Some aspects of the arithmetic of functions fields related to Drinfeld Modules

Mohamed El Kati

THÈSE DE DOCTORAT DE L'ÉTABLISSEMENT UNIVERSITE BOURGOGNE FRANCHE-COMTE

PREPARÉE À L'UNIVERSITÉ DE FRANCHE COMTÉ

École doctorale $n°553$

Carnot Pasteur

Doctorat de Mathématiques

Par

EL KATI Mohamed

Quelques aspects de l'arithmétique des corps de fonctions en lien avec les modules de Drinfeld

Thèse présentée et soutenue au Laboratoire de Mathématiques de Besançon

le 19 septembre 2022

Composition du Jury :

Movahhedi, Abass C	Professeur à l'université de Limoges	Président
Assim, Jilali	Professeur à l'université Moulay Ismail Meknès-Maroc	Rapporteur
Bayad, Abdelmejid	Maître de Conférences à l'université d'Évry Val d'Essonne	Rapporteur
Armana, Cécile	Maîtresse de conférences à Université de Franche-Comté	Examinatrice
Oukhaba, Hassan	Maître de Conférences à l'université de Franche-Comté	Directeur de thèse

ECOLE DOCTORALE
CARNOT - PASTEUR

Titre : Quelques aspects de l'arithmétique des corps de fonctions en lien avec les modules de Drinfeld.

Mots clés : Corps de fonctions- Modules de Drinfeld- Modules de Carlitz- Points de torsion- Groupe de Galois

Résumé : Le but de cette thèse est l'étude de trois aspets concernant l'arithmétique des corps de fonctions en lien avec les modules de Drinfeld. Dans la première partie, nous travaillons au-dessus d'un corps de fonctions rationnelles $\mathbb{F}_q(T)$. Nous introduisons et nous étudions la notion de polynômes définissant des unités sur les racines de translatés de polynômes de Carlitz.
Dans la seconde partie nous continuons de travailler au-dessus d'un corps de fonctions rationnelles $\mathbb{F}_q(T)$. Nous proposons un analogue des polynômes de Laguerre classiques. Nous montrons, entre autres, que le groupe de Galois du $n^{\text{ième}}$ polynôme sur $\mathbb{F}_q(T)$ est le groupe général linéaire $GL_n(\mathbb{F}_q)$.
Dans la dernière partie nous considérons le contexte suivant. Soit $k/\mathbb{F}_q$ un corps global de fonctions algébriques. Soit ∞ une place de k. Soit A l'anneau des éléments de k réguliers en dehors de ∞. Soit ρ un A-module de Drinfeld de rang 1 et normalisé par rapport à une fonction signe fixée. Soit H_A^* le corps normalisant de ρ. Soit B la clôture intégrale de A dans H_A^*. Soit $\mathfrak{m}$ un idéal de A. Nous étudions alors la structure du B-module $B\Lambda_{\mathfrak{m}}$ engendré par les points de $\mathfrak{m}$-torsion du module de Drinfeld ρ, ainsi que son rang.

Title : Some aspects of the arithmetic of functions fields related to Drinfeld Modules.

Keywords : Functions field- Drinfeld modules- Carlitz modules- Torsion points- Galois group.

Abstract : The aim of this thesis is the study of three aspects concerning the arithmetic of functions fields related to the Drinfeld modules. In the first part, we work over a rational functions field $\mathbb{F}_q(T)$. We introduce and study the notion of polynomials defining units on the roots of translates of Carlitz polynomials.
In the second part we continue to work over a rational function field $\mathbb{F}_q(T)$. We propose an analogue of the classical Laguerre polynomials. We show, among other things, that the Galois group of the n^{th} polynomial over $\mathbb{F}_q(T)$ is the general linear group $GL_n(\mathbb{F}_q)$.
In the last part we considered the following context. Let $k/\mathbb{F}_q$ be a global algebraic function field. Let ∞ be a place of k. Let A be the ring of elements of k regular outside ∞. Let ρ a Drinfeld A-module of rank one and sgn-normalized with respect to a fixed sign function. Let H_A^* be the normalizing field of ρ with respect to sgn. Let B be the integral closure of A in H_A^*. Let $\mathfrak{m}$ be an ideal of A. We focused on the study of the structure of the B-module $B\Lambda_{\mathfrak{m}}$ generated by the $\mathfrak{m}$-torsion points of the Drinfeld module ρ, as well as its rank.

UBFC UNIVERSITÉ BOURGOGNE FRANCHE-COMTÉ
Université Bourgogne Franche-Comté
32, avenue de l'Observatoire
25000 Besançon

Dédicaces

Je dédie cette thèse accompagnée d'un profond amour :

- À ma mère, celle qui m'a arrosée de tendresse et d'espoir.
- À mon père, qui m'a toujours encouragé dans mes études.
- À ma chère épouse Sanae, son amour et ses sacrifices m'ont procuré confiance et stabilité, aux moments difficiles.

C'est un moment de plaisir de dédier cette thèse, à mes chères filles : Noura, Maryam et Hiba.

Remerciements

Je voudrais tout d'abord exprimer ma vive reconnaissance à Monsieur HASSAN OUKHABA, qui m'a encadré tout au long de cette thèse et qui m'a fait partager ses intuitions. Il m'a aidé par ses commentaires, ses conseils et ses suggestions à développer mes capacités d'intuition et de rédaction des résultats scientifiques, et m'a ouvert le chemin pour lancer mes premières publications dans des journaux spécialisés. J'ai appris beaucoup de son talent, de son expérience et des discussions que j'ai eues avec lui le long de ces années de thèse. Il m'a toujours entouré de sa confiance et m'a encouragé à venir à bout de ce travail. Je le remercie pour tout ce qu'il a fait pour moi et de m'avoir honoré par son acceptation de diriger ma thèse.

Je remercie aussi les Professeurs Mokhtar-Kharroubi Mustapha de l'université de Franche-Comté et Bayad Abedlmejid de l'université d'Évry Val d'Essonne, qui ont accepté d'être parmi les membres du comité de suivie de ma thèse. J'adresse tous mes remerciements à Monsieur Jilali Assim, Professeur à l'université Moulay Ismail Meknès-Maroc, ainsi qu'à Monsieur Bayad Abedlmejid, Professeur à l'université d'Évry Val d'Essonne, de l'honneur qu'ils m'ont fait en acceptant d'être rapporteurs de cette thèse.

J'exprime ma gratitude à Monsieur Movahhedi, Chazad, Professeur à l'université de Limoges et à Madame Cécile Armana, Professeure à l'Université de Franche-Comté, qui ont bien voulu être examinateurs.

En fin, je suis aussi reconnaissant à madame Martine Gautheron, gestionnaire au bureau des écoles doctorales Environnement-Santé et Carnot-Pasteur, qui, par sa gentillesse, m'a apportée son aide dans toutes les tâches administratives durant ces années de thèse.

Table des matières

Résumé

Le but de cette thèse est l'étude de trois aspects concernant l'arithmétique des corps de fonctions en lien avec les modules de Drinfeld.

Dans la première partie, nous travaillons au-dessus d'un corps de fonctions rationnelles $\mathbb{F}_q(T)$. Nous introduisons et nous étudions la notion de polynômes définissant des unités sur les racines de translatés de polynômes de Carlitz.

Dans la seconde partie nous continuons de travailler au-dessus d'un corps de fonctions rationnelles $\mathbb{F}_q(T)$. Nous proposons un analogue des polynômes de Laguerre classiques. Nous montrons, entre autres, que le groupe de Galois du $n^{\text{ième}}$ polynôme sur $\mathbb{F}_q(T)$ est le groupe général linéaire $GL_n(\mathbb{F}_q)$.

Dans la dernière partie nous considérons le contexte suivant. Soit $k/\mathbb{F}_q$ un corps global de fonctions algébriques. Soit ∞ une place de k. Soit A l'anneau des éléments de k réguliers en dehors de ∞. Soit ρ un A-module de Drinfeld de rang 1 et normalisé par rapport à une fonction signe fixée. Soit H_A^* le corps normalisant de ρ. Soit B la clôture intégrale de A dans H_A^*. Soit $\mathfrak{m}$ un idéal de A . Nous étudions alors la structure du B-module $B\Lambda_{\mathfrak{m}}$ engendré par les points de $\mathfrak{m}$-torsion du module de Drinfeld ρ, ainsi que son rang.

Abstract

The aim of this thesis is the study of three aspects concerning the arithmetic of functions fields related to the Drinfeld modules.

In the first part, we work over a rational functions field $\mathbb{F}_q(T)$. We introduce and study the notion of polynomials defining units on the roots of translates of Carlitz polynomials.

In the second part we continue to work over a rational function field $\mathbb{F}_q(T)$. We propose an analogue of the classical Laguerre polynomials. We show, among other things, that the Galois group of the n^{th} polynomial over $\mathbb{F}_q(T)$ is the general linear group $GL_n(\mathbb{F}_q)$.

In the last part we considered the following context. Let $k/\mathbb{F}_q$ be a global algebraic function field. Let ∞ be a place of k. Let A be the ring of elements of k regular outside ∞. Let ρ a Drinfeld A-module of rank one and sgn-normalized with respect to a fixed sign function. Let H_A^* be the normalizing field of ρ with respect to sgn. Let B be the integral closure of A in H_A^*. Let $\mathfrak{m}$ be an ideal of A. We focused on the study of the structure of the B-module $B\Lambda_\mathfrak{m}$ generated by the $\mathfrak{m}$-torsion points of the Drinfeld module ρ, as well as its rank.

Introduction générale

Cette thèse est organisée en trois chapitres. Chaque chapitre traite d'une question particulière concernant l'arithmétique des corps de fonctions, en lien avec les modules de Drinfeld.

Ainsi, le premier chapitre est dédié à la caractérisation des polynômes définissant une infinité d'unités. Expliquons de quoi il s'agit. Soit $q = p^n$ la puissance d'un nombre premier p, et soit $\mathbb{F}_q$ le corps fini à q éléments. Posons $A = \mathbb{F}_q[T]$, où T est une variable formelle. Soit $\overline{k}$ une clôture algébrique du corps $k = \mathbb{F}_q(T)$. Notons $\overline{k}\{\{\tau\}\}$ (resp. $\overline{k}\{\tau\}$) la $\overline{k}$-algèbre des séries (resp. polynômes) en le Frobenius τ vérifiant la relation

$$\tau r = r^q \tau, \quad \forall r \in \overline{k}.$$

Nous utiliserons dans les deux premiers chapitres le module de Carlitz ρ qui est par définition l'homomorphisme de $\mathbb{F}_q$-algèbres $\rho : \mathbb{F}_q[T] \longrightarrow k\{\tau\}$ tel que l'image de T est $\rho_T = \tau + T\tau^0$. Alors le Théorème 1.4.1, qui est le résultat principal de ce premier chapitre, peut être énoncé comme suit. Soient $a, b \in A$ tels que $a \neq b$. Soit Γ un ensemble infini de polynômes unitaires $N \in A$. Soit $f \in A[X]$ un polynôme irréductible. Supposons que pour tout $N \in \Gamma$, les éléments $\rho_N(\alpha) - a$ et $\rho_N(\alpha) - b$ sont des unités de $A[\alpha]$ pour toute racine α du polynôme f. Alors si $q > 2$ le polynôme f vérifie une des conditions suivantes.
1) Il existe $\varepsilon \in \mathbb{F}_q^*$ et un polynôme unitaire $M \in A$ tel que $f = \varepsilon \Phi_M$, où Φ_M est le polynôme cyclotomique défini dans [16, section 2]. De plus, $a, b \in \mathbb{F}_q^*$ et M divise tous les polynômes $N \in \Gamma$.
2) Le polynôme f appartient à l'ensemble $\Delta_{a,b}$, qui consiste en tous les polynômes irréductibles $g \in A[X]$ tel qu'il existe une suite de polynômes unitaires $(N_i)_{i\in\mathbb{N}}$, $N_i \in A$, dont les degrés forment une suite strictement croissante $(d_i)_{i\in\mathbb{N}^*}$ et tel que g divise tous les polynômes

$$\frac{(\rho_{N_i}(X) - a)}{b - a} - \Big(\frac{\rho_{N_0}(X) - a}{b - a}\Big)^{p^{d_i}}, \quad i \geq 1.$$

Il est donc intéressant de répondre à la question suivante.

– Q_1. Peut-on décrire explicitement l'ensemble $\Delta_{a,b}$?

Le deuxiéme chapitre est consacré à la construction et l'étude, pour tout entier naturel n, d'un

polynôme linéaire

$$\mathcal{L}_{n,\rho} = e_\rho(\tau)\Psi^n(\log_\rho(\tau)\tau^n) \in A\{\tau\},$$

où $e_\rho(\tau)$ et $\log_\rho(\tau)$ désignent respectivement l'exponentielle et le logarithme du module de Carlitz ρ. L'opérateur $\Psi : \overline{k}\{\{\tau\}\} \longrightarrow \overline{k}\{\{\tau\}\}$ est tel que

$$\Psi(\sum_{i=0}^{\infty} c_i\tau^i) = \sum_{i=1}^{\infty} c_i[i]\tau^{i-1},$$

où on a posé $[i] = T^{q^i} - T$, pour tout entier naturel i. Nous attirons l'attention du lecteur que l'application $\Delta(f) = \Psi(f) \cdot \tau$ est une $\overline{k}$-dérivation de $\overline{k}\{\{\tau\}\}$. Les polynômes $\mathcal{L}_{n,\rho}$ sont défini par analogie avec les polynômes de Laguerre classiques

$$L_n(x) = \frac{e^x}{n!}\frac{d^n}{dx^n}(e^{-x}x^n).$$

L'intérêt des polynômes $\mathcal{L}_{n,\rho}$ est qu'ils ont un comportement similaire à celui des $L_n(x)$. Ils vérifient en particulier la relation de récurrence

$$\mathcal{L}_{n+1,\rho} = \mathcal{L}_{n,\rho}([n+1] + [n] - \tau) - \mathcal{L}_{n-1,\rho}[n]^2.$$

Le résultat le plus remarquable au sujet de ces polynômes est le Théorème 2.3.18, où nous prouvons que le groupe de Galois sur le corps $k = \mathbb{F}_q(T)$ de $\mathcal{L}_{n,\rho}(X)$ est isomorphe au groupe général linéaire $\mathrm{GL}_n(\mathbb{F}_q)$,

$$\mathrm{Gal}(\mathcal{L}_{n,\rho}(X)/k) \simeq \mathrm{GL}_n(\mathbb{F}_q),$$

en analogie totale avec le vieux résultat de Schur dans [34], qui affirme que le groupe de Galois sur le corps $\mathbb{Q}$ de $L_n(X)$ est isomorphe au groupe symétrique S_n. Dès lors se pose les questions suivantes :

– Q_2. Étendre la définition de $\mathcal{L}_{n,\rho}$ pour obtenir l'analogue des polynômes de Laguerre généralisés.

– Q_3. Étendre toutes ces constructions au cas d'un corps global de fonctions algébriques à une variable.

Dans le troisième chapitre nous nous penchons sur le calcul du rang d'un certain module lié aux points de torsion d'un module de Drinfeld. Rappelons le contexte. Soit $k/\mathbb{F}_q$ un corps global de fonctions algébriques. Soit ∞ une place de k. Soit A l'anneau des éléments de k réguliers en dehors de ∞. Soit ρ un A-module de Drinfeld de rang 1 et normalisé par rapport à une fonction signe fixée. Soit H_A^* le corps normalisant de ρ, qui est tout simplement le corps engendré par les coefficients des polynômes ρ_x, $x \in A$. Notons aussi E_ρ le sous-espace vectoriel de $H_A^*\{\tau\}$ engendré par les polynômes ρ_x, $x \in A$. Alors nous montrons dans le Théorème 3.4.10, que l'espace vectoriel quotient $H_A^*\{\tau\}/E_\rho$ est de dimension inférieure ou égale au genre g de k,

$$\dim_{H_A^*}(H_A^*\{\tau\}/E_\rho) \leq g,$$

avec égalité si le degré de la place ∞ est égal à 1. Cela pose deux questions, Q_4 et Q_5, à savoir

– Q_4. A-t-on l'égalité $\dim_{H_A^*}(H_A^*\{\tau\}/E_\rho) = g$ dans tous les cas ?

– Q_5. Que se passe-t-il si on considère des modules de Drinfeld de rang supérieur à 1 ?

Soit maintenant B la clôture intégrale de A dans H_A^*. Soit $\mathfrak{m}$ un idéal de A et soit $\Lambda_\mathfrak{m}$ l'ensemble des racines de $\rho_\mathfrak{m}$. Nous savons que $\Lambda_\mathfrak{m}$ est un A-module isomorphe à $A/\mathfrak{m}$. Nous avons aussi réussi à montrer dans le Théorème 3.4.13, que si $\mathfrak{m}$ est premier à un certain idéal $\mathfrak{m}_\rho$ alors le B-module engendré par $\Lambda_\mathfrak{m}$, que nous noterons $B\Lambda_\mathfrak{m}$, est libre de rang

$$\mathrm{rang}_B(B\Lambda_\mathfrak{m}) = \dim_{\mathbb{F}_q}(A/\mathfrak{m}),$$

au moins si $q > 2$. Nous avons aussi une formule dans le cas $q = 2$. Nous sommes parvenus à déterminer l'idéal $\mathfrak{m}_\rho$ dans de nombreux cas, notamment, si $d_\infty = 1$ et $g \leq 1$ alors $\mathfrak{m}_\rho = A$. D'où les questions

– Q_6. Que vaut l'idéal $\mathfrak{m}_\rho$ en général ?

– Q_7. Dans le cas où $\mathfrak{m}_\rho \neq A$, quelle serait la structure du B-module $B\Lambda_\mathfrak{m}$ ainsi que son rang ?

Chapitre 1

Polynômes définissant des unités dans les corps de fonctions

Nous introduisons dans ce chapitre la notion de polynômes définissant des unités dans le cas des corps de fonctions rationnelles, en utilisant la théorie cyclotomique de Carlitz. Nous nous inspirons en cela du travail d'Osnel Broche et Ángel del Río, publié en 2016, cf. [4].

Dans tout ce chapitre on fixe un corps fini $\mathbb{F}_q$ à q éléments, où q est une puissance d'un nombre premier p. On notera $k = \mathbb{F}_q(T)$ le corps de fonctions rationnelles de variable T sur $\mathbb{F}_q$. On considère $A = \mathbb{F}_q[T]$ et $v_\infty : k \longrightarrow \mathbb{R} \sqcup \{\infty\}$ la valuation donnée par $v_\infty(\frac{1}{T}) = 1$. On note k_∞ le complété de k pour la v_∞-topologie. On note $\mathbb{C}_\infty$ le complété d'une clôture algébrique de k_∞, muni d'une extension de v_∞ notée aussi de la même façon. L'anneau A est un sous-anneau discret de k_∞, de plus k_∞/A est compact. Ce contexte est anologue à la situation classique :

$$A \sim \mathbb{Z}, \quad k \sim \mathbb{Q}, \quad \text{et } k_\infty \sim \mathbb{R}$$

1.1 Théorie algébrique des modules de Carlitz

1.1.1 L'action du module de Carlitz.

Soit $\overline{k}$ une clôture algébrique du corps $k = \mathbb{F}_q(T)$. Notons $\overline{k}\{\{\tau\}\}$ (resp. $\overline{k}\{\tau\}$) la $\overline{k}$-algèbre des séries (resp. polynômes) en le Frobenius τ vérifiant la relation

$$\tau r = r^q \tau, \quad \forall r \in \overline{k}.$$

Définition 1.1.1. On appelle module de Carlitz, l'homomorphisme de $\mathbb{F}_q$-algèbres

$\rho : A \longrightarrow k\{\tau\}$ donné par

$$\rho_T = T + \tau.$$

Pour tout $a \in A$ on note ρ_a l'image de a par ρ.

Proposition 1.1.2. *[16, propostion 1.1] Soit a un élément de A de degré d, alors*

$$\rho_a(\tau) = \sum_{i=0}^{d} \begin{bmatrix} a \\ i \end{bmatrix} . \tau^i$$

où chaque $\begin{bmatrix} a \\ i \end{bmatrix}$ est un polynôme de A de degré $(d-i)q^i$. De plus $\begin{bmatrix} a \\ 0 \end{bmatrix} = a$ et $\begin{bmatrix} a \\ d \end{bmatrix}$ est le coefficient dominant de a.

Définition 1.1.3. Pour tout $a \in A$ de degré d, on pose

$$\rho_a(X) = \sum_{i=0}^{d} \begin{bmatrix} a \\ i \end{bmatrix} . X^{q^i} \in A[X]$$

Le module de Carlitz nous permet de définir une nouvelle structure de A-module sur $\overline{k}$ (ou sur $\mathbb{C}_\infty$), dite action du module de Carlitz, donnée par :

$$a.u = \rho_a(u), \quad \forall a \in A, \quad \forall u \in \overline{k} \text{ ou } u \in \mathbb{C}_\infty$$

N.B : On peut utiliser la notation $\rho_a(u) = u^a$, intoduite par Hayes dans [16].

Pour $a \in A$, on note par Λ_a l'ensemble des points de a-torsion de $\overline{k}$; C'est l'ensemble des éléments $u \in \overline{k}$ tels que $\rho_a(u) = 0$. Alors Λ_a est un sous-A-module de $\overline{k}$. Puisque ρ_a est séparable, Λ_a est un $\mathbb{F}_q$-espace vectoriel de dimension d.

