq K_0$ que prouve le lemme suivant.

Lemme 2.3.19. *Sous les hypothèses et les notations de la proposition précédente, K_0 est l'extension abélienne non-ramifiée maximale de $\widetilde{K}$ contenue dans L.*

Preuve : Soit K_0' la p-extension abélienne non-ramifiée maximale de $\widetilde{K}$ telle que $K_0 \subseteq K_0' \subseteq L$. Notre but est de prouver qu'elle est abélienne

donc en particulier galoisienne ... On commence par construire le diagramme d'extensions suivant :



Pour tout $\sigma \in Gal(L/K)$, $\sigma(K_0')$ est la p-extension non-ramifiée maximale de $\sigma(\widetilde{K}) = \widetilde{K}$. De l'unicité de l'extension non-ramifiée maximale, on déduit que $\sigma(K_0') = K_0'$ et par conséquent K_0' est galoisienne. En outre et grâce à une remarque antérieure, K_∞/K est totalement ramifiée quand K_0'/K est non-ramifiée ainsi on a l'isomorphisme $Gal(K_0'/K) \simeq Gal(K_0'K_\infty/K_\infty)$ qui assure que $Gal(K_0'/K)$ est abélien par conséquent $K_0' = K_0$, ce que l'on voulait. On remarque que l'extension $K_\infty\tilde{K}$ est galoisienne sur K étant donné que K_∞/K et $\tilde{K}/K$ le sont ; ainsi $Gal(L/K_\infty\tilde{K})$ peut être vu comme un sous-groupe normal de $Gal(L/K)$ et par conséquent un sous-Λ-module de X_∞ noethérien et de torsion. On dispose enfin d'une suite exacte :

$$0 \to Y \hookrightarrow X_\infty \twoheadrightarrow \mathbb{Z}_p \to 0$$

On est alors en mesure d'énoncer le résultat majeur suivant :

Théorème 2.3.20. *Soient K_∞/K une $\mathbb{Z}_p$-extension géométrique satisfaisant l'hypothèse F.R.P. et p^{e_n} la puissance de p divisant le nombre de classes de K_n, alors il existe des entiers $\lambda \geq 0$, $\mu \geq 0$ et ν tels que pour n suffisamment grand, on ait la formule asymptotique :*

$$e_n = \lambda n + \mu p^n + \nu$$

où λ et μ sont les invariants d'Iwasawa du Λ-module $Y = Gal(L/K_\infty\widetilde{K})$.

Corollaire 2.3.21. *Soient K_∞/K une $\mathbb{Z}_p$-extension de corps de fonctions géométrique et L sa p-extension non-ramifiée maximale telle que $X_\infty = Gal(L/K_\infty)$. ALors, $\mu(X_\infty) = \mu(K_\infty/K)$ et $\lambda(X_\infty) = \lambda(K_\infty/K) + 1$.*

Preuve : C'est une conséquence immédiate de l'existence de la suite exacte :

$$0 \to Y \hookrightarrow X_\infty \twoheadrightarrow \mathbb{Z}_p \to 0$$

et du caractère additif des invariants d'Iwasawa λ et μ via :

$$\mu(X_\infty) = \mu(K_\infty/K) + \mu(\mathbb{Z}_p)$$

$$\lambda(X) = \lambda(K_\infty/K) + \lambda(\mathbb{Z}_p)$$

sachant $\mu(\mathbb{Z}_p) = 0$ et $\lambda(\mathbb{Z}_p) = 1$ puisque $(\mathbb{Z}_p) \simeq \Lambda/ < T >$, d'où le résultat.

2.4 Les $\mathbb{Z}_p$-extensions géométriques : un analogue cyclotomique ?

Un candidat a été postulé par Aiba en 2003 dans un article paru aux Acta Arithmetica et intitulé *"On the vanishing of Iwasawa invariants of geometric cyclotmic $\mathbb{Z}_p$-extensions"* et qui est rendu naturel en vertu de la proposition :

Proposition 2.4.1. *Soit k_∞/k une $\mathbb{Z}_p$-extension géométrique sur le corps rationnel $k = \mathbb{F}_q[T]$ avec un nombre fini de places ramifiées. On a alors les assertions suivantes :*

1. *S'il existe un unique premier de k ramifié dans k_∞/k alors les invariants d'Iwasawa associés à cette dernière sont tels que :*
$$\lambda(k_\infty/k) = \mu(k_\infty/k) = \nu(k_\infty/k) = 0.$$
2. *S'il existe au moins deux places de k ramifiées dans k_∞/k alors $\lambda(k_\infty/k) > 0$ ou $\mu(k_\infty/k) > 0$.*

On a vu que dans le cas de l'extension cyclotomique $\mathbb{Q}_\infty$ de $\mathbb{Q}$ les invariants d'Iwasawa étaient nuls et que l'on baptisait "extension cyclotomique" d'un corps de nombres K le compositum $K\mathbb{Q}_\infty$, aussi au vu de l'énoncé précédent on introduit dans le cadre des corps de fonctions géométriques la définition naturelle suivante :

Définition 2.4.2. *Soit k_∞/k une $\mathbb{Z}_p$-extension géométrique de $k = \mathbb{F}_q[T]$ non-ramifiée en dehors d'un unique premier. Si l'on note K une extension finie de k, on pose : $K_\infty = Kk_\infty$. On appelle alors K_∞ la $\mathbb{Z}_p-$extension géométrique cyclotomique associée à K.*

On se souvient avoir souligné lors d'un alinéa précédent qu'il semblait un petit peu abusif de présenter comme "analogues" l'extension cyclotomique d'un corps de nombres et la $\mathbb{Z}_l$-extension arithmétique associée à un corps de fonctions tant leur comportement diffère du point de vue de la ramification ; à cet égard, la définition proposée par Aiba semble des plus satisfaisante néammoins une obstruction subsiste dont on trouve l'origine par exemple dans l'article de Golod et Kisilevsky auquel fait référence Aiba pour justifier son candidat. Ils proposent en effet la construction de $\mathbb{Z}_p$-extensions géométriques, ramifiées en une seule place pour lesquelles le nombre de classes $h(K_n)$ que l'on sait minoré deviendrait arbitrairement grand lorsque $n \to \infty$ et ce faisant ils mettent en évidence que le concept de $\mathbb{Z}_p$-extension géométrique cyclotomique est encore incertain ... A défaut de régler définitivement la qestion (peut-être finalement en considérant illusoire cette quête de "l'analogue perdu "), on propose dans la section suivante de s'arrêter sur la construction astucieuse de Ch. Li [7] et J. Zhao d'une $\mathbb{Z}_p$-extension géométrique de $K = \mathbb{F}_q(T)$, cyclotomique au sens où elle provient de l'analogue

[7] il s'agit d'un ancien élève de Rosen reconverti depuis ... dans la finance

dans les corps de fonctions des extensions du même nom (dont nous rappellerons sous forme d'un tableau les propriétés essentielles) et dont le nombre de classes $h(K_n)$ se rapproche autant que possible de la borne inférieure.

2.4.1 Les extensions cyclotomiques dans les corps de fonctions.

Introduction

L'étude systématique des extensions cyclotomiques du corps des rationnels a débuté au 19-ième siècle avec les travaux de Kummer et furent déterminant dans sa contribution sur le travail du dernier théorème de Fermat. Comme nous avons eu l'occasion de le rappeler l'étude des tours cyclotomiques de corps de nombres s'est développée sous l'impulsion de K. Iwasawa dans les années 50, une de ses applications majeures étant l'obtention de la formule asymptotique décrivant l'évolution du cardinal de la p-partie du groupe de classes au fur et à mesure que l'on monte dans la tour. La théorie des corps de fonctions cyclotomiques a quant à elle vu le jour dans les années 30 avec les travaux de Carlitz qui va donner son nom à un certain module bâti sur l'anneau de polynômes $\mathbb{F}_q[T]$ en une indéterminée. Étant donné P un polynôme de $\mathbb{F}_q[T]$ fixé, on peut utiliser le module de Carlitz pour construire une extension $K(P)$ de $K = \mathbb{F}_q(T)$ dite "cyclotomique" et dont les propriétés interviennent de façon essentielle dans l'étude des extensions abéliennes de K (en particulier en vue d'une formulation d'un analogue dans le cadre des corps de fonctions du théorème de Kronecker-Weber).[8] Par la suite, les idées développées par Carlitz ont été génralisées indépendamment par Drinfeld et Hayes pour un corps global de caractéristique p.

A propos du module de Carlitz...

On suppose fixée une clôture algébrique $\overline{K}$ de $K = \mathbb{F}_q(T)$ et l'on considère ϕ et $\mu_T \in \mathrm{End}_{\mathbb{F}_q}(\overline{K})$ tels que :

$$\begin{array}{rcl} \phi : \overline{K} & \to & \overline{K} \\ u & \mapsto & u^q \end{array}$$

$$\begin{array}{rcl} \mu_T : \overline{K} & \to & \overline{K} \\ u & \mapsto & \mu_T(u) = Tu \end{array}$$

[8] [29]

On dote ainsi le $\mathbb{F}_q$-espace vectoriel $\overline{K}$ d'une structure de $\mathbb{F}_q[T]$-module via :

$$\begin{array}{rcl} \mathbb{F}_q[T] \times \overline{K} & \to & \overline{K} \\ (f(T), u) & \mapsto & u^{f(T)} = f(\phi + \mu_T)(u) \end{array}$$

Ce $\mathbb{F}_q[T]$-module est un *module de Carlitz*, c'est-à-dire un module de Drinfeld de rang 1. Maintenant, pour tout polynôme unitaire $M \in \mathbb{F}_q[T]$, on considère le $\mathbb{F}_q[T]$-module :

$$\Lambda_M := \{\lambda \in \overline{K} / u^M = 0\}$$

des points de M-division (ou M-torsion).
Λ_M ainsi construit est doté d'une structure de $\mathbb{F}_q[T]$-module isomorphe en tant que tel à $\dfrac{R_T}{(M)}$.

Exemple :
On suppose $p = q = 2$ et l'on se propose de déterminer μ_{T^2+T+1}.
D'après ce qui précède, on a :

$T \mapsto \tau + T$ où $\tau : x \mapsto x^q$ désigne l'endomorphisme de Frobenius de $\overline{K}$; ainsi :

$$\begin{array}{rcl} T^2 = T.T \mapsto (\tau + T) \circ (\tau + T) & = & \tau^2 + T\tau + \tau T + T^2 Id \\ & = & \tau^2 + (T^2 + T)\tau + T^2 Id \end{array}$$

(en vertu de la relation de commutation : $\tau T = T^2 \tau$)

D'où finalement :

$T^2 + T + 1 \mapsto \tau^2 + (T^2 + T + 1)\tau + (T^2 + T + 1)Id$; l'action sur $\overline{K}$ est alors donnée par :

$$\begin{array}{rcl} \mu_{T^2+T+1}(\lambda) & = & \lambda^4 + (T^2 + T + 1)\lambda^2 + (T^2 + T + 1)\lambda \\ & = & \lambda[\lambda^3 + (T^2 + T + 1)\lambda + (T^2 + T + 1)] \end{array}$$

Remarque : Le polynôme $\lambda^3 + (T^2 + T + 1)\lambda + (T^2 + T + 1)$ est irréductible sur $K = \mathbb{F}_2(T)$ et par conséquent $F := \dfrac{K[\lambda]}{\lambda^3 + (T^2 + T + 1)\lambda + (T^2 + T + 1)}$ est un corps.

2.4.2 Quelques mots du dictionnaire ...

Corps de fonctions	Corps de nombres
Soit $K = \mathbb{F}_q(T)$ le corps des fonctions rationnelles de corps des constantes $k = \mathbb{F}_q$ dont on rappelle ci-dessous une caractérisation. Les propriétés 1 et 2 sont équivalentes : 1. K/k est le corps des fonctions rationnelles 2. le genre de K/k est nul et il existe un diviseur de degré 1	$\mathbb{Q}$ le corps des nombres rationnels
Constantes	Racines de l'unité
$\mathbb{F}_q[T] := R_T$, anneau des entiers associé à $K = \mathbb{F}_q(T)$. Attention, il dépend du choix de l'uniformisante $T \cdots$	$\mathbb{Z}$ anneau des entiers du corps $\mathbb{Q}$
Pour M un polynôme unitaire de $\mathbb{F}_q[T]$ on considère le quotient : $\dfrac{R_T}{(M)}$	Soit $m \in \mathbb{N}$ où m est non-nul ; on considère alors le quotient $\dfrac{\mathbb{Z}}{m\mathbb{Z}}$, anneau des classes résiduelles modulo m.
$\Lambda_{\mathcal{C}}[M] := \Lambda_M$ pour $M \in R_T$. On rappelle qu'un module de Carlitz est un module de Drinfeld de rang 1. 1. Il s'agit d'un R_T-module cyclique possédant exactement $\Phi(M)$ éléments naturellement isomorphe à $\dfrac{R_T}{(M)}$, pour tout $M \in R_T$, $M \neq 0$ 2. Si Λ est un générateur fixé de Λ_M et si $A \in R_T$ alors λ^A est un générateur de Λ_M si et seulement si A et M sont relativement premiers. 3. On peut aussi voir Λ_M comme l'ensemble des zéros d'un polynôme séparable u^M sur R_T (points de M-torsion dans $\overline{K}$) où $$u^M = M(\varphi + \mu_T)(u)$$ avec $\varphi(u) = u^q$. *Propriété* (utile dans les démonstrations) : Soit $M = \alpha\, \Pi P^n$ une factorisation de Men produit de puissances de polynômes irréductibles unitaires, alors on a l'égalité : $$\Lambda_M = \Sigma_{P\|M} \Lambda_{P^n}$$ et cette somme est directe .	On considère l'ensemble S défini comme suit : $$S = \{1 - \zeta_m^i \text{ avec } 0 \leq i \leq m\}$$
$\lambda_P \in \Lambda_P$ avec $\lambda_P \neq 0$ tel que $\Lambda_P = (\lambda_P)$.	$\zeta_p - 1$ avec p premier impair.

Définition : On note $\Phi(M)$ l'ordre du groupe des unités (i.e. des éléments inversibles) du quotient $\frac{R_T}{(M)}$ ainsi donc $$\Phi(M) = \sharp(\frac{R_T}{(M)})^\times)$$ *Propriété* : Si M est de degré $d \geq 1$, on a la formule : $$\Phi(M) = q^d \, \Pi_{i=1}^r (1 - q^{-d_i})$$ où $d_1, d_2, \cdots, d_r$ sont les degrés des polynômes unitaires irreductibles sur $\mathbb{F}_q$ divisant M.	$\varphi(m)$, la fonction d'Euler classique satisfaisant : $$\varphi(m) = \sharp((\mathbb{Z}/m\mathbb{Z})^\times)$$
On définit maintenant ce que l'on appelle le *n-ième corps cyclotomique* associé à K. On pose : $$K_M := \ K_{\mathcal{C},M} = K(\Lambda_M).$$ Il s'agit du sous-corps de $\overline{K}$ engendré sur K par les éléments de Λ_M. **Théorème 2.4.3.** *: K_M/K est une extension géométrique de corps des constantes $\mathbb{F}_q$.*	Soit une racine primitive m-ième de l'unité, on définit le m-ième corps cyclotomique associé à $\mathbb{Q}$ via $$K_m = \mathbb{Q}(\zeta_m)$$
Si m et N sont deux polynômes unitaires copremiers dans R_T alors K_{MN} est le compositum de K_M et K_N.	Soient m et n deux entiers naturels non-nuls premiers entre eux. On désigne par α (resp β) une racine primitive m-ième (resp. n-ième) de l'unité dans $\mathbb{C}$ alors : $$\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha\beta)$$ et $$\mathbb{Q}(\alpha) \cap \mathbb{Q}(\beta) = \mathbb{Q}$$
Comme Λ_M est l'ensemble des zéros d'un polynôme séparable u^M sur $R_T \subset K$, l'extension $K(\Lambda_M)/K$ est galoisienne finie de groupe de Galois abélien. **Théorème 2.4.4.** *Le groupe de Galois $G_M = Gal(K(\Lambda_M)/K)$ est isomorphe au groupe des unités de $\frac{R_T}{(M)}$. L'extension galoisienne $K(\Lambda_M)/K$ est abélienne de degré $\Phi(M)$.* On a : $$[K(\Lambda_M) : K] = \ \Pi_{P\|M}[K(\Lambda_{P^n}) : K]$$ $$[K(\Lambda_M) : K] = \ \Pi_{P\|M}\Phi(P^n)$$ $$[K(\Lambda_M) : K] = \Phi(M)$$	Soient $\zeta_m \in \mathbb{C}$ une racine primitive m-ième de l'unité et $K_m = \mathbb{Q}(\zeta_m)$ alors $K_m/\mathbb{Q}$ est une extension abélienne de degré $\varphi(m)$ de groupe de Galois isomorphe à $(\frac{\mathbb{Z}}{m\mathbb{Z}})^\times$.
Soit λ_M un générateur de Λ_M . On note $\mathcal{O}_{K_M}$ la clôture intégrale de R_T dans K_M alors $\mathcal{O}_{K_M} = R_T[\lambda_M]$	$\mathbb{Z}[\zeta_m]$ anneau des entiers de $\mathbb{Q}(\zeta_m)$

Sont ramifiés dans $K_M = K(\Lambda_M)$:

- les premiers P tels que $P|M$ (*totalement ramifiés*) et la place à l'infini P_∞ (*modérement ramifiée*).
- En particulier, $ord_{\mathfrak{P}}(\lambda) = 1$ si $\mathfrak{P}$ désigne l'unique premier de K_M au-dessus de P.
- $K(\Lambda_M)_{\mathfrak{P}}/K_{\mathfrak{P}}$ est totalement ramifiée de degré $\Phi(M)$ (où $\mathfrak{P}$ désigne l'unique premier de K_M au-dessus de P).
- La place à l'infini se décompose en $(\frac{\Phi(M)}{q-1})$ premiers dans $K_M = K(\Lambda_M)$ et l'on a $e_\infty = q-1$ $f_\infty = 1$.

Soit $\zeta_\mu \in \mathbb{C}$ une racine primitive m-ième de l'unité et $K_m = \mathbb{Q}(\zeta_m)$. L'idéal $p\mathbb{Z}$ associé au nombre premier p est ramifié dans K_m si et seulement si $p|m$. Soit f le plus entier positif tel que :

$$p^f \equiv 1 (\text{mod } m)$$

alors $P = p\mathbb{Z}$ se décompose en $\phi(m)/f$ premiers de degré f dans K_m.

- On considère le sous-groupe de G_M défini comme suit :

$$J = \{\sigma_a, a \in (\mathbb{F}_q)^*\}$$

où $\sigma_a(\lambda) = a\lambda$ pour $\lambda \in \Lambda_M$; J ainsi défini est le groupe d'inertie ($\simeq$ groupe de décomposition) de toute place de K_M au-dessus de l'infini .

On désigne par $\mathbb{Q}_m^+$ le sous-corps réel maximal de

$$\mathbb{Q}(\zeta_m + \zeta_m^{-1})$$

La place archimédienne de $\mathbb{Q}$ dite "place à l'infini" se décompose complètement dans $\mathbb{Q}_m^+$ et tout premier au-dessus de cette dernière se ramifie dans $\mathbb{Q}_m$.

Par la théorie de Galois, on associe à J le sous-corps K_M^+ de K_M ; il s'agit du plus grand sous-corps de dans lequel l'∞ est totalement décomposée. En outre, tout premier de au-dessus de la place à l'infini est totalement et modérément ramifiée dans $K_M = K(\Lambda_M)$.

- $Gal(K_M/K_M^+) \simeq (\mathbb{F}_q)^*$, les unités non-nulles de l'anneau $\mathbb{F}_q[T]$.
- $[K_M : K_M^+] = q-1$
- Si $K_M = K(\Lambda_M) = K(\lambda_M)$ alors :

$$K_M^+ = K(\lambda_M^{q-1})$$

On rappelle l'isomorphisme :

$$Gal(\mathbb{Q}_m/\mathbb{Q}^+) \simeq \{+/-1\}$$

Symbole d'Artin : Soit P un polynôme unitaire irréductible de $\mathbb{F}_q[T]$ ne divisant pas M, alors le symbole d'Artin en la place associée à P noté $(\frac{K_M/K}{P})$ est égal à σ_P où l'on rappelle :

$$\sigma_P(\lambda) = \lambda^P, \quad \forall\, \lambda \in K_M$$

.

L'automorphisme d'Artin associé à l'idéal premier $p\mathbb{Z}$ est défini par :

$$\sigma_p : \zeta_m \mapsto \zeta_m^p$$

où $(p, m) = 1$.

Théorème 2.4.5. *Toute extension abélienne de K dans laquelle la place à l'infini est* modérément ramifiée *est un sous-corps d'une extension arithmétique d'un corps cyclotomique K_M pour un certain $M \in R_T$.*

Théorème 2.4.6. *(Kronecker-Weber) Toute extension abélienne finie du corps des rationnels $\mathbb{Q}$ est contenue dans une extension cyclotomique $\mathbb{Q}(\zeta_n)$ pour un certain entier naturel n.*

Application à la théorie du corps de classes :

De nouveau on suppose que $K = \mathbb{F}_q(T)$ et l'on note $R_T = \mathbb{F}_q[T]$. Ainsi pour tout polynôme $M \in R_T$ (non-constant), il existe une extension abélienne L_M/K telle que :

1. $Gal(L_M/K) \simeq (R/M)^\times/\mathbb{F}_q^\times$
2. La place à l'infini de K se décompose complètement dans L_M ; en particulier, $\mathbb{F}_q$ est le corps des constantes de L_M (extension géométrique).
3. Si $P \in R$ est irréductible et co-premier à M alors la place associée à P est non-ramifiée dans L_M/K et son groupe de décomposition est engendré par l'image de P dans $(R/M)^\times/\mathbb{F}_q^\times$.

Les conditions ci-dessus déterminent L_M de façon unique ; en outre, si L/K est une extension abélienne dans laquelle la place à l'infini est totalement décomposée alors il existe un $M \in R$ tel que $L \subseteq L_M$ (analogue du théorème de *Kronecker-Weber*).

Cas Particulier : On suppose que $M = P^n$ est une puissance d'un polynôme unitaire irréductible de R_T.
En appliquant les résultats précédents on obtient que :

1. Λ_M est un R_T-module cyclique.
2. Si l'on suppose que $\deg(P) = d$ alors toute place de K, exception faite pour P et P_∞ est non-ramifiée dans $K(\Lambda_M)$. En outre, on a :

$$e_P = \Phi(M) = q^{d(n-1)}(q-1).$$

La place à l'infini se décompose en $\dfrac{\Phi(M)}{q-1}$ premiers dans $K(\Lambda_M)$ et l'indice de ramification e_∞ est égal à $q-1$ pour chacune des places au-dessus de la place à l'infini de K. En effet, soit $\mathfrak{P}$ une place de $K(\Lambda_M)$ telle que $\mathfrak{P}|P_\infty$; puisque l'extension est galoisienne de degré $\Phi(M)$, il suffit de prouver que $e_{\mathfrak{P}} = q-1$ et $f_{\mathfrak{P}} = 1$. Soit $\mathfrak{p}$ une place de au-dessous de $\mathfrak{P}$ (et donc au-dessus de P_∞). On a le diagramme suivant :

$$\begin{array}{ccc} K(\Lambda_{P^m}) & & \mathfrak{P} \\ | & & \\ K(\Lambda_P) & & \mathfrak{p} \\ | & & \\ K & & P_\infty \end{array}$$

On conclut alors par un argument de transitivité en montrant que

$$e_{\mathfrak{P}/\mathfrak{p}} = f_{\mathfrak{P}/\mathfrak{p}} = 1$$

et

$$e_{\mathfrak{p}/P_\infty} = q-1\ ,\ f_{\mathfrak{p}/P_\infty} = 1.$$

Enfin, si $h(K(P^n))$ désigne le nombres de classes du n-ième corps cyclotomique $K(P^n)$, ce dernier se décompose sous la forme :

$$\mathrm{h}(K(P^n)) = \mathrm{h}(K(P^n))^+ + \mathrm{h}(K(P^n))^-.$$

Les similitudes de comportements que nous espérons avoir mis en évidence dans le tableau récapitulatif rend naturel l'idée de s'intéresser, comme dans le cas des corps de nombres, à la tour "cyclotomique" dont le premier étage serait justement le corps $K(P)$. Plus précisément, on considère la suite d'extensions :

$$K \subseteq K(P) \subseteq K(P^2) \subseteq \cdots K(P^n) \subseteq \cdots$$

et l'on se demande si comme dans le cas des corps de nombres l'on pourrait obtenir des renseignements sur l'évolution de la taille de la p-partie des groupes de classes associés à chaque $K(P^n)$ (vu comme l'analogue de $\mathbb{Q}(\zeta_{p^n})$ si $\zeta_{p^n} = e^{2i\pi/n}$). Li Guo et L. Shu dans un article (1999) intitulé "Class Numbers of Cyclotomic Function Fields" [24] se sont intéressés à ce problème et ont obtenu le résultat suivant :

Théorème 2.4.7. *La puissance de p divisant $h(K(P^n))^+$ (respectivement $h(K(P^n))^-$ est au moins égale à :*

$$\frac{a^+}{p-1}\frac{q^{(n-1)deg\ P}-1}{n}$$

(resp. $\dfrac{a^-}{p-1}\dfrac{q^{(n-1)deg\ P}-1}{n}$ *) où a^+ (resp. a^-) est un entier positif dépendant uniquement de $K(P)$.*

La comparaison avec les extensions cyclotomiques de corps de nombres est sans appel; au lieu d'une croissance linéaire en fonction de n, nous obtenons une croissance "au moins" exponentielle ! Ceci vient du fait que la tour considérée est bien plus grosse qu'une $\mathbb{Z}_p$-extension aussi on imagine de construire une extension de corps de fonctions (nécessairement géométrique) provenant de la tour cyclotomique et dont on s'attendrait à ce que le comportement se rapproche suffisamment de cette dernière pour suppléer au vrai-faux analogue présenté dans le cadre des extensions arithmétiques.

2.4.3 Un exemple de construction de $\mathbb{Z}_p$-extension géométrique utilisant les modules de Carlitz

On pourrait faire le choix de spécifier dès à présent le contexte très général dans lequel se placent les auteurs [9] au cas classique et maintes fois évoqué du corps des fonctions rationnelles affecté de la place à l'infini d'uniformisante associée $\frac{1}{T}$ mais cela reviendrait à amputer la théorie des corps de fonctions cyclotomiques d'une part de son extrême richesse et somme toute de sa complexité, aussi, dans un premier temps, nous nous en tiendrons aux notations et hypothèses prescrites par Li et Zhao. Ainsi donc, on considère $\mathbb{F}_q$ le corps fini à q éléments où $q = p^\alpha$ et l'on note $K = \mathbb{F}_q(T)$. On désigne par ∞ une place fixée (dite à "l'infini") de K de degré d_∞ et d'uniformisante π_∞. On note A l'anneau constitué des éléments de K holomorphe en dehors de l'infini, i.e. des fonctions régulières en dehors de l'∞ dont on rappelle qu'il est de Dedekind (exemple : dans le cas particulier où l'on prend pour place à l'infini la place $< 1/T >$, $d_{1/T} = 1$ et $A = \mathbb{F}_q[T]$). Si l'on note K_∞ le corps local, résultat de la complétion, le groupe multiplicatif $K_\infty^\times$ admet une décomposition selon :

$$K_\infty^\times \simeq F_\infty^\times . \pi_\infty^{\mathbb{Z}} . U_\infty^{(1)}$$

où $F_\infty := \mathbb{F}_{q^{d_\infty}}$

Ceci posé, on est en mesure d'introduire le concept de *"fonction signe"* qui peut être vue comme une tentative de généralisation de la notion d'unitarité pour les polynômes et dont l'effet est une certaine rigidification des structures que l'on dit alors "normalisée". Plus précisément :

Définition 2.4.8. *On appelle fonction* "fonction signe" *et l'on note "sgn" un homorphisme :*

$$sgn : K_\infty^\times \to F_\infty^\times$$

trivial sur $U_\infty^{(1)}$ et tel que $sgn \restriction_{F_\infty^\times} = id_{F_\infty^\times}$. On la prolonge à K_∞ tout entier en posant : $sgn(0) = 0$.

Remarques et Commentaires :

1. En toute rigueur, on devrait noter cette application "sgn_∞" car cette dernière dépend *fondamentalement* du choix de la place à l'infini et donc de l'uniformisante associée. En particulier, une fonction signe peut être perçue comme une projection sur le groupe multiplicatif $\mathbb{F}_\infty^\times$ (en particulier, *sgn* est surjectif).
2. Dans le cas particulier où l'on prend pour (A, ∞) l'anneau de polynômes $(\mathbb{F}_q[T], 1/T)$, on obtient que $sgn(P) = 1 \Leftrightarrow P \in A$ est unitaire. Dans ce contexte, on peut voir dans cette notion de "signe" une généralisation de celle, usuelle, qui affecte les nombres réels.
   Plus généralement, on dira que $x \in K_\infty$ est *positif* si $sgn(x) = 1$.

[9] [41]

On a en outre la proposition suivante :

Proposition 2.4.9. *Si sgn et sgn′ sont des fonctions "signe" sur K_∞ alors il existe $\zeta \in F_\infty^\times$ tel que :*

$$sgn(x) = \ sgn'(x).\zeta^{-v_\infty(x)}$$

En particulier, le nombre de fonctions "signe" sur K_∞ est égal à $q^{d_\infty} - 1 := \kappa.(q-1)$.

Preuve : Elle nous donne l'occasion de rappeler que les éléments x non-nuls de la complétion K_∞ de K en la place à l'∞ (de degré d_∞ supposée fixée) admettent un développement en série formelle de la forme : $x = \sum_{\nu \geq n} c_\nu \pi^\nu$ où $c_\nu \in \ F_\infty$ et $n = v_\infty(x)$ si v_∞ désigne la valuation associée. On définit alors $\deg(x) = \ -d_\infty.v_\infty(x)$ et l'on pose $N(x) := q^{\deg(x)}$; reste pour justifier le résultat ci-dessus à introduire l'application

$$\begin{array}{rcl} \Psi : K_\infty^\times & \twoheadrightarrow & F_\infty^\times \\ x & \mapsto & \dfrac{sgn(x)}{sgn'(x)} \end{array}$$

qui se factorise au travers de $v_\infty : K_\infty \to \mathbb{Z}$.

On va revenir dans quelques instants sur la signification arthmétique de l'entier κ évoqué ci-dessus en le présentant comme le degré d'une certaine extension du corps de classes de Hilbert H_K de K mais on peut dès à présent revenir sur une remarque faite au chapitre 1 selon laquelle le statut invariablement ultramétrique des places d'un corps de fonctions ne devait pas manquer d'en simplifier l'arithmétique pour constater à quel point elle est erronée. S'il permet de fixer les idées, le choix d'une place à l'infini (et donc d'un degré à l'infini) n'a rien d'anodin au point de risquer parfois de les figer.

Le corps de classes de Hilbert normalisé [10]

Précaution : Dans toute la suite, on suppose la place à l'infini fixée.