Théorème 1.1.4. *[16, Theorem 1.6] Le A-module Λ_a est cyclique, isomorphe à A/aA, où aA est l'idéal de A engendré par a.*

Corollaire 1.1.5. *[16, Corollary 1.8] Le A-module Λ_a admet exactement $\phi(a)$ générateurs. Plus précisément, si λ est un générateur de Λ_a et $b \in A$, alors $\rho_b(\lambda)$ est un générateur si et seulement si a et b sont premiers entre eux, où $\phi(a)$ est l'ordre du groupe multiplicatif de l'anneau A/aA.*

1.1.2 Le corps de fonctions cyclotomique $k(\Lambda_a)$.

Soit $a \in A$ un polynôme de degré strictement positif. Considérons l'extension de corps $k(\Lambda_a)$ de k engendrée par le A-module fini Λ_a. Soit λ un générateur du A-module cyclique Λ_a. Puisque $\rho_b(\lambda) \in A[\lambda]$ pour tout $b \in A$, on a $k(\Lambda_a) = k(\lambda)$. Aussi, puisque Λ_a est l'ensemble des racines du

polynôme séparable $\rho_a(x) \in A[x] \subseteq k[x]$, l'extension $k(\Lambda_a)/k$ est Galoisienne finie. Les éléments de Λ_a sont entiers sur A car le coefficient dominant de $\rho_a(x)$ est dans $\mathbb{F}_q$. De plus, si O_a désigne la fermeture intégrale de A dans $k(\Lambda_a)$, alors on a $O_a = A[\lambda]$, voir [26, Proposition 12.9].

Soit G_a le groupe de Galois de l'extension $k(\Lambda_a)/k$. Puisque l'action du module de Carlitz est donnée par des polynômes à coefficients dans k, alors cette action commute avec celle de G_a sur $\overline{k}$. Si on fixe un générateur λ de Λ_a, alors chaque $\sigma \in G_a$ est déterminé par son action sur λ. Ainsi, $\sigma(\lambda) = \rho_b(\lambda)$ pour un certain b de A premier à a, car σ transporte un générateur de Λ_a à un autre générateur de Λ_a. De plus, b ne dépend pas du choix de λ. Ainsi, l'application

$$\Psi_a : \sigma \longmapsto b \ mod \ aA$$

définit bien un morphisme de groupes injectif de G_a dans le groupe des unités $(A/aA)^*$ de l'anneau $A/(aA)$. On a les résultats suivants,

Théorème 1.1.6. *[26, Theorem 12.8] Soit $a \in A$, et écrivons $a = \alpha P_1^{e_1} ... P_t^{e_t}$ sa décomposition en polynômes irréductibles, où $\alpha \in \mathbb{F}_q$ et les P_i sont des polynômes unitaires irréductibles de A. Alors, $k(\Lambda_a)$ est le compositum des corps $k(\Lambda_{P_i^{e_i}})$. Les places correspondants aux idéaux premiers P_iA, $1 \leq i \leq t$, sont les seules places finies de k ramifiées dans $k(\Lambda_a)/k$. On a $[k(\Lambda_a) : k] = \phi(a)$, en particulier Ψ_a est un isomorphisme.*

Théorème 1.1.7. *[26, Theorem 12.10] Soit $b \in A$ un polynôme unitaire, irréductible premier à a. Alors, l'automorphisme d'Artin de l'idéal premier bA dans l'extension $k(\Lambda_a)/k$ est l'automorphisme σ_b qui à chaque $\lambda \in \Lambda_a$ associe $\rho_b(\lambda)$. Soit f le plus petit entier tel que $b^f \equiv 1 \ mod \ aA$. Alors, bO_a est le produit de $\dfrac{\phi(a)}{f}$ idéaux premiers dont le degré résiduel égal à f. En particulier, bA se décompose totalement si et seulement si $b \equiv 1 \ mod \ aA$.*

1.1.3 Ramification en ∞.

On note par ∞ la place de k donnée par la valuation v_∞.

Théorème 1.1.8. *[26, Theorem 12.14] Soit $J = \left\{\sigma_\alpha \in G_a |\ \alpha \in \mathbb{F}_q^*\right\}$ et posons $k(\Lambda_a)^+$ le corps fixé par J. Alors ∞ se décompose totalement dans $k(\Lambda_a)^+$ et chaque premier au dessus de ∞ dans $k(\Lambda_a)^+$ est totalement et modérement ramifié dans $k(\Lambda_a)$. En particulier, l'indice de ramification de ∞ dans l'extension $k(\Lambda_a)/k$ est $e_\infty = q - 1$.*

Corollaire 1.1.9. *Pour tout $a \in A$, le corps des constantes $k(\Lambda_a)$ est $\mathbb{F}_q$. C'est à dire, L'extension $k(\Lambda_a)/k$ est géométrique.*

1.2 Polynôme définissant des unités dans les corps de fonctions

Sot M un élément non nul de A, d'après les rappels faits dans les sections précédentes on sait que si λ est un générateur du A-module Λ_M alors les autres générateurs sont λ^N, où $N \in A$ est premier à M. De plus, le polynôme irréductible de λ sur k est

$$\Phi_M(X) = \prod_{N \in S} (X - \lambda^N),$$

où S est un système complet de représentant des classes inversibles de l'anneau A/MA. Il est clair que $\Phi_M(X) \in A[X]$.

Définition 1.2.1. Soient $a, N \in A$ tels que $N \neq 0$, et soit $f \in A[X]$. Si $f \neq 0$ alors les propriétés suivantes sont équivalentes
1) L'image de f dans $A[X]/(X^N - a)A[X]$ est inversible.
2) Il existe $p, q \in A[X]$ tel que $f(X)p(X) + (X^N - a)q(X) = 1$
3) $f(\lambda)$ est une unité dans $A[\lambda]$ pour toute racine λ de $X^N - a$.
De plus, si f est irréductible alors les trois propriétés ci-dessus sont équivalentes à
4) $\alpha^N - a$ est une unité dans $A[\alpha]$ pour toute racine α de f.
Lorsque la propriété 1) est satisfaite, on dit que f définit des unités sur les racines de $\rho_N(X) - a$.

1.3 Les polynômes cyclotomiques définissant des unités

Notre objectif dans cette section, est de donner la liste complète des pairs $\{a, \Phi_M\}$ tels que $a \in A$ et Φ_M définit des unités sur les racines de $\rho_N(X) - a$ pour une infinité de polynômes unitaires $N \in A$. Nous utiliserons les propriétés des polynômes cyclotomiques Φ_M, où $M \in A$. On notera $Div(M)$ l'ensemble des diviseurs unitaires de M, et comme d'habitude, on note μ la fonction de Möbius sur A.

1. On a
$$X^M = \prod_{D \in Div(M)} \Phi_D(X), \tag{1.3.1}$$

2. D'après l'inversion de Möbius on obtient
$$\Phi_M(X) = \prod_{D \in Div(M)} \left(X^D\right)^{\mu(\frac{M}{D})}, \tag{1.3.2}$$

3. Pour des polynômes unitaires irréductibles deux à deux distincts $P_1, P_2, \ldots, P_r$ dans A, et des entiers positifs $\alpha_1, \ldots, \alpha_r$ on a

$$\Phi_{P_1^{\alpha_1}\cdots P_r^{\alpha_r}}(X) = \Phi_{P_1P_2\cdots P_r}\left(X^{P_1^{\alpha_1-1}\cdots P_r^{\alpha_r-1}}\right). \tag{1.3.3}$$

4. Si M et L sont premiers entre eux et unitaires dans A, on a

$$\Phi_{ML}(X) = \prod_{D\in Div(M)} \Phi_L\left(X^D\right)^{\mu\left(\frac{M}{D}\right)}. \tag{1.3.4}$$

5. Pour $M \neq 1$ unitaire dans A, on a

$$\sum_{D\in Div(M)} \mu(D) = 0. \tag{1.3.5}$$

Pour tout polynôme non nul $M \in A$, on note $\lambda_M \in \overline{k}$ une racine fixée de $\Phi_M(X)$.

Lemme 1.3.1. *Soient $M, N, a \in A$ tels que M et N sont des polynômes unitaires. Soit $D = \dfrac{M}{\gcd(M,N)}$. Alors les propriétés suivantes sont équivalentes*
a) Φ_M définit des unités sur les racines de $\rho_N(X) - a$.
b) $\lambda_D - a$ est une unité dans $A[\lambda_M]$.
c) $\lambda_D - a$ est une unité dans $A[\lambda_D]$.
d) $\Phi_D(a) \in \mathbb{F}_q^*$.

Démonstration. Voir la preuve de [4, Proposition 3]. □

Corollaire 1.3.2. *Soit $a \in \mathbb{F}_q^*$ et soit $M_1, \ldots, M_s \in A$ des polynômes unitaires. Alors le polynômes $f = \Phi_{M_1}\cdots\Phi_{M_s}$ définit des unités sur les racines de $\rho_N(X) - a$ pour tout N multiple commun des polynômes M_i, $i = 1, \ldots s$.*

Démonstration. Soit $N \in A$ unitaire multiple commun des polynômes M_i, $i = 1, \ldots s$. D'après la Définition 1.2.1, $f = \Phi_{M_1}\cdots\Phi_{M_s}$ définit des unités sur les racines de $\rho_N(X) - a$ si, et seulement si, pour tout $i \in \{1, \ldots, s\}$ le polynôme Φ_{M_i} définit des unités sur les racines de $\rho_N(X) - a$. D'après le Lemme 1.3.1, ceci est équivalent à $\Phi_{D_i}(a) \in \mathbb{F}_q^*$ pour tout $i \in \{1, \ldots, s\}$, où $D_i = \dfrac{M_i}{\gcd(M_i, N)}$. Or on a supposé que M_i divise N, donc $D_i = 1$ d'où $\Phi_{D_i}(a) = a$. □

Étudions maintenant la condition $\Phi_M(a) \in \mathbb{F}_q^*$.

Lemme 1.3.3. *Soit M un polynôme non nul dans A. Soit w une valuation normalisée de $k(\Lambda_M)$ au-dessus de v_∞. Soit λ un élément non nul de Λ_M. Alors on a $w(\lambda) \geq 0$ ou $w(\lambda) = -1$.*

Démonstration. On sait, d'après le Théorème 1.1.8 que $w = (q-1)v_\infty$ sur k. Notons $deg(M)$ par d et le coefficient dominant de M par a_d.

Si $d = 1$ alors, grâce à la Proposition 1.1.2, on a $0 = \lambda^M = a_1\lambda^q + M\lambda$. Puisque $\lambda \neq 0$ on obtient immédiatement que $w(\lambda) = -1$. Si $d \geq 2$ et $w(\lambda) < 0$ alors pour tout $i \in \{0, \dots, d\}$ on a

$$w\left(\begin{bmatrix} M \\ i \end{bmatrix} \lambda^{q^i}\right) = f(i),$$

où $f(x) = -(q-1)(d-x)q^x + w(\lambda)q^x$ et $\begin{bmatrix} M \\ i \end{bmatrix}$ est définit dans la Proposition 1.1.2. Or la fonction f est strictement décroissante sur $[0, d-1]$. Ainsi on a

$$w\left(\sum_{i=0}^{d-1} \begin{bmatrix} M \\ i \end{bmatrix} \lambda^{q^i}\right) = \min_{0\leq i\leq d-1}\left(w\left(\begin{bmatrix} M \\ i \end{bmatrix} \lambda^{q^i}\right)\right) = w\left(\begin{bmatrix} M \\ d-1 \end{bmatrix} \lambda^{q^{d-1}}\right) = q^{d-1}(w(\lambda) - (q-1)).$$

L'équation $\lambda^M = 0$ implique alors $w\left(\lambda^{q^d}\right) = q^{d-1}(w(\lambda) - (q-1))$ et donc $w(\lambda) = -1$. □

Proposition 1.3.4. *Soit M un polynôme non nul dans A et soit $a \in A$. Alors*

$$\Phi_M(a) \in \mathbb{F}_q^* \Longrightarrow \begin{cases} a \in \mathbb{F}_q^* & si \quad \deg(M) = 0, \\ a \in \mathbb{F}_q & si \quad \deg(M) > 0 \quad et \quad q \geq 3, \\ a = M + 1 & si \quad \deg(M) = 1 \quad et \quad q = 2, \\ deg(a) \leq 1 & si \quad \deg(M) \geq 2 \quad et \quad q = 2. \end{cases}$$

Démonstration. Le cas $\deg(M) = 0$ est trivial puisque, si $M = a_0 \in \mathbb{F}_q^*$ alors $X^M = a_0X$ et $\Phi_M(X) = X$. Supposons que $\deg(M) \geq 1$ et soit $\mathbb{U}_M$ l'ensemble des racines de Φ_M. Soit w une valuation normalisée de $k(\Lambda_M)$ au-dessus de v_∞. Supposons qu'on a $\deg(a) > 1$ ou $q > 2$ et $\deg(a) = 1$, alors grâce au Lemme 1.3.3 on a $w(a) = -(q-1)deg(a) < -1 \leq w(\lambda)$, pour tout $\lambda \in \mathbb{U}_M$. Si $\Phi_M(a) \in \mathbb{F}_q^*$ alors

$$0 = w\left(\Phi_M(a)\right) = \sum_{\lambda\in\mathbb{U}_M} w(a - \lambda) = \deg(\Phi_M)w(a).$$

Ceci implique que $\deg(\Phi_M) = 0$, ce qui est absurde. Ainsi nous avons nécessairement $\deg(a) \leq 1$. De plus si $q > 2$ alors $a \in \mathbb{F}_q$. Reste à vérifier que si $q = 2$ et, M et a sont de degré 1 alors $a = M + 1$. Or si $M = T + a_0 \in A$, alors $\rho_{T+a_0}(X) = X^2 + (T + a_0)X$ et $\Phi_M(X) = X + T + a_0$. Donc $\Phi_M(a) \in \mathbb{F}_q^*$ si et seulement si $a = M + 1$. □

Proposition 1.3.5. *Supposons $q > 2$. Soit M un polynôme unitaire non nul dans A et soit $a \in A$. Alors*

$$\Phi_M(a) \in \mathbb{F}_q^* \iff \begin{cases} a \in \mathbb{F}_q^* & si \quad \deg(M) = 0 \ (M = 1), \\ a = 0 & si \quad \deg(M) > 0 \ et \ M \ n'est \ pas \ puissance \ d'un \ polynôme \ irréductible. \end{cases}$$

Démonstration. Le cas $M = 1$ est trivial. Supposons que $\deg(M) \geq 1$. Selon la Proposition 1.3.4 on doit considérer les cas suivants :

1. Le cas $a = 0$ et $M = P^n$, où P est un polynôme unitaire irréductible dans A. D'après la formule (1.3.2) on a $\Phi_M(X) = X^{P^n}/X^{P^{n-1}}$, et en particulier $\Phi_M(0) = P \notin \mathbb{F}_q^*$.

2. Le cas $a = 0$ et $M = P_1^{\alpha_1} \cdots P_r^{\alpha_r}$, où $P_1, \ldots, P_r$ sont des polynômes unitaires distincts irréductibles dans A et $\alpha_1, \ldots, \alpha_r$ sont des entiers positifs. Alors en évaluant en 0, l'égalité polynômiale $\dfrac{X^M}{X} = \prod_{D \in Div(N), D \neq 1} \Phi_D(X)$ déduite de la formule (1.3.1), on obtient $M = \prod_{D \in Div(N), D \neq 1} \Phi_D(0)$. Or puisque $\Phi_{P_i^e}(0) = P_i$ pour tout entier positif e on trouve la relation

$$\prod_{D \in \Xi} \Phi_D(0) = 1,$$

où Ξ est l'ensemble des diviseurs unitaires de M qui ne sont pas puissance de polynômes irréductibles. Ce qui prouve que $\Phi_M(0) \in \mathbb{F}_q^*$.

3. Le cas $a \in \mathbb{F}_q^*$ et $M = P^n$, où P est un polynôme unitaire irréductible dans A. Là encore, on va utiliser l'égalité $\Phi_M(X) = X^{P^n}/X^{P^{n-1}}$. Puisque la suite $\big((d-i)q^i\big)_i$ est strictement décroissante sur $[0, d-1]$ pour tout $d \geq 1$, on voit d'après la formule (1.1.2) que le degré en T de a^{P^n} est égale à $q^{n\deg(P)-1}$. Ainsi, si $n \geq 2$ alors le degré de $\Phi_M(a)$ est $q^{n\deg(P)-1} - q^{(n-1)\deg(P)-1} \neq 0$. Si $n = 1$ le degré de $\Phi_M(a)$ est $q^{\deg(P)-1} \neq 0$.

4. Le cas $a \in \mathbb{F}_q^*$ et $M = P_1^{\alpha_1} \cdots P_r^{\alpha_r}$, où $P_1, \ldots, P_r$ sont des polynômes unitaires irréductibles distincts dans A et $\alpha_1, \ldots, \alpha_r$ sont des entiers positifs. Posons $N = P_1^{\alpha_1 - 1} \cdots P_r^{\alpha_r - 1}$ et $b = a^N$. Si $N \neq 1$ alors $\deg(b) = q^{\deg(N)-1}$, en particulier $b \notin \mathbb{F}_q$. Puisque $\Phi_M(a) = \Phi_{P_1 \ldots P_r}(b)$ d'après la formule (1.3.3), on déduit que $\Phi_M(a) \notin \mathbb{F}_q^*$ grâce à la Proposition 1.3.4. Si $N = 1$ alors d'après la formule (1.3.2) on a $\Phi_M(a) = \prod_{D \in Div(M)} \big(a^D\big)^{\mu(\frac{M}{D})}$ et $q\deg\left(\Phi_M(a)\right) = \sum_{D \in Div(M), D \neq 1} \mu(\frac{M}{D}) q^{\deg(D)}$. L'hypothèse $\Phi_M(a) \in \mathbb{F}_q^*$ implique l'égalité $\sum_{D \in Div(M), D \neq 1} \mu(\frac{M}{D}) q^{\deg(D)} = 0$. Pour $i \in \{1, 2\}$ notons Ω_i l'ensemble des $D \in Div(M)$, $D \neq 1$ et $\mu(\frac{M}{D}) = (-1)^i$. Puisque $r \geq 2$ les ensembles Ω_1 et Ω_2 sont non vides et la dernière égalité s'écrit de la façon suivante.

$$\sum_{D \in \Omega_1} q^{\deg(D)} = \sum_{D \in \Omega_2} q^{\deg(D)}.$$

Or on peut facilement montrer la relation

$$\prod_{i=1}^{r}(1-q^{\deg(P_i)})-1=\begin{cases}\displaystyle\sum_{D\in\Omega_2}q^{\deg(D)}-\sum_{D\in\Omega_1}q^{\deg(D)} & \text{si } r \text{ est paire,}\\ \displaystyle\sum_{D\in\Omega_1}q^{\deg(D)}-\sum_{D\in\Omega_2}q^{\deg(D)} & \text{si } r \text{ est impaire.}\end{cases} \tag{1.3.6}$$

Ceci implique que $\prod_{i=1}^{r}(1-q^{\deg(P_i)})=1$, mais cela est impossible.

Ce qui achève la preuve de la Proposition. □

Lemme 1.3.6. *On suppose $q=2$. Alors*

(i) $\rho_{T^n}(1)=T+1$ et $\rho_{(T+1)^n}(1)=T$, pour tout entier $n>0$.

(ii) $\Phi_{T^n}(1)=\Phi_{(T+1)^n}(1)=1$, pour tout entier $n>1$.

(iii) $\rho_D(1)=(D(0)-D(1))\,T+D(1)$, pour tout polynôme $D\in\mathbb{F}_2[T]$. En particulier, si $D(0)=D(1)=1$ on a $\rho_D(1)=1$.

Démonstration. On montre (i) par récurrence sur l'entier n. On déduit (ii) de (i) puisque on a $\Phi_{P^n}(X)=\dfrac{X^{P^n}}{X^{P^{n-1}}}$ pour tout polynôme irréductible P dans A. Quant à (iii), il suffit de noter que $D=D(0)+\sum_{k=1}^{d}T^{n_k}$, et ensuite appliquer (i). □

Proposition 1.3.7. *On suppose $q=2$ et $a\in\mathbb{F}_2$. Écrivons $M=T^{\alpha}(T+1)^{\beta}N$, avec N unitaire et premier à $T(T+1)$. Alors $\Phi_M(a)=1$ si, et seulement si, l'une des conditions suivantes est satisfaite :*

(1) $a=0$ et M n'est pas une puissance d"un polynôme irréductible,

(2) $a=1$ et $M=1$,

(3) $a=1$, $\deg(M)\geq 2$, $N\neq 1$ et $(\alpha,\beta)\neq(1,1)$,

(4) $a=1$, $\deg(M)\geq 2$, $N=1$ mais $\alpha\neq 1$ et $\beta\neq 1$,

(5) $a=1$, $(\alpha,\beta)=(1,1)$ et N n'est pas une puissance d'un polynôme irréductible.

Démonstration. Puisque le cas $\deg(M)=0$ est évident et, puisque le cas $\deg(M)=1$ est impossible d'après la Proposition 1.3.4, on suppose que $\deg(M)\geq 2$. Alors en raisonnant comme le cas $q>2$, on peut montrer que $\Phi_M(0)=1 \iff M$ n'est pas une puissance d'un polynôme irréductible. Si $a=1$ on obtient les résultats suivants.