On considère l'anneau de Dedekind A définit précédemment et l'on note $\mathcal{I}(A)$ (resp.$\mathcal{P}(A)$) son groupe des idéaux fractionnaires associé (resp. des idéaux fractionnaires principaux non-nuls). On pose alors :

$$\mathcal{P}^+(A) := \{xA \ / \ sgn(x) = 1 \ , x \in A\}.$$

[10] Cette notion a été re-introduite par Anglès et Jaulent dans [4] sous le nom de *corps de classes de Hilbert au sens restreint* dans le cas particulier où $\infty =< 1/T >$

Il s'agit d'un sous-groupe de $\mathcal{I}(A)$ et l'on note $Pic^+(A) := \mathcal{I}(A)/\mathcal{P}^+(A)$ le groupe-quotient associé que dans [29] Hayes baptise, parfaisant ainsi l'analogie avec le cas des corps de nombres, *"narrow class group"*(littéralement "groupe de classes restreint" pour signifier le caractère rigide qui est inhérent à l'adjonction d'une fonction "signe"). On vérifie alors que si l'on note $h(A)$ le cardinal de $Pic(A)$, on a la relation :

$$h^+(A) := |Pic^+(A)| = \kappa.h(A)$$

avec $\kappa = (\mathcal{P}(A) : \mathcal{P}^+(A))$. En particulier, on dispose d'une suite exacte :

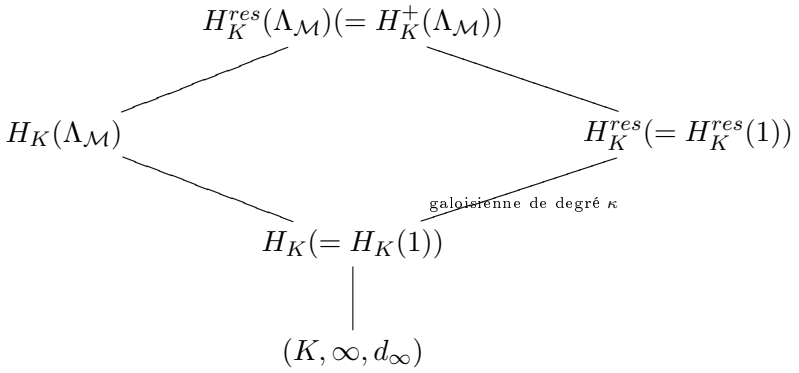
$$1 \to \mathcal{P}(A)/\mathcal{P}^+(A) \hookrightarrow Pic^+(A) \twoheadrightarrow Pic(A) \to 1$$

Entrer dans les détails de la construction nous entrainerait malheureusement trop loin car il nous faudrait revenir plus profondément sur la notion de modules de Drinfeld, omniprésente, néammoins l'idée générale réside dans le fait que l'on peut réaliser $Pic^+(A)$ comme le groupe de Galois d'une extension de K de degré $h^+(A)$ notée, sans grande originalité, H_A^+ telle que :

1. l'extension H_A^+/K soit non-ramifiée en toute place finie $\mathfrak{p}$ de K.
2. $H_A \subseteq H_A^+$ et l'extension galoisienne H_A^+/H_A résultante, de degré κ, est totalement ramifiée au-dessus de l'∞.

En particulier, lorsque $d_\infty = 1$, les notions de corps de classes de Hilbert et corps de classes de Hilbert *au sens restreint* coïncident et c'est pourquoi il est terriblement restrictif dans les discussions de s'en tenir au sacro-saint couple $(\mathbb{F}_q(T), < 1/T >)$.

On résume dans le diagramme ci-après les différentes étapes de notre incursion :



Description des extensions :

- $H_K := H(1)$ désigne le corps de classes de Hilbert de K i.e. l'extension non-ramifiée maximale totalement décomposée en l'∞ de groupe d'idèles associé $K^\times(U_{(1)}.K_\infty^\times) \subset \mathcal{J}_K$ le groupe des idèles de K.

- H_K^{res} désigne le corps de classes de Hilbert *au sens restreint* ie l'extension de H_K non-ramifiée en les places finies et totalement ramifiée en l'∞ de groupe d'idèles associé $K^\times(U_{(1)}.(\pi)^{\mathbb{Z}}.U_\infty^{(1)}.\mathbb{F}_q^\times)$.

- $\mathcal{M}$-corps cyclotomique, non-ramifié en dehors des diviseurs de $\mathcal{M}$, totalement ramifié en les diviseurs de $\mathcal{M}$ et totalement décomposé en l'∞ de groupe d'idèles associé $K^\times(K_\infty^\times.U_{\mathcal{M}})$.

- $\mathcal{M}$-ième corps cyclotomique *au sens restreint* ie non-ramifiée en dehors des diviseurs de $\mathcal{M}$, totalement ramifié en les diviseurs de $\mathcal{M}$ et modérément ramifiée en l'∞ de groupe d'idèles associé $K^\times(U_{\mathcal{M}}.(\pi)^{\mathbb{Z}}.U_\infty^{(1)})$.

avec :

- $\mathcal{M} = \prod_{\mathfrak{P}} \mathfrak{P}^{\mathfrak{m}_{\mathfrak{P}}}$
- $U_{\mathcal{M}} = \prod_{\mathfrak{P}\nmid\infty} U^{(m_{\mathfrak{P}})}$
- $K_\infty \simeq \mathbb{F}_{q^{d_\infty}} \cdot (\pi)^{\mathbb{Z}} \cdot U_\infty^{(1)}$
- $\kappa := [H_K^{res} : H_K] = \dfrac{q^{d_\infty}-1}{q-1}$; en particulier, $\kappa = 1 \Leftrightarrow d_\infty = 1$.

Application à la construction d'une $\mathbb{Z}_p$-extension "cyclotomique" de corps de fonctions.

On considère pour corps de base le corps de classes de Hilbert de K, $H_K := H$ que l'on suppose (dans un souci de simplification) confondu avec le corps de classes de Hilbert au sens restreint. Le but est de construire une $\mathbb{Z}_p$-extension géométrique de H_K ramifiée en une seule place $\mathfrak{P}$ que l'on convertira en une $\mathbb{Z}_p$-extension de K "par intersection."
Stratégie : elle nous est familière car calquée sur celle employée lors de la construction de l'extension cyclotomique du corps des rationnels (et par compositum d'un corps de nombres $K/\mathbb{Q}$) et que nous avons brièvement rappelée en début de chapitre. Ainsi, on remarque que comme dans le cas des corps de nombres, le degré $\Phi(P^n)$ (analogue de $\varphi(p^n)$) du n-ième corps cyclotomique est le résultat du produit d'une puissance de q (et donc de p) par un nombre non-divisible par p. On cherche donc à exiber le sous-corps de $H(\mathfrak{p}^{\mathfrak{m}})$ fixé par le sous-groupe de $Gal(H(\mathfrak{p}^m)/H)$ constitué des éléments d'ordre premier à p (où l'on a noté $H(\mathfrak{p}^m) := H(\Lambda_{\mathfrak{p}^m})$).

Ce qui nous facilitait la tâche dans le cas de $\mathbb{Q}$, c'était la structure de $Gal(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q})$ et plus précisément, l'isomorphisme
$Gal(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}) \simeq \mathbb{Z}/(p-1) \times \mathbb{Z}/p^{(n-1)}\mathbb{Z}$; par conséquent on va chercher, cette fois dans le contexte des corps de fonctions cyclotomiques, à décrire $(A/\mathfrak{p}^m)^\times \simeq Gal(H(\mathfrak{p}^m)/H)$.
Pour ce faire, on se ramène à un problème "local" via un résultat d'algèbre commutative qui dit la chose suivante :

Lemme 2.4.10. *Sous les hypothèses précédentes, on note $A_{(\mathfrak{p})}$ le localisé de A en l'idéal premier (donc maximal puisque A est de Dedekind) $\mathfrak{p}$. $A_{(\mathfrak{p})}$ est un anneau local, d'unique idéal maximal $S^{-1}\mathfrak{p}$ (si $S = A \setminus \mathfrak{p}$) tel que :*

$$A/\mathfrak{p}^m \simeq A_{(\mathfrak{p})}/(\mathfrak{p}A_{(\mathfrak{p})})^m$$

En outre, on montre que :

Lemme 2.4.11. *Si l'on note comme ci-dessus $A_{(\mathfrak{p})}$ le localisé de A en l'idéal premier $\mathfrak{p}$ et $\mathcal{P}$ l'unique idéal maximal associé à une uniformisante π, on a :*

$$(A_{(\mathfrak{p})}/\mathcal{P}^m)^\times \simeq (A_{(\mathfrak{p})}/\mathcal{P})^\times \times \prod_{i,j} < 1+w_i\pi^j >,\ 1 \leq i \leq r,\ 1 \leq j < m \text{ et } (j,p) = 1$$

où $\{w_i\}_i \in A_{(\mathfrak{p})}$ est un système de relèvements d'une base de $A_{(\mathfrak{p})}/\mathcal{P}$ vu comme $\mathbb{F}_p$-espace vectoriel.

Remarque : Bien entendu, dans le cas où $d_\infty \neq 1$, on a : $1 \leq i \leq d_\infty r$.
Conclusion : On a un isomorphisme *"global"* :

$$G = Gal(H(\mathfrak{p}^m)/H) \simeq (A/\mathfrak{p}^m)^\times \simeq (A/\mathfrak{p})^\times \times \prod_{i,j} < 1 + w_i\pi^j >$$

On suppose $w_1 = 1, S = w_i\ , 1 \leq i \leq r$ et l'on fixe l un entier positif premier à p (le cas le plus intéressant étant lorsque $l = 1$). Soit E_m le sous-corps de $H(\mathfrak{p}^m)$ fixe par le sous-groupe $(A/\mathfrak{p})^\times \times \prod_{i,j} < 1 + w_i\pi^j >$ où le produit parcourt la famille des $1 + w_i\pi^j$ privée de $1 + \pi^l$. Ainsi donc, $Gal(E_m/H) \simeq < 1 + \pi^l >$ d'ordre p^{f_m} avec $f_m = \lceil log_p(m/l) \rceil$. Reste à faire tendre m vers l'infini pour obtenir une $\mathbb{Z}_p$-extension L_∞ de H à ceci près qu'en général, le sous-corps E_m ne coïncide pas avec le m-ième étage de la tour d'extensions associée. On pose alors $L_n := E_m$ si $m = l(p^n - 1)$ et l'on vérifie que E_m est une extension de H_K totalement décomposée en l'infini, non-ramifiée en les places finies, exceptées celles au-dessus de $\mathfrak{p}$. En effet, on a vu précédemment que l'extension cyclotomique $H(\Lambda_{\mathfrak{P}^m})$ était non-ramifiée sur H sauf en les places au-dessus de l'infini et les places $\mathfrak{P}$ telles $\mathfrak{P}|\mathfrak{p}$. Si l'on

note L le corps fixé par le sous-groupe de $(A/\mathfrak{p}^m)^\times$ constitué des éléments d'ordre $|(A/\mathfrak{p})^\times|$ (i.e. $Gal(L/H) \simeq \prod_{i,j} < 1 + w_i\pi^j >$) alors via un résultat de Hayes ([29]), la place à l'infini se décompose dans L et par conséquent cette dernière se décompose aussi dans la p-entension $E_m \subseteq L$. Finalement, on énonce :

Proposition 2.4.12. *Soit L_∞ la $\mathbb{Z}_p$-extension contenue dans $H(\Lambda_\infty) := \cup_m H(\Lambda_{\mathfrak{P}^m})$ associée au sous-groupe engendré par $1 + w_i\pi^l$, alors le sous-corps L_n de $H(\mathfrak{p}^{l(p^n-1)})$ fixé par $< 1 + w_i\pi^l >$ représente le n-ième étage de la tour d'extensions sous-jacente.*

Construction d'une $\mathbb{Z}_p$-extension de K.

On suppose que $p \nmid h_K$ le nombre de classes de K et l'on note $G(m)$ le groupe de Galois de l'extension E_m/K où E_m est associée à un générateur $1 + w_i\pi^l$. Ainsi, $G(m) \simeq Gal(E_m/H) \times Gal(H/K)$ apparaît comme le produit direct d'un p-groupe par un groupe d'ordre premier à p (ce qui justifie l'hypothèse de divisibilité sur le nombre de classes de K), ainsi donc il existe un unique sous-groupe de $G(m)$ isomorphe à $Gal(H/K)$ et l'on note F_m le corps fixé par ce dernier. En d'autres termes, $E_m = H.F_m$ avec E_m non-ramifiée sur F_m et F_m/K totalement ramifiée en $\mathfrak{p}$. On a alors le théorème suivant [41] :

Théorème 2.4.13. *On considère K comme ci-dessus avec $(p, h_K) = 1$, alors $\cup_m F_m$ est une $\mathbb{Z}_p-$ extension géométrique de K et si l'on note g'_n et h'_n respectivement le genre et le nombre de classes associés au n-ième étage $F_{l(p^n-1)}$ de la tour alors on a :*

$$g'_n \sim \frac{l}{2(p+1)} p^{2n} \quad (n \to \infty)$$

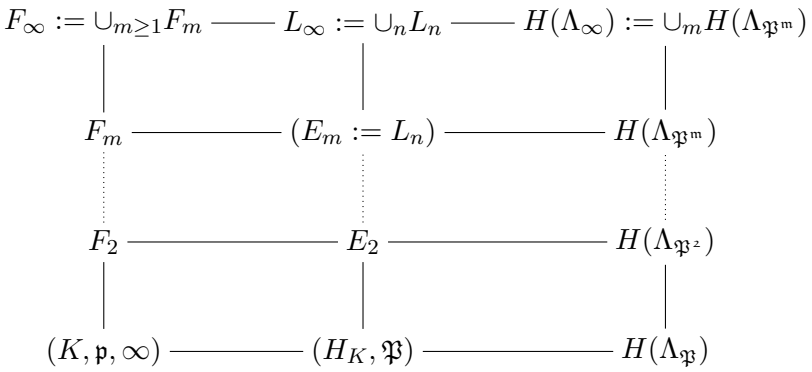
$$h'_n \sim \frac{l}{2(p+1)} p^{2n} log\ q \quad (n \to \infty)$$

Remarque : Dans le cas où l'on ne spécifie plus que la place à l'infini de K est de degré 1, on est tenu de supposer qu'elle est néammoins de degré premier à p et les relations ci-dessus deviennent :

$$g'_n \sim \frac{l d_\infty}{2(p+1)} p^{2n} \quad (n \to \infty)$$

$$h'_n \sim \frac{l d_\infty}{2(p+1)} p^{2n} log\ q \quad (n \to \infty)$$

Diagramme Récapitulatif :



Chapitre 3

A propos d'une conjecture de Gross

3.1 Motivation

Soit F un corps fini à q éléments ($q = p^\alpha$ pour p un nombre premier impair). On désigne par K un corps de fonctions algébriques d'une variable de corps des constantes F et l'on se donne K_∞ une $\mathbb{Z}_p$-extension de K de groupe de Galois $\Gamma \simeq (\mathbb{Z}_p, +)$. Soit maintenant S un ensemble fini de places ramifiées de K_∞/K ; si l'on désigne par $\mathcal{C}_{\infty,S}(p)$ la p-partie du groupe des S-classes d'idéaux de K_∞ alors Γ, en tant que groupe topologique, agit de manière naturelle sur cette dernière et l'on peut légitimement se demander si les invariants par cette action, à savoir $\mathcal{C}_{\infty,S}(p)^\Gamma$ (vu comme sous-groupe de $\mathcal{C}_{\infty,S}(p)$) est *d'ordre fini*. Reste à comprendre pourquoi l'on peut voir dans ce problème posé un analogue de *la* (ou plutôt "d'une") Conjecture de Gross et c'est un article d'Iwasawa intitulé : "On Cohomology Groups of Units for $\mathbb{Z}_p$-extensions "qui va nous permettre de faire le lien jusqu'à rendre naturelle une assimilation qui pourrait de prime abord paraître quelque peu abusive en rappelant qu'étant donnée une $\mathbb{Z}_p$-extension de corps de nombres de type C.M, la finitude de $\mathcal{C}_{\infty,S}(p)^{-\Gamma}$ (resp. $\mathcal{C}_{\infty,S}(p)^{+\Gamma}$) est équivalente à la Conjecture de Gross (resp. à la Conjecture de Leopoldt dont on rappelle qu'elle a été démontrée dans le contexte des corps de fonctions par Kisilevsky en 1992).

Dans le cas d'une $\mathbb{Z}_p$-extension arithmétique, la finitude du groupe $\mathcal{C}_{\infty,S}(p)$ est obtenue via des arguments purement algébriques relevant essentiellement de la théorie des modules noethériens ; en revanche les choses ne se passent pas si tranquillement lorsque l'on considère des $\mathbb{Z}_p$-extensions *géométriques* et c'est donc sur cette famille que les efforts des auteurs se portent jusqu'à obtenir, à grand renfort du formalisme de Witt dont les grands axes ont été rappelés lors du chapitre 2, une condition *nécessaire et suffisante* formulée en terme de normes de S-unités garantissant la finitude de $\mathcal{C}_{\infty,S}(p)^\Gamma$.

Plus précisément, les conditions aux normes -obtenues notamment grâce à une formule des classes ambiges-, seront répertoriées dans une matrice carrée $\mathcal{M}$ d'ordre $|S|-1$ à coefficients dans $\mathbb{Z}_p$, l'anneau des entiers p-adiques. *Le caractère inversible de cette dernière entrainera la finitude de* $\mathcal{C}_{\infty,S}(p)^{\Gamma}$ *et la réciproque sera assurée dès lors que la matrice* $\mathcal{M}$ *sera à coefficients dans* $\mathbb{Q}$.

3.1.1 Quelques mots sur la théorie de la S-ramification

On se donne K/F un corps de fonctions algébriques supposé fixé de corps des constantes F et l'on désigne par $S \subseteq S_K$ un ensemble fini de places de K (supposé *non vide*). On pose alors :

$$\mathcal{O}_S := \{a \in K / \mathrm{ord}_P(a) \geq 0, \forall P \notin S\}$$

Il s'agit de l'anneau des S-entiers associé à K ; il est muni d'une structure d'anneau de Dedekind et satisfait : $\mathcal{O}_S = \bigcap_{P \notin S} \mathcal{O}_P$ et les éléments de $\mathcal{O}_S$ sont exactement les fonctions S-entières à savoir celles qui n'admettent de pôles qu'en S. On peut montrer qu'il existe une correspondance bijective $S \leftrightarrow \mathcal{O}_S$ entre les sous-ensembles non-vide de places de K et les anneaux de Dedekind de corps de fractions K. On définit alors naturellement le groupe des S-unités via :

$$E_S = \{a \in K^{\times} / \mathrm{ord}_P(a) = 0,\ \forall P \notin S\}.$$

En particulier, $E_S = \mathcal{O}_S^{\times}$ où désigne le groupe des éléments inversibles de l'anneau des S-entiers $\mathcal{O}_S$. On remarque en outre que $F^{\times} \subseteq E_S$ et l'on va montrer que le groupe quotient résultant $E_S/F^{\times}$ est un groupe abélien libre de type fini.
On introduit ensuite le groupe des S-diviseurs de K, noté $\mathcal{D}_{S,K} := \mathcal{D}_S$ que l'on définit comme le sous-groupe de $\mathcal{D} := \mathcal{D}_K$ engendré par l'ensemble des places de $S_K - S$. En particulier, si l'on note $\deg(S)$ le pgcd des degrés des places appartenant à S, on pose pour le degré d'un S-diviseur : $\deg(\mathcal{D}_S) = \mathbb{Z}\deg S$.
Enfin, étant donné un élément $a \in K^{\times}$, on définit le S-diviseur associé par :

$$(a)_S = \sum_{P \notin S} \mathrm{ord}_P(a).P$$

Un tel diviseur $(a)_S$ pour $a \in K^{\times}$ est appelé *S-diviseur principal*. L'ensemble des S-diviseurs principaux forment un sous-groupe de $\mathcal{D}_S$ noté P_S. Le groupe quotient résultant $\mathcal{D}_S/P_S := \mathcal{C}l_S$ (pour $\mathcal{C}l(\mathcal{O}_S)$ et que l'on note aussi parfois $\mathcal{C}_S$) est appelé *groupe des S-classes*, son cardinal $h_S := |Cl_S|$ *le nombre de S-classes* et l'on a la suite exacte :

$$1 \to P_S \hookrightarrow \mathcal{D}_S \twoheadrightarrow \mathcal{C}l_S \to 1$$

On peut vérifier que le groupe $\mathcal{C}l_S$ est isomorphe au groupe des classes d'idéaux de l'anneau de Dedekind $\mathcal{O}_S$. Reste à introduire $\mathcal{D}(S)$ le sous-groupe de $\mathcal{D}$ engendré par les premiers appartenant à l'ensemble fini S et l'on pose sans surprise : $P(S) := P \cap \mathcal{D}(S)$.
On considère maintenant l'application $\deg : \mathcal{D} \to \mathbb{Z}$ dont l'image est un idéal de $\mathbb{Z}$. Soit donc $i\mathbb{Z}$ ce dernier (*remarque* : dans le cas où F est fini, on doit à F.K. Schmidt la surjectivité de "deg") ; de la même façon, l'image de $\mathcal{D}(S)$ est un idéal principal de $\mathbb{Z}$ noté $d\mathbb{Z}$ où d est égal au PGCD de l'ensemble $\{\deg P / P \in S\}$. On dispose alors des suites exactes :

$$1 \to F^\times \hookrightarrow E(S) \twoheadrightarrow P(S) \to 1$$

$$0 \to \mathcal{D}(S)^0/P(S) \hookrightarrow \mathcal{C}l^0 \to \mathcal{C}l_S \twoheadrightarrow \mathcal{C} \to 0$$

où $\mathcal{C}$ désigne un groupe cyclique d'ordre d/i.

Remarques :
- Ces deux suites exactes et leurs suites longues de cohomologie associées seront le point de départ de l'article de Villa-Madan dont l'étude détaillée sera l'objet du paragraphe 3.
- Dans le cas où le corps des constantes du corps de fonctions considéré est supposé fini, on dispose d'un analogue du théorème des S-unités, généralisation au contexte de la S-ramification du théorème de structure des unités de Dirichlet pour les corps de nombres. Ainsi on montre que $E_S/F^\times$ est un groupe abélien libre de rang $|S| - 1$ où $|S|$ désigne le cardinal de l'ensemble fini S de places distinguées.
- L'indice $(\mathcal{D}_S^0 : (E_S))$ où $\mathcal{D}_S^0 := \mathcal{D}_S \cap \mathcal{D}_K^0$ est baptisé S-régulateur et noté parfois reg_S. Plus généralement, pour tout sous-groupe U d'indice fini dans E_S, on définit son régulateur $\mathrm{reg}(U)$ comme l'indice $(\mathcal{D}_S^0 : U)$. En particulier, $\mathrm{reg}_S = \mathrm{reg} E_S$.

Définition 3.1.1. *On se donne L/K une extension abélienne de corps de fonctions et l'on considère S un ensemble fini de places de K. On désigne par $\mathcal{O}_{S,K}$ l'anneau des S-entiers de K et par $\mathcal{O}_{S,L}$ sa clôture intégrale dans L. On appelle* S-corps de classes de Hilbert *de $\mathcal{O}_{S,L}$ et l'on note H_L^S l'extension abélienne non-ramifiée maximale S-décomposée de L. On introduit alors la notion de S-corps des Genres $\mathcal{H}_{L/K}^S$ de L/K que l'on définit comme l'extension abélienne maximale de K contenue dans H_L^S.*

3.1.2 Une inspiration venue de Chevalley (via Iwasawa)...

On se propose dans cette section de revenir sur quelques-unes [1] des idées maîtresses développées dans l'article de K. Iwasawa intitulé : *"On Cohomo-*

[1] Comme il est matériellement impossible de s'attarder sur certains résultats cohomologiques relatifs à la théorie de la S-ramification, nous nous permettons un renvoi à [48]

logy Groups of Units for $\mathbb{Z}_p$-Extensions" [2] espérant ainsi introduire le plus naturellement possible la question que se proposent de résoudre Villa et Madan dans le contexte des corps de fonctions. On se place dans le contexte suivant : soient K/k une extension galoisienne arbitraire de corps de nombres et S un ensemble de places finies (i.e. ultramétriques) de k. On désigne par E_S le groupe des S-unités de K, puis respectivement par I_S, P_S et C_S les groupes des S-idéaux, son sous-groupe des S-idéaux principaux et le groupe des S-classes de K associé. On rappelle à cette occasion que l'on dispose des résultats cohomologiques suivants : $H^1(I_S) = 0$ et $H^1(K^\times) = 0$; ainsi en utilisant les isomorphismes $P_S = K^\times/E_S$ et $C_S = I_S/P_S$ on déduit les suites exactes longues de cohomologie associées :

$$0 \to E_S^\Gamma \to k^\times \to P_S^\Gamma \to H^1(E_S) \to 0 \tag{3.1}$$

$$0 \to H^1(P_S) \to H^2(E_S) \to H^2(K^\times) \to H^2(P_S) \to H^3(E_s) \to \cdots \tag{3.2}$$

$$0 \to P_S^\Gamma \to I_S^\Gamma \to C_S^\Gamma \to H^1(P_S) \to 0 \tag{3.3}$$

$$0 \to H^1(C_S) \to H^2(P_S) \to H^2(I_S) \to \cdots \tag{3.4}$$

où $\Gamma = Gal(K/k)$.
Si maintenant on note $P_{k,S}$ le groupe des S-idéaux principaux de k, la première suite exacte entraîne l'isomorphisme $H^1(E_S) \simeq P_S^\Gamma/P_{k,S}$ et la troisième devient :

$$0 \to H^1(E_S) \to I_S^\Gamma/P_{k,S} \to C_S^\Gamma \to H^1(P_S) \to 0.$$

Dans la suite exacte (2), on pose :

$$X = Im(H^2(E_S) \to H^2(K^\times))$$
$$Y = Im(H^2(K^\times) \to H^2(P_S)) = Ker(H^2(P_S) \to H^3(E_S))$$

de sorte que les suites :

$$0 \to H^1(P_S) \to H^2(E_S) \to X \to 0$$

et

$$0 \to X \to H^2(K^\times) \to Y$$

sont exactes. Via (4), on peut voir $H^1(C_S)$ comme un sous-groupe de $H^2(P_S)$ via :

$$H^1(C_S) = Ker(H^2(P_S) \to H^2(I_S)$$

et donc

$$0 \to Y \cap H^1(C_S) \to H^1(C_S) \to H^3(E_S)$$

est exacte. On pose alors :

$$\mathcal{B}_S = Ker(H^2(K) \to H^2(I_S))$$

où l'application est induite par : $\vartheta : K^\times \to I_S, \ \ \alpha \mapsto (\alpha)$.

[2] American Journal of Math. **105**, p 189-200, 1983 .

Proposition 3.1.2. *Il existe une suite exacte (dite des "classes ambiges") :*

$$0 \to H^1(E_S) \to I_S^\Gamma/P_{k,S} \to C_S^\Gamma \to H^2(E_S) \to \mathcal{B}_S \to H^1(C_S) \to H^3(E_S)$$

où $\mathcal{B}_S = Ker(H^2(K) \to H^2(I_S))$ *et* $\Gamma = Gal(K/k)$.

Après ces considérations générales, on se restreint au cas particulier où K est une $\mathbb{Z}_p$-extension d'un corps de nombres algébriques k. Dans toute la suite, on désigne par :

- S un ensemble de places finies de k,
- S_0 l'ensemble des places de k ramifiées dans K (qui est donc fini),
- $t(K/k) := t$ le nombre de places de S finiment décomposées dans K,
- $u(K/k) := u$, le nombre de places de k n'appartenant pas à S et ramifiées dans K.

Remarque : Dans le cas où S est vide, u désigne simplement le nombre de places de k ramifiées dans K). Par définition, on a donc l'isomorphisme : $\Gamma = Gal(K/k) \simeq \mathbb{Z}_p$ et le groupe Γ étant un pro-p-groupe libre, on a que pour tout $n \geq 3$, $H^n(\Gamma, A) = 0$ quel que soit A un Γ-module discret. En outre, dans le cas où A est un groupe abélien de torsion, $H^2(\Gamma, A) = 0$ et par conséquent pour tout Γ-module discret A, l'application $x \mapsto px$ induit un homomorphisme surjectif :

$$p : H^2(\Gamma, A) \twoheadrightarrow H^2(\Gamma, A)$$

Comme $H^3(E_S) = H^3(\Gamma, E_S) = 0$, la proposition précédente assure l'existence d'une suite exacte :

$$0 \to H^1(E_S) \to I_S^\Gamma/P_{k,S} \to C_S^\Gamma \to H^2(E_S) \to \mathcal{B}_S \to H^1(C_S) \to 0$$

Raffinement :

Ici $I_S^\Gamma/P_{k,S}$ et C_S^Γ peuvent être remplacés par respectivement $I_S^\Gamma/P_{k,S}(p)$ et $C_S^\Gamma(p) = C_S(p)^\Gamma$ leurs p-parties associées étant donné que tous les autres termes figurant dans la suite exacte sont des groupes abéliens p-primaires.

Si l'on note $\varphi_S : H^2(K/k, E_S) \to \mathcal{B}_S$, alors on a le lemme suivant :

Lemme 3.1.3. *Les assertions suivantes sont équivalentes :*

1. φ_S *est surjective*
2. $C_S(p)^\Gamma$ *est fini*
3. $H^1(K/k, C_S) = 0$

En outre, si φ_T *est surjective pour un certain sous-ensemble* T *de* S *alors* φ_S *est aussi surjective.*

Avec pour conséquence, la proposition :

Proposition 3.1.4. *Si l'on suppose que φ_S est surjective alors $Ker(\varphi_S)$ est fini et l'on a :*

$$H^1(K/k, E_S) \sim (\mathbb{Q}_p/\mathbb{Z}_p)^u$$
$$H^2(K/k, E_S) \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^{t+u-1}$$

Une question légitime alors revient à se demander si l'on sait exhiber des cas pour lesquels l'application φ_S est effectivement surjective car la condition (2) est suffisamment forte pour qu'à l'inverse l'on sache sans difficulté produire des exemples de $\mathbb{Z}_p$-entensions pour lesquelles $C_S(p)^\Gamma$ est infini. La réponse n'est donc pas simple et nécessite que l'on introduise une définition avant de se restreindre, compte tenu de la dernière assertion du lemme 2, au cas où $S_0 \subseteq S$:

Définition 3.1.5. *On dit que l'extension K/k est une $\mathbb{Z}_p$-extension de type* CM *(pour "Complex Multiplication") si k et K sont des corps de type CM.*

Malheureusement cette hypothèse n'est pas suffisamment contraignante pour assurer dans tous les cas la surjectivité de φ_{S_0} mais elle permet néammoins de produire certains exemples où les choses se passent bien...

Étant donné k un corps de nombres fixé, Iwasawa fait remarquer que la $\mathbb{Z}_p$-extension de k pour laquelle le nombre $u \geq 1$ de places ramifiées dans K est minimal (dans l'ensemble de la famille de toutes les $\mathbb{Z}_p$-extensions de k) vérifie $C_S(p)^\Gamma$ fini ; ainsi donc $\varphi := \varphi_\emptyset$ est surjective et l'on en déduit que tout corps de nombres K admet au moins une $\mathbb{Z}_p$-extension pour laquelle φ est surjective (en particulier, φ_S est surjective $\forall\ S$).
On suppose maintenant que k est un corps totalement réel et l'on désigne par k_∞ la $\mathbb{Z}_p$-extension cyclotomique associée *ie* le résultat du compositum $k\mathbb{Q}_\infty$ où $\mathbb{Q}_\infty$ désigne l'extension cyclotomique de $\mathbb{Q}$. La Conjecture de Leopoldt (si elle est satisfaite), assure que sous ces hypothèses, k_∞ est l'unique $\mathbb{Z}_p$-extension de k pour p fixé. On déduit alors de ce qui précède que, $\forall\ S$, φ_S est surjective et qu'en particulier, on a (voir proposition 3) :

$$\begin{aligned} H^1(k_\infty/k, E) &\sim (\mathbb{Q}_p/\mathbb{Z}_p)^u \\ H^2(k_\infty/k, E) &\simeq (\mathbb{Q}_p/\mathbb{Z}_p)^{u-1} \end{aligned}$$

où $E := E_\emptyset$.

L'étape ultime consiste à supposer que K/k est une $\mathbb{Z}_p$-extension de type CM à laquelle on associe K^+/k^+ sa $\mathbb{Z}_p$-extension de sous-corps réels maximaux. Si S est supposé invariant sous l'action de la conjugaison complexe τ, alors φ_S induit deux applications selon :

$$\varphi_S^+ : H^2(K/k, E_S)^+ \to \mathcal{B}_S^+$$

$$\varphi_S^- : H^2(K/k, E_S)^- \to \mathcal{B}_S^-$$

selon que la conjugaison complexe agit via $+/-1$. En particulier, pour p un nombre premier impair, on a : $\varphi_S = \varphi_S^+ \oplus \varphi_S^-$ où φ_S^+ n'est rien d'autre que l'application originelle restreinte au cas totalement réel K^+/k^+ traité plus haut. D'autre part, le fait que φ_S^- soit surjective pour $S = S_0$ puis pour tous les ensembles S tels que $S_0 \subseteq S$ n'est autre que *la conjecture de Gross* exposée dans [22] et vérifiée dans le cas où $k/\mathbb{Q}$ est abélienne...

C'est enfin en soulignant (avec les notations d'Iwasawa) la similitude du comportement de X_∞^- pour les corps de nombres et X_∞ pour les corps de fonctions que Gold et Kisilevsky dans l'article déjà cité : *On Geometric $\mathbb{Z}_p$ Extensions of Function Fields* viennent accréditer la formulation du problème soulevé par Villa et Madan.

Remarque : Comme dans le cas particulier où $k/\mathbb{Q}$ est supposée abélienne la conjecture de Leopoldt est aussi démontrée, on en déduit que $\forall\ p > 2$ et sous ces hypothèses de commutativité pour $Gal(k/\mathbb{Q})$ l'application φ_S est surjective pour tout S contenant S_0.

3.2 L'article de Villa-Madan

Soit L/K une extension cyclique de corps de fonctions de corps des constantes k supposé fini[3] (on parle parfois de "congruence function field"). On désigne par S un ensemble fini de place de K et on s'autorisera l'abus de langage qui consiste à conserver cette notation pour désigner les places de L au-dessus de S. On rappelle que lors de notre aparté sur la S-ramification, on avait mis en évidence l'existence de deux suites exactes :

$$1 \to E_S \hookrightarrow L^\times \twoheadrightarrow P_S \to 1$$

$$1 \to P_S \hookrightarrow \mathcal{D}_S \twoheadrightarrow \mathcal{C}_S \to 1 \quad (a)$$

où :

- E_S désigne le groupe des S-unités de L
- P_S le sous-groupe des diviseurs principaux de L
- $\mathcal{D}_S$ le groupe des S-diviseurs du corps L
- $\mathcal{C}_S = \mathcal{C}_{L,S}$ le groupe des S-classes de diviseurs de L

A la suite exacte courte (a), on associe selon le procédé usuel la suite exacte longue de cohomologie :

$$1 \to H^0(P_S) \hookrightarrow H^0(\mathcal{D}_S) \to H^0(\mathcal{C}_S) \to H^1(P_S) \to H^1(\mathcal{D}_S) \to H^1(\mathcal{C}_S) \to \cdots$$

où $H^i(A)$ désigne le i-ème groupe de cohomologie (au sens de Tate) $H^i(G, A)$ avec $G = Gal(L/K)$ cyclique et A un G-module. Les propriétés et définitions

[3] Manuscripta Math. **61**, p 327-345 (1988)

des premiers groupes de cohomologie permettent de re-écrire la suite exacte longue ci-dessus sous la forme :

$$1 \to P_S^G \hookrightarrow \mathcal{D}_S^G \to \mathcal{C}_S^G \to H^1(P_S) \to 1 \to H^1(\mathcal{C}_S) \to \cdots$$

On déduit de ce qui précède le triplet de suites exactes suivantes dont on va pouvoir tirer quelques informations :

$$1 \to \frac{\mathcal{D}_S^G}{P_S^G} \hookrightarrow \mathcal{C}_S^G \twoheadrightarrow H^1(P_S) \to 1$$

$$E_S^G = E_{K,S} \to (L^\times)^G = K^\times \hookrightarrow P_S^G \to H^1(E_S) \to 1$$

car en vertu du théorème 90 de Hilbert [4] $H^1(L^\times) = 0$

$$1 \to H^1(P_S) \hookrightarrow H^2(E_S) \xrightarrow{\phi} H^2(L^\times)$$

Comme l'on travaille dans le contexte cyclique très favorable cohomologiquement parlant, on dispose des isomorphismes :

$$H^2(E_S) \simeq H^0(E_S) = \frac{E_S^G}{\mathrm{N}_{L/K}(E_S)}$$

et

$$H^2(L^\times) \simeq H^0(L^\times) = \frac{(L^\times)^G}{\mathrm{N}_{L/K}(L^\times)} = \frac{K^\times}{\mathrm{N}_{L/K}(L^\times)}$$

comme conséquence de la théorie du corps de classes. De ceci, l'on déduit :

$$H^1(P_S) \simeq Ker(\phi) \simeq \frac{E_S^G \cap N_{L/K}(L^\times)}{N_{L/K}(E_S)}$$

L'interprétation en terme de cardinaux de la suite exacte

$$1 \to P_S^G \hookrightarrow \mathcal{D}_S^G \to \mathcal{C}_S^G \to H^1(P_S) \to 1$$

donne la relation : $|\mathcal{C}_{L,S}^G| = |C_S^G| = |H^1(P_S)|.(I_S^G : P_S^G)$; et finalement :

$$|\mathcal{C}_{L,S}^G| = \frac{(E_S^G \cap N_{L/K}(L^\times) : N_{L/K}(E_S)).(\mathcal{D}_S^G : \mathcal{D}_{K,S}).(\mathcal{D}_{K,S} : P_{K,S})}{(P_S^G : P_{K,S})}$$

où l'on rappelle par exemple que l'indice $(\mathcal{D}_S^G : \mathcal{D}_{K,S})$ désigne le cardinal du groupe-quotient $\dfrac{\mathcal{D}_S^G}{\mathcal{D}_{K,S}}$. Enfin, on déduit de :

$$\begin{array}{ccccccccc} E_{K,S} & \longrightarrow & K^\times & \xrightarrow{\tau} & P_S^G & \xrightarrow{\delta} & H^1(E_S) & \longrightarrow & 1 \\ & & & & \downarrow & \nearrow_{\sim} & & & \\ & & & & P_S^G/Ker(\delta) & & & & \end{array}$$

[4] Ce résultat est en fait dû à E. Noether (1882 – 1935) ; il s'agit d'une généralisation du "Satz 90" extrait du livre de Hilbert (1862 – 1943) : Die Theorie der algebraischen Zahlkörper.

l'égalité : $(P_S^G : P_{K,S}) = |H^1(E_S)|$ via $Ker\ \delta = \text{Im}\ \tau$.

En rassemblant chacune des étapes précédentes, on obtient "la" *formule des classes ambiges* dans le cas des extensions cycliques de corps de fonctions, à savoir :

$$|\mathcal{C}_{L,S}^G| = \frac{|\mathcal{C}_{K,S}|.e.\varphi(E_S)}{(E_S^G : E_S^G \cap N_{L/K}L^\times)}$$

où $\varphi(E_S)$ désigne le quotient de Herbrand associé à E_S *ie* $\varphi(E_S) = \dfrac{\sharp H^0(E_S)}{\sharp H^1(E_S)}$ et $(\mathcal{D}_S^G : \mathcal{D}_{K,S}) = \text{e} = \prod_{i=1}^r e_i$ où e_i désigne l'indice de ramification associé à une place de K non-incluse dans S et qui se ramifie dans L (en particulier, $e_i > 1$).

Remarque à propos de l'entier $e = \prod_{i=1}^r e_i$:

Étant donnée une extension galoisienne L/K de corps de fonctions (nécessairement géométrique), on dispose, si $\{P_1, P_2, \cdots, P_t\}$ désignent les premiers de K qui se ramifient dans L d'indice de ramification respectif e_i, $1 \leq i \leq t$ d'une suite exacte :

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathcal{C}_K & \xrightarrow{\theta} & \mathcal{D}_L^G/P_K & \xrightarrow{\varphi} & \sum \dfrac{\mathbb{Z}}{\mathbb{Z}e_i} & \longrightarrow & 0 \\ & & & & \downarrow & \nearrow_{\sim} & & & \\ & & & & \dfrac{\mathcal{D}_L^G/P_K}{Ker\varphi} & & & & \end{array}$$

avec $Ker\varphi = Im\theta = \mathcal{D}_K/P_K$.

De la définition de $\mathcal{C}_K = \mathcal{D}_K/P_K$, on déduit que prouver cette dernière revient à justifier l'isomorphisme $\mathcal{D}_L^G/\mathcal{D}_K \simeq \sum_i e_i\mathbb{Z}$. Soit donc $\mathfrak{p}$ un premier de K. L'extension L/K étant supposée galoisienne, toutes les places $\mathfrak{P}$ au-dessus de $\mathfrak{p}$ sont affectées du même indice de ramification par conséquent sa décomposition dans L est de la forme : $\mathfrak{p} = (\mathfrak{P}_1\mathfrak{P}_2\cdots\mathfrak{P}_g)^e = \Phi(\mathfrak{p})^{\mathfrak{e}}$. On vérifie alors immédiatement que les diviseurs constituent un système libre de générateurs pour $\mathcal{D}_L^G$ d'où le résultat.

La prochaine étape consiste à traduire ces résultats dans le cas où l'on ne considère plus seulement une extension cyclique L/K mais une *tour* d'extensions cycliques ...

Contexte :
- Soit k un corps fini de caractéristique $p > 0$
- $K = K_0$ un corps de fonctions algébriques d'une variable de corps des constantes k
- K_n/K_0 une extension cyclique de degré p^n supposée géométrique de groupe de Galois G_n
- Enfin, on note T_0 un ensemble fini de places de K_0 et T_n les places de K_n au-dessus de T_0. On suppose en outre que T_0 contient au moins une place totalement ramifiée $\mathcal{Q}$.

Soit E_{n,T_n} le groupe des T_n-unités dans K_n. En transportant au rang n, la formule des classes ambiges établie plus haut devient :

$$|\mathcal{C}_{K_n,T_n}^{G_n}| = \frac{|\mathcal{C}_{K_0,T_0}|.e_{(n)}.\varphi(E_{K_n,T_n})}{(E_{K_0,T_0} : E_{K_0,T_0} \cap N_{n,0}(K_n^\times))}$$

où $e_{(n)} = (\mathcal{D}_{K_n,T_n}^{G_n} : \mathcal{D}_{K_0,T_0})$ et $G_n := Gal(K_n/K_0) \simeq \dfrac{\mathbb{Z}}{p^n\mathbb{Z}}$

Suivant la même argumentation qui prévaut dans le cas des corps de nombres, on établit que le quotient de Herbrand relatif aux T_n-unités du corps K_n/K est égal à :

$$\varphi(E_{K_n,T_n}) = \prod_{\mathfrak{P}\in T_0-\mathcal{Q}} e_{\mathfrak{P}} f_{\mathfrak{P}} = p^{n(v-1)}. \prod_{\mathfrak{P}\in T_0'} f_{\mathfrak{P}}$$

où :
- T_0' désigne l'ensemble des places de T_0 non-ramifiées ,
- v le nombre de premiers dans T_0 qui se ramifient dans K_n.

En remplaçant dans l'expression précédente, on obtient une formule des classes ambiges au rang n selon :

$$|\mathcal{C}_{K_n,T_n}^{G_n}| = \frac{|\mathcal{C}_{K_0,T_0}|.\prod_{\mathfrak{P}\in T_0'} f_{\mathfrak{P}}.e_{(n)}.p^{n(v-1)}}{(E_{K_0,T_0} : E_{K_0,T_0} \cap N_{n,0}(K_n^\times))}$$

Dans le but d'obtenir quelques simplications, on suppose dorénavant que $T_0 = S$, l'ensemble des premiers ramifiés ainsi pour tout n : $S = T_0 = T_n$, $|S| = s = v$ et $e_{(n)} = 1$; on obtient alors la relation :

$$|\mathcal{C}_{K_n,T_n}^{G_n}| \sim \frac{p^{n(s-1)}}{(E_{K_0,T_0} : E_{K_0,T_0} \cap N_{n,0}(K_n^\times))}.$$

On rappelle qu'étant données deux suites numériques $\{B_n\}$ et $\{C_n\}$, $B_n \sim C_n$ signifie que $\lim_{n\to\infty} \dfrac{|B_n|}{|C_n|} = d$, où d est un réel strictement positif. On a alors la proposition suivante :

Proposition 3.2.1. *On considère K_∞/K_0 une $\mathbb{Z}_p$-extension géométrique et l'on désigne comme précédemment par K_n le n-ième étage de la tour associée. On a alors :*

1. $E_{n,S} = E_{0,S}$ *pour tout* n.
2. $E_{n,S} \simeq k^\times.\mathbb{Z}^{s-1}\ \forall\ n \in \mathbb{N}$

Idée de la preuve :

1. On est ramené à montrer l'inclusion $E^S_{K_n} \subseteq E^S_{K_0}$. Soit η un élément de $E_{n,S}$. Si les places de S ne sont pas décomposées dans K_n/K_0, le diviseur (η) associé est ambige (*ie* fixé par le groupe de Galois cyclique $G_n := Gal(K_n/K_0) =< \sigma >$); ainsi $\eta^{1-\sigma}$ est une unité de K_n et par conséquent un élément γ de $k^\times$. Il suit que $\gamma^{p^n} = \gamma^{[K_n:K_0]} = N_{K_n/K_0}(\gamma) = N_{K_n/K_0}(\eta^{1-\sigma}) = 1$; par conséquent, $\gamma = 1$ i.e. $\eta \in K_0$ d'où l'égalité.
2. On applique le point précédent et le théorème de structure des S-unités de Dirichlet dans un corps global.

On déduit de la proposition précédente les égalités suivantes :

$$N_{K_n/K_0}(E_{n,S}) \overset{(1)}{=} N_{K_n/K_0}(E_{0,S}) = E^{p^n}_{0,S}$$

et

$$(E_{0,S} : N_{K_n/K_0}(E_{n,S})) = p^{n(s-1)}$$

ainsi donc, la formule des classes ambiges "au rang n" devient :

$$\begin{aligned} |\mathcal{C}^{G_n}_{K_n,S}| &\sim \frac{(E_{0,S} : N_{K_n/K_0}(E_{n,S}))}{(E_{0,S} : E_{0,S} \cap N_{K_n/K_0}(K_n^\times))} \\ &= (E_{0,S} \cap N_{K_n/K_0}(K_n^\times) : N_{K_n/K_0}(E_{n,S})), \end{aligned}$$

égalité qui reste valide lorsque l'on remplace $\mathcal{C}_{K_n,S}$ par sa p-partie que l'on notera $\mathcal{C}_{K_n,S}(p)$.

L'*injectivité*[5] de l'application $\vartheta : \mathcal{C}_{K_n,S}(p) \hookrightarrow \mathcal{C}_{K_{n+1},S}(p)$, nous permet de considérer la limite inductive de ces p-groupes via

$$\mathcal{C}_{K_\infty,S}(p)^\Gamma := \cup_n \mathcal{C}_{K_n,S}(p)^{G_n}$$

ainsi donc, la finitude de $\mathcal{C}_{K_\infty,S}(p)^\Gamma$ est équivalente à l'assertion :

$$(E_{0,S} \cap N_{K_n/K_0}(K_n^\times) : N_{K_n/K_0}(E_{n,S})) \sim 1$$

ce qui signifie en d'autres termes que cette suite d'indices reste bornée $\forall\ n$ (ou encore $(E_{0,S} : E_{0,S} \cap N_{K_n/K_0}(K_n^\times)) \sim p^{n(s-1)}$). On énonce :

[5] On revient plus longuement sur cette propriété p 133 de ce mémoire

Proposition 3.2.2. *Soit K_∞/K_0 une $\mathbb{Z}_p$-extension de corps satisfaisant aux hypothèses précédentes, alors les assertions suivantes sont équivalentes :*

1. $\mathcal{C}_{K_\infty,S}(p)^\Gamma$ *est fini.*
2. $(E_{0,S} : E_{0,S} \cap N_{K_n/K_0}(K_n^\times)) \sim p^{n(s-1)}$
3. $(E_{0,S} \cap N_{K_n/K_0}(K_n^\times) : N_{K_n/K_0}(E_{n,S})) \sim 1$

Dans la suite des investigations, c'est via la formulation (2) que l'on tâchera d'atteindre l'analogue de la conjecture de Gross ... Comme cela a été très brièvement suggéré dans l'introduction, on cherche à associer à la $\mathbb{Z}_p$-extension géométrique K_∞/K_0 une matrice carrée $\mathcal{M}$ d'ordre $|S|-1$ (une sorte de matrice-régulateur) dont le caractère inversible garantira la véracité de l'énoncé de la Conj.G. considéré. Pour ce faire, on utilise la tour d'extensions finies sous-jacente et l'on se propose d'associer à chaque étage fini n (i.e. à chaque extension K_n/K de degré p^n) une matrice carrée $\mathcal{M}_n$ d'ordre $|S|-1$ que l'on veut inversible. La suite $(\mathcal{M}_n)_n$ ainsi construite, il restera à s'assurer qu'elle est de Cauchy dans un espace de matrices approprié et à définir comment le caractère inversible "passe à la limite"... Utiliser les étages finis de la tour c'est-à-dire les K_n de degré p^n sur K_0, cela signifie en particulier exploiter la manière dont en caractéristique p elles sont générées, c'est donc dans cette phase que la théorie d'Artin-Schreier-Witt, dont les grandes lignes ont été exposées précédemment, va prendre toute son importance.
On se place dorénavant dans le contexte suivant :

- On désigne par $S = \{P_1, P_2, \cdots, P_t\}$ l'ensemble des places de $K_0 := K$ qui se ramifient dans la $\mathbb{Z}_p$-extension K_∞/K. En particulier, $|S| = t$.
- $\forall n \geq 0$, $E_{n,S} = E_{0,S}$ où $E_{n,S} \simeq k^\times . \mathbb{Z}^{t-1}$
- Grâce à une proposition précédente, on dispose de l'équivalence :

$$\mathcal{C}_{K_\infty,S}(p)^\Gamma \text{fini (i.e. Conj. Gross satisfaite)} \Leftrightarrow (E_{0,S} : E_{0,S} \cap N_{K_n/K_0}(K_n^\times)) \sim p^{n(s-1)}$$

S'intéresser au comportement de l'indice $(E_{0,S} : E_{0,S} \cap N_{K_n/K_0}(K_n^\times))$, c'est en particulier se concentrer sur les éléments de K_0 (qui seront des S-unités de ce corps) qui peuvent être représentés comme la norme d'un élément de K_n. Or en vertu du Principe de Hasse, on a que α est une norme dans K_n/K_0 si et seulement s'il s'agit d'une norme de l'extension locale $K_{n,\mathfrak{p}}/K_{0,\mathfrak{p}}$ associée et ce, pour toute place $\mathfrak{p}$ de K_0 (pour ne pas alourdir les notations, on a noté $\mathfrak{p}$ la place de K_n au-dessus de $\mathfrak{p}$).
Comme sous nos hypothèses, l'ensemble S est exactement constitué des premiers ramifiés et qu'en vertu de la théorie du corps de classes toutes les unités sont des normes dans une extension locale non-ramifiée, il suit qu'*une S-unité est une norme globale si et seulement s'il s'agit d'une norme locale*

où les localisés sont pris en toutes les places de S. On rappelle à ce propos qu'étant donnés P un polynôme irréductible sur $\mathcal{O}_{K_0}[T]$ de degré d et $\mathfrak{p}$ la place associée, on a l'isomorphisme $K_{0,\mathfrak{p}} \simeq \mathbb{F}_{q^d}((T))$ où $K_{0,}$ désigne le complété de K_0 en $\mathfrak{p}$. On dispose en outre d'un plongement naturel :

$$i_{\mathfrak{p}} : K_0 \hookrightarrow K_{0,\mathfrak{p}}$$

auquel nous ferons implicitement référence par la suite. Le critère normique de Witt dont le principe a été rappelé au cours du premier chapitre va donc faire office d'outil préférentiel pour résoudre ce problème.
Soient L/K une extension cyclique *de corps locaux* telle que $[L : K] = p^n$ paramétrée par le vecteur de Witt de longueur n : $(\beta_0, \beta_1, \cdots, \beta_{n-1})$ et α un élément non nul de K_0. On rappelle que la classification de ces derniers entraine que K est isomorphe à un corps de séries de Laurent $k'((T))$ où k' un corps fini. On désigne par F l'unique extension non-ramifiée de $\mathbb{Q}_p$ telle que $\mathcal{O}_F/M_F \simeq k'$ où $\mathcal{O}_F$ désigne l'anneau des entiers local associé à F et M_F son idéal maximal. On choisit $A, B_0, B_1, \cdots, B_i, \cdots, B_{n-1}$ dans $\mathcal{O}_F((T))$ tels que soit satisfait le système de congruences suivant pour $0 \leq i \leq n-1$:[6]

$$A \equiv \alpha[M_F]$$

$$B_i \equiv \beta_i[M_F]$$

On introduit alors l'invariant déjà rencontré :

$$\mathrm{Res}(\frac{dA}{A}).(\frac{B_0^{pn}}{p^n} + \cdots + \frac{B_{n-1}}{p}) = \gamma$$

où $\frac{dA}{A}$ désigne la dérivée logarithmique $\frac{d}{dT}(\ln A(T))$ et si l'on note "Tr" la trace de F sur $\mathbb{Q}_p =$ Frac$(\mathbb{Z}_p)$, on a alors :
$\mathrm{Tr}(\gamma) = \frac{m}{p^n} = b + \frac{a}{p^n}$ avec $a \in \mathbb{Z}, 0 \leq a < p^n$, $a \in \mathbb{Z}_p$. En particulier, $\mathrm{Tr}(\gamma) \bmod 1 = \frac{a}{p^n}$ et le critère normique de Witt donne :

$$\alpha \text{ est une norme dans L} \Leftrightarrow \mathrm{Tr}(\gamma) \equiv 0 \bmod 1.$$

Remarque technique : Sans vouloir entrer plus avant dans les détails, l'utilisation du théorème de Grunwald-Hasse-Wang affirme qu'il existe une extension normale $E/\mathbb{Q}$ telle que $Gal(E/\mathbb{Q}) \simeq Gal(F/\mathbb{Q}_p)$. L'inclusion $\mathcal{O}_E \subset \mathcal{O}_F$ qui en résulte nous permet de supposer que la suite d'éléments
$A, B_0, B_1, \cdots, B_i, \cdots, B_{n-1} \in \mathcal{O}_E((T))$.
En particulier, $p^n \mathrm{Tr}(\gamma) \in \mathbb{Z}_p \cap \mathbb{Q} = \mathbb{Z}_{(p)}$ où $\mathbb{Z}_{(p)}$ désigne le localisé de $\mathbb{Z}$ en l'idéal premier $p\mathbb{Z}$.

[6] Cette manipulation permet de passer de la caractéristique p>0 à la caractéristique nulle.

Étant donné $S = \{P_1, P_2, \cdots, P_t\}$ les premiers ramifiés dans K_∞/K_0, Villa et Madan considèrent les entiers non-nuls a_i, b_i et h_i tels que $(\frac{P_i^{a_i}}{P_t^{b_i}})$ soit de degré nul (on rappelle que l'ensemble des diviseurs principaux forme un sous-groupe du groupe des diviseurs de degré nul) et $(\frac{P_i^{a_i}}{P_t^{b_i}})^{h_i} = (\delta_i)$ soit un diviseur principal dans K_0. Dans la perspective d'utilisation du critère de Witt, on effectue un transfert de la caractéristique $p > 0$ à la caractéristique nulle selon :

$$\delta_j \hookrightarrow \gamma_{j,i} \rightsquigarrow \pi_{j,i}$$

$$\beta_0 \hookrightarrow \beta_{n,0} \rightsquigarrow B_{n,0}$$

On définit alors :

$$a_{j,i}^{(n,m)} = \text{Tr Res}[(\frac{d\pi_{j,i}}{d\pi_{i,j}}.\frac{1}{\pi_{j,i}}).B_{n,i}^{p^m}.d\pi_{i,j}] \ \in \ \mathbb{Z}_{(p)}$$

pour $1 \leq i, j \leq t-1$ tel que $a_{j,i}^{(n,m)} \equiv a_{j,i}^{(n,k)} \bmod p^{m+1} \ \forall \ k \geq m$.

Soit maintenant $\alpha = \delta_1^{\varepsilon_1}.\cdots.\delta_i^{\varepsilon_i}.\cdots.\delta_{t-1}^{\varepsilon_{t-1}}$ une S-unité appartenant au sous-groupe engendré par les $\{\delta_i\}_{1\leq i\leq t-1}$ (d'indice fini dans celui des S-unités) que l'on relève en caractéristique 0 selon le procédé évoqué précédemment en $A_i = \pi_{1,i}^{\varepsilon_1}.\cdots.\pi_{t-1,i}^{\varepsilon_{t-1}}$. De $(\star)$, on déduit :

$$\text{Tr Res}(\frac{dA_i}{A_i}).(\sum_{s=0}^{n-1}\frac{B_{s,i}^{p^{n-1-s}}}{p^{n-s}}) = \sum_{j=0}^{t-1}(\frac{1}{p^n}\varepsilon_j c_{j,i}^{(n)})$$

où $c_{j,i}^{(n)} = \sum_{s=0}^{n-1} p^s a_{j,i}^{(s,n-1-s)}$ pour $n \geq 1$ et vérifie la relation de congruence $c_{j,i}^{(n+1)} \equiv c_{j,i}^{(n)} + p^n a_{j,i}^{(n,0)} \bmod p^n$.

En utilisant le principe de Hasse, α étant une S-unité, on a que :

α est *une norme globale* dans K_n/K_0 *si et seulement si* α est une norme locale en chacun des $P_i \quad \forall\ 1 \leq i \leq t-1$ i.e., par utilisation du critère de Witt,

$$\Leftrightarrow \sum_{j=0}^{t-1}(\varepsilon_j c_{j,i}^{n}) \equiv 0\ [p^n]$$

pour $1 \leq i \leq t-1$.

C'est ici que la matrice $\mathcal{M}_n$ associée au n-ième étage de la tour K_n/K apparaît car l'on peut interpréter la relation $\sum_{j=0}^{t-1}\varepsilon_j c_{j,i}^{(n)}$ comme le i-ème terme

a_i résultant du produit matriciel de $\mathcal{M}_n$ avec le vecteur colonne $(\varepsilon_i)_{1\leq i\leq t-1}$ si :

$$\mathcal{M}_n = \begin{pmatrix} c_{1,1}^{(n)} & c_{2,1}^{(n)} & \cdots & c_{t-1,1}^{(n)} \\ c_{1,2}^{(n)} & c_{2,2}^{(n)} & \cdots & c_{t-1,2}^{(n)} \\ \vdots & \vdots & \ddots & \vdots \\ c_{1,t-1}^{(n)} & c_{2,t-1}^{(n)} & \cdots & c_{t-1,t-1}^{(n)} \end{pmatrix}$$

Lemme 3.2.3. *La suite $\{\mathcal{M}_n\}_{n\geq 1}$ est une suite de Cauchy dans $M_{t-1}(\mathbb{Z}_p)$.*

Idée de la preuve : On vérifie que les matrices $\mathcal{M}_n$ et $\mathcal{M}_{n+1}$ sont liées par la relation $\mathcal{M}_{n+1} = \mathcal{M}_n + p^n\mathcal{D}_n$ où $\mathcal{D}_n$ est une matrice à coefficients dans $\mathbb{Z}_{(p)}$.

En particulier, $\mathbb{Z}_p$ étant complet, la suite $\{\mathcal{M}_n\}_{n\geq 1}$ converge et l'on note $\mathcal{M}$ sa limite.

Quelques Remarques :

1. On suppose que la matrice $\mathcal{M} = \lim_n(\mathcal{M}_n)$ est de rang $t-1$. Ceci signifie qu'il existe un entier N tel que $\forall\, n \geq N$, $\text{rang}(\mathcal{M}_n) = t-1$, ce qui revient à dire que $\det(\mathcal{M}_n) \neq 0$.
2. Étant donné un nombre premier p on désigne par v_p la valuation p-adique associée. Pour toute suite $(b_n)_n$ d'éléments de $\mathbb{Q}_p$ telle que $\lim_{n\to\infty}(b_n) = b_0$ on a $\lim_{\,n\to\infty}(v_p(b_n)) = v_p(b_0)$. En particulier,

$$\begin{aligned} \lim_{n\to\infty}(v_p(\det \mathcal{M}_n)) &= v_p(\det \mathcal{M}) \\ &= a \in \mathbb{Z} \end{aligned}$$

   et d'après la remarque (1) on en déduit l'existence d'un N tel que $\forall n \geq N, v_p(\det\mathcal{M}_n) = a$.
3. Maintenant si $X = (x_1, x_2, \cdots, x_{t-1}) \in \mathbb{Q}_p^{t-1}$, on définit la quantité $\| X \|_p = \max_{1\leq i\leq t-1}(|x_i|_p)$ ou de manière équivalente $v_p(X) := \min_{1\leq i\leq t-1}(v_p(x_i)$ et l'on vérifie que $\| \, . \, \|_p$ est une norme satisfaisant $\| X + Y \|_p \leq \text{Max}\{\| X \|_p, \| Y \|_p\}$.