1. Si $M=T^{\alpha}$ ou $M=(T+1)^{\alpha}$ avec $\alpha\geq 2$, alors $\Phi_M(1)=1$ grâce au Lemme 1.3.6.

2. Si $M = T(T+1)$ alors $\Phi_M(1) = 0$ puisque on a $\Phi_{T(T+1)}(X) = X + 1$.
3. Si $M = T^\alpha(T+1)^\beta$ avec $\alpha > 1$ et $\beta > 1$, alors $1^{T^{\alpha-1}(T+1)^{\beta-1}} = 0$ grâce au Lemme 1.3.6, en particulier $\Phi_M(1) = \Phi_{T(T+1)}(1^{T^{\alpha-1}(T+1)^{\beta-1}}) = \Phi_{T(T+1)}(0) = 1$.
4. Si $M = T(T+1)^\beta$ avec $\beta > 1$, alors $\Phi_M(1) = \Phi_{T(T+1)}(1^{(T+1)^{\beta-1}}) = \Phi_{T(T+1)}(T) = T + 1$.
5. Si $M = T^\alpha(T+1)$ avec $\alpha > 1$, alors $\Phi_M(1) = \Phi_{T(T+1)}(1^{T^{\alpha-1}}) = \Phi_{T(T+1)}(T+1) = T$.
6. Si $M = T^\alpha(T+1)^\beta N$ avec $(\alpha, \beta) \neq (1,1)$ et $N \neq 1$ unitaire et premier à $T(T+1)$, alors d'une part, d'après l'étude précédente on a $\Phi_{T^\alpha(T+1)^\beta}(1) \neq 0$, d'autre part, d'après l'assertion (iii) du Lemme 1.3.6 on a $1^D = 1$ pour tout diviseur unitaire D de N. Les formules (1.3.4) et (1.3.5) impliquent
$$\Phi_M(1) = \prod_{D \in Div(N)} \left(\Phi_{T^\alpha(T+1)^\beta}(1^D)\right)^{\mu\left(\frac{N}{D}\right)} = \left(\Phi_{T^\alpha(T+1)^\beta}(1)\right)^{\sum_{D \in Div(N)} \mu\left(\frac{N}{D}\right)} = 1.$$
7. Si $M = T(T+1)N$ avec N unitaire et premier à $T(T+1)$, alors en utilisant la formule (1.3.4) et le fait que $\Phi_{T(T+1)}(X) = X + 1$ on obtient
$$\begin{aligned}\Phi_M(X) = \prod_{D \in Div(N)} \left(\Phi_{T(T+1)}(X^D)\right)^{\mu\left(\frac{N}{D}\right)} &= \prod_{D \in Div(N)} \left(X^D + 1\right)^{\mu\left(\frac{N}{D}\right)} \\ &= \prod_{D \in Div(N)} \left((X+1)^D\right)^{\mu\left(\frac{N}{D}\right)} = \Phi_N(X+1).\end{aligned}$$
Donc $\Phi_M(1) = \Phi_N(0)$. Ainsi $\Phi_M(1) = 1$ si, et seulement si, N n'est pas puissance d'un polynôme irréductible.

Ce qui achève le preuve du Lemme. □

Lemme 1.3.8. *On suppose $q = 2$. Alors on a :*

(i) $T^{T^n} = 0$ et $(T+1)^{(T+1)^n} = 0$, pour tout entier n positif.

(ii) $T^D = D(0).T$ et $(T+1)^D = D(1).(T+1)$, pour tout polynôme $D \in \mathbb{F}_2[T]$.

Démonstration. On montre (i) par récurrence sur n. Pour montrer (ii) il suffit de remarquer que $D = D(0) + \sum_{k=1}^{d} T^{n_k} = D(1) + \sum_{k=1}^{d'} (T+1)^{m_k}$, et ensuite appliquer (i). □

Proposition 1.3.9. *On suppose $q = 2$ et soit $a = T$ ou $a = T + 1$. Soit $M = a^n N$, avec N unitaire et premier à a, et n est un entier positif. Alors $\Phi_M(a) = 1$ si, et seulement si, $n \neq 1$ et $N \neq 1$ ou $n = 1$ et N n'est pas puissance d'un polynôme irréductible.*

Démonstration. Selon la Proposition 1.3.4, on a $\Phi_M(a) = 1$ implique que $M = a + 1$ ou $\deg(M) \geq 2$. Supposons que $\deg(M) \geq 2$. Alors, on doit considérer les cas suivants.

1. Si $n \geq 2$ et $N = 1$ alors d'après la formule (1.3.3) et le Lemme 1.3.8 on a $\Phi_M(a) = \Phi_a(a^{a^{n-1}}) = \Phi_a(0) = a$.
2. Si $n \neq 1$ et $N \neq 1$ alors puisque $\Phi_{a^n}(a) = a$ même pour $n = 0$ on obtient

$$\Phi_M(a) = \prod_{D \in Div(N)} \left(\Phi_{a^n}(a^D)\right)^{\mu\left(\frac{N}{D}\right)} = \prod_{D \in Div(N)} \left(\Phi_{a^n}(a)\right)^{\mu\left(\frac{N}{D}\right)} = \prod_{D \in Div(N)} (a)^{\mu\left(\frac{N}{D}\right)} = 1$$

   d'après la formule (1.3.4), le Lemme 1.3.8 et la formule (1.3.5).
3. Si $n = 1$ alors puisque $\Phi_a(X) = X + a$ on a

$$\begin{aligned}\Phi_M(X) = \prod_{D \in Div(N)} \left(\Phi_a(X^D)\right)^{\mu\left(\frac{N}{D}\right)} &= \prod_{D \in Div(N)} \left(X^D + a\right)^{\mu\left(\frac{N}{D}\right)} \\ &= \prod_{D \in Div(N)} \left((X+a)^D\right)^{\mu\left(\frac{N}{D}\right)} = \Phi_N(X+a),\end{aligned}$$

   d'après la formule (1.3.4) et le Lemme 1.3.8 (ii). On obtient l'égalié $\Phi_M(a) = \Phi_N(0)$. Ainsi $\Phi_M(a) = 1$ si, et seulement si, N n'est pas puissance d'un polynôme irréductible.

Ce qui achève la preuve de la Proposition. □

1.4 Résultat principal du chapitre

Dans cette dernière section nous allons montrer notre résultat principal du chapitre 1 sur les polynômes définissant une infinité d'unités. A cette fin, nous introduisons les sous-ensembles de $A[X]$ suivants, notés $\Delta_{a,b}$, où $a, b \in A$ sont des éléments distincts de A. Par définition $f \in \Delta_{a,b}$ si, et seulement si, f est irréductible dans $A[X]$ et il existe une suite infinie de polynômes unitaires $(N_i)_{i\in\mathbb{N}}$ dont les degrés forment une suites d'entiers strictement croissante $(d_i)_{i\in\mathbb{N}^*}$ tels que f divise tous les polynômes

$$\frac{(X^{N_i} - a)}{b - a} - \left(\frac{X^{N_0} - a}{b - a}\right)^{p^{d_i}}, \quad i \geq 1.$$

Notre argument crucial dans la démonstration du Théorème 1.4.1 est le suivant. Soit L un corps de fonctions global et soit $\mathbb{F}$ le corps des constantes de L. Soit S un ensemble fini de premier fini de L. Alors l'équation Diophantienne $X + Y = 1$ admet un nombre fini de solutions (u, v) telles que u et v sont des S-unités non constantes dans L et telles que l'extension $L/\mathbb{F}(u)$ est séparable [26, Theorem 7.19]. Mais comme on peut facilement vérifier les couples (u^{p^n}, v^{p^n}) satisfont aussi à l'équation $X + Y = 1$, sont des S-unités non constantes dans L alors que les extensions $L/\mathbb{F}(u^{p^n})$ sont inséparables. Ce phénomène nous amène à conclure qu'un polynôme f vérifiant les hypothèses

du théorème 1.4.1, peut avoir des facteurs irréductibles qui ne sont peut-être pas nécessairement des polynômes cyclotomiques, mais plutôt des éléments de $\Delta_{a,b}$. À ce stade cet ensemble nous semble mystérieux. Nous espérons pouvoir décrire complètement ses éléments dans un futur proche.

Théorème 1.4.1. *Soit $f \in A[X]$ et soient $a, b \in A$ tels que $a \neq b$. Soit $\Gamma \subseteq A$ un ensemble infini. On suppose que f définit des unités sur les racines de $\rho_N(X) - a$ et sur les racines de $\rho_N(X) - b$ pour tout $N \in \Gamma$. Soit $g \in A[X]$ un facteur irréductible de f. Alors g satisfait à l'une des conditions suivantes.*
1) Il existe $\varepsilon \in \mathbb{F}_q^*$ et un polynôme unitaire $M \in A$ tel que $g = \varepsilon\Phi_M$. De plus, si $q > 2$ alors $a, b \in \mathbb{F}_q^*$ et M divise tous les polynômes $N \in \Gamma$. Si $q = 2$ alors a et b sont de degré au plus égale à 1 et M est explicitement décrit dans la Proposition 1.3.7 et la Proposition 1.3.9.
2) Le polynôme g appartient à $\Delta_{a,b}$.

Démonstration. Soit $\alpha \in \overline{k}$ une racine de g. Les hypothèses impliquent qu'il existe une suite infinie de polynômes unitaires $N_0, N_1, \ldots, N_i, N_{i+1}, \ldots$ dont les degrés forment une suite croissante telle que $\alpha^{N_i} - a$ et $\alpha^{N_i} - b$ sont des unités dans $A[\alpha]$. Soit S_0 l'ensemble des places v de $L = k(\alpha)$ telles que $b - a$ ou α n'est pas unité en v. Soit S_∞ l'ensemble des places de L au dessus de la place infinie. Alors $S = S_0 \cup S_\infty$ est fini. Soit $\mathcal{O}_S$ l'anneau de Dedekind des éléments de L qui sont entiers en toute place $v \notin S$. Alors $A[\alpha] \subset \mathcal{O}_S$, En particulier si on pose

$$U_i = \frac{b - \alpha^{N_i}}{b - a} \quad \text{et} \quad V_i = \frac{\alpha^{N_i} - a}{b - a},$$

alors U_i et V_i sont des unités de $\mathcal{O}_S$, et sont tels que $U_i + V_i = 1$. Considérons l'application $\Psi : \mathbb{N} \longrightarrow \mathcal{O}_S^* \times \mathcal{O}_S^*$ définie par $\Psi(i) = (U_i, V_i)$, où $\mathcal{O}_S^*$ est le groupe des unités de $\mathcal{O}_S$. Si l'application Ψ est non injective, alors il existe $i_0 < i_1$ tel que $\alpha^{N_{i_1} - N_{i_0}} = 0$. En particulier g est égal, à une constante non nulle prés, à un polynôme cyclotomique Φ_M. De plus, grâce au Lemme 1.3.1, pour tout $N \in \Gamma$ on a $\Phi_{D_N}(a) \in \mathbb{F}_q^*$ et $\Phi_{D_N}(b) \in \mathbb{F}_q^*$, où $D_N = \dfrac{M}{\gcd(M, N)}$. Si $q > 2$, alors puisque $a \neq b$ on déduit de la Proposition 1.3.5 que $a, b \in \mathbb{F}_q^*$ et $D_N = 1$, en d'autres termes M divise tous les polynômes N. Si $q = 2$, on a d'après la Proposition 1.3.4, que $\deg(a) \leq 1$ et $\deg(b) \leq 1$, les polynômes correspondants sont décrits dans Proposition 1.3.7 et Proposition 1.3.9.

Supposons que l'application Ψ est injective. Alors, d'après [26, Theorem 7.19], il existe u et v dans $\mathcal{O}_S^*$ et deux suites d'entiers strictement croissantes $(i_j)_{j\in\mathbb{N}}$ et $(d_j)_{j\in\mathbb{N}}$ telles que

$$U_{i_j} = u^{p^{d_j}} \quad \text{et} \quad V_{i_j} = v^{p^{d_j}}.$$

Ce qui implique les relations

$$\frac{\alpha^{N_{i_j}} - a}{b - a} = \Big(\frac{\alpha^{N_{i_0}} - a}{b - a}\Big)^{p^{d_j - d_0}}, \quad \text{pour tout } j \geq 0.$$

En d'autres termes, g divise dans $A[X]$ tout les polynômes

$$\frac{(b-a)^{p^{d_j-d_0}}}{(b-a)}(X^{N_{i_j}}-a)-\left(X^{N_{i_0}}-a\right)^{p^{d_j-d_0}}, \quad j\geq 0.$$

C'est exactement la définition de $g \in \Delta_{a,b}$. □

Chapitre 2

Polynômes de type Laguerre sur le corps de fonctions rationnelles

Dans ce deuxième chapitre nous continuons à explorer les propriétés de polynômes liés aux modules de Carlitz. En effet, les notations étant celles du chapitre 1, nous allons introduire une suite de polynômes $(\mathcal{L}_{n,\rho})_n$, éléments de $k\{\tau\}$, ayant un comportement similaire au polynômes de Laguerre classiques. Nous montrerons en particulier que le groupe de Galois de $\mathcal{L}_{n,\rho}(X)$ sur $\mathbb{F}_q(T)$ est le groupe général linéaire $GL_n(\mathbb{F}_q)$. On conservera les notations du chapitre 1, ainsi, $A = \mathbb{F}_q[T]$, où $\mathbb{F}_q$ est le corps fini à q éléments, et $k = \mathbb{F}_q(T)$.

2.1 Polynômes de type Laguerre sur le corps de fonctions rationnelles

Le $n^{\text{ième}}$ polynôme de Laguerre classique est défini par la formule

$$L_n(x) = \frac{e^x}{n!}\frac{d^n}{dx^n}(e^{-x}x^n),$$

à partir de laquelle on déduit que $\widetilde{L}_n(x) = n!L_n(x)$ vérifie la relation

$$\widetilde{L}_{n+1}(x) = (n+1-x)\widetilde{L}_n(x) + x\widetilde{L}'_n(x). \tag{2.1.1}$$

qui implique en particulier que le polynôme $L_n(x)$ est de degré n et de coefficient dominant égal à $\dfrac{(-1)^n}{n!}$. La dérivation $D(f(x)) = xf'(x)$ appliquée à $\widetilde{L}_n(x)$ donne

$$D(\widetilde{L}_n(x)) = n\big(D(\widetilde{L}_{n-1}(x)) - x\widetilde{L}_{n-1}(x)\big).$$

Cela implique la formule

$$\widetilde{L}_{n+1}(x) = (2n+1-x)\widetilde{L}_n(x) - n^2\widetilde{L}_{n-1}(x), \tag{2.1.2}$$

et aussi l'équation différentielle

$$D^2(\widetilde{L}_n(x)) - xD(\widetilde{L}_n(x)) + nx\widetilde{L}_n(x) = 0. \tag{2.1.3}$$

Ce qui est encore remarquable, c'est le fait que $\widetilde{L}_n$ est irréductible dans $\mathbb{Q}[T]$. Cela a été prouvé pour la première fois par Schur dans [34]. Il a également prouvé que le groupe Galois sur $\mathbb{Q}$ de $\widetilde{L}_n$ est égale au groupe symétrique S_n.

2.2 Les polynômes $\mathcal{L}_{n,\rho}$

Dans la suite de ce chapitre, nous continuons de noter $\rho : \mathbb{F}_q[T] \longrightarrow k\{\tau\}$ le module de Carlitz caractérisé par la condition $\rho_T = T + \tau$. On rappelle que la fonction exponentielle de Carlitz $e_\rho(\tau) \in k\{\{\tau\}\}$ est l'unique élément de $k\{\{\tau\}\}$ qui satisfait à la multiplication complexe

$$\rho_a(\tau) \cdot e_\rho(\tau) = e_\rho(\tau) \cdot a\tau^0, \quad \text{pour tout } a \in \mathbb{F}_q[T],$$

et dont le terme constant égal à 1. On a

$$e_\rho(\tau) = \sum_{i=0}^{\infty} \frac{\tau^i}{D_i},$$

où $D_0 = 1$, et $D_i = (T^{q^i} - T)D_{i-1}^q$, voir [13, Definition 3.2.7]. La fonction logarithme de Carlitz est la fonction inverse de $e_\rho(\tau)$ dans $k\{\{\tau\}\}$. En d'autres termes on a

$$e_\rho(\tau) \cdot \log_\rho(\tau) = \log_\rho(\tau) \cdot e_\rho(\tau) = \tau^0.$$

On déduit de l'équation fonctionnelle de $e_\rho(\tau)$ la relation suivante

$$\log_\rho(\tau) \cdot \rho_a(\tau) = a \cdot \log_\rho(\tau), \quad \text{pour tout } a \in \mathbb{F}_q[T].$$

On rappelle le dévellopement en série de $log_\rho(\tau)$, on a

$$\log_\rho(\tau) = \sum_{i=0}^{\infty} (-1)^i \frac{\tau^i}{L_i},$$

où $L_0 = 1$, et $L_i = (T^{q^i} - T)L_{i-1}$, voir [13, page 56].

Définition 2.2.1. Pour tout entier naturel i, on pose $[i] = T^{q^i} - T$ et on note Δ et Ψ les opérateurs $\overline{k}$-linéaires définis sur $\overline{k}\{\{\tau\}\}$ par

$$\Delta(\sum_{i=0}^{\infty} c_i\tau^i) = \sum_{i=0}^{\infty}[i]c_i\tau^i \quad \text{et} \quad \Psi(\sum_{i=0}^{\infty} c_i\tau^i) = \sum_{i=1}^{\infty}[i]c_i\tau^{i-1}.$$

Lemme 2.2.2. *L'opérateur Δ est une $\overline{k}$-dérivation de $\overline{k}\{\{\tau\}\}$. De plus, on a*

$$\Delta(e_\rho(\tau)) = \tau \cdot e_\rho(\tau) \quad \textit{et} \quad \Delta(\log_\rho(\tau)) = -\log_\rho(\tau)\cdot\tau.$$

Démonstration. C'est une simple vérification basée en particulier sur la relation $[i+j] = [i] + [j]^{q^i}$. □

Les propriétés suivantes de l'application Ψ sont facile à vérifier. Soit $f(\tau), g(\tau) \in \overline{k}\{\{\tau\}\}$ et soit $a \in \overline{k}$. Alors on a

$$\Psi(f(\tau)g(\tau)) = \Psi(f(\tau))\delta(g(\tau)) + f(\tau)\Psi(g(\tau)),$$

où $\delta(g(\tau)) = \tau\cdot g(\tau)\cdot\tau^{-1}$. Si n est un entier strictement positif alors on a,

$$\Psi^n(f(\tau)\cdot\tau) = \Psi^n(f(\tau))\cdot\tau + \Psi^{n-1}(f(\tau))\cdot[n] \tag{2.2.1}$$

et

$$\Psi^n(f(\tau)\cdot a\tau^0) = \Psi^n(f(\tau))\cdot a^{q^n} \quad \text{(par récurence)}. \tag{2.2.2}$$

Définition 2.2.3. Pour un entier naturel n, on pose

$$\mathcal{L}_{n,\rho} = e_\rho(\tau)\Psi^n(\log_\rho(\tau)\tau^n).$$

Un calcul facile donne

$$\mathcal{L}_{0,\rho} = \tau^0, \qquad \mathcal{L}_{1,\rho} = -\tau + [1]\tau^0 \qquad \text{et} \qquad \mathcal{L}_{2,\rho} = \tau^2 - ([2]+[2]^q)\tau + [1][2]\tau^0.$$

Proposition 2.2.4. *Pour tout entier naturel n, on a*

$$\mathcal{L}_{n+1,\rho} = \mathcal{L}_{n,\rho}[n+1] - \tau\mathcal{L}_{n,\rho} + \Delta(\mathcal{L}_{n,\rho}). \tag{2.2.3}$$

En particulier $\mathcal{L}_{n,\rho} \in \mathbb{F}_q[T]\{\tau\}$ et est de degré n comme polynôme en τ. Si $a_{i,n}$ est le coefficient de τ^i dans $\mathcal{L}_{n,\rho}$, alors on a la relation

$$a_{i,n+1} = a_{i,n}[n+1]^{q^i} - a_{i-1,n}^q + a_{i,n}[i],$$

On en déduit par récurence que

$$a_{0,n} = [1][2]\cdots[n] = L_n \quad \textit{et} \quad a_{n,n} = (-1)^n.$$

Démonstration. On remarque d'abord que $\mathcal{L}_{n+1,\rho} = e_\rho(\tau)\Psi^{n+1}(f(\tau)\tau)$, où $f(\tau) = \log_\rho(\tau)\tau^n$. D'après l'équation (2.2.1) on a $\Psi^{n+1}(f\tau) = \Delta(\Psi^n(f)) + \Psi^n(f)[n+1]$. Cela donne l'égalité

$$\mathcal{L}_{n+1,\rho} = e_\rho(\tau)\Delta(\log_\rho(\tau)\mathcal{L}_{n,\rho}) + \mathcal{L}_{n,\rho}[n+1].$$

On en déduit notre relation (2.2.3) grâce au Lemme 2.2.2. Les autres assertions de la proposition sont des conséquences directes de la formule (2.2.3). □

Puisque nous avons déjà calculé le polynôme $\mathcal{L}_{2,\rho}$, la formule (2.2.3) donne

$$\mathcal{L}_{3,\rho} = -\tau^3 + ([3] + [3]^q + [3]^{q^2})\tau^2 - (([2] + [2]^q)[3]^q + [2][3])\tau + [1][2][3]\tau^0.$$

Proposition 2.2.5. *Pour tout entier positif n nous avons*

$$\Delta(\mathcal{L}_{n,\rho}) = \tau\mathcal{L}_{n,\rho} - \mathcal{L}_{n,\rho}\tau + (\Delta(\mathcal{L}_{n-1,\rho}) - \tau\mathcal{L}_{n-1,\rho})[n]. \tag{2.2.4}$$