Conséquence : Si $E = (e_{i,j})$ est une matrice à coefficients dans $\mathbb{Q}_p$ i.e. $E \in M_{t-1}(\mathbb{Q}_p)$, on pose :

$$\| E \|_p = \text{Max}\{|e_{i,j}|\} \Leftrightarrow v_p(E) = \min_{i,j}\{v_p(e_{i,j})\}.$$

De ceci, on déduit qu'étant données deux matrices E et D, on a le système d'inégalités :

$$\| E.D \|_p \leq \| E \|_p \, . \, \| D \|_p$$

$$\Leftrightarrow v_p(E.D) \geq v_p(E) + v_p(D).$$

En particulier, *si E est inversible* on obtient :

$$0 = v_p(E.E^{-1}) \ \geq \ v_p(E) + v_p(E^{-1}) \ \text{ ie } \ v_p(E^{-1}) \leq \ -v_p(E).$$

Ces quelques remarques appliquées au contexte de l'article de Villa-Madan conduisent à l'interprétation suivante :

$$a = v_p(\det\mathcal{M}_n) = \ v_p(\sum_{\sigma\in S_{t-1}} (-1)^{sgn\sigma} \prod c^{(n)}_{i,\sigma(i)}) \geq \min\{v_p(c^{(n)}_{i,j})\}$$

entraîne $v_p(e^{(n)}_{i,j}) \leq a$ pour un couple d'indices (i,j) et par conséquent $v_p(\mathcal{M}_n) \leq a$. En outre, $v_p(\mathcal{M}_n^{-1}) \leq -v_p(\mathcal{M}_n)$ et l'on vérifie que l'on a :

$$-v_p(\det\mathcal{M}_n) = -a \leq v_p(\mathcal{M}_n^{-1}) \leq -v_p(\mathcal{M}_n)$$

D'autre part, on dispose de la relation matricielle :

$$\mathcal{M}_n^{-1} = (\det \mathcal{M}_n)^{-1}.\Theta$$

où $\Theta := (\xi^n_{i,j})_{i,j} \in M_{(t-1,t-1)}(\mathbb{Q}_p)$ est la co-matrice associée à $\mathcal{M}_n$. On note $\mathcal{M}_n^{-1} = (b_{i,j})_{1\leq i,j\leq t-1}$.

Puisque $\mathcal{M}_n \in M_{(t-1,t-1)}(\mathbb{Z}_p)$, on a que $\xi^{(n)}_{i,j} \in \ \mathbb{Z}_p$ et par conséquent, $v_p(\xi^{(n)}_{i,j}) \geq 0$ d'où :

$$v_p(b_{i,j}) = v_p((\det\mathcal{M}_n)^{-1}.\xi^{(n)}_{i,j}) = -v_p(\det\mathcal{M}_n) + v_p(\xi^{(n)}_{i,j}) \geq -a + 0 \geq -a$$

Ainsi, $v_p(\mathcal{M}_n^{-1}) = \min_{i,j}\{v_p(b_{i,j})\} \geq -a$ ie $-v_p(\det\mathcal{M}_n) = -a \leq v_p(\mathcal{M}_n^{-1}) \leq v_p(\mathcal{M}_n)$.

On en vient au lemme suivant :

Lemme 3.2.4. *Si l'on note $\mathcal{M} = lim_n\mathcal{M}_n$, alors on a l'équivalence :*

$$\mathcal{M}.(\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_{t-1})^T = 0 \Leftrightarrow \alpha = \delta_1^{\varepsilon_1} \cdots \delta_i^{\varepsilon_i} \cdots \delta_{t-1}^{\varepsilon_{t-1}} \in \bigcap_{n\geq 0} N_{n,0}K_n$$

où $(\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_{t-1})^T$ désigne le vecteur colonne associé.

Preuve :
($\Leftarrow$) : On suppose $\alpha \in \bigcap_{n\geq 0} \ N_{n,0}K_n$, ce qui signifie que $\alpha \in N_{n,0}K_n$ pour tout n, ainsi donc on a par le critère de Witt que $\forall\, n, \mathcal{M}_n.(\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_{t-1})^T \equiv 0\ [p^n]$ ou encore que $\mathcal{M}.(\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_{t-1})^T = \lim_n \mathcal{M}_n.(\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_{t-1})^T = 0$

d'où le résultat.
($\Rightarrow$) Réciproquement, si $\mathcal{M}.(\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_{t-1})^T = 0$ alors,

$$\lim_n \mathcal{M}_n.(\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_{t-1})^T = 0$$

et l'on a le système de congruences :

$$\sum_{j=0}^{t-1} \varepsilon_j c_{i,j}^{(n+1)} \equiv 0 \bmod p^{m_n}$$

pour $1 \leq i \leq t-1$ où m_n désigne l'exposant minimal pour lequel, $\forall i$ convenable, ce système est satisfait. On a alors $\lim_n(m_n) = \infty$. On affirme que l'on peut montrer que pour tout n, $m_n \geq n$; en effet, raisonnons par l'absurde en supposant qu'il existe un entier naturel n pour lequel $m_n < n$. De la relation $\mathcal{M}_{n+1} = \mathcal{M}_n + p^n D_n$ évoquée précédemment, on déduit que pour tout $i = 1, 2, \cdots, t-1$:

$$\sum_{j=0}^{t-1} \varepsilon_j c_{j,i}^{(n+1)}) = \sum_{j=0}^{t-1} \varepsilon_j c_{j,i}^{(n)} + p^n \sum_{j=0}^{t-1} \varepsilon_j d_{j,i}^{(n)}.$$

En particulier, étant donné i fixé, on a :

$$v_p(\sum_{j=0}^{t-1} \varepsilon_j c_{j,i}^{(n}) = m_n < n \leq v_p(\sum_{j=0}^{t-1} \varepsilon_j d_{j,i}^{(n)})$$

et par conséquent, $v_p(\sum_{j=0}^{t-1} \varepsilon_j c_{j,i}^{(n+1)}) = m_n$.
Il suit que $v_p(\sum_{j=0}^{t-1} \varepsilon_j c_{j,i}^{(k)}) = m_n \ \forall k \geq n$ et l'on aurait alors que :
$\lim_n \mathcal{M}_n.(\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_{t-1})^T \neq 0$, ce qui conduit à une contradiction. Ainsi, $\forall n, m_n \geq n$ et par le critère de Witt, $\alpha = \delta_1^{\varepsilon^1} \cdots \delta_i^{\varepsilon^i} \cdots \delta_{t-1}^{\varepsilon_{t-1}}$ est une norme quel que soit n.

Cet aparté un peu technique et finalement assez rébarbatif va néammoins nous permettre de démontrer la proposition suivante qui constitue le résultat essentiel de l'article.

Proposition 3.2.5. *Soit $\mathcal{M} \in M_{t-1}(\mathbb{Z}_p)$ la matrice décrite ci-dessus ; on a alors l'implication suivante :*
$\mathcal{M}$ inversible $\Rightarrow$ *la $\mathbb{Z}_p$-extension associée K_∞/K satisfait la Conjecture de Gross (au sens précédent).*

Preuve :
(*Prémiminaire : on rappelle que dire que $\mathcal{M} := lim_n\ \mathcal{M}_n$ est inversible signifie qu'il existe $N \in \mathbb{N}$ tel que $\forall n \geq N$, $\mathcal{M}_n$ soit inversible.*)

Soit donc $\alpha = \delta_1^{\varepsilon_1}.\cdots.\delta_i^{\varepsilon_i}.\cdots.\delta_{t-1}^{\varepsilon_{t-1}}$ une norme dans K_n ; d'après le critère de Witt, on dispose de la relation de congruence :

$$\mathcal{M}_n.(\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_{t-1})^T = (\rho_1, \rho_2, \cdots, \rho_{t-1})^T \equiv\ 0\ [p^n].$$

De ceci et conformément à la remarque préliminaire, on déduit que $\forall n \geq N$:

$$\begin{aligned}(\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_{t-1})^T &= \mathcal{M}_n^{-1}.(\rho_1, \rho_2, \cdots, \rho_{t-1})^T \\ &= (\sum_{j=1}^{t-1} b_{1,j}^j \rho_j, \cdots, \sum_{j=1}^{t-1} b_{t-1,j}\rho_j)^T\end{aligned}$$

i.e. $\varepsilon_i = \sum_{j=1}^{t-1} b_{i,j}\rho_j$ d'où :

$$\forall\ n \geq N, v_p(\varepsilon_i) \geq \min\{v_p(b_{i,j}) + v_p(\rho_j)\} \geq v_p(\mathcal{M}_n^{-1}) + n \geq -a + n$$

(cf. étapes précédentes). Par conséquent,

$$(E_{0,S} : E_{0,S} \cap N_{0,S}K_n^{\times}) \geq p^{(n-a)(t-1)} \sim p^{n(t-1)}.$$

D'autre part,

$$(E_{0,S} : E_{0,S} \cap N_{0,S}K_n^{\times}) \leq (E_{0,S} : N_{n,0}E_{n,S}) = (E_{0,S} : E_{n,S}^{p^n}) \sim p^{n(t-1)},$$

d'où : $(E_{0,S} : E_{0,S} \cap N_{0,S}K_n^{\times}) \sim p^{n(t-1)}$ assertion équivalente à la finitude de $\mathcal{C}_{\infty}^{\Gamma}(p)$; le résultat en découle.

Raffinement : Dans le cas où la matrice $\mathcal{M}$ est à coefficients rationnels, la réciproque est vraie et l'on peut démontrer le théorème suivant :

Théorème 3.2.6. *L'analogue de la conjecture de Gross considéré est satisfait* si et seulement si *la matrice* $\mathcal{M} \in M_{t-1}(\mathbb{Q})$ *est inversible.*

Remarque : La raison pour laquelle on est contraint de se restreindre à une matrice à coefficients rationnels s'explique par le fait que l'on utilise dans le courant de la preuve l'assertion suivante : si $\mathcal{C}(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{t-1})^T = 0$, alors $\varepsilon_i = 0\ \forall\ i$ ce qui permet de conclure au caractère inversible de $\mathcal{C}$. Or cette implication n'est vraie que dans le cas où $\mathcal{C} \in \mathcal{M}_{t-1}(\mathbb{Q})$ et devient fausse lorsque $\mathcal{C}$ est simplement un élément de $\mathcal{M}_{t-1}(\mathbb{Z}_p)$ comme le montre le contre-exemple suivant :

$$C = \begin{pmatrix} 1 & \alpha \\ 0 & 0 \end{pmatrix}$$

où

$$\alpha \in Z_p,$$

Dans ce cas, $\mathcal{C}$ n'est pas inversible et cependant,

$$C(\varepsilon_1, \varepsilon_2)^T = 0 \quad (\varepsilon_i \in \mathbb{Z})$$

entraine bien

$$\varepsilon_i = 0, \quad i = 1, 2.$$

Exemple 1 [7] : On se donne $\beta_0 = \dfrac{1}{(T-1)(T-2)}$ et $\beta_i = 0 \ \forall \ i \geq 1$. Comme $\beta_0 \notin \{\alpha^p - \alpha, \alpha \in K_0 = \mathbb{F}_q(T)\}$, le vecteur de Witt de longueur infinie $(\beta_0, \beta_1, \cdots, \beta_{n-1}, \cdots)$ détermine une $\mathbb{Z}_p$-extension K_∞/K_0 dans laquelle seuls les premiers associés à $P_1 = T-1$ et $P_2 = T-2$ se ramifient (voir le critère établi par Schmid) et admettent pour diviseur associé, respectivement, $(1)_0 - (\infty)_\infty$ et $(2)_0 - (\infty)_\infty$. Ainsi donc, $\sharp(S) = 2$ avec $S = \{\mathfrak{p}_1, \mathfrak{p}_2\}$ et l'on désigne par $K_{0,\mathfrak{p}_1}$ le complété de K_0 en $\mathfrak{p}_1$. Comme $\deg(P_1) = 1$, on dispose de la description suivante : $K_{0,\mathfrak{p}_1} \simeq \mathbb{F}_q((T-1)) \simeq \mathbb{F}_q((x))$. On désigne par F l'unique extension non-ramifiée de $\mathbb{Q}_p$ telle que $\mathcal{O}_F/M_F \simeq \mathbb{F}_q$ et l'on pose : $\delta_1 = \frac{T-1}{T-2}$ (remarque : si l'on reprend les notations utilisées précédemment, on se trouve dans le cas très simplifié où $a_1 = b_1 = h_1 = 1$ car le diviseur $(\frac{T-1}{T-2})$ est un diviseur principal de K_0). On note alors dans le contexte local, $\pi_{1,1}$ (resp.$B_{n,1}$) un relèvement en caractéristique 0 de δ_1 (resp. de β_n) et ce, pour tout $n \geq 0$. La forme particulièrement simple du vecteur de Witt paramétrant la $\mathbb{Z}_p$-extension K_∞/K_0 nous permet de choisir $B_{n,1} = 0 \ \forall \ n \geq 1$... De

$$\delta_1 = \frac{T-1}{T-2} = \frac{x}{x-1} = -x.(\frac{1}{1-x}) = -x.(\sum_{n\geq 0} x^n),$$

on déduit : $\pi_{1,1} = -x.((\sum_{n\geq 0} x^n))$. De la même façon, on a :

$$B_{0,1} = \frac{1}{(T-1)(T-2)} = \frac{1}{x.(x-1)} = \frac{-1}{x}.(\sum_{n\geq 0} x^n)$$

$$B_{n,1} = 0 \ \forall \geq \ 1.$$

Comme $S = \{\mathfrak{p}_1, \mathfrak{p}_2\}$, la matrice $\mathcal{M}_n$ associée au n-ième étage de la tour d'extensions est d'ordre 1×1 et son unique coefficient est donné par :

$$c_{1,1}^{(n)} = \sum_{t=0}^{n-1} p^t a_{1,1}^{(t,n-t-1)} \ \forall \ \geq \ 1$$

[7] tiré de l'article de Lam-Estrada et Villa-Salvador intitulé : *Some remarks on the theory of cyclotomic function fields* - Rocky Mountain Journal of Mathematics vol. **31** - 2001

où

$$a_{1,1}^{(t,n-t-1)}\text{Tr}\ \ \text{Res}(\frac{d\pi_{1,1}}{\pi_{1,1}}.B_{t,1}^{p^{n-t-1}}).$$

Ainsi donc si $t>0$, $a_{1,1}^{(t,n-t-1)}=0$ et l'on a donc :

$$c_{1,1}^{(n)}=a_{1,1}^{(0,n-1)}=\text{Tr}\ \ \text{Res}(\frac{d\pi_{1,1}}{\pi_{1,1}}.B_{0,1}^{p^{n-1}}).$$

Reste à s'assurer que :

$$\begin{aligned}\frac{d\pi_{1,1}}{\pi_{1,1}}.B_{0,1}^{p^{n-1}} &= \frac{1}{x(1-x)}.\,b_{0,1}^{p^{n-1}}dx\\ &= \frac{-1}{x^{p^{n-1}+1}}.(1+x+x^2+\cdots)^{p^{n-1}+1}\end{aligned}$$

d'où l'on déduit que $\text{Res}(\frac{d\pi_{1,1}}{\pi_{1,1}}.B_{0,1}^{p^{n-1}})\in\mathbb{Z}^{\times}$, ainsi $c_{1,1}^{(n)}\in\mathbb{Z}^{\times}$. La matrice $\mathcal{M}$ est donc inversible et la $\mathbb{Z}_p$-extension associée vérifie la conjecture de Gross.

Exemple 2 : Le but est de construire une $\mathbb{Z}_p$-extension que l'on supposera (totalement) ramifiée en seulement deux places et pour laquelle la Conjecture de Gross est mise en défaut, c'est-à-dire que les éléments vont être choisis (construits par récurrence en fait)de sorte que soit satisfait $\mathcal{M}_n\equiv\ 0\ \text{mod}\ p^n$ et ce, $\forall\ n$ ce qui équivaut à : $\mathcal{M}=\lim_{n\to\infty}\mathcal{M}_n=0$ d'où le résultat. On se donne $B_0=\dfrac{3x^2-1}{x^2.(x-1)}$; ainsi $S=\{P_0,P_1\}$. Comme précédemment, on pose alors :

$$A=(\frac{1-x}{x})^{\varepsilon}$$

et un rapide calcul montre que :

$$\frac{dA}{A}=-\varepsilon.(\frac{1}{x(1-x}})=-\varepsilon.(\frac{1}{x}+\frac{1}{1-x})$$

et par conséquent :

$$B_0.\frac{dA}{A}=-\varepsilon.(\frac{3x^2-1}{x^3.(x-1)}+\frac{3x^2-1}{x^2.(x-1)^2})dx$$

d'où :

$$B_0.\frac{dA}{A}=-D_x\{\varepsilon.\frac{3x+1}{2x^2.(x-1))^2}\}$$

et donc $\mathcal{M}_1=0$. Dans le procédé récurrent que l'on se propose d'utiliser, cette étape peut être vue comme l'initialisation ...
On suppose (hypothèse de récurrence) maintenant construite la famille de

n éléments $\{B_0, B_1, \cdots, B_{n-1}\}$ tels que $\mathcal{M}_i \equiv 0 \bmod p^i$ pour $1 \leq i \leq n$. On déduit du couple de relations $c_{j,i}^{(n+1)} \equiv c_{j,i}^{(n)} + p^n a_{j,i}^{(n,0)} \bmod p^n$. (vue précédemment) et $\mathcal{M}_n \equiv 0 \bmod p^n$ que $\mathcal{M}_{n+1} = p^n(a_n + b_n)$ où $a_n = a_{1,1}^{(n,0)}$et$b_n \in \mathbb{Z}_p$. Ainsi donc, on a $\mathcal{M}_{n+1} \equiv 0 \bmod p^{n+1} \Leftrightarrow a_n + b_n \equiv 0 \bmod p$. On pose alors : $B_n = \dfrac{r_n}{x.(x-1)}$ et par conséquent $a_n = 2r_n$. Enfin, si l'on suppose que p est impair, on peut choisir $r_n \in \mathbb{Z}$ de sorte que $2r_n \equiv -b_n[p]$ auquel cas la Conjecture de Gross pour la $\mathbb{Z}_p$-extension ainsi construite n'est pas satisfaite.

Ces exemples nous permettent de mettre en exergue ce que l'on pressentait lors de l'exposition de l'article dans toute sa généralité, à savoir à quel point la méthode exhibée, si elle est originale et astucieuse, reste fastidieuse à mettre en place et ce quand bien même la $\mathbb{Z}_p$-extension considérée est paramétrée par un vecteur de Witt dont la forme est extrêmement simple. Qu'il s'agisse de l'article de Villa-Madan (1988) ou de celui de Villa-Salvador (2001), les illustrations se limitent au cas où le cardinal de S est égal à deux, ce qui peut sembler un petit peu restrictif quand bien même on est amené pour pouvoir raisonner à supposer qu'il n'existe qu'un nombre fini de premiers ramifiés. L'idée donc de contourner la méthode proposée par les auteurs en espérant gagner en simplicité semble donc naturelle et sera l'objet du chapitre 4 qui à défaut de traiter de "simplicité" sera abordé sous le jour de la "semi-simplicité" ... Mais auparavant, un complément qui nous sera utile dans la suite :

3.3 Premiers pas en Théorie des Genres ...

Le principe selon lequel le dictionnaire "bilingue" reliant corps de nombres et corps de fonctions se serait, au fil des ans et des constructions, enrichi des corps de fonctions *vers* les corps de nombres est mis en défaut en ce qui concerne la théorie des genres étant donné que la définiton de corps des genres émerge pour la première fois dans le contexte des corps de nombres en 1959 avec les travaux de Fröhlich et qu'il faudra attendre les années 90 (1992) pour que R. Clément dans un article intitulé *"The Genus Field of Algebraic Fonction Field"* [8] s'essaie à construire une théorie analogue dont on propose de donner quelques éléments ci-après.

On se place dans le contexte suivant :

Soient K un corps de fonctions de corps des constantes $\mathbb{F}_q$ (où $q = p^\alpha$) et S un ensemble fini de place, à priori quelconque. Étant supposée fixée une clôture algébrique $\overline{K}$ de K, on désigne par L une extension finie de degré m (dans le cas qui nous intéresse, à savoir celui considéré par Villa-Madan

[8] paru au Journal of Number Theory **40** p 359-375

dans leur article, S sera tout simplement l'ensemble -supposé fini- des places de K qui se ramifient dans L et $m = p^n$). On note S_L l'ensemble des places de L au-dessus de $S := S_K$ et $\mathcal{J}_L$ le groupe des idèles de L dont on rappelle une définition ci-après.

Définition 3.3.1. *Étant donné un corps global K (i.e. un corps muni d'une formule du produit), on appelle* idèle *de K un élément a du produit direct $\prod_{\mathfrak{p}\in Pl(K)} K_\mathfrak{p}^\times$ où $K_\mathfrak{p}^\times$ désigne le groupe multiplicatif associé au corps local $K_\mathfrak{p}$ complet pour la topologie $\mathfrak{p}$-adique tel que si l'on note $a_\mathfrak{p}$ sa composante d'indice p, on ait $v_\mathfrak{p}(a) = 0$ pour presque toute place $\mathfrak{p}$ de K.*

L'ensemble des idèles d'un corps global K est un groupe (non-topologique) pour la multiplication composante par composante que l'on note généralement $\mathcal{J}_K$ et qui, muni d'une topologie appropriée devient un groupe abélien, séparé et localement compact essentiel dans la formulation de la théorie globale du corps de classes. On remarque que le groupe multiplicatif $K^\times$ de K s'identifie au sous-groupe de $\mathcal{J}_K$ constitué des idèles $(a_\mathfrak{p})$ dont chaque coordonnée est égale à un élément fixé non-nul de K (en effet, via la formule du produit on a que si $a \in K^\times$ alors $v_\mathfrak{p}(a) = 0$ pour presque toute place $\mathfrak{p}$ de K). On parle pour les éléments de $K^\times$ d'idèles principaux et comme dans le cas des idéaux, on baptise *groupe des classes d'idèles* le quotient : $\mathcal{C}(K) = \dfrac{\mathcal{J}_K}{K^\times}$. Enfin, étant donnée L une extension finie de K, on pose :

$$\begin{array}{rcl} N : \mathcal{J}_L & \to & \mathcal{J}_K \\ (z_\mathfrak{P}) & \mapsto & \displaystyle\prod_\mathfrak{p}(\prod_{\mathfrak{P}|\mathfrak{p}} N_{L_\mathfrak{P}/K_\mathfrak{p}}(z_\mathfrak{P})) := \prod_{\mathfrak{p}\in Pl_K} x_\mathfrak{p} \end{array}$$

L'application ainsi définie, appelée "Norme d'idèles", est un morphisme continu qui envoit le groupe des idèles principaux de L dans celui de K. Elle induit donc, par passage au quotient, un morphisme de $\mathcal{C}(L)$ dans $\mathcal{C}(K)$ noté abusivement $N_{L/K}$ et permet d'énoncer, comme dans le cas des idéaux, un théorème 90 de Hilbert pour les idèles.

Cela précisé, on revient à la théorie des genres et l'on pose, pour toute place v de L, $\mathcal{U}_L^{S_L} := \prod_{v\in S_L} L_v^\times \cdot \prod_{v\notin S_L} U_v$ où L_v désigne le complété de L en v et U_v le groupe des unités (i.e. des inversibles) $\mathcal{O}_v^\times$ de l'anneau de valuation $\mathcal{O}_v$ associé à v. On dira d'une place qu'elle est "finie" s'il s'agit d'une place de L n'appartenant pas S_L. On déduit de la finitude du groupe de Picard $\mathrm{Pic}(\mathcal{O}_{L,S_L})$ que $L^\times\mathcal{U}_L$ est un sous-groupe de $\mathcal{J}_L$ d'indice fini et l'on note $H_L^{S_L}$ l'unique extension abélienne de L dans $\overline{K}$ qui lui correspond. On parle pour $H_L^{S_L}$ de S_L-corps (ou plus simplement de S-corps) de classes de Hilbert de L. La théorie du corps de classes nous donne une interprétation de $H_L^{S_L}$ comme étant l'extension abélienne maximale de L dans $\overline{K}$ S_L-décomposée (i.e. totalement décomposée en les places au-dessus de S_L).

Remarque : Dans le cas particulier où l'on prend pour S l'ensemble des places à l'infini de K (c'est-à-dire les places de K au-dessus de la place à l'infini $< \frac{1}{T} >$ du corps des fonctions rationnelles $\mathbb{F}_p(T)$, on retrouve la définition du corps de classes de Hilbert "ordinaire" (comprendre "au sens de Rosen") pour les corps de fonctions, à savoir l'extension abélienne maximale de L non-ramifiée aux places finies et dans laquelle toute place de L telle que $\mathfrak{p}|\infty$ se décompose totalement.

Pour présenter la notion de S-corps des genres, on commence par faire l'hypothèse simplificatrice selon laquelle l'extension L/K est *abélienne* (pour finalement se restreindre au cas où elle est *cyclique* de degré p^n puisqu'il s'agit là du cadre qui nous intéresse).[9] Soit donc $L \subset \overline{K}$ une extension finie de K de degré m et de groupe de Galois $G = Gal(L/K)$ supposé abélien. On désigne par $\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_t$ les places de K ramifiées dans L et par e_i, $1 \leq i \leq t$ l'indice de ramification associé. Pour chaque place w de S i.e. telle que $v|w$, on note $m_w = e_{v/w}.f_{v/w}$ le degré de l'extension locale L_v/K_w.
On pose alors la définition suivante :

Définition 3.3.2. *On appelle S_L-corps des genres de L/K et l'on note $\mathcal{H}^S_{L/K}$, l'extension abélienne maximale de K contenue dans le S_L-corps de classes de Hilbert $H_L^{S_L}$. On pose alors : $\mathcal{G}^S_{L/K} := Gal(\mathcal{H}^S_{L/K}/L)$ le groupe de Galois associé, appelé encore "quotient des S-genres".*

Remarque : Le S-corps des genres de L/K contient le S_K-corps de classes de Hilbert de K.

Théorème 3.3.3. *(Formule des Genres)*

$$[\mathcal{H}^S_{L/K} : L] = \sharp(Pic(\mathcal{O}_{(K,S)})).\frac{\prod_{i=1}^t e_i . \prod_{w\in S} m_w}{[L:K].(E_K^S : E_K^S \cap N(\mathcal{U}_L))}$$

Preuve (idée) : Dans son article, R. Clément montre que le sous-groupe des idèles de K associé par la théorie du corps de classes à l'extension abélienne $\mathcal{H}^S_{L/K}/L)$ est $K^\times N(\mathcal{U}_L^{S_L})$; de l'isomorphisme $Gal(\mathcal{H}^S_{L/K}/K) \simeq \dfrac{\mathcal{J}_K}{K^\times N(\mathcal{U}_L^{S_L})}$, on déduit successivement :

$$\begin{aligned}
[\mathcal{H}^S_{L/K} : K] &= (\mathcal{J}_K : K^\times N(\mathcal{U}_L^{S_L})) \\
&= (\mathcal{J}_K : K^\times \mathcal{U}_K^{S_K})(K^\times \mathcal{U}_K^{S_K} : K^\times N(\mathcal{U}_L^{S_L})) \\
&= (\mathcal{J}_K : K^\times \mathcal{U}_K^{S_K})(\mathcal{U}_K^{S_K} : N(\mathcal{U}_L^{S_L})(K^\times \cap \mathcal{U}_K^{S_K} : K^\times \cap N(\mathcal{U}_L^{S_L}))^{-1}.
\end{aligned}$$

[9] Pour voir exposée la Théorie des Genres dans toute sa généralité, on pourra consulter l'article co-écrit par B. Anglès et J.F. Jaulent intitulé : Théorie des Genres des corps globaux Manuscripta Math.**101**, (2000)

En outre,

$K^\times \cap \mathcal{U}_K^{S_K} = E_{S,K}$ et si $\alpha \in E_{S,K} \cap N(L^\times)$ alors α est une norme locale en chaque place de K, autrement dit $\alpha \in K^\times \cap N(U_L^{S_L})$.
Réciproquement, si $G = Gal(L/K)$ est cyclique, alors on l'inclusion inverse $K^\times N(U_L^{S_L}) \subseteq E_{S,K} \cap N(L^\times)$ d'où l'égalité.

On conclut en remarquant que $(\mathcal{J}_K : K^\times \mathcal{U}_K^{S_K}) = \sharp(\mathrm{Pic}(\mathcal{O}_{K,S_K}))$ et en rappelant un résultat démontré dans [65] selon lequel :

$$(\mathcal{U}_K^{S_K} : N_{L/K}(\mathcal{U}_L^{S_L})) = \prod_{w \in S_K} m_w \prod_{i=1}^{t} e_i.$$

On peut préciser :

Proposition 3.3.4. *Lorsque l'extension L/K est cyclique de groupe de Galois $G =< \sigma >$, le quotient des S-genres s'identifie au plus grand quotient du groupe des S-classes $Pic(\mathcal{O}_{L,S})$ de L sur lequel G opère trivialement et l'on a l'isomorphisme :*

$$^\Gamma Pic(\mathcal{O}_{L,S}) := \frac{Pic(\mathcal{O}_{L,S})}{Pic(\mathcal{O}_{L,S})^{\sigma-1}} \simeq \mathcal{G}_{L/K}^S.$$

Preuve : Il s'agit d'une conséquence du Principe de Hasse (applicable ici puisque l'on s'est restreint au cas cyclique) et du théorème 90 de Hilbert pour les idèles. En effet, si l'on suit l'article cité précédemment d'Anglès et Jaulent, rédigé dans un cadre tout à fait général, il est dit à l'occasion de la proposition 2.1.3(ii) qu'étant donnée une extension abélienne L/K de corps globaux, le groupe d'idèles de L associé au S-corps des genres $\mathcal{H}_{L/K}^S$ est le saturé pour la norme $N_{L/K}^{-1}(N_{L/K}(\mathcal{U}_L^{S_L})K^\times)L^\times$ du groupe $\mathcal{U}_L^{S_L}L^\times$. Dans le cas cyclique, les choses se formulent plus simplement ... Soit donc x un élément de $\mathcal{J}_L$ tel que $x \in N_{L/K}^{-1}(N_{L/K}(\mathcal{U}_L^{S_L})K^\times)L^\times$; alors $N_{L/K}(x) = N_{L/K}(u)k$ où $u \in U_L^{S_L}$ et $k \in K^\times$. Ainsi donc les propriétés multiplicatives de l'application "norme" entraînent que $N_{L/K}(x/u) = k = N_{L/K}(l)$ pour $l \in L^\times$ et ce, en vertu du principe de Hasse. Par conséquent, on a que $N_{L/K}(x) = N_{L/K}(u).N_{L/K}(l) = N_{L/K}(ul)$ d'où $x = ul$ à un élément de norme 1 près, c'est-à-dire que $x = ul\vartheta$ où $N_{L/K}(\vartheta) = 1$; il suit que dans le cas cyclique : $N_{L/K}^{-1}(N_{L/K}(\mathcal{U}_L^{S_L})K^\times)L^\times = \mathcal{U}_L^{S_L}L^\times\mathcal{J}_L^1$ si $\mathcal{J}_L^1$ désigne le sous-groupe des idèles de L de norme 1. Maintenant, de $N(x/ul) = 1$, on déduit grâce au théorème 90 de Hilbert pour les idèles que $x/lu = y^{\sigma-1}$ avec $y \in \mathcal{J}_L$, c'est-à-dire que $x \in \mathcal{J}_L^{\sigma-1}\mathcal{U}_L^{S_L}L^\times$ d'où finalement, $\mathcal{G}_{L/K}^S \simeq \mathcal{J}_L/\mathcal{J}_L^{\sigma-1}\mathcal{U}_L^{S_L}L^\times$.

Remarques :
1- On rappelle qu'étant donné M un G-module où $G =< \sigma >$ est un groupe cyclique, on dispose d'une suite exacte reliant le sous-groupe des "invariants" (mesurant le défaut d'injectivité) à celui des "co-invariants"(qui mesure le défaut de surjectivité) :

$$0 \longrightarrow M^G \hookrightarrow M \xrightarrow{\sigma-1} M \twoheadrightarrow {}^GM \longrightarrow 0$$

En particulier, si l'on note

$$q(M) = \frac{|M^G|}{|{}^GM|}$$

(q pour "quotient de Herbrand"), on a que $q(M) = 1$ si M est fini. Cette observation appliquée au groupe fini $\mathrm{Pic}(\mathcal{O}_{L,S})$ entraine que dans le cas cyclique, les ordres respectifs du quotient des genres et du sous-groupe des classes ambiges (*ie* stable par l'action de G) sont égaux ...

2- Une utilisation du corps des genres pour les corps de nombres qui permet de toucher du doigt l'importance de cette notion est donnée par le résultat suivant, conjecturé par T. Tannaka et démontré par F. Terada :
Soient K un corps de nombres et L/K une extension cyclique finie, alors toutes les classes ambiges de L (c'est-à-dire les classes laissées stables par l'action du groupe de Galois $Gal(L/K)$) capitulent dans le corps des genres associé à L. Dans le cas particulier où L/K est une extension cylique de degré p premier, il s'agit d'un résultat dû à Hilbert, connu sous le nom de *Théorème* 94, qui prouve qu'il existe au moins une classe non-triviale de K qui capitule dans L. En outre, Hilbert avait démontré qu'étant donnés σ un générateur de $Gal(L/K)$, $N_{L/K}$ la norme associée, E_L, E_L^1, respectivement, les groupes des unités de L et le sous-groupe des unités de L de norme 1, le groupe des classes de K qui capitulent dans L est isomorphe au groupe-quotient : $E_L^1/E_L^{1-\sigma} = H^1(E_L)$. Nous verrons à l'occasion du chapitre 4 que dans le cas des p-extensions cycliques de corps de fonctions, tout ne se passe pas nécessairement de la même façon ...

Remarque : Dans [15], C. Thiébaud et V. Fleckinger ont démontré en utilisant la théorie des modules de Carlitz l'analogue dans le cadre des corps de fonctions du théorème de Furuya (1977) selon lequel tout idéal ambige d'une extension abélienne de $\mathbb{Q}$ devient principal dans son corps des genres. On énonce ainsi :

Théorème 3.3.5. *Soit $K = k(X)$ le corps de fonctions associé à une courbe X projective, lisse, géométriquement connexe et définie sur le corps fini $k = \mathbb{F}_q$. Soit ∞ un diviseur premier de K (i.e. un point fermé de X) supposé fixé et de degré d_∞. On note L/K une extension abéliennne finie modérément*

ramifiée en l'∞ et l'on suppose que le groupe de décomposition $D_\infty(L/K)$ se réduit au groupe d'inertie $I_\infty(L/K)$. Si maintenant l'on désigne par S_L l'ensemble des places de L au-dessus de ∞ alors tout idéal ambige de $\mathcal{O}_{S_L}$ devient principal ("capitule") dans le S-corps des genres de L/K. [10]

[10] au sens de [4]

Chapitre 4

Perspectives métabéliennes

4.1 La conjecture de Gross : re-vision...

4.1.1 L'article de Greenberg : ses grandes lignes

Comme il s'agira pour nous d'une source d'inspiration, nous débutons ce chapitre par un bref résumé de l'article de Greenberg : *"On a Certain p-Adic Representation"*[1] sans toutefois entrer plus avant dans les détails concernant les diverses structures algébriques mises en jeu car nous aurons l'occasion d'y revenir plus précisément par la suite.
On se donne p un nombre premier impair, K une extension *abélienne* de $\mathbb{Q}$ de degré fini et l'on considère K_∞/K la $\mathbb{Z}_p$-extension cyclotomique associée à K ; en particulier, on a l'isomorphisme : $Gal(K_\infty/K) \simeq \mathbb{Z}_p$. Si l'on désigne par γ un générateur topologique fixé du groupe procyclique $\Gamma := Gal(K_\infty/K)$, Greenberg se propose (entre autre chose) de déterminer la puissance de T que l'on peut mettre en facteur dans le polynôme caractéristique de $\gamma - 1(\leftrightarrow T)$ où $\gamma - 1$ agit sur un certain espace vectoriel à déterminer (on rappelle à cette occasion qu'une représentation p-adique d'un groupe G- en l'occurence le groupe profini $Gal(K_\infty/K)$- consiste en la donnée d'un $\mathbb{Q}_p$-espace vectoriel V de dimension finie et d'un homomorphisme continu $g : G \to Aut_{\mathbb{Q}_p}(V)$)...
On note K_n l'unique sous-corps de K_∞ tel que $[K_n : K] = p^n$ et l'on désigne par A_n la p-partie de son groupe de classes d'idéaux. On déduit de la relation d'inclusion $K_n \hookrightarrow K_m$ si $m \geq n \geq 0$, le système d'homomorphismes
$A_n \to A_m$ et l'on pose $A := \varinjlim A_n$. Si l'on considère A en tant que groupe abélien (i.e. $\mathbb{Z}$-module) discret, son dual de Pontrjagin $X := \hat{A}$ est un pro-p-groupe abélien naturellement doté d'une structure de $\mathbb{Z}_p$-module[2]. On pose alors : $V := X \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ où $\mathbb{Q}_p = \mathrm{Frac}(\mathbb{Z}_p)$. On prolonge alors l'action de

[1] Inventiones Math. **21**, 117-124 (1973)

[2] On rappelle que la dualité de Pontrjagin (1908 – 1988) induit une équivalence de catégories entre d'une part *groupes abéliens compacts* et *groupes abéliens discret* et d'autre part entre les *groupes abéliens profinis* et *les groupes abéliens discrets de torsion.*

$Gal(K_\infty/K)$ sur A en une action sur X via :

$$\begin{array}{rcl} Gal(K_\infty/K) \times X & \to & X := \mathrm{Hom}(A, \mathbb{Q}_p/\mathbb{Z}_p) \\ (g, x) & \mapsto & g.x : a \mapsto (g.x)(a) = x(g(a)) \end{array}$$

ce qui permet de définir, via l'application $X \to V$ telle que $x \mapsto x \otimes 1$ une action sur V et ce faisant une repésentation p-adique (on dote ainsi V d'une structure de $\mathbb{Q}_p[\Gamma]$-module où $\Gamma = Gal(K_\infty/K)$). Soit maintenant $V_0 = \{v \in V | \ (\gamma - 1)^t.v = 0\}$ pour un certain t à déterminer. Dans le cas où K est un corps *totalement réel* Greenberg montre que $V_0 = 0$. Pour se faire, on considère $\Gamma_n = Gal(K_n/K)$ le groupe cyclique d'ordre p^n engendré par $\gamma_n := \gamma_{|K_n}$ et l'on pose :

$$B_n := A_n^{\Gamma_n} = \{c \in A_n | c^\gamma = c\}$$

On énonce alors la proposition suivante :

Proposition 4.1.1. *L'ordre de B_n est borné et la borne ne dépend que du corps de base K et de p.*

Reste à considérer l'homomorphisme $i_n : A_n \to A$ induit par l'injection : $K_n \hookrightarrow K_\infty$ et à poser $B = A^\Gamma$. On vérifie alors que $B = \cup_{n=1}^{\infty} i_n(B_n)$ d'où l'on déduit que $|B| < \infty$ est fini ; par conséquent $|X/(\gamma - 1)X| < \infty$ et $V_0 = 0$.
Si maintenant on suppose K *totalement imaginaire* et si l'on désigne par K^+ le sous-corps totalement réel associé ($[K : K^+] = 2$) alors une preuve (dont nous retraçons les grandes étapes dans le paragraphe suivant) utilisant l'analogue p-adique du théorème de Baker-Brumer[3] relatif à l'indépendance des logarithmes permet d'obtenir que si s désigne le nombre de places de K^+au-dessus de p décomposées dans K alors $\dim_{\mathbb{Q}_l}(V_0) = s$ et qu'en outre $(\gamma - 1).v = 0 \ \forall \ \ v \in V_0$ (ie $t = 1$), par conséquent l'action de $Gal(K_\infty/K)$ sur V_0 est semi-simple.
Ainsi donc, les $\mathbb{Z}_p$-extensions *cyclotomiques* des corps de nombres abéliens (réels ou imaginaires) sont semi-simples (au sens précédent).

4.1.2 Les principales étapes de la preuve

La Conjecture de Leopoldt : l'énoncé

La conjecture de Leopoldt se rapporte au rang p-adique du groupe des unités E_K d'un corps de nombres K. Ainsi, si $\mathfrak{p}$ désigne une place ultramétrique de K et si l'on note $U_\mathfrak{p}$ le groupe des unités relatif à la complétion $K_\mathfrak{p}$ de K en $\mathfrak{p}$, la conjecture de Leopoldt prédit que le rang p-adique[4] de

[3] voir par exemple [69]

[4] On appelle $\mathbb{Z}$-rang (resp. $\mathbb{Z}_p$-rang) d'un $\mathbb{Z}$-module de type fini (resp. d'un $\mathbb{Z}_p$-module de type fini) le rang du quotient de ce dernier par son sous-groupe de torsion.

l'adhérence $\overline{E}_K$ de E_K dans $\mathcal{U}_p := \prod_{\mathfrak{p}|p} U_\mathfrak{p}$ est égal au nombre de Dirichlet $r_1 + r_2 - 1$.

Plus précisément, on se donne K une extension finie de $\mathbb{Q}$ de degré n ; on désigne par E_K le groupe des unités de K (i.e. le groupe constitué des éléments inversibles de l'anneau des entiers $\mathcal{O}_K$ correspondant) et par $U_\mathfrak{p}$ le groupe des unités associé à la complétion de K en $\mathfrak{p}$. On pose $\mathcal{U}_p := \prod_{\mathfrak{p}|p} U_\mathfrak{p}$ et l'on considère l'injection naturelle (une unité globale est une unité localement partout) :

$$\begin{array}{rcl} E_K & \overset{i}{\hookrightarrow} & \mathcal{U}_p := \displaystyle\prod_{\mathfrak{p}|p} U_\mathfrak{p} \\ \varepsilon & \mapsto & (\varepsilon, \varepsilon, \cdots, \varepsilon, \cdots) \end{array}$$

appelée "plongement diagonal".

Conséquence : Dans toute la suite on identifiera E_K et son image via i.

En tant que groupe topologique, on dispose pour $\mathcal{U}_p$ de l'isomorphisme suivant (on rappelle que $\mathbb{Z}_p$, l'anneau des entiers p-adiques, est principal) :

$$\mathcal{U}_p \overset{\mathbb{Z}_p}{\simeq} \mathbb{Z}_p^n \times T$$

où :

$$\begin{array}{rcl} n & = & [K : \mathbb{Q}] \\ & = & \displaystyle\sum_{\mathfrak{p}|p} (e_{\mathfrak{p}/p}.f_{\mathfrak{p}/p}) \\ & = & \displaystyle\sum_{\mathfrak{p}|p} d_{\mathfrak{p}/p} \end{array}$$

Cela est une conséquence de la structure de $U_\mathfrak{p} \simeq \mu_\mathfrak{p}^0 \times \mu_\mathfrak{p}^1 \times \mathbb{Z}_p^{d_{\mathfrak{p}/p}}$ (où l'on a noté $\mu_\mathfrak{p}^0$ le groupe discret formé des racines de l'unité de $K_\mathfrak{p}$ d'ordre premier à p et $\mu_\mathfrak{p}^0$ le groupe cyclique des racines p-primaires dans $K_\mathfrak{p}$) et de la définition du $\mathbb{Z}_p$-rang rappelée précédemment. En effet, ne contribue à la détermination du $\mathbb{Z}_p$-rang de $\mathcal{U}_p := \prod_{\mathfrak{p}|p} U_\mathfrak{p}$ que le facteur :

$$\begin{array}{rcl} \displaystyle\prod_{\mathfrak{p}|\mathfrak{p}} \mathbb{Z}_p^{d_{\mathfrak{p}/p}} & \simeq & \mathbb{Z}_p^{\Sigma_{\mathfrak{p}|p} d_{\mathfrak{p}/p}} \\ & = & \mathbb{Z}_p^{\Sigma_{\mathfrak{p}|p} e_{\mathfrak{p}/p}.f_{\mathfrak{p}/p}} \\ & = & \mathbb{Z}_p^n \end{array}$$

On note $\overline{E}_K$ l'adhérence de E_K dans $\mathcal{U}_p$ (d'où la structure de $\mathbb{Z}_p$-module héritée de celle de $\mathcal{U}_p$). Si maintenant r_1 et r_2 désignent respectivement le nombre de plongements réels et le nombre de plongements complexes de K dans $\mathbb{C}$, on sait grâce au théorème de structure des unités de Dirichlet que le $\mathbb{Z}$-rang de E_K est égal à $r_1 + r_2 - 1$. On en déduit que :

$$\overline{E}_K \overset{\mathbb{Z}_p}{\simeq} \mathbb{Z}_p^c \times T'$$

où $c \leq r_1 + r_2 - 1$ et T' est un groupe fini. La conjecture de Leopoldt assure que l'on a l'égalité : $c = r_1 + r_2 - 1$.

Remarque : Une manière de voir l'inégalité $c \leq r_1 + r_2 - 1$ consiste à écrire : $c = (r_1 + r_2 - 1) - \delta(K, p)$, ce qui permet d'introduire la notion de "défaut de Leopoldt" pour le couple (K, p) selon :

$$\delta(K, p) = rg_{\mathbb{Z}} E_K - rg_{\mathbb{Z}_p} \overline{E}_K$$

Ce dernier mesure à quel point le couple (K, p) est loin de satisfaire la conjecture de Leopoldt en p, situation idéale qui se traduit naturellement par $\delta(K, p) = 0$.

Variante : Il arrive que l'on raisonne plus volontiers sur le groupe $E_K^{(1)}$ définit comme suit :

$$E_K^{(1)} := \{\varepsilon \in E_K | \varepsilon \equiv 1 \ [\mathfrak{p}] \quad \forall\, \mathfrak{p}|p\}$$

qui est un sous-groupe d'indice fini de E_K. Cela est rendu d'autant plus naturel que la tensorisation par l'anneau des entiers p-adiques a pour effet de tuer les racines de l'unité de K d'ordre premier à p, à savoir le groupe $\mu_p^0 = \prod_{\mathfrak{p}|p} \mu_{\mathfrak{p}}^0$. Comme précédemment, on désigne alors par $\overline{E_K^{(1)}}$ la fermeture de l'image de $E_K^{(1)}$ dans le groupe topologique produit[5] $\prod_{\mathfrak{p}|p} U_{\mathfrak{p}}^{(1)}$ où l'on rappelle que le sous-groupe $U_{\mathfrak{p}}^{(1)}$ des unités principales est un $\mathbb{Z}_p$-module noethérien. Étant donné le plongement diagonal :

$$\begin{array}{rcl} i : E_K^{(1)} & \hookrightarrow & \displaystyle\prod_{\mathfrak{p}|p} U_{\mathfrak{p}}^{(1)} \\ \varepsilon & \mapsto & (\varepsilon, \varepsilon, \cdots, \varepsilon, \cdots) \end{array}$$

on considère :

$$\begin{array}{rcl} i \otimes Id_{\mathbb{Z}_p} : E_K^{(1)} \otimes \mathbb{Z}_p & \to & U_{\mathfrak{p}}^1 \otimes \mathbb{Z}_p \simeq U_{\mathfrak{p}}^1 \\ (\varepsilon \underset{\mathbb{Z}}{\otimes} z) & \mapsto & i(\varepsilon) \underset{\mathbb{Z}_p}{\otimes} z \end{array}$$

[5]Lorsque K est un corps de nombres réel abélien, on dit que $\prod_{\mathfrak{p}|p} U_{\mathfrak{p}}^{(1)}$ est le groupe des unités "semi-locales".

Notant $i_{\mathbb{Z}_p} := i \otimes Id_{\mathbb{Z}_p}$, on obtient finalement que le plongement i induit par extension des scalaires à $\mathbb{Z}_p$, l'homomorphisme canonique :

$$\begin{array}{rcl} i_{\mathbb{Z}_p} : E_K^{(1)} \underset{\mathbb{Z}}{\otimes} \mathbb{Z}_p & \rightarrow & \prod_{\mathfrak{p}|p} U_{\mathfrak{p}}^{(1)} := \mathcal{U}_p^{(1)} \\ \varepsilon \otimes z & \mapsto & i(\varepsilon)^z \end{array}$$

L'idée intuitive qui nous conduit alors à penser que $i_{\mathbb{Z}_p}$, comme i dont elle provient, est encore injective constitue le résultat prédit par la conjecture de Leopoldt.
En d'autres termes, on pose :

$$\begin{array}{rcl} rg_{\mathbb{Z}}(E_K^{(1)}) & = & r_1 + r_2 - 1 \\ rg_{\mathbb{Z}_p}(\overline{E_K^{(1)}}) & = & (r_1 + r_2 - 1) - \delta(K,p), \quad \delta \in \mathbb{N}. \end{array}$$

et l'on conjecture $\delta(K,p) = 0$.

Voici donc résumé en quelques lignes le contenu de la conjecture. Pour être tout à fait rigoureux, on devrait parler de conjecture de Leopoldt *généralisée* ; en effet cette dernière a été énoncée sous sa forme initiale (1962) en terme de non-nullité d'un certain régulateur pour une classe de corps bien particulière, à savoir les corps de nombres totalement réels (i.e. pour lesquels $r_2 = 0$).

Les outils

Notion de Régulateur p-adique d'un corps de nombres :

1. *Le cas classique* (Le contexte est celui du théorème de structure des unités de Dirichlet)

   On considère K un corps de nombres et pour $r = r_1 + r_2 - 1$, on se donne $\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_r$ un système de r unités indépendantes de K.
   Soient maintenant $(\sigma_i)_i$ la famille des (r_1+2r_2) plongements canoniques de K dans $\mathbb{C}$ où :

   $$\sigma_i, \quad 1 \leq i \leq r_1 \quad \text{correspondent aux plongements réels}$$

   $$\sigma_i, \overline{\sigma_i} \quad r_1 + 1 \leq i \leq r_1 + r_2 \quad \text{désignent les plongements complexes}$$

   On introduit enfin la normalisation :

   $$\begin{array}{rcl} \delta_i & = & 1 \quad \text{si } \sigma_i \text{ est réel} \\ \delta_i & = & 2 \quad \text{sinon} \end{array}$$

et l'on définit :

$$\mathcal{R}_K(\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_r) := |det(\delta_i \; log|\varepsilon_j^{\sigma_i}|)_{1 \leq i,j \leq r}|$$

Définition 4.1.2. *Si* $\{\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_r\}$ *est une base du groupe des unités de* K *modulo les racines de l'unité, on appelle régulateur de* K *la quantité* $\mathcal{R}_K := \mathcal{R}_K(\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_r)$.

Conséquence :
Le théorème des unités de Dirichlet peut s'énoncer comme suit :

Théorème 4.1.3. *Pour tout corps de nombres* $K/\mathbb{Q}$*, on a :* $\mathcal{R}_K \neq 0$.

La définition du régulateur d'un corps de nombres K offre la possibilité d'illustrer le principe directement tiré de l'interprétation de la formule du produit selon lequel toutes les valeurs absolues sur K ont une contribution (un poids) équivalente ; aussi si l'on se souvient que les places de $\mathbb{Q}$ sont en bijection avec l'ensemble $\infty, 2, 3, \cdots$, il est naturel de vouloir concrétiser cette idée de symétrie en définissant la notion de régulateur p-adique.

2. *Généralisation au cas p-adique (p nombre premier fixé)*

On suppose pour simplifier que K est un corps de nombres totalement réel de degré n et l'on désigne par $(\sigma_i)_i$ une famille de $(n-1)$ $(= r_1 - 1)$ plongements de K dans $\mathbb{C}_p$.

Définition 4.1.4. *Etant donné* $\{\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_{n-1}\}$ *un système d'unités fondamentales de* K*, on appelle* régulateur p-adique de K *la quantité :*

$$\mathcal{R}_{K,p}(\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_{n-1}) := det(log_p(\sigma_i(\varepsilon_j))_{1 \leq i,j \leq n-1}).$$

En toute rigueur, cette définition n'est pas entièrement satisfaisante et recèle quelques ambigüités ; en particulier, une modification de l'ordonnancement des σ_i peut introduire un facteur (-1).

Remarque : A propos du logarithme p-adique log_p...
Pour tout corps local $K_\mathfrak{p}$ (i.e. toute extension finie de $\mathbb{Q}_p$), on sait définir de manière unique une application :

$$log_p : K_\mathfrak{p}^\times \to K_\mathfrak{p}$$

dite "logarithme p-adique" satisfaisant à la condition de normalisation $log_p(p) = 0$ et à l'équation fonctionnelle : $log_p(xy) = log_p(x) + log_p(y)$. On étend naturellement cette définition à $\overline{\mathbb{Q}_p}$ puis par continuité en une fonction

$$log_p : \mathbb{C}_p^\times \to \mathbb{C}_p$$

Plus précisément, on énonce sous forme de proposition le résultat suivant :

Proposition 4.1.5. *Il existe une unique extension de log_p à $\mathbb{C}_p^\times$ satisfaisant :*

1. $log_p(p) = 0$
2. $log_p(xy) = log_p(x) + log_p(y),\ \forall\ x, y\ \in\ \mathbb{C}_p^\times$

À ce stade on dispose de tous les outils permettant d'énoncer le résultat suivant qui constitue la version initiale de la conjecture de Leopoldt :

Théorème 4.1.6. *Etant donné K un corps totalement réel (i.e. $r_2 = 0$), on a l'équivalence :*

$$\mathcal{R}_p(K) \neq 0 \Leftrightarrow \textit{le } \mathbb{Z}_p\textit{-rang de } \overline{E_K^{(1)}} \textit{ est exactement } r = r_1 - 1.$$

Corollaire 4.1.7. *Si $K/\mathbb{Q}$ est une extension abélienne alors le $\mathbb{Z}_p$-rang de $\overline{E_K^{(1)}}$ est égal au nombre de Dirichlet $r = r_1 + r_2 - 1$.*

Pour déduire ce corollaire du théorème précédent on utilise le résultat suivant :

$$K/\mathbb{Q} \text{ abélienne} \Rightarrow \mathcal{R}_p(K) \neq 0$$

qui se démontre grâce à un résultat profond généralement connu sous le nom de théorème de Brumer (1967), traduction p-adique d'un théorème de transcendance de Baker et qui s'énonce comme suit :

Théorème 4.1.8. *(Baker-Brumer) Soient $\{\alpha_1, \alpha_2, \cdots, \alpha_n\}$ des éléments de $\mathbb{C}_p$ tels que $\{log_p(\alpha_1), log_p(\alpha_2), \cdots, log_p(\alpha_n)\}$ soient linéairement indépendants sur le corps de rationnels alors ils le sont encore sur $\overline{\mathbb{Q}}$, où $\overline{\mathbb{Q}}$ désigne la clôture algébrique de $\mathbb{Q}$ dans $\mathbb{C}_p$.*

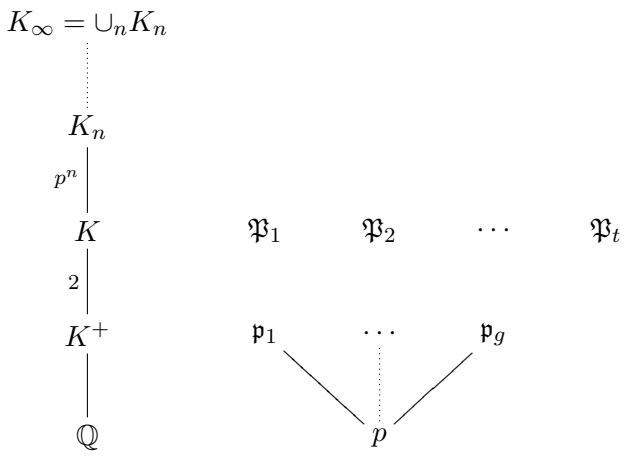
Dans [20], Greenberg utilise pour terminer la preuve qui permet de conclure au caractère semi-simple de la $\mathbb{Z}_p$-extension cyclotomique une argumentation en tout point semblable dont la clé est comme ci-dessus le théorème d'indépendance p-adique.

4.1.3 L'article de Greenberg

Contexte

On désigne par :
- p un nombre premier fixé
- K un corps de nombres totalement imaginaire (c'est-à-dire une extension quadratique d'un corps totalement réel) supposé abélien (en particulier, K satisfait la conjecture de Leopoldt)
- K^+ son sous-corps réel maximal
- g le nombre de places de K^+ au-dessus de p
- s le nombre de tels premiers qui se décomposent dans K (i.e. $s =$ 0 ou g).

– et enfin $K_\infty := \cup_n K_n$ la $\mathbb{Z}_p$-extension cyclotomique associée à K.



Dans toute la suite, on supposera $s = g$. En outre, on remarque qu'en vertu de la relation $B = \cup_{n\geq 1} i_n(B_n)$ où l'on a posé $B_n := A_n^\Gamma$ on est ramené, pour prouver que l'ordre de B est borné, à justifier que B_n satisfait cette propriété pour n suffisamment grand.

Préliminaires : le cas totalement réel

On se donne K un corps de nombres (que l'on supposera plus loin abélien et totalement réel[6]) et l'on note K_∞/K la $\mathbb{Z}_p$-extension cyclotomique associée de groupe de Galois $\Gamma =< \gamma >$ où γ désigne un générateur topologique supposé fixé. On désigne par γ_n la restriction de ce dernier au n-ième étage K_n de la tour d'extensions sous-jacente et l'on pose :

– L la p-extension abélienne non-ramifiée maximale de K
– L_n la p-extension abélienne non-ramifiée maximale de K_n
– L'_n l'extension abélienne maximale de $K \subseteq L_n$
(en particulier, $L'_n \cap K_\infty = K_n$ pour $n \gg 0$)
– F la p-extension abélienne p-ramifiée [7] maximale de K ($F \supseteq L'_n$)

Stratégie : La théorie du corps de classes nous permet de reformuler le problème en interprétant l'ordre $|B_n| = (A_n : A_n^{\gamma-1})$ comme le degré de l'extension L'_n/K_n ; ainsi donc on est ramené à prouver que $[L'_n : K_n]$ est borné

[6] On peut supposer plus généralement que K vérifie la Conjecture de Leopoldt, ce qui est en particulier vrai lorsque K est abélien.

[7] Une extension est dite "p-ramifiée" lorsqu'elle est non-ramifiée aux places finies étrangères à p. La famille des $\mathbb{Z}_p$-extensions de corps de nombres en est un exemple.

à partir d'un certain rang.

On a vu, à l'occasion de la présentation de la conjecture de Leopoldt, que le $\mathbb{Z}_p$-rang du groupe $\overline{E_K^{(1)}}$ pouvait se mettre sous la forme :

$$(r_1 + r_2 - 1) - \delta(K, p)$$

où $\delta(K,p) \in \mathbb{N}$ désigne le "défaut de Leopoldt". Il suit de ce rappel que le $\mathbb{Z}_p$-rang du quotient $Z := \dfrac{\prod_{\mathfrak{p}|p} U_{\mathfrak{p}}^{(1)}}{\overline{E_K^{(1)}}}$ vaut exactement $r_2 + 1 + \delta(K,p)$ or par la théorie du corps de classes, on a l'isomorphisme : $Z \simeq Gal(F/L)$ d'où l'on déduit :

$$\begin{aligned} rg_{\mathbb{Z}_p}(Gal(F/L)) &= rg_{\mathbb{Z}_p}(Gal(F/K)) \\ &= r_2 + 1 + \delta(K,p) \end{aligned}$$

Dans le cas qui nous intéresse où K est *totalement réel* (i.e. $r_2 = 0$) et *abélien* ($\delta(K,p) = 0$), on obtient :

$$Gal(F/K) \simeq \mathbb{Z}_p \times T$$

avec T un groupe fini.

En particulier, la théorie de Galois donne $[F : K_\infty] < \infty$.

De l'inclusion $L'_n \subseteq F$, on déduit la suite d'égalités :

$$[L'_n : K_n] \underset{n \gg 0}{=} [L'_n : L'_n \cap K_\infty] \underset{\text{Noether}}{=} [L'_n K_\infty : K_\infty] \leq [F : K_\infty]$$

d'où le résultat.

Le cas totalement imaginaire : stratégie

Pour justifier la démarche qui consiste à relier l'énoncé la Conjecture de Gross généralisée à un critère de semi-simplicité, on se propose de mettre en évidence une correspondance entre les objets qu'introduit Greenberg pour organiser sa preuve et la formule des classes ambiges que nous avons rappelée par exemple à l'occasion du chapitre 3. Dans un premier temps, l'auteur introduit le produit :

$$\mathcal{L}_i := \prod_{\mathfrak{L}_i | \mathfrak{P}_i} \mathfrak{L}_i$$

pris sur l'ensemble des relèvements dans K_n de l'idéal $\mathfrak{P}_i$ de K pour $1 \leq i \leq t$ puis considère naturellement le sous-groupe de A_n et d'indice fini dans B_n, noté D_n, constitué des classes d'idéaux construites à partir des idéaux de

la forme $\prod_{i=1}^{t} \mathcal{L}_i^{a_i}$, ce qui revient en d'autres termes à "éliminer", parmi les idéaux ambiges (ou classes ambiges), les classes d'ambiges c'est-à-dire celles provenant de classes d'idéaux de K pour ne retenir, si elles existent, que celles non-triviales et qui nous préoccupent... Cela précisé, on consigne dans la suite et de manière synthétique les différentes étapes qui conduisent au résultat exposé dans [20].
Conformément au travail conduit à l'occasion des préliminaires dans le cas totalement réel, on ne retiendra dorénavant des objets à considérer que la partie "moins" associée (à savoir, celle sur laquelle l'action de la conjugaison complexe $\tau \in Gal(K/K^+)$ n'est pas triviale).

1. **Première étape** : On rappelle que le but est de prouver que l'action du groupe profini Γ sur V_0 (ici V_0^-) est semi-simple et pour ce faire, il est suffisant de justifier que l'on dispose de l'égalité :
   $(\gamma-1)V^- = (\gamma-1)^2V^-$ et donc, en terme de cardinal, que $\mid \dfrac{(\gamma-1)X^-}{(\gamma-1)^2X^-} \mid$ est fini.