Démonstration. D'une part nous avons,

$$\begin{aligned}
\Delta(\mathcal{L}_{n,\rho}) &= \Delta(e_\rho(\tau)\Psi^n(\log_\rho(\tau)\tau^n)) \\
&= \tau e_\rho(\tau)\Psi^n(\log_\rho(\tau)\tau^n) + e_\rho(\tau)\Delta(\Psi^n(\log_\rho(\tau)\tau^n)) \\
&= \tau\mathcal{L}_{n,\rho} + e_\rho(\tau)\Delta(\Psi^n(\log_\rho(\tau)\tau^n)).
\end{aligned}$$

D'autre part, le calcul de $\Delta(\log_\rho(\tau)\tau^n)$ donne la relation

$$\Psi(\log_\rho(\tau)\tau^n) = -\log_\rho(\tau)\tau^n + \log_\rho(\tau)[n]\tau^{n-1},$$

puis en appliquant Ψ^{n-1} on obtient

$$\Psi^n(\log_\rho(\tau)\tau^n) = -\Psi^{n-1}(\log_\rho(\tau)\tau^n) + \Psi^{n-1}(\log_\rho(\tau)[n]\tau^{n-1}),$$

puis

$$\begin{aligned}
\Delta(\Psi^n(\log_\rho(\tau)\tau^n)) &= \Psi^{n+1}(\log_\rho(\tau)\tau^n)\tau \\
&= -\Psi^n(\log_\rho(\tau)\tau^n)\tau + \Psi^n(\log_\rho(\tau)[n]\tau^{n-1})\tau \\
&= -\Psi^n(\log_\rho(\tau)\tau^n)\tau + \Psi^n(\log_\rho(\tau)\tau^{n-1}a)\tau \qquad (a^{q^{n-1}} = [n]) \\
&= -\Psi^n(\log_\rho(\tau)\tau^n)\tau + \Psi^n(\log_\rho(\tau)\tau^{n-1})a^{q^n}\tau \qquad \text{(d'après (2.2.2))} \\
&= -\Psi^n(\log_\rho(\tau)\tau^n)\tau + \Psi^n(\log_\rho(\tau)\tau^{n-1})\tau[n] \\
&= -\log_\rho(\tau)\mathcal{L}_{n,\rho}\tau + \Delta(\log_\rho(\tau)\mathcal{L}_{n-1,\rho})[n] \\
&= -\log_\rho(\tau)\mathcal{L}_{n,\rho}\tau - \log_\rho(\tau)\tau\mathcal{L}_{n-1,\rho}[n] + \log_\rho(\tau)\Delta(\mathcal{L}_{n-1,\rho})[n].
\end{aligned}$$

D'où la formule (2.2.4). □

Corollaire 2.2.6. *Pour tout entier positif n nous avons*

$$\mathcal{L}_{n+1,\rho} = \mathcal{L}_{n,\rho}([n+1]+[n]-\tau) - \mathcal{L}_{n-1,\rho}[n]^2 \tag{2.2.5}$$

Démonstration. D'après la formule (2.2.3) nous avons $\mathcal{L}_{n+1,\rho} = \mathcal{L}_{n,\rho}[n+1] - \tau\mathcal{L}_{n,\rho} + \Delta(\mathcal{L}_{n,\rho})$. Or on sait, grâce à la formule (2.2.4) que $\Delta(\mathcal{L}_{n,\rho}) = \tau\mathcal{L}_{n,\rho} - \mathcal{L}_{n,\rho}\tau + (\Delta(\mathcal{L}_{n-1,\rho}) - \tau\mathcal{L}_{n-1,\rho})[n]$. Cela donne

$$\mathcal{L}_{n+1,\rho} = \mathcal{L}_{n,\rho}[n+1] - \mathcal{L}_{n,\rho}\tau + (\Delta(\mathcal{L}_{n-1,\rho}) - \tau\mathcal{L}_{n-1,\rho})[n].$$

Maintenant, si on remplace n par $n-1$ dans la formule (2.2.3) on obtient $\mathcal{L}_{n,\rho} - \mathcal{L}_{n-1,\rho}[n] = \Delta(\mathcal{L}_{n-1,\rho}) - \tau\mathcal{L}_{n-1,\rho}$. D'où la proposition. □

Proposition 2.2.7. *Pour tout entier naturel n on a*

$$\Delta^2(\mathcal{L}_{n,\rho}) - \tau\Delta(\mathcal{L}_{n,\rho}) + \mathcal{L}_{n,\rho}([n+1]-[1])\tau = \Lambda(\tau\mathcal{L}_{n,\rho} - \mathcal{L}_{n,\rho}\tau),$$

où $\Lambda(f) = \Delta(f) - \tau f$.

Démonstration. Appliquons Δ à la formule (2.2.3), et écrivons la formule (2.2.4) pour $n+1$ au lieu de n. Nous obtenons alors

$$\begin{aligned}\Delta(\mathcal{L}_{n,\rho})[n+1] - \Delta(\tau\mathcal{L}_{n,\rho}) + \Delta^2(\mathcal{L}_{n,\rho}) &= \Delta(\mathcal{L}_{n+1,\rho}) \\ &= \tau\mathcal{L}_{n+1,\rho} - \mathcal{L}_{n+1,\rho}\tau + (\Delta(\mathcal{L}_{n,\rho}) - \tau\mathcal{L}_{n,\rho})[n+1].\end{aligned}$$

Maintenant, il suffit d'utiliser encore une fois la formule (2.2.3) en remplaçant $\mathcal{L}_{n+1,\rho}$ par $\mathcal{L}_{n,\rho}[n+1] - \tau\mathcal{L}_{n,\rho} + \Delta(\mathcal{L}_{n,\rho})$ pour obtenir la formule souhaitée. □

Ainsi, nous avons montré le

Théorème 2.2.8. *Pour tout entier naturel n, la série $\mathcal{L}_{n,\rho} \in \mathbb{F}_q[T]\{\tau\}$. Son degré en tant que polynôme en τ est n. Le coefficient de τ^n est $(-1)^n$. De plus on a*
1. $\mathcal{L}_{n+1,\rho} = \mathcal{L}_{n,\rho}[n+1] - \tau\mathcal{L}_{n,\rho} + \Delta(\mathcal{L}_{n,\rho})$.
2. $\mathcal{L}_{n+1,\rho} = \mathcal{L}_{n,\rho}([n+1]+[n]-\tau) - \mathcal{L}_{n-1,\rho}[n]^2$. $(n>0)$
3. $\Delta^2(\mathcal{L}_{n,\rho}) - \tau\Delta(\mathcal{L}_{n,\rho}) + \mathcal{L}_{n,\rho}([n+1]-[1])\tau = \Lambda(\tau\mathcal{L}_{n,\rho} - \mathcal{L}_{n,\rho}\tau)$,
où $\Lambda(f) = \Delta(f) - \tau f$ et $[n] = T^{q^n} - T$.

Définition 2.2.9. Pour tout entier naturel n on pose

$$\mathcal{L}_{n,\rho}(X) = \sum_{i=0}^{n} a_{i,n} X^{q^i} = (-1)^n X^{q^n} + \cdots + [1][2]\cdots[n]X.$$

Proposition 2.2.10. *Les coefficients $a_{i,n}$ de $\mathcal{L}_{n,\rho}$ sont divisible par $[n]$ pour tout $i < n$. En particulier $\mathcal{L}_{n,\rho}(X)/X$ est Eisentein en tout diviseur irréductible de $[n]$ de degré n.*

Démonstration. Pour tout entier naturel $m \leq n$, on pose

$$\mathcal{P}_{n,m}(\tau) = e_\rho(\tau)\Psi^m(\log_\rho(\tau)\tau^n).$$

Par exemple on a $\mathcal{P}_{n,0}(\tau) = \tau^n$, $\mathcal{P}_{n,1}(\tau) = -\tau^n + [n]\tau^{n-1}$ et $\mathcal{P}_{n,n}(\tau) = \mathcal{L}_{n,\rho}$. Les polynômes $\mathcal{P}_{n,m}(\tau)$ et $\mathcal{P}_{n,m+1}(\tau)$ sont reliés par la formule

$$\mathcal{P}_{n,m+1}(\tau) = -\delta(\mathcal{P}_{n,m}(\tau)) + \Psi(\mathcal{P}_{n,m}(\tau)), \quad \text{pour tout } m < n, \tag{2.2.6}$$

on en déduit que $\mathcal{P}_{n,2}(\tau) = (\tau^2 - ([n] + [n]^q)\tau + [n-1][n]\tau^0)\tau^{n-2}$. On peut encore utiliser la formule (2.2.6) pour montrer par récurrence sur m que $\mathcal{P}_{n,m}$ est de degré n, et que ses coefficients, à l'exception du coefficient dominant, sont multiples de $[n]$ dans $\mathbb{F}_q[T]$. Puisque on a $a_{0,n} = [1][2]\cdots[n]$, la proposition suit. □

2.3 Le groupe de Galois de $\mathcal{L}_{n,\rho}(X)$

Soit V_n l'ensemble des racines de $\mathcal{L}_{n,\rho}(X)$ dans $\overline{k}$. Il est clair que V_n est un $\mathbb{F}_q$-espace vectoriel de dimension n. Le corps $\mathcal{N}_{n,\rho} = k(V_n)$ est une extension Galoisienne de k puisque $\mathcal{L}_{n,\rho}(X)$ est séparable. Notons $G_{n,k}$, le groupe de Galois de $\mathcal{N}_{n,\rho}/k$. Pour toute $\mathbb{F}_q$-base $Z = (z_1, \ldots, z_n)$ de V_n, on définit le morphisme de groupes

$$\Psi_{n,Z} : G_{n,k} \longrightarrow GL_n(\mathbb{F}_q)$$

qui à chaque élément de $G_{n,k}$ associe la matrice de sa restriction à V_n dans la base $(z_1, \ldots, z_n)$. Il est clair que $\Psi_{n,Z}$ est injectif et que $\Psi_{1,Z}$ est un isomorphisme. Dans la suite nous utiliserons le "déterminant de Moore"

$$\Delta(z_1, \ldots, z_n) = \begin{pmatrix} z_1 & z_2 & \ldots & z_n \\ z_1^q & z_2^q & \ldots & z_n^q \\ \vdots & \vdots & \ldots & \vdots \\ z_1^{q^{n-1}} & z_2^{q^{n-1}} & \ldots & z_n^{q^{n-1}} \end{pmatrix}$$

Le lecteur peut consulter [32] et [13] pour une présentation détaillée des proporiétés de ce déterminant. En particulier, d'après [13, Corollary 1.3.8] on a

$$\Delta(z_1, \ldots, z_n)^{q-1} = [1][2]\cdots[n]. \tag{2.3.1}$$

Il est facile de vérifier que pour tout $\sigma \in \mathrm{Gal}(\mathcal{N}_{n,\rho}/k)$ on a

$$\sigma(\Delta(z_1,\ldots,z_n)) = \det(\Psi_{n,Z}(\sigma))\Delta(z_1,\ldots,z_n), \tag{2.3.2}$$

Pour étudier les propriétés de $\Psi_{n,Z}$ pour $n \geq 2$ nous devons explorer certains sous-groupes de décomposition de $G_{n,k}$. Mais introduisons d'abord quelques notations. Pour tout polynôme irréductible $P(T) \in \mathbb{F}_q[T]$, désignons k_P le complété de k relativement à la place déterminée par P et soit Ω_P un corps complet et algébriquement clos contenant k_P. Notons v_P la valuation de Ω_P qui satisfait à $v_P(P) = 1$. On fixe un k-plongement

$$\pi_P : \overline{k} \longrightarrow \Omega_P$$

et posons $V_{n,P} = \pi_P(V_n)$. Le plongement π_P détermine une unique place $\widetilde{P}$ de $\overline{k}$ au-dessus de la place de k associée à P. Le sous-groupe de décomposition de $G_{n,k}$ en $\widetilde{P}$ est isomorphe à $\mathrm{Gal}(k_P(V_{n,P})/k_P)$.

2.3.1 Le sous-groupe de décomposition de $G_{n,k}$ en $\widetilde{P}$ pour les polynômes P de degré n

Fixons un polynôme irréductible $P \in \mathbb{F}_q[T]$ de degré n. Puisque $\mathcal{L}_{n,\rho}(X)/X$ est Eisentein en P et $q^n - 1$ premier à p, on déduit que le groupe de Galois $\mathrm{Gal}(k_P(V_{n,P})/k_P)$ est cyclique d'ordre $q^n - 1$ et que l'extension $k_P(V_{n,P})/k_P$ est totalement modérément ramifiée. Alors on a

Corollaire 2.3.1. *Il existe dans $G_{n,k}$ un automorphisme τ d'ordre $q^n - 1$. De plus, pour tout $z \in V_n \setminus \{0\}$ on a $V_n \setminus \{0\} = \{\tau^i(z), 0 \leq i \leq q^n - 2\}$.*

Démonstration. C'est une simple conséquence du fait que $\mathrm{Gal}(k_P(V_{n,P})/k_P)$ est cyclique et que $k_P(\pi_P(z)) = k_P(V_{n,P})$. □

2.3.2 Le sous-groupe de décomposition de $G_{n,k}$ en $\widetilde{T}$

Nous commençons notre étude concernant ce sous-groupe, en décomposant $\mathcal{L}_{n,\rho}(X)/X$ dans $k_T[X]$ en utilisant son polygone de Newton associé. Soit $a_{i,n,m}$ les coefficients de $\mathcal{P}_{n,m}$. De la formule (2.2.6), on déduit que

$$a_{n,n,m} = (-1)^m \quad \text{et} \quad a_{i,n,m} = 0 \text{ si } i < n - m. \tag{2.3.3}$$

De plus,

$$a_{i,n,m+1} = a_{i+1,n,m}[i+1] - a_{i,n,m}^q. \tag{2.3.4}$$

Lemme 2.3.2. *Pour tout $m \leq n$ et tout $i \in \{n-m, n-m+1, \ldots, n\}$ on a*

$$v_T(a_{i,n,m}) = n - i.$$

Démonstration. La formule est facilement déduite par récurence sur m des formules (2.3.3) et (2.3.4). □

Proposition 2.3.3. *Les points $A_i = (q^i - 1, v_T(a_{i,n}))$ sont exactement les sommets du polygone de Newton de $\mathcal{L}_{n,\rho}(X)/X$ en T. En particulier,*

$$\mathcal{L}_{n,\rho}(X)/X = g_1(X) \cdots g_n(X),$$

où, $g_1(X), \ldots, g_n(X)$ sont des polynômes irréductibles de $k_T[X]$. Le degré de chaque $g_i(X)$ est $q^{i-1}(q-1)$ et si $\lambda \in \Omega_T$ est une racine de $g_i(X)$ alors

$$v_T(\lambda) = \frac{1}{q^{i-1}(q-1)}.$$

Démonstration. d'après le Lemme 2.3.2 le polygone de Newton de $\mathcal{L}_{n,\rho}(X)/X$ en T est l'enveloppe convexe inférieure des points

$$(0, n), (q-1, n-1), \ldots, (q^{n-1} - 1, 1), (q^n - 1, 0).$$

Une vérification rapide des pentes du polygone défini par les points ci-dessus montre qu'il s'agit des sommets de notre polygone de Newton. Le reste de la proposition est une application directe de la méthode NP, voir [15, Theorem 7.4] ou [13, Proposition 2.6]. □

Proposition 2.3.4. *Soit $\lambda_1, \ldots, \lambda_n$ des éléments de $V_{n,T}$ tels que $g_i(\lambda_i) = 0$.*
1. L'ensemble $(\lambda_1, \ldots, \lambda_n)$ est une $\mathbb{F}_q$-base de $V_{n,T}$.
2. Les racines de $g_i(X)$ sont tous les sommes $a_1\lambda_1 + \cdots + a_{i-1}\lambda_{i-1} + a_i\lambda_i$, où $a_1, \ldots, a_{i-1} \in \mathbb{F}_q$ et $a_i \in \mathbb{F}_q^\times$.
3. Le sous-espace vectoriel de $V_{n,T}$ engendré par $(\lambda_1, \ldots, \lambda_i)$ est l'ensemble des racines du produit $g_1(X) \cdots g_i(X)$.

Démonstration. Clair, puisque $v_T(\lambda_n) < v_T(\lambda_{n-1}) < \cdots < v_T(\lambda_1)$. □

Pour déterminer le groupe $\mathrm{Gal}(k(V_{n,T})/k_T)$ nous allons utiliser quelques méthodes utilisées en théorie des groupes formels de Lubin-Tate. Pour tout $i \in \{1, \ldots, n\}$ on pose

$$f_i(X) = (-1)^i X g_1(X) \cdots g_i(X).$$

Sans perte de généralité, nous pouvons supposer que le coefficient dominant de chaque $g_i(X)$ est -1. On sait d'après la Proposition 2.3.4 que $g_1(X), \dots, g_n(X)$ sont des polynômes d'Eisentein. ceci implique que $f_i(X)$ est de la forme

$$f_i(X) = X^{q^i} + f_{i,i-1}X^{q^{i-1}} + \cdots + f_{i,0}X,$$

où$f_{i,j} \in k_T$ sont tels que $v_T(f_{i,j}) > 0$ et $v_T(f_{i,0}) = i$. Considérons le polynôme $[T] = X^q + TX$ et soient $[T^i]$ par récurrence par la formule $[T^{i+1}] = [T^i] \circ [T]$. Ces polynômes sont bien connus dans la théorie de Lubin-Tate. En particulier on a

$$[T^i](X) = X^{q^i} + t_{i,i-1}X^{q^{i-1}} + \cdots + t_{i,0}X, \quad \text{avec} \quad v_T(t_{i,j}) > 0 \text{ et } t_{i,0} = T^i.$$

Soit k_T^{ur} l'extension maximale non ramifiée de k_T dans Ω_T. Soit $L = \overline{k_T^{ur}}$ la clôture de k_T^{ur} dans Ω_T. Puisque $f_{i,0}/T^i$ est une unité, on déduit de [33, Proposition 3.2] ou [29, Lemma 3.11] l'existence d'une unité $u \in L$ telle que

$$\frac{\varphi^i(u)}{u} = \frac{f_{i,0}}{T^i},$$

où φ est l'extension à L de l'automorphisme de Frobenius de k_T^{ur}/k_T. D'après [33, Proposition 3.1] il existe une unique série formelle $\theta_i(X) \in \mathcal{O}_L[[X]]$ telle que

$$f_i \circ \theta_i = \theta_i^{\varphi^i} \circ [T^i].$$

La série formelle $\theta_i(X)$ est additive, en d'autres termes, on a $\theta_i(X+Y) = \theta_i(X) + \theta_i(Y)$. Elle satisfait aussi à l'équation $\theta_i(aX) = a\theta_i(X)$, pour tout $a \in \mathbb{F}_q$. Donc, si V_{f_i} (resp. $V_{[T^i]}$) est l'ensemble des racines de f_i (resp. $[T^i]$) alors θ_i donne un isomorphisme

$$\theta_i : V_{[T^i]} \longrightarrow V_{f_i},$$

de $\mathbb{F}_q$-espaces vectoriels. Exactement comme dans [29, Lemma 4.10], on déduit que $L(V_{f_i}) = L(V_{[T^i]})$ et même

$$k_T^{ur}(V_{f_i}) = k_T^{ur}(V_{[T^i]}),$$

grâce à [29, Lemma 3.1]. Mais on sait, d'après [29, Proposition 5.2], que le corps $k_T^{ur}(V_{[T^i]})$ est une extension abelienne totalement ramifiée de k_T^{ur} et $[k_T^{ur}(V_{[T^i]}) : k_T^{ur}] = (q-1)q^{i-1}$. On déduit alors ce qui suit

Corollaire 2.3.5. *Soit $(\lambda_1, \dots, \lambda_n)$ une famille comme dans la Proposition 2.3.4. Alors pour tout $i \in \{1, \dots, n\}$, le corps $k_T(V_{f_i}) = k_T(\lambda_1, \dots, \lambda_i)$ est une extension abelienne totalement ramifiée de k_T, et on a $[k_T(V_{f_i}) : k_T] = (q-1)q^{i-1}$. En particulier on a $k_T(V_{f_i}) = k_T(\lambda_i)$.*

Pour la suite on choisit $\mu_n \in V_{[T^n]} \setminus V_{[T^{n-1}]}$ et pour $i \in \{1, \dots, n\}$ on pose $\mu_i = [T^{n-i}](\mu_n)$. Alors $(\mu_1, \dots, \mu_n)$ est une $\mathbb{F}_q$-base de $V_{[T^n]}$.