   – *Réductions* :
   (a) Comme on a posé : $X^- = \widehat{A^-}$ et $B^- = (A^-)^\Gamma$ (où $\widehat{\cdot}$ désigne la dualité de Pontrjagin), il suffit de voir que $(A^-/B^-)^\Gamma$ est fini.
   (b) En outre $A := \varinjlim A_n$, aussi par un procédé classique précédemment évoqué, on se restreint à montrer que l'ordre de $(A_n^-/B_n^-)^{\Gamma_n}$ reste borné lorsque $n \to \infty$.
   (c) Enfin, en vertu de l'inclusion $D_n^- \subseteq B_n^-$ avec $(B_n^- : D_n^-)$ borné, on est ramené à prouver que l'ordre de $(A_n^-/D_n^-)^{\Gamma_n}$ est borné lorsque n devient arbitrairement grand.
2. **Deuxième étape** : On introduit l'ensemble :
   $$H_n := \{\alpha \in K_n |\ \alpha^{1+\tau} = 1 \text{ et } (\alpha) = \text{un produit des } \mathcal{L}_i\}$$
   i.e.,
   $$H_n := \{\alpha \in K_n |\ N_{K/K^+}(\alpha) = 1 \text{ et } (\alpha) = \text{un produit des } \mathcal{L}_i\}$$
   Il s'agit d'un sous-groupe du groupe des p-unités de K_n (i.e., des unités au-dessus de p) qui coïncide avec le groupe des p-unités imaginaires de K_n si l'on suppose que les places $\mathfrak{P}$, $1 \leq i \leq t$ de K au-dessus de p sont totalement ramifiées dans K_n. L'objectif est alors de décrire $(A_n^-/D_n^-)^{\Gamma_n}$ au moyen de H_n.
3. **Troisième étape** : On introduit :
   $$M_n := \{c \in A_n^- \text{ tels que } c^{\gamma-1} \in D_n^-\}$$

qui satisfait $M_n/D_n^- = (A_n^-/D_n^-)^{\Gamma_n} \supseteq M_n/B_n^-$ et permet de définir (voir[20]) un homomorphisme,

$$\varphi : M_n \to H_0/N_{n,0}(H_n)$$

tel que :

$$\begin{aligned} B_n^- &\subseteq Ker(\varphi) \\ Im(\varphi) &\subseteq \frac{H_0 \cap N_{n,0}(K_n^\times)}{N_{n,0}(H_n)} \end{aligned}$$

Du théorème de factorisation des homomorphismes, on déduit le diagramme suivant :

$$\begin{array}{ccc} M_n & \xrightarrow{\varphi} & Im(\varphi) \\ \downarrow & \nearrow & \\ M_n/B_n^- & & \end{array}$$

Conséquence : on est ainsi ramené à prouver que l'indice normique $(H_0 \cap N_{n,0}(K_n^\times) : N_{n,0}(H_n))$ est borné.

– Réductions :

(a) On se propose de montrer que $(H_0 \cap N_{n,0}(K_n^\times) : H_0^{p^n})$ est borné.

(b) Si l'on note $\mathcal{K}_i, i \geq 0$ (fini) le corps de décomposition de l'un des premiers de K_i au-dessus de p (en particulier $\mathcal{K}_i$ est le plus grand sous-corps de K_i dans lequel p se décompose totalement), Greenberg justifie qu'il est alors suffisant de démontrer que l'indice $(\mathcal{H}_0 \cap N_{n,0}(\mathcal{K}_n^\times) : \mathcal{H}_0^{p^n})$ reste borné.

4. **Quatrième étape** : On suppose dorénavant que K ($\equiv \mathcal{K}$) est un corps de nombres totalement imaginaire, abélien de degré $2g$ et dans lequel p (l'idéal $p\mathbb{Z}$) est totalement décomposé i.e. :
$\forall \ \mathfrak{P}|p$, $e_{\mathfrak{P}/p} = f_{\mathfrak{P}/p} = 1$ (comme conséquence, on a que toutes les places de K au-dessus de p sont totalement ramifiées dans K_∞). Le raisonnement (local) à venir est en tout point à rapprocher de celui exhibé plus haut lors de la présentation de la conjecture de Leopoldt ; ainsi, on introduit le $\mathbb{Z}_p$-module $\mathcal{U} := \prod_{\mathfrak{P}|p} U_{\mathfrak{P}} = U_p^g$ où U_p désigne le groupe des unités p-adiques. En particulier, on dispose de l'isomorphisme de $\mathbb{Z}_p$-module suivant :

$$\mathcal{U} \simeq \mathbb{Z}_p^g \times T$$

avec T fini (donc de $\mathbb{Z}_p$-rang nul) et l'on note ψ l'application :

$$\psi : H_0 \hookrightarrow \mathcal{U}$$

dont on vérifie qu'elle est injective.
En outre, on montre que $\eta \in N_{n,0}(K_n^\times) \Leftrightarrow \psi(\eta) \in \mathcal{U}^{p^n}$ d'où l'on déduit l'égalité indicielle :

$$(H_0 \cap N_{n,0}(K_n^\times) : H_0^{p^n}) = (\psi(H_0) \cap \mathcal{U}^{p^n} : \psi(H_0^{p^n})) \quad (*)$$

Reste donc à montrer que $(*)$ est borné lorsque $n \to \infty$.
On pose alors $H := \psi(H_0)$ et l'on désigne par $\overline{H}$ l'adhérence de H dans $\mathcal{U}$. De ce fait, $\overline{H}$ admet une décomposition sous la forme : $\mathbb{Z}_p^{s'} \times T'$ avec T' un groupe fini et $s' \leq s$. Pour conclure, reste à remarquer que l'indice $(H \cap \mathcal{U}^{p^n} : H^{p^n})$ est borné *si et seulement si* $s = s'$; on est ainsi ramené à prouver que si s $(= g)$ éléments sont indépendants sur H alors, ils le sont encore sur $\overline{H}$ c'est-à-dire "p-adiquement" et ceci découle de l'utilisation du théorème de Baker-Brumer rappelé plus haut.

Conclusion :

On introduit au rang $n \geq 0$ le mécanisme de correspondance suivant :

$$\begin{array}{rcl}
\textit{Greenberg} & \longleftrightarrow & \textit{Formule des classes ambiges} \\
H_n & \longleftrightarrow & E_{n,S} \\
(H_0 : N_{n,0}(H_n)) & \longleftrightarrow & (E_{0,S} : N_{K_n/K_0}(E_{n,S})) \quad \text{(numérateur)} \\
(H_0 : H_0 \cap N_{n,0}(K_n^\times) & \longleftrightarrow & (E_{0,S} : E_{0,S} \cap N_{K_n/K_0}(K_n^\times)) \quad \text{(dénominateur)} \\
|\dfrac{H_0 \cap N_{n,0}(K_n^\times)}{N_{n,0}(H_n)}| \text{ borné} & \longleftrightarrow & (E_{0,S} \cap N_{K_n/K_0}(K_n^\times) : N_{K_n/K_0}(E_{n,S})) \sim 1 \\
 & \longleftrightarrow & \mathcal{C}_{K_\infty,S}(p)^\Gamma \text{ fini} \\
 & \longleftrightarrow & \text{Conjecture de Gross } \textit{généralisée} \quad \text{(à définir)}
\end{array}$$

*Remarque** : Des exemples de non-semi-simplicité pour des $\mathbb{Z}_p$-extensions de corps abéliens *non-cyclotomiques* ont été construits indépendamment par Jaulent et Kisilevsky.

4.1.4 La conjecture de Gross généralisée

Le contexte est celui décrit dans l'article de Jaulent et Sands : "*Sur quelques modules d'Iwasawa semi-simples*" à savoir : K un corps de nombres, p un nombre premier et $K_\infty = \cup_{n\in\mathbb{N}} K_n$ une $\mathbb{Z}_p$-extension de K. On fixe γ un générateur topologique du groupe procyclique $\Gamma = Gal(K_\infty/K)$ et l'on désigne par Λ l'algèbre d'Iwasawa associée. Le contexte étant celui des corps de nombres, on rappelle que le groupe de Galois $\mathcal{C}_{K_\infty}$ de la pro-p-extension abélienne non-ramifiée maximale C_∞ de K_∞ est un Λ-module noethérien de

torsion [8]. On dispose donc d'un pseudo-isomorphisme :

$$\mathcal{C}_{K_\infty} \sim \oplus_P (\oplus_{i=1}^{n_P} \Lambda / P^{\nu_{Pi}} \Lambda)$$

où l'on a vu lors du chapitre 2 que P parcourt l'ensemble des idéaux de hauteur 1 de Λ, la quantité n_P mesure quant à elle le nombre de P-facteurs et les ν_{Pi} constituent pour chaque P une suite décroissante d'entiers naturels non-nuls. En outre, si

$$F_{\mathcal{C}_{K_\infty},\gamma} = \prod_{n_P \neq 0} \prod_{i=1}^{n_P} P^{\nu_{Pi}}$$

représente le polynôme caractéristique associé au Λ-module $\mathcal{C}_{K_\infty}$, son diviseur,

$$\mathcal{M}_{\mathcal{C}_{K_\infty},\gamma} = \prod_{n_P \neq 0} P^{\nu_{P1}}$$

est appelé "*polynôme minimal*" dudit module, c'est-à-dire le plus petit polynôme Q de l'anneau factoriel $\mathbb{Z}_p[\gamma - 1]$ pour lequel le module $\mathcal{C}_{K_\infty}^Q$ (notation multiplicative) est fini i.e. pseudo-nul.
On dit que $\mathcal{C}_{K_\infty}$ est *semi-simple* (respectivement semi-simple en P), lorsque $\mathcal{M}_{\mathcal{C}_{K_\infty},\gamma}$ est sans facteur carré (respectivement lorsque P^2 ne divise pas $\mathcal{M}_{\mathcal{C}_{K_\infty},\gamma}$ c'est-à-dire lorsque ν_{P_1} vaut 1 pour $n_P > 0$).
Le cas le plus porteur en termes d'informations arithmétiques est celui où le polynôme distingué P n'est autre qu'un polynôme cyclotomique (on a rappelé à l'occasion du chapitre 2 le rôle fondamental joué par cette famille en théorie d'Iwasawa), c'est-à-dire un polynôme de la forme :

$$\begin{aligned} \omega_0 &= \gamma - 1 \text{ si } n = 0 \\ \omega_n &= \frac{\gamma^{p^n} - 1}{\gamma^{p^{n-1}} - 1} = \gamma^{p^{n-1}(l-1)} + \cdots + \gamma^{p^{n-1}} + 1 \quad \text{sinon} \end{aligned}$$

En effet, le quotient $\mathcal{C}_{K_\infty}/\mathcal{C}_{K_\infty}^{\omega_n}$ s'interprète alors à l'aide de la théorie des genres ; ainsi, si K_n désigne le sous-corps de K_∞ fixé par γ^{p^n}, le quotient $\mathcal{C}_{K_\infty}/\mathcal{C}_{K_\infty}^{\gamma^{p^n}-1}$ est isomorphe au groupe de Galois de la sous-extension maximale de C_∞ qui est abélienne sur K_n et par conséquent sa détermination relève de la théorie des Genres (voir fin du chapitre 3). Si l'on s'en tient à ce contexte, le premier résultat de semi-simplicité a été celui obtenu par Greenberg évoqué lors du paragraphe précédent, raffiné par la suite dans les travaux de L.J. Federer et B. H. Gross. Notre but dans les quelques lignes à suivre est de suggérer comment l'on peut justement traduire "la" conjecture de Gross en terme de semi-simplicité ...

[8] Dans le cas où K_∞ est une $\mathbb{Z}_p$-extension géométrique de corps de fonctions, le groupe de Galois associé à la pro-p-extension abélienne non-ramifiée maximale est isomorphe à $\mathbb{Z}_p \times X_\infty$ où X_∞ est un Λ-module de torsion sous l'hypothèse FRP.

On s'intéresse à la filtration du Λ-module $\mathcal{C}_{K_\infty} = \varprojlim_n(\mathcal{C}_{K_n})$ associée aux noyaux (respectivement co-noyaux) itérés de la multiplication par T ($\leftrightarrow \gamma - 1$) et l'on garde en tête que les classes d'idéaux ambiges sont de deux types : celles provenant de classes d'ambiges (i.e. de classes d'idéaux étendus) et les autres.
Ce que l'on souhaite pour conclure ou non à la semi-simplicité, c'est déterminer la puissance de T qui intervient dans le polynôme minimal, c'est-à-dire la valuation T-adique $v_T(\mathcal{M}_{\mathcal{C}_{K_\infty},\gamma})$. La stratégie peut être décrite en termes très simples ; on commence, si cela est possible, par mettre T en facteur dans le polynôme minimal (à ce stade $v_T(\mathcal{M}_{\mathcal{C}_{K_\infty},\gamma}) \geq 1$) et l'on s'intéresse au facteur restant en se demandant s'il ne serait pas lui-même factorisable par T. Si oui, $v_T(\mathcal{M}_{\mathcal{C}_{K_\infty},\gamma}) \geq 2$ et il est inutile de poursuivre car l'on est dès lors assuré de la non-semi-simplicité en T. Arithmétiquement parlant, la première étape consiste à s'intéresser au sous-groupe ambige $Cl_{K_n}^{\Gamma_n}$ que l'on approche dans un premier temps par les classes d'ambiges à savoir les éléments de $Cl_{K_n}(S)$ où S désigne l'ensemble des places totalement ramifiées. Dans un deuxième temps, on cherche s'il existe des classes ambiges autres que celles, naturelles, provenant des idéaux ambiges et pour ce faire on forme le quotient : $Cl_{K_n}^S := Cl_{K_n}/Cl_{K_n}(S)$. On déduit alors du caractère borné de la suite des $(Cl_{K_n}^S)^{\Gamma_n}$ l'assertion de semi-simplicité. On énonce :

Conjecture de Gross généralisée (Jaulent) : *Lorsque S désigne l'ensemble des p-places (i.e. au-dessus de p, les seules susceptibles de se ramifier dans une $\mathbb{Z}_p$-extension de corps de nombres) et K_∞/K est la $\mathbb{Z}_p$-extension cyclotomique, le cardinal de $(Cl_{K_n}^S)^{\Gamma_n}$ est borné $\forall$ n.*

C'est en nous référant à ce nouvel aspect de la Conjecture de Gross que nous allons essayer d'aborder le cas des corps de fonctions...

4.2 La méthode des φ-composantes : heuristique

Comme nous l'avons suggéré à l'occasion du chapitre 3, nous souhaiterions aborder la question formulée par Villa et Madan par un chemin détourné de sorte d'essayer de nous affranchir d'un formalisme calculatoire à ce point exigeant que contre toute attente il s'avère une obstruction au caractère pressenti effectif de la méthode employée. Malheureusement, nous ne sommes pas parvenu à obtenir un résultat pleinement satisfaisant et/ou "exempt" d'une certaine technicité et c'est la raison pour laquelle nous consacrons quelques lignes d'introduction à l'exposition de la stratégie que nous nous proposons de suivre par la suite.
Comme cela est souvent le cas en théorie des nombres (mais des méthodes similaires sont employées en géométrie différentielle par exemple), on pense

devant un objet un peu récalcitrant à faire appel au Principe *"Local-Global"* que nous avons utilisé à maintes reprises dans le contexte particulier des S-unités et qui consiste à "découper" un être mathématique (dans le cas qui nous préoccupe : suivant des caractères irréductibles φ), en étudier les composantes (φ-composantes...) avant de les rassembler (ou de les "relever") pour obtenir une description que l'on espère raisonnable de l'objet de départ. Un exemple, peut-être élémentaire mais finalement très parlant car nous le suivrons à la lettre, concerne la réduction des endomorphismes telles qu'elle est présentée dans le second cycle. Étant donnés k un corps supposé commutatif, V un k-espace vectoriel de dimension finie n et f un k-endomorphisme de V, on dote ce dernier d'une structure de module sur l'anneau principal $k[X]$ selon :

$$\begin{array}{rcl} k[X] \times (V,+) & \to & V \\ (P(X), v) & \mapsto & P.v := P(f)(v) \end{array}$$

où si $P(X) = \sum_{i=0}^{n} a_i X^i$, $P(f) = a_0 Id_V + a_1 f + ... + a_n f^n$ désigne le polynôme associé à l'endorphisme f. Muni de cette action de X sur V, V est un $k[X]$-module de type fini de torsion et admet en tant que tel (conséquence du théorème de la base adaptée) une décomposition de la forme :

$$\pi : V \tilde{\to} \frac{k[X]}{Q_1} \times \frac{k[X]}{Q_2} \times \cdots \times \frac{k[X]}{Q_r}$$

où $Q_1, Q_2, \cdots, Q_r \in k[X]$ sont des polynômes non-constants, unitaires satisfaisant la relation de divisibilité $Q_1 | Q_2 | \cdots | Q_r$. On dit que les polynômes Q_i ainsi définis sont les invariants de similitudes de f ; reste, $\forall\ 1 \leq i \leq r$, à définir $v_i \in V$ par : $\pi(v_i) = e_i := (0, \cdots, 0, 1, 0, \cdots, 0)$ et à poser

$$V_i := k[X]v_i = \{Q.v_i,\ Q \in k[X]\}$$

On vérifie alors que V_i est un $k[X]$-module isomorphe à $k[X]/Q_i$ d'annulateur $Q_i k[X]$ *stable par* f + ; par conséquent V admet la décomposition en somme directe $V \simeq \oplus_{i=1}^{r} V_i$. En outre, si l'on appelle n_i le degré de Q_i alors le système $\{v_i, f(v_i), \cdots, f^{n-1}(v_i)\}$ est une base de V_i comme k-espace vectoriel. Ainsi donc, caractériser l'endomorphisme f (par exemple : est-il diagonalisable ?) revient par restriction à regarder comment il se comporte sur chaque sous-espace V_i dit "caractéristique". Pour prolonger le parallèle avec la situation à laquelle nous confronter plus avant, précisons que là où l'on a projeté suivant les e_i, nous serons amenés à projeter suivant une famille d'idempotents orhogonaux indexés par des caractères irréductibles. Reste que cette opération de projection ne comporte pas toujours comme on le souhaiterait aussi pour pouvoir associer un foncteur exact à cette dernière et travailler dans des conditions agréables nous serons amener à nous placer dans un

cadre dit "semi-simple". A cet égard, on rappelle que si k est parfait, alors f est diagonalisable dans une extension L de k si et seulement si son polynôme minimal est sans facteur carré. Ces derniers (à savoir les endomorphismes diagonalisables) admettent une autre caractérisation sur laquelle nous reviendrons à savoir que f est diagonalisable *ssi* tout sous-$k[X]$-module W de V possède un supplémentaire S i.e. : $V = W \oplus S$. Un tel $k[X]$-module est alors dit *"semi-simple"*. Le pont est dressé ...

4.3 Histoire de caractères ... Quelques rappels

Étant donné un groupe fini G, on appelle "algèbre de groupe sur G à coefficients dans $\mathbb{Z}$", l'anneau dont les éléments sont les combinaisons linéaires formelles $\Sigma_{\sigma\in G} a_\sigma \sigma, a_\sigma \in \mathbb{Z}$, la somme de deux tels éléments étant définie composante par composante et le produit via la formule :

$$(\Sigma_{\sigma\in G} a_\sigma \sigma)(\Sigma_{\tau\in G} b_\tau \tau) = \Sigma_{\gamma\in G}(\Sigma a_\sigma b_\tau)\gamma.$$

Soit maintenant $\rho : G \to \mathrm{Aut}(V)$ où V désigne un groupe abélien alors V est naturellement doté d'une structure de $\mathbb{Z}[G]$-module via :

$$\begin{array}{rcl} \mathbb{Z}[G] \times V & \to & v \\ (\sum_{\sigma\in G} a(\sigma)\sigma, u) & \mapsto & \prod_{\tau\in G} (\sigma v)^{a(\sigma)} \end{array}$$

Bien entendu, on peut généraliser le contexte en ne supposant plus seulement que V est un groupe abélien mais un module sur un anneau commutatif R; dans ce cas,

$$\rho : G \to Aut_R(V)$$

ce qui signifie en particulier que les actions conjointes de G et R sur V commutent. Soit $f : G \to R^\times$ un homomorphisme de G dans le groupe des unités de R (ie des inversibles) que l'on peut étendre en un homorphisme d'anneaux via :

$$f(\sum_{\sigma\in G} a(\sigma)\sigma) = \sum_{\sigma\in G} a(\sigma) f(\sigma).$$

Réciproquement, étant donné un homomorphisme d'anneaux (ou plus précisément de R-algèbres), on obtient immédiatement par restriction à G un homomorphisme $G \to R^\times$. La mise en évidence d'une telle équivalence ouvre la voie de l'étude de la théorie des représentations de groupes dont nous ne faisons ci-après que rappeler quelques-uns des principes auxquels nous serons amenés à nous référer par la suite (pour plus de détails, on pourra consulter par exemple [11],[17] ou encore [62]).

Définition 4.3.1. *Étant donnés k un corps commutatif et G un groupe fini, on appelle* représentation de G *un homomorphisme $\rho : G \to GL(V)$ où V désigne un k-espace vectoriel de dimension finie.*

Exemple : Dans le cas particulier où l'on prend pour G un groupe fini d'ordre d tel que $(d,l)=1$ et V un $\mathbb{Q}_l$-espace vectoriel de dimension finie n, on parle pour $\rho_l : G \to Gl_n(\mathbb{Q}_l)$ de représentation l-adique.

Remarques :
1- La donnée d'une représentation d'un groupe G correspond à celle d'une action de groupe de G sur V définie selon :

$$\begin{array}{rcl} G \times V & \to & V \\ (g,v) & \mapsto & g.v := \rho(g)v \end{array}$$

à laquelle on impose en plus la linéarité des fonctions $\rho(g)$, c'est-à-dire à une structure de $k[G]$-module ... Cela semble de bonne augure au sens où l'on dispose pour l'algèbre de groupe $k[G]$ du théorème de structure suivant :

Théorème 4.3.2. *(Maschke) Soient G un groupe fini d'ordre d et k un corps commutatif tel que $(Car(k),d)=1$ alors $k[G]$ est semi-simple i.e. il admet une décomposition en somme directe de sous-modules simples).*

2- Une représentation d'un groupe G consistant en la donnée d'un espace vectoriel V, on appelle *dimension de la représentation*, la dimension du k-espace vectoriel associé.
3- Pour éviter les ennuis, on supposera dans toute la suite que k est soit un corps algébriquement clos de caractéristique zéro soit un corps algégriquement clos de caractéristique p tel que $(p,|G|)=1$. Ce faisant, nous retrouvons dans le cas où $R=k$ les hypothèses que nous avions formulées précédemment.

Définition 4.3.3. *Si ρ est une représentation du groupe G, on appelle* caractère associé à *ρ l'application*

$$\begin{array}{rcl} \varphi_V : G & \to & k \\ g & \mapsto & Tr(\rho(g)) \end{array}$$

En particulier, $\varphi_V(e) = dim_k(V)$ si e désigne l'élément neutre du groupe G.

Exemple : *La représentation triviale*
La représentation *triviale* d'un groupe G sur un espace vectoriel V est celle relative à l'application "triviale" :

$$\rho : G \to GL(V)$$

$$g \mapsto Id_V.$$

De l'identification $V=k$, on déduit qu'elle est de dimension 1 et l'on note φ_1 le caractère associé à ρ. On parle alors de caractère *unitaire* ; il satisfait

la relation suivante : $\varphi_1(g) = 1 \ \ \forall g \in \ G$.

Opérations sur les caractères-Définitions : Elles sont naturellement héritées des opérations pratiquées sur les espaces vectoriels et se répercutent sur les caractères qui leur sont associés.

1. Deux représentations $\rho : G \to GL(V)$ et $\mu : G \to GL(W)$ d'un même groupe G sont dites *équivalentes* s'il existe un isomorphisme $\theta : V \to W$ tel que :
$$\forall \ g \in \ G, \mu(g) \circ \theta = \theta \circ \rho(g)$$
En particulier, deux représentations équivalentes sont associées au même caractère.

2. *Notion de sous-représentation* : Soit (V, ρ) une représentation de G ; un sous-espace $W \subseteq V$ est dit *invariant par* ρ (ou par G indifféremment) si : $\forall g \in G, \rho(g)W \subseteq W$ (ce qui entraîne $\rho(g)W = W$). Cela a alors un sens de parler de la représentation ρ *restreinte* à W ; il s'agit de la représentation notée $\rho_{|W}$ de G dans W. On parle aussi pour une représentation restreinte à un sous-espace invariant de *sous-représentation.* De là découle la définition naturelle suivante :

   Définition 4.3.4. *Une représentation ρ de G est dite irréductible si les seuls sous-espaces vectoriels de V invariants par ρ sont $\{0\}$ et V. On qualifiera d'irréductible, le caractère associé à une représentation irréductible.*

3. *Somme directe de représentations* : Étant données (ρ_1, V_1), (ρ_2, V_2) des représentations de G, $\rho_1 \oplus \rho_2$:
$$\rho_1 \oplus \rho_2 : G \to GL(V_1 \oplus V_2)$$
est une représentation de G appelée *somme directe* de ρ_1 et ρ_2 telle que : $\rho_1 \oplus \rho_2(g)(v_1, v_2) = (\rho_1(g)(v_1), \rho_2(g)(v_2))$.
Le caractère associé $\varphi_{V_1 \oplus V_2}$ satisfait alors : $\varphi_{V_1 \oplus V_2}(g) = \varphi_{V1(g)} + \varphi_{V_2(g)}$.
Remarques :
- Une somme directe de représentations irréductibles n'est pas irréductible... En revanche, on qualifie de *complètement réductible* une représentation qui est la somme directe de représentations irréductibles et on appelle *caractère virtuel* une combinaison linéaire finie de caractères irréductibles.
- On peut définir par récurrence la somme directe de m représentations irréductibles. Si en outre, au sein de la somme ρ_1 est répétée s_1 fois, ρ_2 s_2 fois etc ..., on appelera s_i *la multiplicité* de ρ_i dans ρ.

4. *Produit tensoriel de représentations* : Étant données (ρ_1, V_1), (ρ_2, V_2) des représentations de G, on définit le produit tensoriel

$\rho_1 \otimes \rho_2 : G \to GL(V_1 \otimes V_2)$ de ces dernières via :

$$(\rho_1 \otimes \rho_2)(g)(v_1 \otimes v_2) = \rho_1(g)(v_1) \otimes \rho_2(g)(v_2).$$

En outre, le caractère associé à un produit tensoriel de représentations est le produit des caractères ie : $\varphi_{\rho_1 \otimes \rho_2}(g) = \varphi_{\rho_1}(g).\varphi_{\rho_2}(g)$.

5. *Représentations induites* : Soient G un groupe fini d'ordre d et H un sous-groupe de G ; on note $\rho : G \to GL(V)$ une représentation linéaire de G et $\rho_{|H}$ sa restriction à H au sens précédent.

   Définition 4.3.5. *On dit que la représentation ρ de G dans V est* induite *par la représentation ϑ de H dans W si V est égal à la somme directe des $W_\sigma, (\sigma \in G/H)$ ie : $V = \oplus_{\sigma \in G/H} W_\sigma$. Si l'on note $|H| = h$ et R le système de représentants de G/H, on a :*

$$\forall u \in G, \text{ on a} : \varphi_\rho(u) = \frac{1}{h} \sum_{s \in G} \varphi(s^{-1}us)$$

et réciproquement :

$$\varphi_\rho(u) = \sum_{r \in R} \varphi_\vartheta(r^{-1}ur)$$

Exemple (qui reviendra régulièrement dans la suite) :
On considère Δ un groupe fini d'ordre d réalisé comme le groupe de Galois d'une extension abélienne K/F d'un corps global (si F est de caractéristique p, on rappelle que $(d, p) = 1$). Étant donnée $\mathfrak{p}$ une place de F, on définit : $\Delta_\mathfrak{p} := \{\sigma \in \Delta \text{ tels que : } \sigma(\mathfrak{p}) = \mathfrak{p}\}$; il s'agit d'un sous-groupe (distingué) de $\Delta := Gal(K/F)$ appelé *groupe de décomposition* en $\mathfrak{p}$; il fixe le plus grand sous-corps de K/F dans lequel $\mathfrak{p}$ se décompose totalement.

On définit sur l'ensemble des caractères un produit scalaire selon :

$$< \varphi, \chi >= \frac{1}{|G|} \sum_{g \in G} \varphi(g^{-1})\chi(g)$$

grâce auquel on va pouvoir réaliser une relecture de certaines des propriétés évoquées plus haut.(grae à nos hypothèses $|G|$ est bien inversible ...)

Lemme 4.3.6. *(Orthonormalité des caractères) Si V_1 et V_2 sont des représentations irréductibles de caractères (irréductibles) respectifs φ_1 et φ_2 alors :*

1. $< \varphi_1, \varphi_2 >= 1$ *si V_1 et V_2 sont G-isomorphes.*
2. $< \varphi_1, \varphi_2 >= 0$ *sinon.*

On en déduit :

Proposition 4.3.7. *Si V est G-isomorphe à $\oplus V_i^{\oplus a_i}$ où les V_i désignent des représentations deux à deux irréductibles et non-G-isomorphes, alors :*

$$s_i = < \varphi_{V_i}, \varphi_V > \ < \varphi_V, \varphi_V > = \sum_i s_i^2.$$

Preuve (idée) : On utilise simplement la décomposition de φ_V selon $\varphi_V = \sum_i s_i \varphi_{V_i}$ puis on applique les relations d'orthogonalité.

avec pour conséquence :

Corollaire 4.3.8. *La représentation (ρ, V) est irréductible si et seulement si $< \varphi_V, \varphi_V >= 1$.*

Notion de φ-composantes :
On se place dans le contexte suivant, à savoir : G un groupe abélien fini d'ordre n, $\hat{G}$ le groupe des caractères associé, R un anneau intègre tel que : $n \in R^\times$ et il existe $r \in R$ non-nul d'ordre n. Pour φ un élément de $\hat{G}$, on définit e_φ l'élément de l'algèbre de groupe $R[G]$ tel que :

$$e_\varphi = \frac{1}{n} \sum_{\sigma \in G} \varphi(\sigma^{-1})\sigma$$

qui existe car l'on a pris soin de s'assurer que n était inversible ... Il est caractérisé par la proposition suivante :

Proposition 4.3.9. *On vérifie que :*

1. $\forall \sigma \in G, \sigma . e_\varphi = \varphi(\sigma) e_\varphi$
2. $\forall \varphi, \psi \in \hat{G}$, *on a :* $e_\varphi e_\psi = \delta(\varphi, \psi) e_\varphi$ *où* $\delta(\varphi, \psi) = 1$ *si* $\varphi = \psi$ *et* 0 *sinon.*
3. $\sum_{\varphi \in \hat{G}} e_\varphi = id_G$ *(idem dans $R[G]$)*
4. *Étant donnés* $\varphi, \psi \in \hat{G}$, *on a :* $\varphi(e_\psi) = \delta(\varphi, \psi)$
5. *L'ensemble* $\{e_\varphi | \varphi \in \hat{G}\}$ *est une R-base de $R[G]$.*

Conséquence-Définition : En vertu du point *2* , on dit que l'ensemble des $(e_\varphi)_{\varphi \in \hat{G}}$ constitue une famille *d'idempotents orthogonaux* pour l'algèbre de groupe $R[G]$. En outre lorsque, φ étant supposé fixé, l'idempotent e_φ associé satisfait l'égalité $e_\varphi . r = r . e_\varphi$, on dit de ce dernier qu'il est *central*. Enfin, on dira d'un idempotent e_φ non-trivial qu'il est *primitif* s'il ne peut s'écrire comme somme de deux idempotents (non-nuls) orthogonaux.

Remarque-Preuve : C'est l'usage répété des relations d'orthogonalité entre caractères qui est l'outil essentiel permettant de prouver cette suite de propriétés ; en outre, on déduit du point 1 l'isomorphisme $R[G]e_\varphi = Re_\varphi$, du point 3 que l'ensemble $\{e_\varphi | \varphi \in \hat{G}\}$ d'idempotents orthogonaux engendre le R-module $R[G]$, reste à tirer l'indépendance linéaire de la relation 2 pour obtenir la propriété fondamentale 5 qui va permettre, après une définition, d'énoncer le théorème de structure que l'on évoquait dans l'introduction :

Définition 4.3.10. *Étant donné $\varphi \in \hat{G}$, on définit :*

$$V(\varphi) := \{v \in V | \sigma v = \varphi(\sigma)v \; \forall \; \sigma \in G\}$$

Il s'agit d'un R-module appelé φ-composantes isotypique de V.

On retient :

Proposition 4.3.11. Sous les hypothèses précédentes, *le $R[G]$-module V est isomorphe à la somme directe de ses φ-composantes i.e. :*

$$V \simeq \oplus_{\varphi \in \hat{G}} V(\varphi)$$

Preuve :

- On commence par expliciter la structure de la φ-composante $V(\varphi)$ en justifiant l'égalité : $V(\varphi) = e_\varphi V(\varphi)$ (il s'agit de la projection de V sur l'idempotent e_φ.) Soit donc $v \in V$ auquel on associe l'élément $e_\varphi v$. De la propriété précédente (point 1), on déduit que $\sigma e_\varphi v = \varphi(\sigma) e_\varphi v$ pour tout $\sigma \in G$ d'où l'inclusion $e_\varphi V \subseteq V(\varphi)$. Réciproquement, si $v \in V(\varphi)$, alors :

  $$e_\varphi . v = \frac{1}{n} \sum_{\sigma \in G} (\varphi(\sigma^{-1})\sigma)v = \frac{1}{n} (\sum_{\sigma \in G} \varphi(\sigma^{-1})\varphi(\sigma))v = v,$$

  ainsi donc $V(\varphi) \subseteq e_\varphi V$ d'où le résultat.

- Le fait que V soit la somme de ses φ-composantes résulte maintenant de l'identité $v = \sum_{\varphi \in \hat{G}} e_\varphi v$ et il reste donc à s'assurer que cette dernière est *directe...*
  On suppose qu'à chaque caractère $\varphi \in \hat{G}$, on peut associer un élément $v_\varphi \in V(\varphi)$ tel que $\sum_{\varphi \in \hat{G}} v_\varphi = 0$ (But : montrer que cet élement est nul...). Pour tout $\psi \in \hat{G}$, on a :

  $$0 = e_\psi (\sum_{\varphi \in \hat{G}} v_\varphi) = \sum_{\varphi \in \hat{G}} e_\psi v_\varphi = \sum_{\varphi \in \hat{G}} e_\psi e_\varphi v_\varphi = e_\psi v_\psi = v_\psi$$

  où l'on a utilisé que l'idempotent e_φ agit comme l'identité sur la φ-composante de V.

Exemple d'application : On prend pour V l'anneau des entiers p-adiques $\mathbb{Z}_p$ et l'on considère Δ un groupe abélien d'ordre n inversible dans $\mathbb{Z}_p$ *ie* tel que $v_p(n) = 0$. L'algèbre de groupe $\mathbb{Z}_p[\Delta]$ ainsi formée admet d'après la discussion précédente une décomposition sous la forme : $\mathbb{Z}_p[\Delta] = \oplus_{\varphi\in\hat{\Delta}}\mathbb{Z}_p[\Delta]e_\varphi$ où $\hat{\Delta}$ désigne le groupe des caractères associé à Δ. En outre, si l'on désigne par M un $\mathbb{Z}_p[\Delta]$-module, alors la décompositon de M en φ-composantes est héritée de celle de $\mathbb{Z}_p[\Delta]$ selon : $M = \oplus_{\varphi\in\hat{\Delta}}M_\varphi$ avec $M_\varphi := Me_\varphi = M \otimes_{\mathbb{Z}} \mathbb{Z}_p[\Delta]e_\varphi$.
Enfin, le foncteur $M \to M_\varphi$ de la catégorie des $\mathbb{Z}_p[\Delta]$-modules est exact ; ainsi à une suite exacte de $\mathbb{Z}_p[\Delta]$-modules :

$$\cdots \to M \to N \to P \to \cdots$$

on associe de manière canonique la suite exacte de ses φ-composantes :

$$\cdots \to M_\varphi \to N_\varphi \to P_\varphi \to \cdots .$$

4.4 Le cas métabélien

4.4.1 Contexte

- Soit K un corps de fonctions sur $\mathbb{F}_q$ (où $q = p^\alpha$). Pour chaque entier naturel n, on définit K_n comme une extension cyclique de degré p^n de $K = K_0$ telle que :
  (i) $\forall\, n \in \mathbb{N},\ \ K_n \subset K_{n+1}$ avec $[K_{n+1} : K_n] = p$.
  (ii) Le corps des constantes de K_n est $k = \mathbb{F}_q$.
  (iii) $K_\infty = \bigcup_n K_n$.
  En d'autres termes, K_∞/K est un $\mathbb{Z}_p$-extension géométrique.

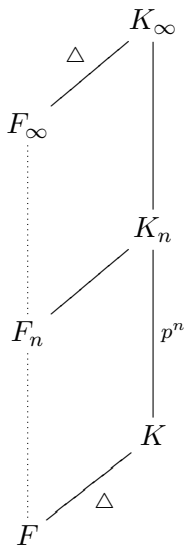
- On se donne S un ensemble fini de places ramifiées (on fera l'hypothèse par la suite que ces dernières le sont totalement).

- On désigne alors par $Cl^S_{K_n}$ le groupe des S-classes de diviseurs de K_n.

4.4.2 Principe de la généralisation du résultat obtenu par Salvador-Madan

On envisage, dans le but de raffiner le critère obtenu dans l'article de Villa-Madan de transporter la $\mathbb{Z}_p$-extension géométrique dans un cadre métabélien en lui adjoignant une extension *horizontale* K/F de degré d premier

à p, de groupe de Galois *abélien* Δ, suivant le schéma ci-dessous :



On suppose que K est une extension *abélienne* d'un corps de fonctions F (on prendra essentiellement pour F le corps des fonctions rationnelles $\mathbb{F}_q(x)$) de degré d premier à p et en outre que l'extension K_∞/F est *galoisienne*. Si l'on note G le groupe de Galois de K_∞/F et $\Gamma = \gamma^{\mathbb{Z}_p}$ celui associé à K_∞/K, on fera l'abus de langage qui consiste à désigner par Δ un relèvement de $Gal(K/F)$ dans G. Ceci précisé, le groupe G s'écrit alors comme le produit semi-direct $\Gamma \rtimes \Delta$. L'application,

$$\begin{array}{rcl} \kappa : \Delta \times \Gamma & \to & \Gamma \\ (\tau, \gamma) & \mapsto & \tau.\gamma = \tilde{\tau}\gamma\tilde{\tau}^{-1} \end{array}$$

qui définit ce dernier se factorise par un caractère p-adique de Δ, ω, selon :

$$\tau.\gamma.\tau^{-1} = \gamma^{\omega(\tau)},\ \forall\ \tau \in Gal(K_\infty/F_\infty) \simeq \Delta.$$

Ainsi donc, Γ et plus généralement les objets à considérer sont dotés d'une structure de $\mathbb{Z}_p[\Delta]$-module où $\mathbb{Z}_p[\Delta]$ est une algèbre galoisienne semi-locale, c'est en particulier le cas pour le groupe de classes $Cl^S_{K_n}$ qui retient notre attention et qui posséde de ce fait une structure de $\mathbb{Z}_p[\Delta]$-module et conjointement une structure de Λ-module.

Remarques :
1- On désigne par $\tilde{\tau}$ un relèvement de τ à G relativement à l'épimorphisme : $G \twoheadrightarrow \Delta$.
2- Le cas $d = 1$ nous replace dans le contexte étudié par Villa et Madan.

Stratégie : Intuitivement, l'intérêt de se placer dans un cadre métabélien réside dans le fait "d'adjoindre", via une extension horizontale (et donc un

groupe de Galois) une deuxième action grâce à laquelle on ne va plus être réduit à considérer le groupe de classes dans son ensemble mais en mesure, en utilisant les caractères de Δ, de le découper par tranche (φ-composantes) et d'étudier chacune d'entre-elles. Pour ce faire, il faut mettre en évidence une structure qui permettent de tenir compte des deux actions (c'est-à-dire pour le groupe de classes de deux structures de modules évoquées précédemment). Du point de vue de l'algèbre, on rappelle qu'étant donnés deux groupes finis Δ et N dont on considère le produit semi-direct $N \rtimes \Delta$, l'action de Δ sur N étant donnée par la conjugaison, on peut remplacer N par l'algèbre de groupe complexe $\mathbb{C}[N]$ et former ainsi un produit $\mathbb{C}[N] \rtimes \Delta$ comme précédemment ; l'algèbre ainsi obtenue peut être vue comme une somme de sous-espaces $\tau\mathbb{C}[N]$ où τ parcourt Δ. Il s'agit de l'algèbre de groupe de $N \rtimes \Delta$. Plus généralement, on peut remplacer $\mathbb{C}[N]$ par une algèbre A sur laquelle est définie une action de Δ pour obtenir ce que l'on appelle un produit croisé. Ainsi le produit croisé est la structure adaptée à la construction d'une algèbre de groupe dans le cas d'un produit semi-direct. Dans notre cas et de notre point de vue (à savoir celui de la théorie algébrique des nombres), N n'est pas un groupe fini mais un groupe *profini* cependant la stratégie reste valable et le candidat que nous retiendrons par la suite sera donc l'algèbre à produit croisé $\mathbb{Z}_p[[\Gamma]][\Delta]$.[9]

4.4.3 Définition de l'algèbre d'Iwasawa généralisée $\Lambda[\Delta]$:

On suppose fixé une fois pour toute l'élément γ tel que $\Gamma = \gamma^{\mathbb{Z}_p}$ et l'on considère la résolvante[10] θ :

$$\theta = \frac{1}{d} \sum_{\tau \in \Delta} \omega(\tau^{-1})(\gamma^{\omega(\tau)} - 1)$$

On peut alors montrer, via la relation de congruence :

$$\theta \equiv \gamma - 1 [(\gamma - 1)^2]$$

que l'algèbre formelle $\mathbb{Z}_p[[\theta]]$ ainsi construite s'identifie de manière canonique avec l'anneau d'Iwasawa $\Lambda = \mathbb{Z}_p[[\gamma - 1]]$ qui, en tant qu'anneau local, régulier et complet (!) est factoriel.
En particulier, l'élément θ engendre l'idéal $(\gamma - 1)\mathbb{Z}_p[[(\gamma - 1)^2]]$ de l'algèbre Λ.

[9] Historiquement, c'est à E. Noether que l'on doit, dans les années 30, l'introduction de la notion de produit croisé d'un corps avec son groupe de Galois, notion qui sera généralisée par la suite par Jacobson puis Bovdi dans les années 60.

[10] Fröhlich a développé des résolvantes plus générales (c'est-à-dire associées à une représentation de degré arbitraire et non plus seulement de degré 1) qui ont permis de généraliser les réultats obtenus par J. Martinet dans sa thèse avant en même temps qu'elles ont inspiré certains travaux de Ph. Cassou-Noguès et M.J. Taylor.

On dispose à ce stade des outils nous permettant de définir l'algèbre qui retiendra notre attention par la suite, à savoir :

$$\Lambda[\Delta] = \mathbb{Z}_p[\Delta][[\theta]] \simeq \mathbb{Z}_p[[\theta]][\Delta]$$

du groupe Δ à coefficient dans Λ "tordue" par la relation

$$\tau\gamma\tau^{-1} = \omega(\tau)\theta, \quad \forall\tau \in \hat{\Delta}.$$

En outre, l'algèbre $\mathbb{Z}_p[\Delta]$ est quant à elle une $\mathbb{Z}_p$-algèbre compacte semi-locale admettant pour système orthogonal la famille $(e_\varphi)_{\varphi\in\hat{\Delta}}$ des éléments :

$$e_\varphi = \frac{1}{d}\sum_{\tau\in\Delta}\varphi(\tau^{-1})\tau$$

pour φ un caractère p-adique irréductible.

Comme l'on a pris la précaution de supposer $(|\Delta|, p) = 1$, on est dans le cas "semi simple" et la décomposition semi-locale de $\mathbb{Z}_p[\Delta]$ s'écrit comme suit

$$\mathbb{Z}_p[\Delta] \simeq \oplus_\varphi \mathbb{Z}_p[\Delta]e_\varphi$$

où $\mathbb{Z}_p[\Delta]e_\varphi = Z_\varphi$ est une extension non- ramifiée de $\mathbb{Z}_p$ de degré $[Z_\varphi, \mathbb{Z}_p] = deg\varphi$. Cet abus de langage trouve sa justification dans le rappel suivant :

$$\mathbb{F}_p = \mathbb{Z}_p[\Delta]/p\mathbb{Z}_p[\Delta] \simeq \mathbb{F}_p[x]/(x^d - 1), \quad \text{si } d = |\Delta|.$$

Dans le cas où $p \nmid |\Delta|$, on dispose de la décomposition suivante de $\mathbb{F}_p[\Delta]$ comme somme directe d'algèbres simples :

$$\mathbb{F}_p[\Delta] \simeq \oplus_\varphi \mathbb{F}_p[\Delta]\bar{e}_\varphi$$

avec $\mathbb{F}_p[\Delta]\bar{e}_\varphi = F_\varphi$ où F_φ est un corps commutatif tel que :

$$[F_\varphi : \mathbb{F}_p] = d_\varphi = deg\varphi.$$

La résolvante θ possède cette propriété intéressante que son action "décale les φ composantes" au sens où :

$$\theta e_\varphi = e_{\varphi\omega}\theta.$$

Cette dernière nous permettra de comparer les φ - composantes d'un $\Lambda[\Delta]$-module M ; en effet, on a la proposition suivante :

Proposition 4.4.1. *Pour tout $\Lambda[\Delta]$-module M, l'opérateur θ donne bien lieu à une suite exacte de modules :*

$$0 \to e_\varphi Ker\theta \to e_\varphi M \xrightarrow{\theta} e_{\varphi\omega} M \to e_{\varphi\omega} Coker\theta \to 0$$

Conséquence : On applique ceci aux groupes de classes $Cl^s_{K_n}$, $n \in \mathbb{N}$, regardée comme $\Lambda[\Delta]$-modules puis à leurs limites inductives et projectives (cas procyclique). Vient alors la suite exacte suivante qui relie φ composantes, groupe des classes ambiges et quotient des genres :

$$1 \to (Cl^S_{K_n})^{\Gamma_n}_\varphi \hookrightarrow \left(Cl^S_{K_n}\right)_\varphi \xrightarrow{\theta} \left(Cl^S_{K_n}\right)_{\omega\varphi} \to {}^{\Gamma_n}\left(Cl^S_{K_n}\right)_{\omega\varphi} \to 1$$

Rappel-Stratégie :

On rappelle que l'interprétation (*une* interprétation) "arithmétique" de la propriété de la non-finitude du S-groupe de classes $(Cl^S_{K_\infty})^\Gamma$ caractérise un défaut de semi-simplicité en T ($\Leftrightarrow \gamma - 1$) du Λ-module $\mathcal{C}_{K_\infty}$ qui s'interprète, rappelons-le, comme le groupe de Galois de la p-extension abélienne non-ramifiée maximale de la $\mathbb{Z}_p$-extension K_∞/K. Plus précisément, $(Cl^S_{K_\infty})^\Gamma$ renseigne sur la présence de classes ambiges dites "exceptionnelles" au sens où elles ne proviennent pas de classes d'ambiges (i.e. de classes bâties à partir des idéaux de S étendus).
En d'autres termes, on dispose de la suite d'implications suivantes :

La propriété de semi-simplicité de $\mathcal{C}_{K_\infty}$ $\Rightarrow$ le quotient des genres et le groupe des classes ambiges sont des $\mathbb{Z}_p[\Delta]$-modules pseudo-isomorphes $\Leftrightarrow$ ces derniers définissent le même caractère.

et l'on raisonne par contraposition ...

Ainsi, après avoir établi la suite exacte des genres et celle des classes ambiges dans notre contexte, on se propose par application de la méthode des φ-composantes de comparer les caractères $\{{}^\Gamma\lambda^S, \lambda^{S\Gamma}\}$ associés pour déduire de condition sur leur différence des critères suffisants de *non-semi-simplicité* de $\mathcal{C}_{K_\infty}$ invalidant par la même la Conjecture de Gross (ou du moins sa version généralisée).

A propos de l'algèbre $\Lambda[\Delta]$:[11]

L'Algèbre d'Iwasawa usuelle Λ	Correspondance	l'Algèbre d'Iwasawa généralisée
On considère l'algèbre d'Iwasawa Λ définie à l'occasion du chapitre 2 via l'isomorphisme $\Lambda \simeq \mathbb{Z}_p[[\gamma - 1]]$ où γ désigne un générateur topologique fixé de $\Gamma \simeq \mathbb{Z}_p$ et l'on rappelle que pour la structure d'anneau sous-jacente, Λ est local, régulier, complet, de dimension de Krull égale à 2 (donc factoriel).	On introduit l'élément "résolvante" θ dont on vérifie qu'il est un générateur de l'algèbre Λ tel que $\theta \equiv \gamma - 1[(\gamma - 1)^2]$ et qui s'avère plus adapté à la définition du produit dans l'algèbre Σ en vertu de la relation de "quasi-commutation" : $\tau\theta\tau^{-1} = \chi(\tau)\theta$	On introduit l'algèbre de groupe $\Sigma := \mathbb{Z}_p[[\theta]][\Delta]$ à coefficient dans l'anneau complet $\mathbb{Z}_p[[\theta]]$ tordue par la relation : $$\tau\theta\tau^{-1} = \omega(\tau)\theta \ \ \forall\, \tau \in \Delta.$$ Il s'agit d'une algèbre *gauche* isomorphe au produit tensoriel $\mathbb{Z}_p[[\theta]] \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[\Delta]$ dont on peut préciser la structure via la décomposition irréductible : $$\Sigma = \oplus_{\phi \in Ind_H^\Delta} \Sigma e_\phi$$ où les idempotents centraux primitifs e_ϕ sont associés aux caractères p-adiques irréductibles du noyau $H = Ker\chi$. En particulier, comprendre Σ, c'est étudier le comportement de ses composantes ϕ-isotypiques $\Sigma_\phi := \Sigma e_\phi$.
Λ-modules de type fini	Λ_ϕ-modules de type fini (en effet, si X est un Σ_ϕ-module noethérien alors il s'agit en particulier d'un Λ_ϕ-module de type fini.)	Σ_ϕ-modules noethériens.
Les idéaux de hauteur 1 dans Λ sont exactement $\mathfrak{p} = (p)$ (ie ceux engendrés par l'uniformisante p associée à l'anneau des entiers p-adiques et $\mathfrak{p} = (F)$ où F désigne un polynôme de Weierstrass irréductible sur $\mathbb{Z}_p$.	...	Pour chaque caractère p-adique φ du groupe Δ, les sous-modules projectifs maximaux de Σ_φ sont regroupés en trois catégories : – l'idéal $p\Sigma_\varphi$ isomorphe à Σ_φ et engendré par l'uniformisante p de l'anneau Z_φ. – l'idéal engendré par la résolvante : $\theta\Sigma_\varphi$ isomorphe à $\Sigma_{\varphi\omega}$ via la relation : $\theta e_\varphi = e_{\varphi\omega}\theta$. – les idéaux associés aux polynômes distingués irréductibles de valuation nulle de l'algèbre gauche $Z_\varphi[\theta^{m_\phi}]$

[11] pour plus de détails, on pourra consulter [35].

Soit X un Λ-module de type fini, alors il existe des entiers $\rho, m, s \geq 0$ et $m_i, n_i \geq 1$ tels que X soit pseudo-isomorphe à un Λ-module élémentaire :

$$M \sim \Lambda^{\rho} \oplus (\bigoplus_{i=1}^{s} \Lambda/p^{n_i}) \oplus$$

$$(\oplus_{i=1}^{m} \Lambda/(f_i(T))^{m_i}$$

où les $f_i(T)$ sont des polynômes distingués irréductibles.

On suppose que l'algèbre $\Lambda[\Delta]$ est abélienne (ie que le caractère ω qui définit l'action est trivial) alors tout $\Lambda[\Delta]$-module noethérien X est pseudo-isomorphe à une somme directe finie de $\Lambda[\Delta]$-modules isotypiques élémentaires. Plus précisément, à chaque caractère p-adique irréductible φ du groupe Δ, on associe un unique triplet $(\rho_\varphi, s_\varphi, t_\varphi)$ d'entiers naturels, une unique suite décroissante $(f_{\varphi,i})_i$ de polynômes distingués de l'anneau $Z_\varphi[\gamma - 1]$ et enfin une unique suite décroissante d'entiers naturel non-nuls $(m_{\varphi,j})$ tels que la φ-composante $X_\varphi := e_\varphi X$ soit $\Lambda[\Delta]$-pseudo-isomorphe à la somme directe :

$$X_\varphi \sim \Lambda_\varphi^{\rho_\varphi} \oplus (\oplus_{i=0}^{s_\varphi} \frac{\Lambda_\varphi}{f_{\varphi,i}\Lambda_\varphi})$$

$$\oplus(\oplus_{i=0}^{t_\varphi} \frac{\Lambda_\varphi}{p^{m_{\varphi,i}}\Lambda_\varphi}).$$

Si ϕ désigne un caractère p-adique du groupe Δ induit par un caractère p-adique irréductible du noyau H, on appelle Σ_ϕ-*module élémentaire*, toute somme directe finie d'exemplaires des modules suivants :

1. les Σ_ϕ-modules projectifs $\Sigma_\varphi = \Sigma_\phi e_\varphi$ associés aux m_ϕ caractères p-adiques irréductibles φ représentés dans ϕ.
2. les quotients $\Sigma_\varphi/\theta^\alpha\Sigma_\varphi$ des modules précédents par leurs sous-modules respectifs engendrés par les puissances de la résolvante θ.
3. les quotients $\Sigma_\varphi/p^\mu\Sigma_\varphi$ associé aux puissances de l'uniformisante p de l'extension non-ramifiée Z_φ de $\mathbb{Z}_p$.
4. les quotients $\Sigma_\varphi/\Sigma e_\varphi f e_\varphi$ associés aux polynômes distingués (ou de Weiertrass) de valuation nulle de l'algèbre gauche $Z_\varphi[\theta^{m_\phi}] \simeq e_\varphi \Sigma e_\varphi$.

Cette description réalisée, on peut alors d'énoncer que tout Σ-module noethérien est pseudo-isomorphe à un Σ-module élémentaire (des conditions supplémentaires permettent de garantir l'unicité). En d'autres termes, si X est un Σ-module noethérien, on a :

$$X \sim \oplus_{\phi \in Ind_H^\Delta} \oplus_{\varphi|\phi} [\Sigma_\varphi^{\rho_\varphi} \oplus$$

$$(\oplus_{i=1}^{s_\varphi} /\theta^{a_{\varphi,i}}\Sigma_\varphi) \oplus$$

$$(\oplus_{i=1}^{t_\varphi} \Sigma_\varphi/p^{n_{\varphi,i}}\Sigma_\varphi) \oplus$$

$$(\oplus_{i=1}^{u_\varphi} \Sigma_\varphi/\Sigma_\varphi f_{\varphi,i})]$$

On introduit pour un Λ-module de type fini X les invariants d'Iwasawa :
- $\rho := rg_{\Lambda} X$, le Λ-rang de X
- $\mu(X) := \Sigma_{i=1}^{m} n_i$, l'invariant μ de X.
- $\lambda(X) := \Sigma_{i=1}^{m} m_i \deg f_i$ l'invariant λ de X
- $f_X(T) := \Pi_{i=1}^{m} f_i(T)^{m_i}$ le polynôme caractéristique de X

et l'on rappelle que dans le cas particulier où X est de torsion (ie $\rho = 0$) alors $\lambda = \dim_{\mathbb{Q}_p} \otimes_{\mathbb{Z}_p} M$ et le polynôme caractéristique de l'endomorphisme de $\mathbb{Q}_p \otimes X$ est donné par la multiplication par T.

Si $\Lambda[\Delta]$ est l'algèbre abélienne associée au groupe Δ et à coefficient dans l'anneau d'Iwasawa $\mathbb{Z}_p[[\theta]]$, on apelle *paramètres* attachés à un $\Lambda[\Delta]$-module noethérien X, les caractères p-adiques du groupe Δ définis à partir des invariants d'Iwasawa des composantes isotypiques de X via :

$$\rho = \Sigma_{\varphi} \rho_{\varphi} \varphi$$

$$\mu = \Sigma_{\mu} \mu_{\varphi} \varphi$$

$$\lambda = \Sigma_{\varphi} \lambda_{\varphi} \varphi$$

où pour chacun des caractères p-adiques irréductibles φ les entiers ρ_{φ} , λ_{φ} et μ_{φ} mesurent respectivement :
- la dimension $dim_{\Lambda_{\varphi}} X_{\varphi}$ de la φ-composante de X.
- le degré $\Sigma_{i=0}^{s_{\varphi}}$ du polynôme caractéristique de son sous-Λ_{φ}-module de torsion.
- la p-valuation $\Sigma_{i=0}^{t_{\varphi}} m_{\varphi,i}$ de ce dernier.

Étant donné X un Σ-module noethérien, on appelle *paramètres* de X les caractères *fractionnaires* définis comme suit :

- $\rho = \Sigma_{\varphi} \rho_{\varphi} \varphi$ *où* :

$$\rho_{\varphi} = \frac{1}{m_{\phi} - 1} \rho_{\varphi\omega^{-k}}$$

-$\mu = \Sigma_{\mu} \mu_{\varphi} \varphi$ *où* :

$$\mu_{\varphi} = \frac{1}{m_{\phi}} \Sigma_{k=0}^{m_{\phi}-1} \Sigma_{i=1}^{t_{\varphi\omega^{-k}}} n_{\varphi\omega^{-k},i}$$

- $\lambda = \Sigma_{\varphi} \lambda_{\varphi} \varphi$ *où* :

$$\lambda_{\varphi} = \frac{1}{m_{\phi}} \Sigma_{k=0}^{m_{\phi}-1} \Sigma_{i=1}^{u_{\varphi\omega^{-k}}} deg f_{\varphi\omega^{-k},i} +$$

$$\Sigma_{k=0}^{m_{\phi}-1} \Sigma_{i=1}^{s_{\varphi\omega^{-k}}} sup\{(\frac{a_{\varphi\omega^{-k},i-k}}{m_{\phi}}), 0\}.$$

Remarques :
- On remarque que les paramètres d'Iwasawa généralisés coïncident avec les paramètres définis ci-contre lorsque que l'on ne retient pour X que sa structure de $\Lambda[H]$-module.
- On dit qu'un Σ-module noethérien est de torsion lorsque sa pseudo-décomposition élémentaire élémentaire ne comporte aucun facteur projectif Σ_{φ}.

Soient M un Λ-module de type fini, de torsion et $n_0 \geq d(M)$ un nombre fixé. On a alors l'égalité asymptotique :

$$\sharp(\frac{M}{\frac{\omega_n}{\omega_0}M}) = p^{\mu p^n + \lambda n + \nu}$$

où $\mu = \mu(M)$, $\lambda = \lambda(M)$, ν est une constante indépendante de n et où l'on a posé :

$$\omega_n = (1+T)^{p^n} - 1.$$

Théorème des paramètres (cas abélien) : Soit X un $\Lambda[\Delta]$-module noethérien de paramètres ρ, μ et λ. Si $\bigtriangledown_n = p^{n+1}\Lambda + \omega_n\Lambda$ désigne l'idéal de l'algèbre d'Iwasawa $\Lambda = \mathbb{Z}_p[[\gamma - 1]]$ engendré par l'élément p^{n+1} et le polynôme $\omega_n = (\gamma^{p^n} - 1)$, il existe un unique caractère p-virtuel ν du groupe Δ, tel que l'ordre $p^{x_n^\varphi}$ de la φ-composante du quotient $X/\bigtriangledown_n X$ soit, pour chaque caractère p-adique φ, asymptotiquement donné par la relation :

$$x_n^\varphi = < \rho, \varphi > (n+1)p^n +$$
$$< \mu, \varphi > p^n +$$
$$< \lambda, \varphi > n + < \mu, \varphi >$$

Théorème des paramètres (cas métabélien) : Soit X un $\Lambda[\Delta]$-module noethérien de paramètres ρ, μ et λ. On pose $\tilde{\bigtriangledown}_n = p^{n+1}\Lambda + \frac{\theta_n}{\theta_0}\Lambda$ l'idéal de l'algèbre d'Iwasawa $\mathbb{Z}_p[[\gamma-1]]$ engendré par l'élément p^{n+1} et le quotient des résolvantes θ_n/θ_0 ; il existe alors un unique caractère p-adique virtuel ν du groupe Δ tel que l'ordre $p^{\tilde{x_n}^\varphi}$ de la φ-composante du quotient $X/\tilde{\bigtriangledown}_n X$ soit donné, pour chaque caractère p-adique φ, asymptotiquement donné par l'identité :

$$\tilde{x_n}^\varphi = < \rho, \varphi > (n+1)\frac{p^n - 1}{m_\phi} +$$
$$< \mu, \varphi > \frac{p^n - 1}{m_\phi} +$$
$$< \lambda, \varphi > n + < \mu, \varphi > .$$

Étant donné X un module d'Iwasawa, on dispose de la suite exacte de $\mathbb{Z}_p$-modules :

$$0 \to X^\Gamma \hookrightarrow X \overset{\gamma-1}{\to} X \twoheadrightarrow X_\Gamma \to 0$$

Dans le cas particulier où $\Lambda[\Delta]$ est une algèbre abélienne (ie que le caractère $\omega \in \Delta$ définissant l'action est trivial), on associe à toute suite exacte de $\Lambda[\Delta]$-modules la suite exacte de ses φ-composantes si φ désigne un caractère irréductible de Δ ; en d'autres termes le foncteur "e_φ" est exact, propriété toujours vérifiée dans le cas *semi-simple*.

Pour tout Σ-module X, l'opérateur θ donne lieu à une suite exacte de C-modules projectifs (où l'on désigne par C le centre de l'algèbre Σ) :

$$0 \to e_\varphi Ker(\theta) \hookrightarrow e_\varphi X \to^\theta e_{\varphi\omega} X$$
$$\twoheadrightarrow e_{\varphi\omega} Coker\theta \to 0.$$

Cette dernière, héritée immédiatement de la relation $e_{\varphi\omega}\theta = \theta e_\varphi$, sera fondamentale dans toute la suite car elle nous permettra de comparer les φ- composantes d'un Σ-module X.

Remarque : Comme dans le cadre classique de la théorie d'Iwasawa, les paramètres ρ, μ et λ associés à un $\Lambda[\Delta]$-module noethérien mesurent avec n la croissance des quotients $\dfrac{X}{\bigtriangledown_n X}$.
Ce sera en particulier le cas lorsque l'on prendra pour X le groupe $Cl_{K_n}^S$ et que l'on s'intéressera à l'évolution de son cardinal le long de la tour d'extensions.