Proposition 2.3.6. *Soit $(\lambda_1, \ldots, \lambda_n)$ la famille définie par $\lambda_i = \theta_n(\mu_i)$ pour $i \in \{1, \ldots, n\}$. Alors $(\lambda_1, \ldots, \lambda_n)$ est une $\mathbb{F}_q$-base de $V_{n,T}$. Soit $f : \mathrm{Gal}(k_T(V_{n,T})/k_T) \longrightarrow GL_n(\mathbb{F}_q)$ le morphisme injectif qui à chaque élément de $\mathrm{Gal}(k_T(V_{n,T})/k_T)$ associe la matrice de sa restriction dans la base $(\lambda_1, \ldots, \lambda_n)$. Alors, pour tout $\sigma \in \mathrm{Gal}(k_T(V_{n,T})/k_T)$ il existe $a_1 \in \mathbb{F}_q^*$ et $a_2, \ldots, a_n \in \mathbb{F}_q$ tels que*

$$f(\sigma) = \begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_n \\ 0 & a_1 & a_2 & \cdots & a_{n-1} \\ 0 & 0 & a_1 & \cdots & a_{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & a_1 \end{pmatrix}.$$

Démonstration. On peut voir tout élément $\sigma \in \mathrm{Gal}(k_T(V_{n,T})/k_T)$ comme un élément de $\mathrm{Gal}(k_T^{ur}(V_{[T^n]})/k_T^u$ Alors il existe $a_1 \in \mathbb{F}_q^*$ et $a_2, \ldots, a_n \in \mathbb{F}_q$ tels que

$$\sigma(\mu_n) = a_1\mu_n + a_2\mu_{n-1} + \cdots + a_n\mu_1.$$

Pour calculer les images de μ_j, il suffit d'appliquer $[T^{n-j}]$ à l'égalité ci-dessus. Ceci donne

$$\sigma(\mu_j) = a_1\mu_j + a_2\mu_{j-1} + \cdots + a_j\mu_1.$$

Pour calculer $\sigma(\lambda_j)$, on applique simplement la série θ_n à l'égalité ci-dessus. □

Corollaire 2.3.7. *Le corps des constantes de $\mathcal{N}_{n,\rho}$ est égal à $\mathbb{F}_q$.*

Démonstration. Ceci découle du fait que l'extension $k_T(V_{n,T})/k_T$ est totalement ramifiée. □

Corollaire 2.3.8. *Il existe une $\mathbb{F}_q$-base $(z_1, \ldots, z_n)$ de V_n telle que l'image de*

$$\mathrm{Gal}(\mathcal{N}_{n,\rho}/k(z_1, \ldots, z_{n-1}, \Delta(z_1, \ldots, z_n)))$$

par $\Psi_{n,Z}$ contient toutes les matrices

$$\begin{pmatrix} 1 & 0 & 0 & \cdots & a \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}, \quad a \in \mathbb{F}_q.$$

Démonstration. On prend $(z_1, \ldots, z_n)$ telle que $(\lambda_1 = \pi_T(z_1), \ldots, \lambda_n = \pi_T(z_n))$ est une base de $V_{n,T}$ comme dans la Proposition 2.3.6. Posons

$$E = k(z_1, \ldots, z_{n-1}, \Delta(z_1, \ldots, z_n)) \text{ et } E_T = k_T(\lambda_1, \ldots, \lambda_{n-1}, \Delta(\lambda_1, \ldots, \lambda_n)).$$

Alors le groupe de décomposition de $\mathrm{Gal}(\mathcal{N}_{n,\rho}/E)$ en $\widetilde{T}$ est isomorphe à $\mathrm{Gal}(k_T(V_{n,T})/E_T)$. En effet, si $\sigma \in \mathrm{Gal}(k_T(V_{n,T})/E_T)$ alors la restriction $res(\sigma)$ de σ à $\mathcal{N}_{n,\rho}$ est telle que

$$\pi_T \circ res(\sigma) = \sigma \circ res(\pi_T),$$

où $res(\pi_T)$ est la restriction de π_T à $\mathcal{N}_{n,\rho}$. L'application $\sigma \longmapsto res(\sigma)$ est l'isomorpisme évoqué. De plus, on déduit de la Proposition 2.3.6 que l'ensemble des matrices $\Psi_{n,Z}(res(\sigma))$, $\sigma \in \mathrm{Gal}(k_T(V_{n,T})/E_T)$, est exactement l'ensemble décrit par la proposition. □

2.3.3 Le groupe $G_{2,k}$

Proposition 2.3.9. *Il existe une $\mathbb{F}_q$-base (z_1, z_2) de V_2 telle que la restriction de $\Psi_{2,Z}$ au groupe $\mathrm{Gal}(\mathcal{N}_{2,\rho}/k(\Delta(z_1, z_2)))$ est un isomorphisme :*

$$\mathrm{Gal}(\mathcal{N}_{2,\rho}/k(\Delta(z_1, z_2))) \simeq SL_2(\mathbb{F}_q).$$

Démonstration. On prend (z_1, z_2) comme dans le corollaire 2.3.8. La formule (2.3.2) implique que

$$\Psi(\mathrm{Gal}(\mathcal{N}_{2,\rho}/k(\Delta(z_1, z_2)))) \subset SL_2(\mathbb{F}_q).$$

Le Corollaire 2.3.8 montre que $\Psi_{2,Z}(\mathrm{Gal}(\mathcal{N}_{2,\rho}/k(\Delta(z_1, z_2)))$ contient toutes les matrices élémentaires $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$, $a \in \mathbb{F}_q$. Soit $\tau \in \mathrm{Gal}(\mathcal{N}_{2,\rho}/k)$ tel que $\tau(z_2) = z_1$. Alors on a $\tau(z_1) = \alpha z_1 + \beta z_2$, avec $\alpha \in \mathbb{F}_q$ et $\beta \in \mathbb{F}_q^*$. De sorte que si on choisit $\sigma \in \mathrm{Gal}(\mathcal{N}_{2,\rho}/k(\Delta(z_1, z_2)))$ tel que

$$\Psi_{2,Z}(\sigma) = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix},$$

alors $\Psi_{2,Z}(\tau^{-1}\sigma\tau) = \begin{pmatrix} 1 & 0 \\ a\beta & 1 \end{pmatrix}$. Puisque ces matrices engendrent $SL_2(\mathbb{F}_q)$ la proposition suit. □

Théorème 2.3.10. *Pour toute $\mathbb{F}_q$-base (z_1, z_2) de V_2, le morphisme de groupes $\Psi_{2,Z}$ est un isomorphisme.*

Démonstration. Il suffit de prouver le théorème pour au moins une base. On choisit (z_1, z_2) comme dans le Corollaire 2.3.8. Dans ce cas, le théorème est une conséquence de la Proposition 2.3.9 et le fait que le degré $[k(\Delta(z_1, z_2)) : k] = q - 1$ puisque $\Delta(z_1, z_2)$ est une racine du polynôme irréductible $X^{q-1} - [1][2]$. □

2.3.4 Le groupe $G_{n,k}$ pour $n \geq 3$

La détermination de $G_{n,k}$, pour $n \geq 3$, nécessite sur l'étude du groupe de décomposition de $G_{n,k}$ en les places au-dessus des polynômes irréductibles dont le degré égale à $n-1$. Fixons alors $S(T) \in \mathbb{F}_q[T]$ un polynôme irréductible de degré $n-1$.

Lemme 2.3.11. *Soit $m \in \{2, \ldots, n\}$, alors $v_S(a_{n-1,n,m}) = 0$ et pour tout $i \in \{n-m, n-m+1, \ldots, n-2\}$ on a $v_S(a_{i,n,m}) = 1$.*

Démonstration. Le lemme peut se démontrer par récurrence sur m en se basant sur les formules (2.3.3) et (2.3.4). □

Proposition 2.3.12. *Les sommets du polygone de Newton de $\mathcal{L}_{n,\rho}(X)/X$ en S sont les points*

$$(0,1), \quad (q^{n-1}-1, 0) \quad et \quad (q^n - 1, 0).$$

En particulier,

$$\mathcal{L}_{n,\rho}(X)/X = h_1(X)h_2(X),$$

où $h_1(X)$ et $h_2(X)$ sont des polynômes de $k_S[X]$ tels que
1. $h_1(X)$ est irréductible de degré $q^{n-1}-1$. Si $\alpha \in \Omega_S$ est une racine de $h_1(X)$ alors

$$v_S(\alpha) = \frac{1}{q^{n-1}-1}.$$

2. Si $\beta \in \Omega_S$ est une racine de $h_2(X)$, alors on a $v_S(\beta) = 0$.

Démonstration. On déduit du Lemme 2.3.11 que le polygone de Newton de $\mathcal{L}_{n,\rho}(X)/X$ en S est l'enveloppe convexe inférieure des points

$$(0,1), (q-1,1), \ldots, (q^{n-2}-1, 1), (q^{n-1}-1, 0), (q^n - 1, 0).$$

Ses sommets sont donc $(0,1)$,$(q^{n-1}-1, 0)$ et $(q^n - 1, 0)$. Le reste de la proposition est une application directe de la méthode NP. □

Proposition 2.3.13. *L'ensemble des racines de $Xh_1(X)$ dans Ω_S est un $\mathbb{F}_q$-espace vectoriel de dimension $n-1$. Soit $\alpha_1, \ldots, \alpha_n$ des éléments de $V_{n,S}$ tels que $h_2(\alpha_n) = 0$ et $(\alpha_1, \ldots, \alpha_{n-1})$ est une $\mathbb{F}_q$-base de l'ensemble des racines de $Xh_1(X)$. Alors la famille $(\alpha_1, \ldots, \alpha_n)$ est une $\mathbb{F}_q$-base de $V_{n,S}$.*

Démonstration. Cette proposition découle directement de la Proposition 2.3.12. □

Lemme 2.3.14. *Le groupe de Galois* $\mathrm{Gal}(\mathcal{N}_{n,\rho}/k)$ *agit transitivement sur l'ensemble des sous-espaces vectoriels de* V_n *de dimension* $n-1$.

Démonstration. Il existe exactement $\dfrac{q^n-1}{q-1}$ sous-espaces de V_n de dimension $n-1$. Soit $z \in V_n \backslash \{0\}$ et soit $\tau \in \mathrm{Gal}(\mathcal{N}_{n,\rho}/k)$ comme dans le Corollaire 2.3.1. Soit M le sous-espace de V_n engendré par $z, \tau(z), \ldots, \tau^{n-2}(z)$. La dimension de M est exactement $n-1$. En fait la famille $z, \tau(z), \ldots, \tau^{n-1}(z)$ est une base de V_n. Les images $\tau^i(M)$, pour $0 \leq i < \dfrac{q^n-1}{q-1}$, sont deux à deux distinctes. En effet, si on a $\tau^i(M) = \tau^j(M)$, avec $0 \leq i \leq j < \dfrac{q^n-1}{q-1}$, alors $\tau^{j-i}(M) = M$. Ceci implique que $\tau^{j-i}(z) = az$, pour un certain $a \in \mathbb{F}_q^*$ et par suite $\tau^{(j-i)(q-1)}$ est l'application identité. Comme l'ordre de τ est égale à q^n-1, on déduit que $i = j$. Ce qui achève la preuve du lemme. □

Proposition 2.3.15. *Il existe une* $\mathbb{F}_q$*-base* $(z_1, \ldots, z_n)$ *de* V_n *telle que*

$$[\mathcal{N}_{n,\rho} : k(z_1, \ldots, z_{n-1}, \Delta(z_1, \ldots, z_n))] \geq q^{n-1} - 1.$$

Démonstration. Soit $(z'_1, \ldots, z'_n)$ une $\mathbb{F}_q$-base de V_n comme dans le Corollaire 2.3.8. On sait, grâce au Lemme 2.3.14 qu'il existe $\gamma \in G_{n,k}$ tel que $(\pi_S(\gamma(z'_1)), \ldots, \pi_S(\gamma(z'_{n-1}))$ est une base de l'ensemble des racines de $Xh_1(X)$. Pour tout $i \in \{1, \ldots, n\}$ on pose $z_i = \gamma(z'_i)$ et $\alpha_i = \pi_S(z_i)$. Posons

$$E = k(z_1, \ldots, z_{n-1}, \Delta(z_1, \ldots, z_n))$$

On sait, grâce au corollarire 2.3.8, que pour tout $a \in \mathbb{F}_q$ il existe $\sigma_a \in \mathrm{Gal}(\mathcal{N}_{n,\rho}/E)$ tel que $\sigma_a(z_n) = z_n + az_1$. On sait d'après la Proposition 2.3.12 et la Proposition 2.3.13 que $k_S(\alpha_1, \ldots, \alpha_{n-1})$ est une extension Galoisienne de k_S. Soit X un système complet de représentants du groupe $\mathrm{Gal}(k_S(\alpha_1, \ldots, \alpha_{n-1})/k_S)$ modulo le groupe de Galois $\mathrm{Gal}(k_S(\alpha_1, \ldots \alpha_{n-1})/k_S(\alpha_1^{q-1})$. Le cardinal de X est égal au degré $[k_S(\alpha_1^{q-1}) : k_S] = \dfrac{q^{n-1}-1}{q-1}$. Pour tout $\tau \in X$ on note par $\widetilde{\tau}$ une extension de τ à $k_S(V_{n,S}) = k_S(\alpha_1, \ldots, \alpha_n)$. La restriction de $\widetilde{\tau}$ à $\mathcal{N}_{n,\rho}$ est un k-automorphisme de $\mathcal{N}_{n,\rho}$, on la note encore par $\widetilde{\tau}$. Il est facile de vérifier que $\widetilde{\tau}^{-1}\sigma_a\widetilde{\tau} \in \mathrm{Gal}(\mathcal{N}_{n,\rho}/E)$. Si $\widetilde{\tau}(z_n) = x_1(\widetilde{\tau})z_1 + \cdots + x_{n-1}(\widetilde{\tau})z_{n-1} + x_n(\widetilde{\tau})z_n$, où $x_1(\widetilde{\tau}), \ldots, x_{n-1}(\widetilde{\tau}) \in \mathbb{F}_q$ et $x_n(\widetilde{\tau}) \in \mathbb{F}_q^\times$ alors on a

$$\widetilde{\tau}^{-1}\sigma_a\widetilde{\tau}(z_n) = z_n + ax_n(\widetilde{\tau})\widetilde{\tau}^{-1}(z_1),$$

Ce qui permet de déduire que l'application $X \times \mathbb{F}_q^\times \longrightarrow \mathrm{Gal}(\mathcal{N}_{n,\rho}/E)$ qui à chaque (τ, a) associe l'automorphisme $\widetilde{\tau}^{-1}\sigma_a\widetilde{\tau}$, est injective. Ce qui achève la preuve de la proposition. □

Corollaire 2.3.16. *Il existe une* $\mathbb{F}_q$*-base* $(z_1, \ldots, z_n)$ *de* V_n *telle que l'ordre du groupe de Galois* $D = \mathrm{Gal}(\mathcal{N}_{n,\rho}/k(z_1, \ldots, z_{n-1}, \Delta(z_1, \ldots, z_n))$ *est exactement* q^{n-1}.

Démonstration. C'est une conséquence de la Proposition 2.3.15 et le fait que l'ordre de D divise q^{n-1}. □

Proposition 2.3.17. *Il existe une $\mathbb{F}_q$-base $(z_1, \ldots, z_n)$ de V_n telle que la restriction de $\Psi_{n,Z}$ à $\mathrm{Gal}(\mathcal{N}_{n,\rho}/k(\Delta(z_1, \ldots, z_n)))$ est un isomorphisme*

$$\mathrm{Gal}(\mathcal{N}_{n,\rho}/k(\Delta(z_1, \ldots, z_n))) \simeq SL_n(\mathbb{F}_q).$$

Démonstration. On choisit $(z_1, \ldots, z_n)$ comme dans le Corollaire 2.3.16. On procède ensuite comme dans la preuve de la Proposition 2.3.9, pour montrer que l'image

$$\Psi_{n,Z}(\mathrm{Gal}(\mathcal{N}_{n,\rho}/k(\Delta(z_1, \ldots, z_n))))$$

contient toutes les matrices élémentaires. Mais, contrairement au cas $n = 2$, ici il faut utiliser le Lemme 2.3.14 et le Corollaire 2.3.16. Par conséquent ce groupe contient $SL_n(\mathbb{F}_q)$. □

Théorème 2.3.18. *Pour toute $\mathbb{F}_q$-base $(z_1, \ldots, z_n)$ de V_n, l'homomorphisme de groupes $\Psi_{n,Z}$ est un isomorphisme.*

Démonstration. Il suffit de montrer le théorème pour au moins une base. On choisit $(z_1, \ldots, z_n)$ comme dans la Proposition 2.3.17. Dans ce cas, le théorème est une conséquence de la Proposition 2.3.17 et le fait que le degré $[k(\Delta(z_1, \ldots, z_n)) : k] = q - 1$ puisque $\Delta(z_1, \ldots, z_n)$ est racine du polynôme irréductible $X^{q-1} - [1][2]\cdots[n]$. □

Chapitre 3

Remarques sur les modules de Drinfeld de rang 1 et leurs points de torsion

On sait que les points de torsion des modules de Drinfeld de rang un sont utilisés pour donner une description explicite des corps de classe. Ils sont également utilisés pour construire des unités, des systèmes d'Euler et des annulateurs des groupes de classes d'idéaux de l'anneau des sections globales de certaines courbes affines. Dans ce chapitre nous voulons étudier la structure de certains modules engendrés par ces éléments de torsion. Le contexte est le suivant. Soit $k/\mathbb{F}_q$ un corps global de fonctions algébriques, où le corps des constantes est $\mathbb{F}_q$ le corps fini à q éléments. On fixe une place ∞ de k de degré $\deg(\infty) = d_\infty$ et soit $A \subset k$ l'anneau des éléments réguliers de k en toutes les places sauf ∞. On sait, d'après [27, Corollary 3.2.8 et Proposition 3.2.9] par exemple, que A est un anneau de Dedekind, et que les premiers de k différents de ∞ correspondent aux idéaux maximaux de A. On note v_∞ la valuation normalisée associée à ∞, soient k_∞ le complété de k pour la v_∞-topolologie et Ω le complété d'une clôture algébrique de k_∞. On note encore v_∞ la valuation sur Ω qui prolonge celle de k. Pour $a \in A$ on appelle degré de a l'entier naturel donné par $\deg(a) = dim_{\mathbb{F}_q} A/aA$, on sait qu'on a $\deg(a) = -v_\infty(a).d_\infty$. Plus généralement, si I est un idéal de A alors le degré de I est défini par la relation $\deg(I) = dim_{\mathbb{F}_q} A/I$. Nous commençons par donner un petit rappel sur les modules de Drinfeld.

3.1 Rappels sur les modules de Drinfeld

On se donne un corps L contenant $\mathbb{F}_q$ et notons $L\{\tau\}$ l'anneau des polynômes en τ muni de la multiplication tordue donnée par

$$\tau a = a^q \tau \quad \text{pour tout } a \in L$$

On fixe une application structurale $\delta : A \longrightarrow L$ de A vers L. Dans la pratique, le morphisme δ est soit l'inclusion, soit la réduction modulo un idéal premier. Si δ est injectif alors on dit que L est sans caractéristique. Si δ est non injectif alors son noyau Q est un idéal premier de A. Dans ce cas, on dit que Q est la A-caractéristique de L. On considére l'application $D : L\{\tau\} \longrightarrow L$ donnée par $D\left(\sum_{i\geq 0} c_i\tau^i\right) = c_0$, elle joue un rôle important dans la définition d'un module de Drinfeld. Nos références pour la présentation suivante sont [26, Chapitre 13], [17] et [18].

Définition 3.1.1. On appelle A-module de Drinfeld sur L tout morphisme d'algébres $\rho : A \longrightarrow L\{\tau\}$ qui à chaque $a \in A$ associe $\rho_a(\tau) \in L\{\tau\}$ tel que, pour tout $a \in A$, $D(\rho_a) = \delta(a)$ et que l'image de ρ n'est pas inclus dans L. On note $Drinf_A(L)$ l'ensemble des A-modules de Drinfeld sur L.

3.1.1 Les A-modules normalisés

On désigne par $\kappa(\infty)$ le corps des constantes de k_∞, il est isomorphe au corps résiduel en ∞, de degré d_∞ sur $\mathbb{F}_q$. Soit $\mathcal{U}_\infty^{(1)}$ le groupe des unités principales en ∞.

Un A-module de Drinfeld ρ sur Ω de rang 1 est dit de caractéristique générique si l'application $x \longmapsto D(\rho_x)$ pour $x \in A$ est l'inclusion $A \hookrightarrow \Omega$. Un tel module est dit normalisé si le coefficient dominant $s_\rho(x)$ de ρ_x appartient à $\kappa(\infty)$ pour tout $x \in A \setminus \{0\}$. On sait d'après [17, Proposition 10.4], que chaque classe d'isomorphisme de A-module de Drinfeld sur Ω contient un A-module normalisé.

Définition 3.1.2. Soit $sgn : k_\infty^* \longrightarrow \kappa(\infty)^*$ une application. On dit que sgn est une fonction signe si :

1. sgn est un morphisme de groupes multiplicatifs.
2. $sgn(\mathcal{U}_\infty^{(1)})$=1
3. sgn induit l'identité sur $\kappa(\infty)^*$

On prend $sgn(0) = 0$. Soit σ un automorphisme de $\kappa(\infty)$. Le composé $\sigma \circ sgn$ est appelé, fonction signe tordue (ou fonction signe tordue de sgn par σ).

Soient sgn et sgn' deux fonctions signe sur k_∞, d'après [18, Lemma 4.2] il existe $a \in \kappa(\infty)^*$ tel que

$$sgn(x) = sgn'(x).a^{\frac{\deg x}{d_\infty}} \tag{3.1.1}$$

pour tout x de k_∞. Ainsi, Il existe exactement $W_\infty = q^{d_\infty} - 1$ fonctions signe sur k_∞.

Soit ρ un A-module de Drinfeld normalisé de caractéristique générique sur Ω. Alors s_ρ est une application multiplicative de $A \setminus \{0\}$ vers $\kappa(\infty)$ et $s_\rho(a) = a$ pour $a \in \mathbb{F}_q^*$. Par conséquent s_ρ s'étend d'une manière unique à k^*. Puisque on a $s_\rho(\mathcal{U}_\infty^{(1)} \cap k^*) = 1$ d'après [18, Lemma 4.4], on déduit que s_ρ est continue sur k^* pour la v_∞-topologie et qu'elle s'étend d'une manière unique à une fonction continue sur k_∞^*, notée aussi s_ρ, elle est triviale sur $\mathcal{U}_\infty^{(1)}$. En fait, s_ρ est une fonction signe tordue sur k_∞^* (voir [18, Proposition 4.5]).

Pour une fonction signe sgn on dit que ρ est sgn-normalisé si ρ est normalisé et que s_ρ est une fonction signe tordue de sgn. D'après [18, Proposition 4.6], chaque module de Drinfeld de caractéristique générique sur Ω est isomorphe à un module sgn-normalisé.

Maintenant, on fixe une fonction signe sgn, et soit ρ un A-module de Drinfeld de caractéristique générique sgn-normalisé sur Ω. Soit $I^*(\rho)$ le sous-corps de Ω engendré par les coefficients de ρ_x, $x \in A$. D'après [17, §8], $I^*(\rho)$ contient le corps de classe de Hilbert H_A, où H_A est l'extension abelienne maximale non ramifiée de k dans laquelle ∞ se décompse totalement. De plus, il existe $w \in \Omega^*$ tel que $\rho' = w.\rho.w^{-1}$ est définie sur H_A. On a $I^*(\rho) \subseteq H_A(w)$, $H_A(w)/H_A$ est une extension de Kummer. En particulier, $I^*(\rho)/k$ est une extension finie séparable.

Définition 3.1.3. Le corps $I^*(\rho)$ ne dépend pas du A-module de Drinfeld de caractéristique générique sgn-normalisé ρ (voir [18, Definition 4.9]), on le note simplement H_A^* ; On l'appelle le corps normalisé associé à la fonction sgn. L'extension H_A^*/H_A est abélienne de degré $r = \dfrac{q^{d_\infty} - 1}{q - 1}$.

Théorème 3.1.4. *[18, Theorem 4.10] L'extension H_A^*/k est abélienne de degré rhd_∞, elle est non ramifiée sauf en ∞, et H_A^*/H_A est totalement ramifiée en ∞.*
où h est le nombre de classe de k.

3.1.2 Une génération du corps normalisé

On fixe ρ comme A-module de Drinfeld sgn-normalisé de caractéristique générique. Soit $\mathfrak{m}$ un idéal entier de A. On note $\Lambda_\mathfrak{m}$ l'ensemble des points de $\mathfrak{m}$-torsion pour l'action de A sur Ω définie par ρ. On rappelle que $\Lambda_\mathfrak{m} \cong A/\mathfrak{m}$ en tant que A-module, ce qui implique que le groupe des A-automorphismes de $\Lambda_\mathfrak{m}$ est isomorphe $(A/\mathfrak{m})^*$. Posons alors $K_\mathfrak{m}$, le corps obtenu par adjonction à H_A^* des éléments de $\Lambda_\mathfrak{m}$. On rappelle que

Puisque $\Lambda_\mathfrak{m}$ est exactement l'ensemble des racines du polynôme linéaire $\rho_\mathfrak{m}(t) \in H_A^*[t]$, l'extension $K_\mathfrak{m}/H_A^*$ est galoisienne. Puisque A agit sur Ω via des polynômes à coefficients dans H_A^*, nous avons un morphisme injectif naturel

$$g_\mathfrak{m} : Gal(K_\mathfrak{m}/H_A^*) \longrightarrow (A/\mathfrak{m})^*$$

ce qui montre que $K_{\mathfrak{m}}/H_A^*$ est abélienne. En fait, $g_{\mathfrak{m}}$ est un isomorphisme et que $[K_{\mathfrak{m}} : H_A^*] = Card(A/\mathfrak{m})^* = \Phi(\mathfrak{m})$ (voir [18, §4]). On rappelle le

Théorème 3.1.5. *[18, §4] L'extension $K_{\mathfrak{m}}/H_A^*$ est abélienne de degré $\Phi(\mathfrak{m})$. Les places correspondants aux idéaux premiers divisant $\mathfrak{m}$ ou au dessus de ∞, sont les seules places de H_A^* ramifiées dans $K_{\mathfrak{m}}/H_A^*$. Soit a un élément de A premier à $\mathfrak{m}$ tel que $sgn(a) = 1$ alors on a*

$$\rho_a(\lambda) = \rho_{\mathfrak{a}}(\lambda) = \lambda^{\sigma_{\mathfrak{a}}},$$

où $\mathfrak{a} = aA$ et $\sigma_{\mathfrak{a}_i}$ est l'automorphisme de $H_A^*(\Lambda_{\mathfrak{m}})/H_A^*$ associé à $\mathfrak{a}$ par l'application d'Artin.

3.2 Rang du module engendré par les points de torsion

Fixons une fonction signe $sgn : k_\infty^\times \longrightarrow \kappa(\infty)^\times$. Soit ρ un A-module de Drinfeld de caractéristique générique et sgn-normalisé, dans le sens de [18, §4]. Soit H_A^* le sous-corps de Ω normalisé par rapport à la fonction sgn. On rappelle que H_A^* est une extension abelienne de k, non ramifiée en toutes places $v \neq \infty$. Le groupe de Galois $\mathrm{Gal}(H_A^*/k)$ est isomorphe au quotient $\mathcal{I}_A/\mathcal{P}_A^*$, où $\mathcal{I}_A$ le groupe des idéaux fractionnaires de A et $\mathcal{P}_A^*$ est le groupe des idéaux fractionnaires principaux xA, avec $x \in k$ non nul et vérifie $sgn(x) = 1$. Dans ce chapitre nous montrons

Théorème 3.2.1. *(Théorème 3.4.10) Soit $E_\rho \subset H_A^*[\tau]$ le H_A^*-espace vectoriel engendré par tous les polynômes ρ_x, $x \in A$. Alors le quotient $R_\rho = H_A^*[\tau]/E_\rho$ est un H_A^*-espace vectoriel de dimension $\leq g$, où g est le genre de k. Si $d_\infty = 1$ alors on a $\dim_{H_A^*}(R_\rho) = g$.*

Pour tout $x \in A$, la multiplication à droite par ρ_x donne une application linéaire de R_ρ, qu'on note par $\Phi_\rho(x)$. Ce qui offre un morphisme d'anneaux

$$\Phi_\rho : A \longrightarrow \mathrm{End}(R_\rho),$$

qu'on peut utiliser pour munir R_ρ d'une structure de A-module ($a.v = \Phi_\rho(a)(v)$). Si $\mathfrak{m} \neq 0$ est un idéal de A, alors le sous-module de R_ρ des points de $\mathfrak{m}$-torsion est donné par

$$X_{\mathfrak{m}} = \{v \in R_\rho,\ \Phi_\rho(a)(v) = 0,\ \text{pour tout } a \in \mathfrak{m}\}.$$

La dimension $\dim_{H_A^*}(X_{\mathfrak{m}})$, semble être liée au rang du B-module engendré par $\Lambda_{\mathfrak{m}}$ noté $B\Lambda_{\mathfrak{m}}$, où B est la fermeture intégrale de A dans H_A^* et $\Lambda_{\mathfrak{m}}$ est le sous-module de $\mathfrak{m}$-torsion de Ω. Rappelons que $\Lambda_{\mathfrak{m}}$ est un A-module. L'action de $a \in A$ sur $\lambda \in \Lambda_{\mathfrak{m}}$ est donnée par $a.\lambda = \rho_a(\lambda)$. Comme le prouve Hayes dans [18, §4] il existe un isomorphisme

$$\Lambda_{\mathfrak{m}} \simeq A/\mathfrak{m}.$$

En particulier $\Lambda_{\mathfrak{m}}$ est un $\mathbb{F}_q$-espace vectoriel de dimension $\deg(\mathfrak{m}) = \dim_{\mathbb{F}_q}(A/\mathfrak{m})$. Puisque chaque $\mathbb{F}_q$-base de $\Lambda_{\mathfrak{m}}$ engendre $B\Lambda_{\mathfrak{m}}$ comme B-module, on a

$$rank_B(B\Lambda_{\mathfrak{m}}) \leq \deg(\mathfrak{m}).$$

Notre second objectif est de démontrer le theorème principal suivant,

Théorème 3.2.2. *(Théorème 3.4.13) Soit $\mathfrak{m}_\rho$ l'idéal introduit dans la définition 3.4.12. Soit $\mathfrak{m} \neq 0$ un idéal de A premier à $\mathfrak{m}_\rho$. Alors le B-module $B\Lambda_{\mathfrak{m}}$ est libre et on a*

$$rank_B(B\Lambda_{\mathfrak{m}}) = \begin{cases} \deg(\mathfrak{m}) - s + 1, & si\ q = 2\ et\ s \geq 1, \\ \deg(\mathfrak{m}), & si\ q > 2\ ou\ (q = 2\ et\ s = 0), \end{cases}$$

où s est le nombre exacte des idéaux premiers $\mathfrak{p}$ divisant $\mathfrak{m}$ et $\deg(\mathfrak{p}) = 1$.

Les preuves des deux Théorèmes sont intimement liées, et reposent essentiellement sur les propriétés arithmétiques des extensions $H^*_A(\Lambda_{\mathfrak{m}})$ prouvées par Hayes dans [17, 18], le théorème de Riemann-Roch et le théorème de densité de Chebotarev. L'idéal $\mathfrak{m}_\rho$ ne dépend pas de ρ. De plus, il est facile de prouver que $\mathfrak{m}_\rho = A$ lorsque $k = \mathbb{F}_q(T)$ et ∞ est le pôle du polynôme T. En fin, On montre que $\mathfrak{m}_\rho = A$ lorsque $d_\infty = 1$ et $g = 1$. Nous ne savons pas si $\mathfrak{m}_\rho = A$ en général.

3.3 Quelques propriétés générales de $B\Lambda_{\mathfrak{m}}$

Nous donnons deux résultats préliminaires. on prouve d'abord l'existence d'une $\mathbb{F}_q$-base de $A/\mathfrak{m}$ avec propriétés particulières. Le deuxième résultat concerne l'additivité des modules $B\Lambda_{\mathfrak{m}}$. Comme d'habitude, le cardinal de l'anneau quotient $A/\mathfrak{m}$ sera noté par $N(\mathfrak{m})$.

Définition 3.3.1. Soit $\mathfrak{m} \neq 0$ un idéal de A. Nous dirons que $\mathfrak{m}$ admet la propriété $(\mathbf{P})$ si l'une des conditions suivantes est satisfaite
1) $q > 2$.
2) $q = 2$ et tout idéal premier $\mathfrak{p}$ de A divisant $\mathfrak{m}$ est tel que $\deg(\mathfrak{p}) \geq 2$.
3) $q = 2$ et $\mathfrak{m} = \mathfrak{p}^n$, où $\mathfrak{p}$ est un idéal premier tel que $\deg(\mathfrak{p}) = 1$.
En particulier, chaque idéal premier de A admet la propriété $(\mathbf{P})$.

Lemme 3.3.2. *On suppose que $\mathfrak{m}$ admet la propriété $(\mathbf{P})$. Alors l'anneau quotient $A/\mathfrak{m}$ admet une $\mathbb{F}_q$-base $(a_1, \ldots, a_{\deg(\mathfrak{m})})$, où les éléments $a_i \in A$ sont premier à $\mathfrak{m}$.*

Démonstration. Le lemme est trivial si $\mathfrak{m}$ est un idéal premier. Supposons que nous ayons prouvé le lemme d'un idéal $\mathfrak{m} \neq (1)$. Soit $\mathfrak{p}$ un idéal premier de A. Démontrons le lemme pour $\mathfrak{n} = \mathfrak{m}\mathfrak{p}$. On utilise pour cela la suite exacte

$$0 \longrightarrow \mathfrak{m}/\mathfrak{n} \longrightarrow A/\mathfrak{n} \longrightarrow A/\mathfrak{m} \longrightarrow 0.$$

Soit $(f_1, \ldots, f_r)$ une base de $A/\mathfrak{m}$ telle que les f_i sont premier à $\mathfrak{m}$. Soit $(g_1, \ldots, g_s)$ une base de $\mathfrak{m}/\mathfrak{n}$, alors $(g_1, \ldots, g_s, f_1, \ldots, f_r)$ est une $\mathbb{F}_q$-base de $A/\mathfrak{n}$. Si $\mathfrak{p} \mid \mathfrak{m}$ alors $(g_1 + f_1, \ldots, g_s + f_1, f_1, \ldots, f_r)$ est une base de $A/\mathfrak{n}$ satisfaisant les conditions du lemme. Supposons maintenant que $\mathfrak{p} \nmid \mathfrak{m}$. Alors les éléments g_i sont premier à $\mathfrak{p}$. Puisque $s = \deg(\mathfrak{p}) < N(\mathfrak{p}) - 1$ il existe $\alpha \in A$ premier à $\mathfrak{p}$ tel que $\alpha - g_j \notin \mathfrak{p}$ pour tout j. Pour tout i on choisit un élément $\widetilde{f}_i \in A$ tel que

$$\widetilde{f}_i \equiv f_i \text{ modulo } \mathfrak{m} \quad et \quad \widetilde{f}_i \equiv \alpha \text{ modulo } \mathfrak{p}.$$

Alors la famille $(g_1 - \widetilde{f}_1, \ldots, g_s - \widetilde{f}_1, \widetilde{f}_1, \ldots, \widetilde{f}_r)$ est une $\mathbb{F}_q$-base de $A/\mathfrak{n}$ dont éléments sont tous premier à $\mathfrak{n}$. Le lemme est maintenant prouvé. □

Remarque. Dans le cas où $k = \mathbb{F}_2(T)$ et $A = \mathbb{F}_2[T]$. Soit $\mathfrak{m} = T(T+1)A$, alors $\mathfrak{m}$ n'admet pas la propriété (**P**) et la conclusion du Lemme 3.3.2 n'est pas satisfaite pour l'anneau $A/\mathfrak{m}$.

Lemme 3.3.3. *Il existe $\beta \in A$ tel que $\beta \equiv 1$ modulo $\mathfrak{m}$ et $sgn(\beta)$ engendre le groupe cyclique $\kappa(\infty)^\times$.*

Démonstration. Soit ε un générateur de $\kappa(\infty)^\times$. Soit $z \in k$ tel que $v_\infty(z - \varepsilon) > 0$, où v_∞ est la valuation normalisée définie par ∞. Alors on a $sgn(z) = \varepsilon$. Écrivons $\mathfrak{m} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_s^{e_s}$, où $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ sont les premiers de A divisant $\mathfrak{m}$. Pour tout $\mathfrak{p}_i$, on désigne par v_i la valution normalisée associée à $\mathfrak{p}_i$. d'après le théorème d'approximation faible, il existe $\alpha \in k$ tel que $v_i(\alpha - 1) = e_i$ et $v_\infty(\alpha - z) > 0$. Donc on a $sgn(\alpha) = \varepsilon$. Écrivons $\alpha = x/y$ avec $x, y \in A$. il est facile de voir que $v_i(x) = v_i(y)$ pour tout i. Maintenant, d'après le théorème d'approximation forte il existe $u \in k$ tel que

$$v_i(u) = -v_i(x), \quad pour\ tout\ i$$
$$v(u) \geq 0 \text{ pour toute valuation normalisée } v \notin \{v_1, \ldots, v_s, v_\infty\}.$$

Les éléments ux et uy sont dans A, ils sont premiers à $\mathfrak{m}$ et $ux \equiv uy$ modulo $\mathfrak{m}$. Soit $x' \in A$ tel que $x'(ux) \equiv 1$ modulo $\mathfrak{m}$. Soit $z_1 = x'ux$ et $z_2 = x'uy$. Alors, on peut prendre l'élément β du lemme comme suit

$$\beta = z_1 z_2^{w_\infty - 1} = \alpha z_2^{w_\infty},$$

où w_∞ est l'ordre du groupe cyclique $\kappa(\infty)^\times$. □

Corollaire 3.3.4. *On suppose que l'idéal* $\mathfrak{m}$ *admet la propriété* (**P**). *Alors l'anneau quotient* $A/\mathfrak{m}$ *admet une* $\mathbb{F}_q$*-base* $(a_1, \ldots, a_{\deg(\mathfrak{m})})$*, où les éléments* $a_i \in A$ *sont premiers à* $\mathfrak{m}$ *et tels que* $sgn(a_i) = 1$*, pour tout* $i \in \{1, \ldots, \deg(\mathfrak{m})\}$.

Démonstration. Soit $(a_1, \ldots, a_{\deg(\mathfrak{m})})$ une $\mathbb{F}_q$-base de $A/\mathfrak{m}$ comme décrite dans le Lemme 3.3.2. Soit $\beta \in A$ l'élément défini dans Lemme 3.3.3. Pour tout i, on pose $a'_i = \beta^{n_i} a_i$, où n_i est un entier positif tel que $sgn(a_i) = sgn(\beta)^{-n_i}$. Alors la famille $(a'_1, \ldots, a'_{\deg(\mathfrak{m})})$ est satisfaite aux conditions du corollaire. □

Lemme 3.3.5. *Soit* $\mathfrak{m}$ *et* $\mathfrak{n}$ *deux idéaux non nuls et premiers entre eux dans* A*, alors*

$$B\Lambda_{\mathfrak{m}} \cap H_A^*(\Lambda_{\mathfrak{n}}) \subset B.$$

Démonstration. Soit $K_{\mathfrak{m}} = H_A^*(\Lambda_{\mathfrak{m}})$ (resp. $K_{\mathfrak{n}} = H_A^*(\Lambda_{\mathfrak{n}})$). Puisque $B\Lambda_{\mathfrak{m}} \cap H_A^*(\Lambda_{\mathfrak{n}}) \subset K_{\mathfrak{m}} \cap K_{\mathfrak{n}}$, il suffit de prouver que $K_{\mathfrak{m}} \cap K_{\mathfrak{n}} \subset H_A^*$. L'hypothése $\mathfrak{m} + \mathfrak{n} = A$ implique que $\Lambda_{\mathfrak{mn}} = \Lambda_{\mathfrak{m}} \oplus \Lambda_{\mathfrak{n}}$, et que le corps $K_{\mathfrak{mn}} = K_{\mathfrak{m}} K_{\mathfrak{n}}$ est le compositum de $K_{\mathfrak{m}}$ et $K_{\mathfrak{n}}$. De plus, on sait d'après [18, §4] que pour tout idéal $\mathfrak{c} \neq 0$ de A le degré $[K_{\mathfrak{c}} : H_A^*]$ est égal à l'ordre du groupe multiplicatif $(A/\mathfrak{c})^\times$ qu'on notera par $\varphi(\mathfrak{c})$. Puisque $\varphi(\mathfrak{mn}) = \varphi(\mathfrak{m})\varphi(\mathfrak{n})$ on déduit que $K_{\mathfrak{m}} \cap K_{\mathfrak{n}} = H_A^*$ ce qui implique le lemme. □

Proposition 3.3.6. *Soit* $\mathfrak{p}$ *un idéal premier de* A*. Supposons qu'on a* $q \neq 2$ *ou* $q = 2$ *et* $\deg(\mathfrak{p}) \geq 2$*. Alors on a*

$$B\Lambda_{\mathfrak{p}^n} \cap B = 0, \quad \textit{pour tout entier positif } n.$$

Démonstration. Démontrons d'abord le lemme pour $n = 1$. Soit $\lambda \in \Lambda_{\mathfrak{p}}$ tel que $\lambda \neq 0$. Alors λ est un générateur du A-module $\Lambda_{\mathfrak{p}}$. Le polynôme irréductible de λ sur H_A^* est $\rho_{\mathfrak{p}}(X)/X$. Puisque $\rho_{\mathfrak{p}} \in H_A^*[\tau]$, il est facile de vérifier que

$$T_{K_{\mathfrak{p}}/H_A^*}(\lambda) = 0 \tag{3.3.1}$$

si $q \neq 2$ ou si $q = 2$ et $\deg(\mathfrak{p}) \geq 2$. On en déduit que si $x \in B\Lambda_{\mathfrak{p}}$ alors $T_{K_{\mathfrak{p}}/H_A^*}(x) = 0$. Puisque $T_{K_{\mathfrak{p}}/H_A^*}(b) = -b$ pour tout $b \in B$, on conclut que $B\Lambda_{\mathfrak{p}} \cap B = 0$. Dans le cas général $n \geq 2$, les hypothèses permettent d'écrire le groupe de Galois $Gal(K_{\mathfrak{p}^n}/H_A^*)$ comme produit direct $G_1 \times G_2$, avec $ord(G_1) = N(\mathfrak{p})^{n-1}$ et $ord(G_2) = (N(\mathfrak{p}) - 1)$. Il est facile de voir que $K_{\mathfrak{p}}$ est le corps stabilisé par le sous-groupe G_1. Soit L le corps stabilisé par G_2, et soit $\widetilde{\lambda}$ un élément de $\Lambda_{\mathfrak{p}^n}$. Nous prétendons que $T_{K_{\mathfrak{p}^n}/L}(\widetilde{\lambda}) = 0$. En effet, on a

$$\rho_{\mathfrak{p}^{n-1}}\Big(T_{K_{\mathfrak{p}^n}/L}(\widetilde{\lambda})\Big) = \rho_{\mathfrak{p}^{n-1}}\Big(\sum_{\sigma \in G_2} (\widetilde{\lambda})^\sigma\Big) = \sum_{\sigma \in G_2} \rho_{\mathfrak{p}^{n-1}}((\widetilde{\lambda})^\sigma) = \sum_{\sigma \in G_2} \big(\rho_{\mathfrak{p}^{n-1}}(\widetilde{\lambda})\big)^\sigma.$$