4.4.4 La suite exacte des genres.

On s'intéresse dans un premier temps à l'évolution du quotient des genres ${}^{\Gamma_n}Cl^S_{K_n}$ le long de la tour d'extensions qui, du fait de son interprétation en termes de théorie du corps de classes, passe bien à la limite projective [12].
A un niveau n fini, on dispose de la suite exacte canonique de modules finis :

$$(ii)\ \ 1 \to E^S_{K_0}/E^S_{K_0}\cap N_{K_n/K_0}(K_n^\times) \hookrightarrow \tilde{\oplus}_{\mathfrak{p}\in S} D_{\mathfrak{p}}(K^S_{n,0}/K_0) \to {}^{\Gamma_n}Cl^S_{K_n} \to Cl^S_{K_0} \to 1$$

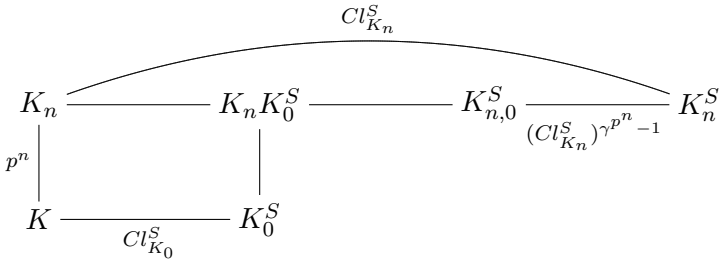
avec :

- $Cl^S_{K_0} = Gal(K_0^S/K_0)$ le groupe de Galois associé à l'extension abélienne non ramifiée S-décomposée maximale sur K_0 (i.e le S-corps de classes de Hilbert associé associé à K_0).

- $Cl^S_{K_n} = Gal(K_n^S/K_n)$ idem sur K_n

- ${}^{\Gamma_n}Cl^S_{K_n} = Gal(K^S_{n,0}/K_n)$ idem que ci-dessus avec en outre *abélienne* sur K_0 (i.e le S-corps des genres attaché à l'extension K_n/K_0).

- $D_{\mathfrak{p}}(K^S_{n,0}/K_0)$ groupe de décomposition de $\mathfrak{p}$ dans l'extension $K^S_{n,0}/K_0 (\simeq \mathbb{Z}/p^n\mathbb{Z})$.



Remarque 4.4.2. *La notation $\widetilde{\oplus}$ signifie que l'on restreint la somme directe aux familles vérifiant la formule du produit i.e.* $\Pi\sigma_{\mathfrak{p}}\,|_{K_n} = 1$.

De la suite exacte (ii), on déduit la formule des genres :

$$|{}^{\Gamma_n}Cl^S_{K_n}| \ \ = \ \ |Cl^S_{K_0}|\frac{\prod_{\mathfrak{p}\in S} d_{\mathfrak{p}}}{p^n(E^S_{K_0} : E^S_{K_0}\cap N_{K_n/K_0}(K_n^\times))} \qquad (4.1)$$

avec $d_{\mathfrak{p}} = p^n$ pour tout $\mathfrak{p} \in S$.
Si l'on note $s = |S|$, le numérateur vaut alors p^{ns} et tout revient donc à

[12] Le quotient des genres s'interprète naturellement via la théorie du corps de classes comme limite projective de quotients de classes d'idéaux ; ce dernier est, en vertu des résultats de structure de la théorie d'Iwasawa, pseudo-isomorphe au dual de Pontryagin de la limite inductive des groupes de classes ambiges attachés aux sous-extensions finies K_n/K_0

évaluer le dénominateur sachant que l'on dispose du théorème de structure suivant des S-unités :

$$E_{K_0}^S \simeq k^\times.\mathbb{Z}^{s-1} \quad \text{où} \quad k = \mathbb{F}_q.$$

Notation : Le facteur $p^n = [K_n : K_0]$ traduit le fait que la somme directe prise sur les groupe de décomposition est *restreinte*, ainsi on a par définition :

$$\widetilde{\oplus}\mathcal{D}_{\mathfrak{p}}(K_{n,0}^S/K_0) \to Gal(K_{n,0}^S/K_0)$$

or comme les places de S sont complètement décomposées dans l'extension horizontale K/F et totalement ramifiées dans l'extension verticale associée, on en déduit : $|\widetilde{\oplus}| = \dfrac{|\oplus|}{[K_n : K_0]} = \dfrac{\prod_{\mathfrak{p}\in S} d_{\mathfrak{p}}}{p^n} \cdots$

4.4.5 La suite exacte des classes ambiges.

L'égalité $E_{K_0}^S = E_{K_n}^S$ entraîne en particulier la trivialité du premier groupe de Cohomologie i.e. $H^1(\Gamma_n, E_{K_n}^S) = 1$ avec $\Gamma_n = Gal(K_n/K_0)$.
Comme ce dernier mesure la S-capitulation au niveau n (i.e. dans K_n/K_0, on en déduit que contrairement à ce qu'il se produit dans les corps de nombres, il n'y a pas de S-capitulation dans K_n/K_0 i.e. $Cl_{K_0}^S \hookrightarrow Cl_{K_n}^S$.
On peut en fait retrouver directement ce résultat ; en effet, si $\mathfrak{a}_0$ désigne un S-diviseur de K_0 qui capitule dans K_n, disons $\mathfrak{a}_0 = (a_n)$ diviseur principal dans K_n, on a,

$$a_n^{\gamma-1} \in E_{K_0}^S = E_{K_n}^S,$$

puis en prenant la même : $a_n^{\gamma-1} = 1$, i.e. $a_n \in K_0$ et $\mathfrak{a}_0$ est principal dans K_0.

En l'absence de S-capitulation et du fait de la trivialité de H^1 des S-unités, la suite exacte des classes ambiges revêt la forme simplifiée suivante :

$$1 \to \mathcal{D}_{K_n}^{S\ \Gamma_n}/\mathcal{D}_{K_0}^S \hookrightarrow Cl_{K_n}^{S\ \Gamma_n}/Cl_{K_0}^S \to E_{K_0}^S \cap N_{K_n/K_0}(K_n^\times)/N(E_n^S) \to 1$$

avec en outre,

$$N_{K_n/K_0}(E_{K_n}^S) = N_{K_n/K_0}(E_{K_0}^S) = E_{K_0}^{Sp^n}.$$

En particulier, si S contient toutes les places ramifiées, le groupe à gauche est trivial et l'on obtient la suite exacte,

$$(iii) \quad 1 \to Cl_{K_0}^S \hookrightarrow Cl_{K_n}^{S\Gamma_n} \to E_{K_0}^S/(E_{K_0}^S)^{p^n} \xrightarrow{\theta} E_{K_0}^S/E_{K_0}^S \cap N(K_n^\times) \to 1$$

qui peut être vue comme duale de la suite (ii) à la différence essentielle près que $\oplus_{\mathfrak{p}\in S} D_{\mathfrak{p}}(K_{n,0}^{ab}/K_0)$ et $E_{K_0}^S/E_{K_0}^{Sp^n}$ ne sont pas nécessairement isomorphes

comme Δ-modules.

Remarque technique : Attention ici au décalage des φ-composantes induit par θ ...

4.4.6 Application au cas métabélien :

A chaque place $\mathfrak{p}$ de F, on associe le caractère $\chi_{\mathfrak{p}} = Ind_{\Delta_{\mathfrak{p}}}^{\Delta} 1_{\Delta_{\mathfrak{p}}}$ défini comme l'induit à Δ du caractère unité attaché au groupe de décomposition $\Delta_{\mathfrak{p}}$ (i.e. le caractère du $\mathbb{Z}_p[\Delta]$-module $\mathbb{Z}_p[\Delta/\Delta_{\mathfrak{p}}]$. Cela étant :

1. Le quotient $E_{K_0}^S/E_{K_0}^{Sp^n}$ est un $\mathbb{Z}/p^n\mathbb{Z}[\Delta]$-module de caractère
$$\chi_S - 1 = \sum_{\mathfrak{p}\in S} \chi_{\mathfrak{p}} - 1$$
En effet, si l'on considère l'extension abélienne de corps de fonctions K/F, de groupe de Galois Δ et S un ensemble fini de places comme précédemment, alors on dispose d'une suite exacte :
$$0 \to k^\times \to E_K(S) \to \mathcal{D}^0(S) \to (fini) \to 0$$
Interprétée en terme de quotient de Herbrand (qui, on le rappelle, ne distingue pas les objets à un fini près), on obtient :
$q(E_K(S)) = q(\mathcal{D}^0(S))$. En outre, on rappelle que :
$$\begin{aligned} \mathcal{D}^0(S) &= \widetilde{\oplus}_{\mathfrak{p}\in S}\mathfrak{p}\mathbb{Z}_{\mathfrak{p}} \\ &= \widetilde{\oplus_{\mathfrak{p}}\oplus_{\mathfrak{P}|\mathfrak{p}}}\mathfrak{P}\mathbb{Z}_p \\ &\simeq \widetilde{\oplus}_{\mathfrak{p}}\mathbb{Z}_p[\Delta/\Delta_{\mathfrak{p}}] \end{aligned}$$
de caractère $\sum_{\mathfrak{p}\in S}\chi_{\mathfrak{p}} - 1$ (le "-1" provenant de ce que la somme directe est restreinte et l'action du caractère $\chi_{\mathfrak{p}}$ consistant à permuter les places de S).
2. Le groupe $\tilde{\oplus}_{\mathfrak{p}\in S} D_{\mathfrak{p}}(K_{n,0}^{ab}/K_0)$ est un $\mathbb{Z}/p^n\mathbb{Z}[\Delta]$-module de caractère $\omega(\chi_S - 1)$; en effet,
$$\tilde{\oplus}_{\mathfrak{p}\in S} D_{\mathfrak{p}} \simeq \Gamma_n \oplus \left(E_{K_0}^S/E_{K_0}^{Sp^n}\right)$$
comme $\mathbb{Z}_p[\Delta]$-module puisque $\Gamma_n = Gal(K_n/K_0)$ est un $\mathbb{Z}/p^n\mathbb{Z}[\Delta]$-module de caractère ω.

Conséquence : On écrit :

$$\begin{aligned} |(Cl_{K_n}^S)_\varphi| &= p^{x_\varphi^S(n)} \quad \textit{terme de classes} \\ |(E_{K_0}^S/E_{K_0}^S \cap N(K_n^\times))_\varphi| &= p^{n_\varphi^S(n)} \quad \textit{terme normique} \\ |(E_{K_0}^S/E_{K_0}^{Sp^n})_\varphi| &= p^{r_\varphi^S(n)} \quad \textit{terme de ramification} \end{aligned}$$

L'exploitation des suites exactes obtenues précédemment permet d'établir la relation suivante :

$$x_\varphi^S(n) - x_{\omega\varphi}^S(n) = x_\varphi^S(0) - x_{\omega\varphi}^S(n) + r_{\omega\varphi}^S(n) - r_\varphi^S(n)$$

Détail :
On part de la suite exacte :

$$1 \to (Cl_{K_n}^S)_\varphi^{\Gamma_n} \hookrightarrow \left(Cl_{K_n}^S\right)_\varphi \to \left(Cl_{K_n}^S\right)_{\omega\varphi} \to^\Gamma \left(Cl_{K_n}^S\right)_{\omega\varphi} \to 1$$

d'où, en terme de cardinaux :

$$\frac{|(Cl_{K_n}^S)_\varphi^{\Gamma_n}||\left(Cl_{K_n}^S\right)_{\omega\varphi}|}{|\left(Cl_{K_n}^S\right)_\varphi||^{\Gamma_n}\left(Cl_{K_n}^S\right)_{\omega\varphi}|} = 1 \Leftrightarrow \frac{|(Cl_{K_n}^S)_\varphi^{\Gamma_n}|}{|^{\Gamma_n}\left(Cl_{K_n}^S\right)_{\omega\varphi}|} = \frac{|\left(Cl_{K_n}^S\right)_\varphi|}{|\left(Cl_{K_n}^S\right)_{\omega\varphi}|}$$

Soit finalement :

$$p^{x_\varphi^S(n) - x_{\omega\varphi}^S(n)} = \frac{|(Cl_{K_n}^S)_\varphi^{\Gamma_n}|}{|^{\Gamma_n}\left(Cl_{K_n}^S\right)_{\omega\varphi}|}$$

Or d'après (ii),

$$|^{\Gamma_n} Cl_{K_n}^S| = \frac{|\tilde{\oplus}_{\mathfrak{p}\in S} D_\mathfrak{p}(K_{n,0}^{ab}/K_0)||Cl_{K_0}^S|}{|E_{K_0}^S/E_{K_0}^S \cap N(K_n^\times)|}$$

et d'après (iii) :

$$|Cl_{K_n}^{S\Gamma_n}| = \frac{|Cl_{K_0}^S||E_{K_0}^S/E_{K_0}^{p^n}|}{|E_{K_0}^S/E_{K_0}^S \cap N(K_n^\times)|}$$

On en déduit :

$$|(Cl_{K_n}^S)_\varphi^{\Gamma_n}| = \frac{|(Cl_{K_0}^S)_\varphi||(E_{K_0}^S/E_{K_0}^{p^n})_{\omega\varphi}|}{|(E_{K_0}^S/E_{K_0}^S \cap N(K_n^\times))_{\omega\varphi}|}$$

$$|^{\Gamma_n}(Cl_{K_n}^S)_{\omega\varphi}| = \frac{|\left(Cl_{K_0}^S\right)_{\omega\varphi}||(\tilde{\oplus}_{\mathfrak{p}\in S} D_\mathfrak{p}(K_{n,0}^{ab}/K_0))_{\omega\varphi}|}{|(E_{K_0}^S/E_{K_0}^S \cap N(K_n^\times))_{\omega\varphi}|}$$

et donc :

$$Z := \frac{|(Cl_{K_n}^S)_\varphi^{\Gamma_n}|}{|^{\Gamma_n}\left(Cl_{K_n}^S\right)_{\omega\varphi}|} = \frac{|\left(Cl_{K_0}^S\right)_\varphi|}{|\left(Cl_{K_0}^S\right)_{\omega\varphi}|} \frac{|(E_{K_0}^S/E_{K_0}^{p^n})_{\omega\varphi}|}{|(\tilde{\oplus}_{\mathfrak{p}\in S} D_\mathfrak{p}(K_{n,0}^S/K_0))_{\omega\varphi}|}$$

$$Z = p^{x_\varphi^S(0) - x_{\omega\varphi}^S(0)} p^{r_{\omega\varphi}^S(n)} p^{-n<\chi_S - 1, \varphi>}$$

$$Z = p^{x_\varphi^S(0) - x_{\omega\varphi}^S(0) + r_{\omega\varphi}^S(n) - r_\varphi^S(n)}$$

Finalement :

$$p^{x_\varphi^S(n)-x_{\omega\varphi}^S(n)} = p^{x_\varphi^S(0)-x_{\omega\varphi}^S(0)+r_{\omega\varphi}^S(n)-r_\varphi^S(n)}$$

et en prenant la valuation p-adique de cette expression, on obtient la relation :

$$x_\varphi^S(n) - x_{\omega\varphi}^S(n) = x_\varphi^S(0) - x_{\omega\varphi}^S(0) + r_{\omega\varphi}^S(n) - r_\varphi^S(n)$$

On utilise maintenant le comportement asymptotique :

$$x_\varphi^S(n) \sim < \mu^S, \varphi > p^n + < \lambda^S, \varphi > n$$

$$r_{\omega\varphi}^S(n) \sim < \chi_S - 1, \varphi > n$$

avec :

$\mu^S = \sum_\varphi \mu_\varphi^S \varphi$

$\lambda^S = \sum_\varphi \lambda_\varphi^S \varphi.$

Les relations d'orthogonalité des caractères donnent :

$$\begin{array}{rcl} x_\varphi^S(n) - x_{\omega\varphi}^S(n) & = & (\mu_\varphi^S - \mu_{\omega\varphi}^S)p^n + (\lambda_\varphi^S - \lambda_{\omega\varphi}^S)n \\ x_\varphi^S(0) - x_{\omega\varphi}^S(0) & = & \mu_\varphi^S - \mu_{\omega\varphi}^S \end{array}$$

On en déduit par identification que :

$$\forall\ \varphi,\ \mu_\varphi^S = \mu_{\omega\varphi}^S.$$

puis,

$$\begin{array}{rcl} (\lambda_\varphi^S - \lambda_{\omega\varphi}^S)n & = & < \chi_S - 1, \omega\varphi > n - < \chi_S - 1, \varphi > n \\ & = & < \chi_S - 1, \omega\varphi > n - < \omega(\chi_S - 1), \omega\varphi > n \\ & = & < (\chi_S - 1)(\omega - 1), \omega\varphi > n \end{array}$$

D'où

$$\lambda_{\omega\varphi}^S - \lambda_\varphi^S = < (\chi_S - 1)(\omega - 1), \omega\varphi >$$

Autre formulation :

$$\begin{array}{rcrcl} (ii) & \text{donne} & {}^\Gamma\lambda^S & = & \omega(\chi_S - 1) - \nu^S \\ (iii) & \text{donne} & \lambda^{S\Gamma} & = & \omega^{-1}(\chi_S - 1) - \omega^{-1}\nu^S \\ (i) & \text{donne} & \lambda^S & = & \lambda^{S\Gamma} - \omega^{-1\Gamma}\lambda^S + \omega^{-1}\lambda^S \end{array}$$

D'où :

$$(1-\omega^{-1})(\lambda^S+(\chi_S-1)) \quad = \quad 0 \tag{4.2}$$

Conséquences :
Si l'on est dans le cas "semi-simple", classes ambiges et quotient des genres donnent le même caractère et l'on peut énoncer :

Théorème 4.4.3. *De l'étude précédente résulte :*

1. *La propriété de* semi-simplicité $\Rightarrow$

   $(ii)=(iii) \Leftrightarrow (\omega-\omega^{-1})(\chi_S-1)=(1-\omega^{-1})\nu \Leftrightarrow (\omega^2-1)(\chi_S-1)=(\omega-1)\nu^S$

   avec $(\omega-1)\nu^S=0 \Leftrightarrow \nu^S$ *est un multiple de* $1+\omega+\cdots+\omega^{n-1}$. *Ce qui produit, par contraposition, des critères suffisants de non semi-simplicité.*

2. (4.2) *fournit des critères suffisants de non trivialité de l'invariant* λ^S *via*

$$(\omega-1)(\lambda^S+(\chi_S-1))\neq 0 \Rightarrow \lambda^S\neq 0.$$

◇ Cas particulier : S'il existe une unique place $\mathfrak{p}$ dans S, alors $\chi_S=\chi_{\mathfrak{p}}$ et le caractère de $\Delta/\Delta_{\mathfrak{p}}$ i.e. par définition la somme des caractères irréductibles de Δ triviaux sur $\Delta_{\mathfrak{p}}$. En particulier le caractère unité n'est pas représenté dans $\chi_{\mathfrak{p}}-1$ i.e. $<\chi_{\mathfrak{p}}-1,1>=0$.

◇ Conséquence :

$$\begin{aligned}\lambda^S_{\omega\varphi}-\lambda^S_{\varphi} &= <(\chi_{\mathfrak{p}}-1)(\omega-1),\omega\varphi> \\ &= <\omega(\chi_{\mathfrak{p}}-1),\omega\varphi>-<\chi_{\mathfrak{p}}-1,\omega\varphi> \\ &= <\chi_{\mathfrak{p}}-1,\varphi>-<\chi_{\mathfrak{p}}-1,\omega\varphi>\end{aligned}$$

Le choix de $\varphi=1$ donne :

$$\begin{aligned}\lambda^S_{\omega}-\lambda^S_{1} &= <\chi_{\mathfrak{p}}-1,1>-<\chi_{\mathfrak{p}}-1,\omega> \\ &= -<\chi_{\mathfrak{p}}-1,\omega>\end{aligned}$$

et donc :

$$\begin{aligned}\lambda^s_{\omega}=\lambda^S_{1} &\Leftrightarrow <\chi_{\mathfrak{p}}-1,\omega>=0 \\ &\Leftrightarrow \omega\nmid(1-\chi_{\mathfrak{p}})\end{aligned}$$

Ainsi si $\omega|(1-\chi_{\mathfrak{p}})$, $\lambda_{\omega}^{S} \neq \lambda_{\omega\varphi}^{S}$ et l'extension considérée n'est pas semi-simple (puisque la semi-simplicité entraînerait $\lambda_{\omega}^{S} = \lambda_{\omega\varphi}^{S}$ pour tout φ).

Problème : Partant du fait que dans le cas des corps de nombres, la $\mathbb{Z}_p$-extension cyclotomique (associée au caractère unité) est semi-simple, on aurait souhaité déterminer si cela était le cas du candidat présenté à l'occasion du chapitre 2 ce qui nous aurait conforté dans l'idée qu'il s'agissait d'un bon analogue mais je ne sais pas comment m'y prendre. En fait, j'aurais voulu paramétrer par des caractères la famille de $\mathbb{Z}_p$-extensions obtenues par troncature d'une extension cyclotomique de corps de fonctions à la manière de Caroll et Kisilevsky dans [7].

Perspectives :

1. S'affranchir de l'hypothèse simplificatrice selon laquelle l'ensemble S est exactement constitué des places ramifiées (totalement) en introduisant l'ensemble $R \setminus S$ des places de F n'appartenant pas à S et sauvagement ramifiées dans L/K.
2. Une autre direction est suggérée par Greenberg dans [20] et propose de comprendre ce que ces résultats de semi-simplicité (ou non-semi-simplicité) pourraient signifier en terme de zéros de fonctions L. Cette perspective (si elle est réalisable) pourrait se révéler d'autant plus riche qu'elle pourrait permettre de dresser un pont entre "vecteurs de Witt" et "caractères" (peut-être en introduisant la notion de vecteurs de Witt χ-isotypiques) puisque finalement dans la quatrième partie nous n'exploitons plus jamais la manière dont sont générées en caractéristique $p > 0$ les extensions de degré une puissance de p. À cet égard, nous précisons que Schmid dans [60] a réalisé une étude des fonctions Zêta et L attachées à une extension d'A.S.W. sur un corps fini.

Bibliographie

[1] A. Aiba, On the vanishing of Iwasawa invariants of geometric cyclotomic $\mathbb{Z}_p$-extensions *Acta Arithmetica* ***108.2,*** (2003)

[2] B. Anglès, On Hilbert class field tower of global function fields *Proceedings of the workshop on Drinfeld modules, modular schemes and applications, Gekeler, E.U. (ed.)* (1997)

[3] B. Anglès, On the Class Group Problem for Function Fields *Journal of Number Theory* ***70,*** $146-159$ (1998)

[4] B. Anglès, J.F. Jaulent, Théorie des Genres des Corps Globaux *Manuscripta Math.* ***101,*** $513-532$(2000)

[5] H. Cartan, S. Eilenberg, Homological Algebra *Princeton University Press* (1956)

[6] Ph. Cassou-Noguès, Algèbre Commutative *Cours de Maîtrise* (2000)

[7] J.E. Carroll, H.H. Kisilevsky, On Iwasawa's λ-invariant for certain $\mathbb{Z}_l$-extension *Acta Arithmetica* ***XL*** (1981)

[8] R. Clément, The Genus Field of an Algebraic Function Field *Journal of Number Theory* ***40,*** $359-375$ (1992)

[9] P.M. Cohn, Basic Algebra : Groups, Rings and Fields *Springer* (2003)

[10] P.M. Cohn, Further Algebra and Applications *Springer* (2003)

[11] C.W. Curtis, I. Reiner, Methods of Representation Theory I *John Wiley and Sons* (1981)

[12] R. Descombes, Éléments de Théorie des Nombres *P.U.F* (1986)

[13] J. Dieudonné, Panorama des Mathematiques Pures - Le choix Bourbachique *Gauthier-Villars* (1977)

[14] I.B. Fesenko, S.V. Vostokov, Local Fields and Their extensions - A Constructive Approach *American Mathematical Society* 121

[15] V. Fleckinger, C. Thiébaud Idéaux ambiges dans les corps de fonctions *Journal of Number Theory* ***100*** $217-227$ (2003)

[16] R. Fraatz, Computation of Maximal Orders of Cyclic Extensions of Function Fields *genehmigte Dissertation-Berlin* (2005)

[17] W. Fulton, J. Harris, Representation Theory : A first Course *Graduate Texts in Mathematics Springer* (1991)

[18] D. Goss, D. Hayes, M. Rosen, The Arithmetic of function fields *Walter de Gruyter- Berlin* (1992)

[19] S. Galovich, M. Rosen, Units and Class Groups in Cyclotomic Function Fields *Journal of Number Theory* ***14,*** 156 – 184 (1982)

[20] R. Greenberg, On a certain l-Adic Representation *Invent. Math.* ***21,*** 117 – 124 (1973)

[21] R. Gold, H. Kisilevsky, On Geometric $\mathbb{Z}_p$-Extensions of Functions Fields *Manuscripta Math.* ***62.2,*** 145 – 161 (1988)

[22] D. Goss, p-adic L-series at $s = 0$ *Jour. Fac. Science, Tokyo university, Sec. IA, Math.* ***28,*** 979 – 994 (1981)

[23] D. Goss, Basic Structures of Function Field Arithmetic *A Series of Modern Surveys in Mathematics-Springer* 35

[24] L. Guo, L. Shu Class Numbers of Cyclotomic Function Fields *Trans. Am. Math. Soc.* ***351,*** 4445 – 4467 (1999)

[25] G. Harder, Wittvektoren *Jahresber. Dtsch. Math. Ver.* ***99.1,*** 18 – 48 (1997)

[26] H. Hasse, Theorie der relativ-zyklischen algebraischen Funktionenkörper, insbesondere bei endlichem Konstantenkörper *J. Reine Angew. Math.* ***172*** 37 – 54 (1934)

[27] D.R. Hayes, Explicit Class Field for Rational Function Fields *Trans. Amer. Math. Soc.* ***189,*** 77 – 91 (1974)

[28] D.R. Hayes, Explicit Class Field Theory in Global Function Fields *Stu. Algebra Number Theory Adv. Math.* ***16,*** 173 – 217 (1980)

[29] D.R. Hayes, A Brief Introduction to Drinfeld Modules *The Aritmetic of Function Fields, de Gruyter, Berlin* (1992)

[30] K. Iwasawa, On Cohomology Groups of Units for $\mathbb{Z}_p$-extensions *Am.J. Math.* ***105,*** 183 – 200 (1983)

[31] S. Iyanaga, The Theory of Numbers *North-Holland Publishing Comp.,* (1975)

[32] N. Jacobson, Basic Algebra II *San Francisco*

[33] J.F. Jaulent, Sur l'indépendance l-adique des nombres algébriques *J. Number Th.* ***20,*** 149 – 158 (1985)

[34] J.F. Jaulent, L'Arithmétique des l-extensions *Thèse d'Etat* (1986)

[35] J.F. Jaulent, J.W. Sands, Sur Quelques Modules d'Iwasawa semi-simples *Compositio Math.* ***99,*** 325 – 341 (1995)

[36] G. Karpilovsky, Topics in Field Theory *North Holland Mathematics Studies* 155 (1989)

[37] A. Kraus, Corps Locaux et Applications *Cours Accéléré de DEA, Université Paris VI*, (2000)

[38] P. Lam-Estrada, G.D. Villa-Salvador, Some Remarks On The Theory of Cyclotomic Function Fields *Rocky Mountain Journal Of Mathematics* ***31.2*** (2001)

[39] D. Le Brigand, Méthodes pour les corps globaux *Cours de DEA* (2002)

[40] C. Li, J. Zhao, Iwasawa Theory of $\mathbb{Z}_p^d$-extensions Over Global Functions Fields *Expo. Math.* ***15,*** 315 – 337 (1997)

[41] C. Li, J. Zhao, Class Number Growth of a Family of $\mathbb{Z}_p$-Extensions over Global Function Fields *Journal of Algebra* ***200,*** 141 – 154 (1998)

[42] M.L. Madan, G.D. Villa-Salvador, On an analogue of a Conjecture of Gross *Manuscripta Math.* ***61,*** 327 – 345 (1988)

[43] M.P. Malliavin, Algèbre Commutative : Applications en géométrie et théorie des nombres *Masson* (1985)

[44] M. Matignon, Théories Galoisiennes *Cours de DEA* (1999)

[45] J.S. Milne, Class Field Theory *http ://www.jmilne.org/math/CourseNotes/math* 776*.pdf*

[46] K. Miyake, Class Field Theory- Its century and Prospect *Advanced Studies in Pure Mathematics* 30 (2001)

[47] J. Neukirch, Algebraic Number Theory *Springer-Verlag* 322 (1999)

[48] J. Neukirch, A. Schmidt, K. Wingberg, Cohomology of Number Fields *A Series of Comprehensive Studies in Mathematics- Springer* 323

[49] B. Oriat, Quelques caractères utiles à l'Arithmétique *Séminaire de Théorie des Nombres -Besançon-* (1974/75)

[50] I. Reiner, Maximal Orders *Academic Press* (1975)

[51] P. Roquette, Class Field Theory in Characteristic p, its origin and development. *http ://www.rzser.uni-heidelberg.de/∼ci3/*

[52] M. Rosen, Ambiguous Divisor Classes in Function Fields *Journal of Number Theory* ***9,*** 160 – 174 (1977)

[53] M. Rosen, S-Units and S-Class group in Algebraic Function Fields *Journal of Algebra* ***26,*** 98 – 108 (1973)

[54] M. Rosen, The Hilbert Class Field in Function Fields *Exp. Math.* ***5,*** 365 – 378 (1987)

[55] M. Rosen, Number Theory in Function Fields *GTM* 210 *Springer* (2002)

[56] I. Rust, O. Scheja, A guide to explicit class field theory in global fonction fields *Proceedings of the workshop on Drinfeld modules, modular schemes and applications, Gekeler, E.U. (ed.)* (1997)

[57] V.H.L. Schmid, Über das Reziprozitätsgesetz in relativ-zyklischen algebraischen Funktionenkörper mit endlichem Konstantenkörper *Math. Zeitschr.* ***40,*** 91 – 109 (1935)

[58] V.H.L. Schmid, Zyklische algebraische Funktionenkörper vom Grade p^n über endlichem Konstankörper der Charakteristik p *J. Reine Angew.* ***175***, 108 – 123 (1936)

[59] V.H.L. Schmid, Zur Arithmetik der zyklischen p-Körper *J. Reine Angew.* ***176***, 161 – 167 (1937)

[60] V.H.L. Schmid, Kongruenzzetafunktionen in zyklischen Körpern *Abhandlungen Preuß. Akad. Wiss. Berlin, Jahrgang* ***14***, (1942)

[61] V.H.L. Schmid, E. Witt, Unverzweigte abelsche Körper vom Exponenten p^n über einem algebraischen Funktionenkörper der Charakteristik p *J. Reine Angew. Math.* ***176***, 168 – 173 (1936)

[62] J.P. Serre, Représentations Linéaires des groupes finis *Hermann* (1971)

[63] S. Shatz, Profinite Groups, Arithmetic, and Geometry *Annals of Mathematics Studies* ***67*** (1972)

[64] H. Stichtenoth, Algebraic Function Fields and Codes *Universitext Springer-Verlag,* (1993)

[65] J.T. Tate, Algebraic Number Theory *Academic Press,* (1967)

[66] O. Teichmüller Zerfallende zyklische p-algebren *J. reine angew. Math.* ***176***, 157 – 160 (1936)

[67] D.S. Thakur, Iwasawa Theory and Cyclotomic Function Fields *Contemporary Mathematics* ***174*** (1994)

[68] T. Tsuji, Semi-local Units Modulo Cyclotomic Units *Journal of Number Theory* ***78***, 1 – 26 (1999)

[69] L.C. Washington, Introduction to Cyclotomic Fields *Springer* 83 Second Edition (1997)

[70] E. Witt, Zyklische Körper und Algebren der Charakteristik p vom Grad p^n *J. Reine Angew. Math.* ***176***, 126 – 140 (1937)