Soit $\rho' = \mathfrak{p}^{n-1} * \rho$ le module de Drinfeld défini par Hayes dans [17, formula (3.3)]. On sait, d'après [17, Theorem 3.10] que $\rho_{\mathfrak{p}^n} = \rho'_{\mathfrak{p}} \cdot \rho_{\mathfrak{p}^{n-1}}$. Cela implique que $\rho_{\mathfrak{p}^{n-1}}(\widetilde{\lambda}) \in \Lambda_{\mathfrak{p}}^{\rho'}$, où $\Lambda_{\mathfrak{p}}^{\rho'}$ est l'ensemble des racines de $\rho'_{\mathfrak{p}}$. On a d'après [18, section 4 page 18] que ρ' est un module de Drinfeld *sgn*-normalisé. En particulier, on a $\Lambda_{\mathfrak{p}}^{\rho'} \subset K_{\mathfrak{p}}$ et

$$\rho_{\mathfrak{p}^{n-1}}\Big(T_{K_{\mathfrak{p}^n}/L}(\widetilde{\lambda})\Big) = \sum_{\sigma \in G_2} \big(\rho_{\mathfrak{p}^{n-1}}(\widetilde{\lambda})\big)^{\sigma} = T_{K_{\mathfrak{p}}/H_A^*}\big(\rho_{\mathfrak{p}^{n-1}}(\widetilde{\lambda})\big) = 0,$$

grâce à (3.3.1). On déduit que $T_{K_{\mathfrak{p}^n}/L}(\widetilde{\lambda}) \in \Lambda_{\mathfrak{p}^{n-1}} \cap L = \{0\}$. Maintenant, par le même argument du cas $n = 1$ on obtient que $B\Lambda_{\mathfrak{p}^n} \cap B = 0$. □

Corollaire 3.3.7. *Soit $\mathfrak{m}, \mathfrak{n}$ deux idéaux non nuls et premiers entre eux dans A. Supposons qu'on a $q \neq 2$ ou $q = 2$ et tout idéal premier $\mathfrak{p}$ de A divisant $\mathfrak{mn}$ est tel que $\deg(\mathfrak{p}) \geq 2$. Alors on a*

$$B\Lambda_{\mathfrak{m}} \cap B\Lambda_{\mathfrak{n}} = B\Lambda_{\mathfrak{m}} \cap B = 0.$$

Démonstration. La preuve est une application directe du Lemme 3.3.5 et de la Proposition 3.3.6. □

Corollaire 3.3.8. *Soit $\mathfrak{m}_1, \ldots, \mathfrak{m}_r$ des idéaux de A tels que $\mathfrak{m}_i + \mathfrak{m}_j = A$ si $i \neq j$. Soit $\mathfrak{m} = \mathfrak{m}_1 \cdots \mathfrak{m}_r$ et supposons que $q \neq 2$ ou $q = 2$ et pour tout idéal premier $\mathfrak{p}$ de A divisant $\mathfrak{m}$ est tel que $\deg(\mathfrak{p}) \geq 2$. alors on a*

$$B\Lambda_{\mathfrak{m}} = B\Lambda_{\mathfrak{m}_1} \oplus \cdots \oplus B\Lambda_{\mathfrak{m}_r}.$$

Démonstration. La décomposition $\Lambda_{\mathfrak{m}} = \Lambda_{\mathfrak{m}_1} \oplus \cdots \oplus \Lambda_{\mathfrak{m}_r}$ montre que $B\Lambda_{\mathfrak{m}} = B\Lambda_{\mathfrak{m}_1} + \cdots + B\Lambda_{\mathfrak{m}_r}$. Pour vérifier que la décomposition est directe, nous pouvons appliquer le Lemme 3.3.5 et le Corollaire 3.3.7. □

Lemme 3.3.9. *Supposons qu'on a $q = 2$. Soit $\mathfrak{p}$ un idéal premier de A tel que $\deg(\mathfrak{p}) = 1$. Alors pour tout entier positif n on a*

$$B\Lambda_{\mathfrak{p}^{n+1}}/B\Lambda_{\mathfrak{p}^n} \simeq B, \quad B\Lambda_{\mathfrak{p}^n} \simeq B^n \quad \text{et} \quad B\Lambda_{\mathfrak{p}^n} \cap B = B\Lambda_{\mathfrak{p}}.$$

De plus, $B\Lambda_{\mathfrak{p}}$ est un idéal principal de B engendré par l'unique élément dans $\Lambda_{\mathfrak{p}} \setminus \{0\}$.

Démonstration. Soit m un entier positif, alors tout élément $\lambda \in \Lambda_{\mathfrak{p}^{m+1}} \setminus \Lambda_{\mathfrak{p}^m}$ donne une $\mathbb{F}_2$-base de $\Lambda_{\mathfrak{p}^{m+1}}/\Lambda_{\mathfrak{p}^m}$. Le B-module $B\Lambda_{\mathfrak{p}^{m+1}}/B\Lambda_{\mathfrak{p}^m}$ est engendré par l'image de λ. Cette image est non nulle puisque $H_A^*(\lambda) = H_A^*(\Lambda_{\mathfrak{p}^{m+1}})$ et le degré $[H_A^*(\Lambda_{\mathfrak{p}^{m+1}}) : H_A^*(\Lambda_{\mathfrak{p}^m})] = 2$, grâce [18, §4]. Cela implique que $B\Lambda_{\mathfrak{p}^{m+1}}/B\Lambda_{\mathfrak{p}^m} \simeq B$ et $B\Lambda_{\mathfrak{p}^{m+1}} \cap B = B\Lambda_{\mathfrak{p}^m} \cap B$. Maintenant, il est facile de vérifier que $B\Lambda_{\mathfrak{p}}$ est un idéal principal de B engendré par l'unique élément de $\Lambda_{\mathfrak{p}} \setminus \{0\}$. Ce qui conclut la preuve de lemme. Nous attirons l'attention du lecteur qu'on a $\mathfrak{p}B = B\Lambda_{\mathfrak{p}}$, grâce à [18, Lemma 4.18]. □

Lemme 3.3.10. *Supposons qu'on a $q = 2$. Soit $\mathfrak{m}$ un idéal non nul A, divisible par deux idéaux premiers $\mathfrak{p}$ et $\mathfrak{q}$ tels que* $\deg(\mathfrak{p}) = \deg(\mathfrak{q}) = 1$. *Alors on a*

$$B\Lambda_{\mathfrak{m}} \cap B = B.$$

Démonstration. Nous devons prouver que $B \subset B\Lambda_{\mathfrak{m}}$. Soit $\lambda_{\mathfrak{p}}$ (resp. $\lambda_{\mathfrak{q}}$) l'unique élémnent dans $\Lambda_{\mathfrak{p}} \setminus \{0\}$ (resp. $\Lambda_{\mathfrak{q}} \setminus \{0\}$). On a $B = \mathfrak{p}B + \mathfrak{q}B = B\Lambda_{\mathfrak{p}} + B\Lambda_{\mathfrak{q}} \subset B\Lambda_{\mathfrak{m}}$. □

Proposition 3.3.11. *Supposons qu'on a $q = 2$. Soit $\mathfrak{m}$ un idéal premier de A divisible seulement par des idéaux premier $\mathfrak{p}$ tels que* $\deg(\mathfrak{p}) = 1$. *Alors $B\Lambda_{\mathfrak{m}}$ est un B-module libre, et on a*

$$rank_B(B\Lambda_{\mathfrak{m}}) = \deg(\mathfrak{m}) - s + 1,$$

où s est le nombre exaxte des idéaux premiers $\mathfrak{p}$ divisant $\mathfrak{m}$.

Démonstration. Le cas $s = 1$ fait partie du Lemme 3.3.9. Supposons que $s \geq 2$ et écrivons $\mathfrak{m} = \mathfrak{n}\mathfrak{p}^e$, où $e \geq 2$ et $\mathfrak{p}$ est un idéal premier tel que $\mathfrak{p} \nmid \mathfrak{n}$. Par le même argument dans la preuve du Lemme 3.3.9, on obtient que $B\Lambda_{\mathfrak{n}\mathfrak{p}^e}/B\Lambda_{\mathfrak{n}\mathfrak{p}^{e-1}} \simeq B$. Si $B\Lambda_{\mathfrak{n}\mathfrak{p}^{e-1}}$ est un B-module libre, alors $B\Lambda_{\mathfrak{n}\mathfrak{p}^e}$ est encore un B-module libre et que $rank_B(B\Lambda_{\mathfrak{n}\mathfrak{p}^e}) = rank_B(B\Lambda_{\mathfrak{n}\mathfrak{p}^{e-1}}) + 1$. Maintenant, supposons que $\mathfrak{m} = \mathfrak{p}_1^{\alpha_1}...\mathfrak{p}_s^{\alpha_s}$, où $s > 1$. Puisque $B\Lambda_{\mathfrak{p}_1...\mathfrak{p}_s} = B$ alors, d'après le Lemme 3.3.10, on déduit que $B\Lambda_{\mathfrak{m}}$ est un B-module libre et que

$$rank_B(B\Lambda_{\mathfrak{m}}) = rank_B(B\Lambda_{\mathfrak{p}_1...\mathfrak{p}_s}) + (\alpha_1 - 1) + ... + (\alpha_s - 1) = \deg(\mathfrak{m}) - s + 1,$$

Ce qui achève la preuve de la proposition. □

3.4 Preuve des principaux résultats

3.4.1 Filtrations de Riemann-Roch

Les espaces de Riemann-Roch sont des ingrédients utilisés dans la preuve des théorèmes 3.4.10 et 3.4.13. Ces $\mathbb{F}_q$-espaces constituent une filtration naturelle de A. Rappelons leur définition. Si $n \in \mathbb{N}$, on pose

$$\mathcal{L}(n\infty) = \{f \in k,\ f \neq 0 \text{ et } div(f) \geq -n\infty\} \cup \{0\}.$$

Il est facile de voir que $\mathcal{L}(n\infty) \subset A$ et que $A = \bigcup_{n\in\mathbb{N}} \mathcal{L}(n\infty)$. d'après le théorème de Riemann-Roch la dimension exacte dimension de l'espace $\mathcal{L}(n\infty)$ est donnée par la formule

$$\dim_{\mathbb{F}_q}\big(\mathcal{L}(n\infty)\big) = nd_\infty + 1 - g + \dim_{\mathbb{F}_q} \mathcal{L}(W - n\infty),$$

où g est le genre de k et W son diviseur canonique. Voir par exemple [27, Theorem 1.5.15]. Nous utiliserons également le produit tensoriel

$$\mathcal{L}_{H_A^*}(n\infty) = H_A^* \otimes_{\mathbb{F}_q} \mathcal{L}(n\infty),$$

Si S est un sous-ensemble de $H_A^*[\tau]$ alors on note par $< S >_{H_A^*}$ le H_A^*-espace vectoriel engendré par S. En particulier, on pose $E_\rho =< \rho_x,\ x \in A >_{H_A^*}$.

Lemme 3.4.1. *Soit $\mathfrak{m} \neq 0$ un idéal de A tel que $\mathfrak{m}$ admet la propriété* (**P**)*. Soit λ un générateur de $\Lambda_\mathfrak{m}$. Soit $P \in E_\rho$ tel que $P(\lambda) = 0$. Alors, on a $P(\mu) = 0$ pour tout $\mu \in \Lambda_\mathfrak{m}$. Autrement dit, il existe $Q \in H_A^*[\tau]$ tel que $P = Q\rho_\mathfrak{m}$.*

Démonstration. Soit $t = \deg(\mathfrak{m})$. Alors d'après le Corollaire 3.3.4, l'anneau $A/\mathfrak{m}$ admet une $\mathbb{F}_q$-base $(a_1, \ldots, a_t)$, où les éléments $a_i \in A$ sont premier à $\mathfrak{m}$ tels que $sgn(a_i) = 1$ pour tout $i \in \{1, \ldots, t\}$. D'après [18, Theorem 4.12] on a

$$\rho_{a_i}(\lambda) = \rho_{\mathfrak{a}_i}(\lambda) = \lambda^{\sigma_{\mathfrak{a}_i}},$$

où $\mathfrak{a}_i = a_i A$ et $\sigma_{\mathfrak{a}_i}$ est l'automorphisme de $H_A^*(\Lambda_\mathfrak{m})/H_A^*$ associé à $\mathfrak{a}_i$ par l'application d'Artin. Donc, puisque P a ses coefficients dans H_A^* on a

$$P(\rho_{a_i}(\lambda)) = P(\lambda)^{\sigma_{\mathfrak{a}_i}} = 0.$$

Maintenant, chaque $\mu \in \Lambda_\mathfrak{m}$ peut s'écrire comme combinaison linéaire sous la forme $\mu = r_1\rho_{a_1}(\lambda) + \cdots + r_t\rho_{a_t}(\lambda)$, où $r_1, \ldots, r_t$ sont dans $\mathbb{F}_q$. Un calcul facile donne

$$P(\mu) = \sum_{i=1}^{t} r_i P(\rho_{a_i}(\lambda)) = 0.$$

La division Euclidienne à droite dans $H_A^*[\tau]$ appliquée à P et $\rho_\mathfrak{m}$ donne $P = Q\rho_\mathfrak{m} + R$, où $Q, R \in H_A^*[\tau]$ et $\deg_\tau(R) < \deg(\mathfrak{m})$. On note $\deg_\tau(R)$ est le degré de R comme polynôme en τ. Puisque $R(\mu) = 0$ pour tout $\mu \in \Lambda_\mathfrak{m}$ on a forcément $R = 0$. □

Pour tout $n \geq 0$ on définit $E_n =< \rho_x,\ x \in \mathcal{L}(n\infty) >_{H_A^*}$. Pour tout entier positif δ on pose $\Xi_{n\delta} : \mathcal{L}_{H_A^*}(n\delta\infty) \longrightarrow E_{n\delta}$ l'application H_A^*-linéaire qui à chaque somme finie $\sum_i a_i \otimes v_i$ associe le polynôme $\sum_i a_i\rho_{v_i}$. Encore, on pose $\widetilde{\Xi}_{n\delta}$ l'application linéaire

$$\mathcal{L}_{H_A^*}(n\delta\infty)/\mathcal{L}_{H_A^*}((n-1)\delta\infty) \longrightarrow E_{n\delta}/E_{(n-1)\delta},$$

déduite de Ξ_n. Dans la suite, on suppose que $\delta \geq 1$ est tel que $\mathcal{L}(\delta\infty) \setminus \mathcal{L}((\delta-1)\infty) \neq \emptyset$ et on fixe $\omega \in \mathcal{L}(\delta\infty) \setminus \mathcal{L}((\delta-1)\infty)$. Nous considérons dans lemme suivant, les applications linéaires $M_\omega : H_A^* \otimes_{\mathbb{F}_q} A \longrightarrow H_A^* \otimes_{\mathbb{F}_q} A$ et $N_w : H_A^*[\tau] \longrightarrow H_A^*[\tau]$ définies par

$$M_\omega\big(\sum a_i \otimes v_i\big) = \sum a_i \otimes \omega v_i \quad et \quad N_\omega(P) = P\rho_\omega.$$

Lemme 3.4.2. *Pour tout $n \geq 1$, les applications $\widetilde{M}_\omega$ et $\widetilde{N}_\omega$, déduites respectivement de M_ω et de N_ω, donnent le diagramme commutatif exact suivant*

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & & & \\
 & & \downarrow & & \downarrow & & & & \\
0 & \longrightarrow & \ker(\widetilde{\Xi}_{n\delta}) & \longrightarrow & \mathcal{L}_{H_A^*}(n\delta\infty)/\mathcal{L}_{H_A^*}((n-1)\delta\infty) & \xrightarrow{\widetilde{\Xi}_{n\delta}} & E_{n\delta}/E_{(n-1)\delta} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow{\scriptstyle \widetilde{M}_\omega} & & \downarrow{\scriptstyle \widetilde{N}_\omega} & & \\
0 & \longrightarrow & \ker(\widetilde{\Xi}_{(n+1)\delta}) & \longrightarrow & \mathcal{L}_{H_A^*}((n+1)\delta\infty)/\mathcal{L}_{H_A^*}(n\delta\infty) & \xrightarrow{\widetilde{\Xi}_{(n+1)\delta}} & E_{(n+1)\delta}/E_{n\delta} & \longrightarrow & 0
\end{array}$$

Démonstration. Il est facile de vérifier que toutes les applications sont bien définies et que le diagramme est commutatif. Donc il suffit de prouver que l'application $\widetilde{M}_\omega$ est injective. Or la multiplication par ω donne une application injective $\mathcal{L}(n\delta\infty)/\mathcal{L}((n-1)\delta\infty) \longrightarrow \mathcal{L}((n+1)\delta\infty)/\mathcal{L}(n\delta\infty)$. Puisque H_A^* est plat sur $\mathbb{F}_q$ on déduit que $\widetilde{M}_\omega$ est aussi injective. □

Corollaire 3.4.3. *La suite $r_n = \dim_{H_A^*}(\ker(\widetilde{\Xi}_{n\delta}))$ est une suite croissante majorée.*

Démonstration. C'est est une conséquence immédiate du lemme ci-dessus et du fait que

$$r_n \leq \dim_{H_A^*}\big(\mathcal{L}_{H_A^*}(n\delta\infty)/\mathcal{L}_{H_A^*}((n-1)\delta\infty)\big) = \dim_{\mathbb{F}_q}\big(\mathcal{L}(n\delta\infty)/\mathcal{L}((n-1)\delta\infty)\big) \leq \delta d_\infty.$$

L'égalité des dimensions est une propriété générale du produit tensoriel. La dernière inégalité est prouvée, par exemple, dans [27, Lemma 1.4.8]. □

Corollaire 3.4.4. *Pour tout entier $n \geq 1$ on a,*

$$\dim_{H_A^*}(E_{n\delta}) = \big(1 - \frac{r(\delta)}{\delta d_\infty}\big)n\delta d_\infty + 1 - g + \sum_{k=1}^{n}(r(\delta) - r_k) + \dim_{\mathbb{F}_q}\mathcal{L}(W - n\delta\infty),$$

où $r(\delta) = \lim\limits_{n\to+\infty} r_n$.

Démonstration. On utilise simplement la formule $\dim_{H_A^*}(E_{n\delta}) = \dim_{H_A^*}(E_0) + \sum\limits_{k=1}^{n}\dim_{H_A^*}(E_{k\delta}/E_{(k-1)\delta})$ et les ingrédients suivants. On remarque d'abord que $E_0 = H_A^*\tau^0$. De plus, on a les suites exactes

$$0 \longrightarrow \ker(\widetilde{\Xi}_{k\delta}) \longrightarrow \mathcal{L}_{H_A^*}(k\delta\infty)/\mathcal{L}_{H_A^*}((k-1)\delta\infty) \xrightarrow{\widetilde{\Xi}_{k\delta}} E_{k\delta}/E_{(k-1)\delta} \longrightarrow 0\,.$$

D'autre part, le théorème de Riemann-Roch offre la dimension exacte des espaces vectoriels

$$\mathcal{L}_{H_A^*}(k\delta\infty)/\mathcal{L}_{H_A^*}((k-1)\delta\infty).$$

Le dernier ingrédient est le Corollaire 3.4.3. □

Corollaire 3.4.5. *Soit δ et $r(\delta)$ comme au-dessus. Soit $\mathfrak{m} \neq 0$ un idéal de A. Si $\mathfrak{m}$ admet la propriété* (**P**) *alors*

$$\big(1 - \frac{r(\delta)}{\delta d_\infty}\big) \deg(\mathfrak{m}) - 1 - g - \delta d_\infty \leq rank_B(B\Lambda_\mathfrak{m}).$$

Démonstration. Prouvons d'abord que $rank_B(B\Lambda_\mathfrak{m}) \geq \dim_{H_A^*}(E_{n\delta})$, où $n = [\frac{\deg(\mathfrak{m}) - 1}{\delta d_\infty}]$. Soit $(P_1, \ldots, P_s)$ est une base de $E_{n\delta}$. Soit λ un générateur de $\Lambda_\mathfrak{m}$, donc on a $\Lambda_\mathfrak{m} = \{\rho_a(\lambda),\ a \in A\}$. Nous prétendons que la famille $\{P_1(\lambda), \ldots, P_s(\lambda)\}$ est libre sur H_A^*. En effet, supposons qu'on une relation linéaire de la forme $b_1 P_1(\lambda) + \cdots + b_s P_s(\lambda) = 0$, où $b_1, \ldots, b_s \in H_A^*$. D'après le Lemme 3.4.1, il existe $Q \in H_A^*[\tau]$ tel que $\sum_{i=1}^{s} b_i P_i = Q\rho_\mathfrak{m}$. Pour $P \in H_A^*[\tau]$ on désigne par $\deg_\tau(P)$ le degré de P comme polynôme en τ. Puisque les polynômes P_i sont dans $E_{n\delta}$ on a

$$\deg_\tau(\sum_{i=1}^{s} b_i P_i) \leq n\delta d_\infty \leq \deg(\mathfrak{m}) - 1.$$

Ce qui implique que $\sum_{i=1}^{s} b_i P_i = 0$. On en déduit que $b_1 = \cdots = b_s = 0$ car $(P_1, \ldots, P_s)$ est libre. Maintenant, pour conclure la preuve du corollaire, nous utilisons simplement le fait que $s = \dim_{H_A^*}(E_{n\delta})$ donné dans le Corollaire 3.4.4 et l'inégalité $n \geq \dfrac{\deg(\mathfrak{m}) - 1}{\delta d_\infty} - 1$. □

Corollaire 3.4.6. *Soit δ et $r(\delta)$ comme au-dessus. Soit $\mathfrak{m} \neq 0$ un idéal de A, alors*

$$rank_B(B\Lambda_\mathfrak{m}) \leq \big(1 - \frac{r(\delta)}{\delta d_\infty}\big) \deg(\mathfrak{m}) + 1 + g + \delta d_\infty + \sum_{k=1}^{+\infty} (r(\delta) - r_k).$$

Démonstration. Soit $n = [\frac{\deg(\mathfrak{m}) - 1}{\delta d_\infty}]$ et soit $\nu = \dim_{\mathbb{F}_q}(\mathcal{L}(n\delta\infty))$. On sait d'après le théorème de Riemann-Roch que $\nu = n\delta d_\infty + 1 - g + \dim_{\mathbb{F}_q} \mathcal{L}(W - n\delta\infty)$. Soit $(e_1, ..., e_\nu)$ une $\mathbb{F}_q$-base de $\mathcal{L}(n\delta\infty)$. Alors $(e_1, ..., e_\nu)$ est encore libre modulo l'idéal $\mathfrak{m}$. En effet, supposons qu'on a une somme $z = r_1 e_1 + \cdots + r_\nu e_\nu \in \mathfrak{m}$, où $r_1, \ldots, r_\nu$ sont dans $\mathbb{F}_q$. Si $z \neq 0$ alors $\deg(z) \geq \deg(\mathfrak{m})$. C'est une contradiction avec le fait que $\deg(z) \leq \max_{1 \leq i \leq \nu}(\deg(r_i e_i)) \leq n\delta d_\infty \leq \deg(\mathfrak{m}) - 1$. Donc $r_1 e_1 + \cdots + r_\nu e_\nu = 0$, ce qui implique que $r_1 = \cdots = r_\nu = 0$. Soit $\nu' = \deg(\mathfrak{m}) - \nu$. Soient $f_1, ..., f_{\nu'}$ des éléments de A tels que $(e_1, ..., e_\nu, f_1, ..., f_{\nu'})$ est une $\mathbb{F}_q$-base de $A/\mathfrak{m}$. Soit λ un générateur de $\Lambda_\mathfrak{m}$, alors l'application $\mathfrak{U} : E_{n\delta} \times (H_A^*)^{\nu'} \longrightarrow H_A^*\Lambda_\mathfrak{m}$ définie par

$$\mathfrak{U}(P, b_1, \ldots, b_{\nu'}) = P(\lambda) + \sum_{j=1}^{\nu'} b_j \rho_{f_j}(\lambda).$$

est surjective. En particulier, on a $rank_B(B\Lambda_\mathfrak{m}) \leq \dim_{H_A^*}(E_{n\delta}) + \nu'$. Un calcul facile en utilisant le fait que $n \geq \dfrac{\deg(\mathfrak{m}) - 1}{\delta d_\infty} - 1$ donne $\nu' \leq \delta d_\infty + g$. On conclut grâce au Corollaire 3.4.4. □

Corollaire 3.4.7. *Soit δ et $r(\delta)$ comme au-dessus. Il existe un idéal $\mathfrak{m}_{\rho,\delta} \neq 0$ de A tel que pour tout idéal $\mathfrak{m} \neq 0$ premier à $\mathfrak{m}_{\rho,\delta}$ on a*

$$rank_B(B\Lambda_{\mathfrak{m}}) = \big(1 - \frac{r(\delta)}{\delta d_\infty}\big)\deg(\mathfrak{m}).$$

Démonstration. Si ce n'est pas le cas alors il existe une infinité d'idéaux premiers $(\mathfrak{p}_i)_{i\in\mathbb{N}}$ tels que le signe de $\varepsilon_i = rank_B(B\Lambda_{\mathfrak{p}_i}) - \big(1 - \frac{r(\delta)}{\delta d_\infty}\big)\deg(\mathfrak{p}_i)$ est indépendant de i. Supposons que $\varepsilon_i > 0$ pour tout i. D'après le Corollaire 3.3.8 et le Corollaire 3.4.6 on a

$$\sum_{i=0}^{n}\varepsilon_i = rank_B(B\Lambda_{\mathfrak{m}_n}) - \big(1 - \frac{r(\delta)}{\delta d_\infty}\big)\deg(\mathfrak{m}_n) \leq 1 + g + \delta d_\infty + \sum_{k=1}^{+\infty}(r(\delta) - r_k),$$

où $\mathfrak{m}_n = \mathfrak{p}_0 \cdots \mathfrak{p}_n$. Ce qui implique que $\lim\limits_{i\to+\infty} \delta d_\infty \varepsilon_i = 0$, et puisque $\delta d_\infty \varepsilon_i \in \mathbb{N}$ donc $\delta d_\infty \varepsilon_i = 0$ pour i suffisament grand. La même contradiction peut être obtenue si l'on suppose que $\varepsilon_i < 0$ pour tout i. Nous laissons les détails au lecteur. □

Proposition 3.4.8. *Pour tout entier $\delta \geq 1$ tel que $\mathcal{L}(\delta\infty) \setminus \mathcal{L}((\delta-1)\infty) \neq \emptyset$, on a $r(\delta) = 0$.*

Démonstration. D'après le Corollaire 3.4.7, on remarque que $r(\delta)/\delta$ est indépendant de δ. Choisissons $\delta' = \delta + \alpha$ tel que α premier à δ. L'égalité $\delta r(\delta') = \delta' r(\delta)$ implique que $\delta \mid r(\delta)$. Encore d'après le Corollaire 3.4.7, on déduit que $d_\infty \mid (\frac{r(\delta)}{\delta})\deg(\mathfrak{m})$ pour tout $\mathfrak{m}$ premier à $\mathfrak{m}_{\rho,\delta}$. Soit α le gcd des $\deg(\mathfrak{m})$ pour les $\mathfrak{m}$ premiers à $\mathfrak{m}_{\rho,\delta}$, alors $d_\infty \mid (\frac{r(\delta)}{\delta})\alpha$. Soit S l'ensemble des places $v \neq \infty$ de k premiers à $\mathfrak{m}_{\rho,\delta}$. L'entier positif α est le gcd des $\deg(v)$, $v \in S$. Si $v \in S$ alors le corps fini $\mathbb{F}_{q^\alpha}$ est un sous-corps du complété k_v de k en v. Ce qui implique que tout premier $v \in S$ se décompose totalement dans $k(\mathbb{F}_{q^\alpha})$. Mais S contient tous, sauf un nombre fini, des premiers de k. Donc, grâce au théorème de densité de Chebotarev [26, Theorem 9.13A], on a forcément $k(\mathbb{F}_{q^\alpha}) = k$. Ainsi $\alpha = 1$ et $d_\infty \mid \frac{r(\delta)}{\delta}$. Si $r(\delta) \neq 0$ alors on a $\delta d_\infty = r(\delta)$, ce qui est évidemment faux. □

3.4.2 Preuve du Théorème 3.2.1

Pour donner la preuve du théorème 3.2.1 nous avons besoin du résultat suivant

Corollaire 3.4.9. *Soit $V \subset A$ un $\mathbb{F}_q$-espace vectoriel de dimension finis inclus dans A. On a*

$$\dim_{H_A^*}(Sp(V)) = \dim_{\mathbb{F}_q}(V),$$

où $Sp(V)$ est le sous H_A^*-espace vectoriel $H_A^*[\tau]$ engendré par les polynômes ρ_v, avec $v \in V$.

Démonstration. Puisque V est contenu dans $\mathcal{L}(n\infty)$ pour n assez grand, on peut prendre $V = \mathcal{L}(n\infty)$, ou même $V = \mathcal{L}(n\delta\infty)$, où δ est un entier positif tel que $\mathcal{L}(\delta\infty) \setminus \mathcal{L}((\delta-1)\infty) \neq \emptyset$. Mais dans ce cas on a $Sp(\mathcal{L}(n\delta\infty)) = E_{n\delta}$, et on sait, grâce à la Proposition 3.4.8 et au Corollaire 3.4.4, que $\dim_{H_A^*}(Sp(\mathcal{L}(n\delta\infty))) = \dim_{\mathbb{F}_q}(\mathcal{L}(n\delta\infty))$. □

Théorème 3.4.10. *Soit $E_\rho \subset H_A^*[\tau]$ le H_A^*-espace vectoriel engendré par tous les polynômes ρ_x, $x \in A$. Alors le quotient $R_\rho = H_A^*[\tau]/E_\rho$ est un H_A^*-espace vectoriel de dimension $\leq g$, où g est le genre de k. Si $d_\infty = 1$ alors on a $\dim_{H_A^*}(R_\rho) = g$.*

Démonstration. Soit $V_n = \{P \in H_A^*[\tau], \quad \deg_\tau(P) \leq nd_\infty\}$, alors les quotients $V_n/E_\rho \cap V_n$ définis une filtartion naturelle $H_A^*[\tau]/E_\rho$. De plus, puisque $E_n \subset E_\rho \cap V_n$ et $E_n = Sp(\mathcal{L}(n\infty))$ on a, d'après le corollaire 3.4.9,

$$\dim_{H_A^*}(V_n/E_\rho \cap V_n) \leq \dim_{H_A^*}(V_n/E_n) = (nd_\infty + 1) - \dim_{\mathbb{F}_q}(\mathcal{L}(n\infty)) \leq g,$$

où la dernière inégalité est obtenue grâce au théorème de Riemann-Roch. Cela prouve qu'on a

$$\dim_{H_A^*}(H_A^*[\tau]/E_\rho) \leq g.$$

Si $d_\infty = 1$ alors on a l'égalité, facile à prouver. En effet, $E_{n+1} \cap V_n = E_n$ pour tout $n \geq 0$. Ce qui implique que $E_\rho \cap V_n = E_n$ pour tout $n \geq 0$ et par suite $\dim_{H_A^*}(H_A^*[\tau]/E_\rho) = g$. □

Remarque. Soit $i_1 < \ldots < i_g$ les g nombres gap de ∞ définis par le Théorème de Gap de Weierstrass (voir par exemple [27, Theorem 1.6.8]). Alors, il est facile de voir que l'espace vectoriel $\mathcal{R} =< \tau^{i_1}, \ldots, \tau^{i_g} >_{H_A^*}$ est tel que $\mathcal{R} \oplus E_n = V_n$ pour tout $n \geq 2g-1$ et également on a $\mathcal{R} \oplus E_\rho = H_A^*[\tau]$.

3.4.3 Preuve du Théorème 3.2.2

Proposition 3.4.11. *Soit $\mathfrak{p}$ un idéal premier de A, alors $x_n = \deg(\mathfrak{p}^n) - rank_B(B\Lambda_{\mathfrak{p}^n})$ est une suite croissante bornée d'entiers positifs. En particulier, on a*

$$rank_B(B\Lambda_{\mathfrak{p}^{n+1}}) - rank_B(B\Lambda_{\mathfrak{p}^n}) = \deg(\mathfrak{p}),$$

pour n assez grand.

Démonstration. La suite x_n est bornée grâce au Corollaire 3.4.5 et à la Proposition 3.4.8. De plus, on a $x_{n+1} - x_n = \deg(\mathfrak{p}) - (rank_B(B\Lambda_{\mathfrak{p}^{n+1}}) - rank_B(B\Lambda_{\mathfrak{p}^n}))$. Soit $(\lambda_1, \ldots, \lambda_u)$, $u = \deg(\mathfrak{p})$, la famille des éléments de $\Lambda_{\mathfrak{p}^{n+1}}$ donnant un $\mathbb{F}_q$-base de $\Lambda_{\mathfrak{p}^{n+1}}/\Lambda_{\mathfrak{p}^n}$. Alors le B-module $B\Lambda_{\mathfrak{p}^{n+1}}/B\Lambda_{\mathfrak{p}^n}$ est engendré par les images de $\lambda_1, \ldots, \lambda_u$ ce qui prouve que $x_{n+1} \geq x_n$. □

Définition 3.4.12. Pour tout idéal premier $\mathfrak{p}$ de A on pose

$$d_{\mathfrak{p}} = \min\{n \geq 0, \text{ tel que pour tout } m \geq n, rank_B(B\Lambda_{\mathfrak{p}^{m+1}}) - rank_B(B\Lambda_{\mathfrak{p}^m}) = \deg(\mathfrak{p})\}.$$

d'après le Corollaire 3.4.7 et la Proposition 3.4.8 on a $d_{\mathfrak{p}} = 0$ pour presque tout idéal premier de A. On définit

$$\mathfrak{m}_\rho = \prod_{\mathfrak{p}} \mathfrak{p}^{d_{\mathfrak{p}}}.$$

où le produit est sur les idéaux premiers de A.

Théorème 3.4.13. *Pour tout idéal $\mathfrak{m} \neq 0$ premier à $\mathfrak{m}_\rho$, le B-module $B\Lambda_{\mathfrak{m}}$ est libre et on a*

$$rank_B(B\Lambda_{\mathfrak{m}}) = \begin{cases} \deg(\mathfrak{m}) - s + 1, & \text{si } q = 2 \text{ et } s \geq 1, \\ \deg(\mathfrak{m}), & \text{si } q > 2 \text{ ou } (q = 2 \text{ et } s = 0), \end{cases} \tag{3.4.1}$$

où s est le nombre exact des idéaux premiers $\mathfrak{p}$ divisant $\mathfrak{m}$ et $\deg(\mathfrak{p}) = 1$.

Démonstration. Supposons d'abord que $q > 2$ ou $q = 2$ et $s = 0$. Écrivons $\mathfrak{m} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$, où $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ sont des idéaux premiers et $e_1, \ldots, e_r$ sont des entiers strictement positifs. Puisque les idéaux $\mathfrak{p}_i$ sont premiers à $\mathfrak{m}_\rho$ on a $d_{\mathfrak{p}_i} = 0$. Cela signifie que $rank_B(B\Lambda_{\mathfrak{p}_i^m}) = \deg(\mathfrak{p}_i^m)$ pour tout $m \geq 1$. Le Corollaire 3.3.8 implique qu'on a $rank_B(B\Lambda_{\mathfrak{m}}) = \deg(\mathfrak{m})$. Supposons maintenent que $q = 2$ et $s \geq 1$. Écrivons $\mathfrak{m} = \mathfrak{m}_1\mathfrak{m}_2$, avec $\mathfrak{m}_1$ et $\mathfrak{m}_2$ sont premiers entre eux et $\mathfrak{m}_2$ divisible par tous les idéaux premiers qui divise $\mathfrak{m}$ et dont le degré égal à 1. Dans une telle situation, nous avons nécessairement $B\Lambda_{\mathfrak{m}} = B\Lambda_{\mathfrak{m}_1} \oplus B\Lambda_{\mathfrak{m}_2}$, grâce au Lemme 3.3.5 et au Corollaire 3.3.7. D'une part, nous avons $rank_B(B\Lambda_{\mathfrak{m}_1}) = \deg(\mathfrak{m}_1)$, d'après la première partie de la preuve. D'autre part, nous savons que $B\Lambda_{\mathfrak{m}_2}$ est libre et $rank_B(B\Lambda_{\mathfrak{m}_2}) = \deg(\mathfrak{m}_2) - s + 1$, grâce à la Proposition 3.3.11, d'où la formule (3.4.1). □

3.5 L'application résidue

Soit $\mathcal{R}$ un supplémentaire de l'espace $E_\rho =< \rho_z, \ z \in A >_{H_A^*}$ dans $H_A^*[\tau]$. Autrement dit, on a

$$\mathcal{R} \oplus E_\rho = H_A^*[\tau]. \tag{3.5.1}$$

Soit $\mathcal{R}_n = \mathcal{R} \cap V_n$, où $V_n = \{P \in H_A^*[\tau], \quad \deg_\tau(P) \leq nd_\infty\}$, alors on a,

$$\mathcal{R}_n \cap E_n \subset \mathcal{R} \cap E_\rho = 0.$$

Ce qui implique que $\dim_{H_A^*}(\mathcal{R}_n) \leq \dim_{H_A^*}(V_n) - \dim_{H_A^*}(E_n) \leq g$. La dernière inégalité est une conséquence du Théorème 3.2.2. Donc, $\mathcal{R}_n = \mathcal{R}$ pour n assez grand. En particulier, $\mathcal{R}$ est un espace vectoriel de dimension finie et on a

$$\mathcal{R} \oplus \big(E_\rho \cap V_n\big) = V_n, \tag{3.5.2}$$

Pour n assez grand, nous utiliserons la décomposition (3.5.1) ci-dessus pour définir un homomorphisme d'anneaux

$$\Phi_{\mathcal{R}} : A \longrightarrow End(\mathcal{R}),$$

où $End(\mathcal{R})$ est l'anneau des endomorphismes de $\mathcal{R}$. Notons $p_{\mathcal{R}}$ l'application de projection $H_A^*[\tau] \longrightarrow \mathcal{R}$ définie par la décomposition (3.5.1). Si $z \in A$ alors on pose $\Phi_{\mathcal{R}}(z) = p_{\mathcal{R}} \circ N_z$, avec $N_z(P) = P\rho_z$, pour tout $P \in \mathcal{R}$. Il est facile de voir qu'on a,

Proposition 3.5.1. *Supposons qu'on a une autre décomposition*

$$\mathcal{R}' \oplus E_\rho = H_A^*[\tau].$$

Soit $\Psi : \mathcal{R}' \longrightarrow \mathcal{R}$ l'isomorphisme défini par $\Psi(P) = p_{\mathcal{R}}(P)$. Alors l'homomorphisme d'anneaux associé $\Phi_{\mathcal{R}'} : A \longrightarrow End(\mathcal{R}')$ est tel que

$$\Phi_{\mathcal{R}'}(z) = \Psi^{-1}\Phi_{\mathcal{R}}(z)\Psi, \text{ pour tout } z \in A.$$

Démonstration. Évident. □

Théorème 3.5.2. *Soit $\mathfrak{m} = zA$ un idéal principal non nul de A de degré dd_∞ suffisamment grand. Si l'idéal $\mathfrak{m}$ a la propriété $(\mathbf{P})$, alors il existe un entier positif $r(z) \leq \dim_{H_A^*} \mathcal{R}$ tel que*

$$rank_B(B\Lambda_{\mathfrak{m}}) = \deg(\mathfrak{m}) - r(z). \tag{3.5.3}$$

De plus, si $\dim_{H_A^*} \mathcal{R} = g$ alors $r(z) = \dim_{H_A^*}(\ker \Phi_{\mathcal{R}}(z))$.

Démonstration. Supposons que d soit suffisamment grand pour avoir $\mathcal{R} \oplus (E_\rho \cap V_d) = V_d$. Si $r = \dim_{H_A^*} \mathcal{R}$ et $s = \dim_{H_A^*}(E_\rho \cap V_d)$ alors nous avons $r + s = \deg(\mathfrak{m}) + 1$. Soit λ un générateur de $\Lambda_{\mathfrak{m}}$ et soit $(P_1, ..., P_{s-1}, P_s)$ un H_A^*-base de $E_\rho \cap V_d$ tel que $P_s = \rho_z$. On prétend que $(P_1(\lambda), ..., P_{s-1}(\lambda))$ est un système libre de l'espace vectoriel $H_A^*\Lambda_{\mathfrak{m}}$. En effet, si $b_1, ..., b_{s-1}$ sont des éléments de H_A^* tels que $\sum_{i=1}^{s-1} b_i P_i(\lambda) = 0$ alors, grâce au Lemme 3.4.1, il existe $Q \in H_A^*[\tau]$ tel que $\sum_{i=1}^{s-1} b_i P_i = Q\rho_{\mathfrak{m}} = Qs_\rho(z)^{-1}\rho_z$. Puisque $\deg_\tau(\sum_{i=1}^{s-1} b_i P_i) \leq \deg(\mathfrak{m})$ alors le polynôme $Q \in H_A^*$. On en déduit que $b_1 = \cdots = b_{s-1} = Q = 0$. Remarquons que

$$\dim_{H_A^*}(H_A^*\Lambda_{\mathfrak{m}}) - (s-1) \leq \deg(\mathfrak{m}) - (s-1) = r.$$

Soit $Q_1, \ldots, Q_r$ des éléments de E_ρ. Pour tout $j = 1, ..., r$, il existe g_j, R_j dans $H_A^*[\tau]$ tels que $R_j = 0$ ou $\deg_\tau(R_j) < \deg(z)$ et

$$Q_j = g_j \rho_z + R_j. \tag{3.5.4}$$

Fixons une base $(\Phi_1, ..., \Phi_r)$ de $\mathcal{R}$ et notons $\phi_{\mathcal{R}}(z)$ la représentation matricielle de l'endomorphisme $\Phi_{\mathcal{R}}(z)$ dans cette base. d'après les équations (3.5.1) et (3.5.2) il existe des éléments $s_i^{(j)}(z), a_i^{(j)}(z) \in H_A^*$ et des polynômes $T_j \in E_\rho \cap V_d$, $G_j \in E_\rho$ tels que

$$R_j = \sum_{i=1}^{r} a_i^{(j)}(z)\Phi_i + T_j \quad et \quad g_j = \sum_{i=1}^{r} s_i^{(j)}(z)\Phi_i + G_j. \tag{3.5.5}$$

Considérons les deux matrices carrées $S(z) = (s_i^{(j)}(z))$ et $M(z) = (a_i^{(j)}(z))$, avec r lignes et r colonnes.

Lemme 3.5.3. *On a* $M(z) = -\phi_{\mathcal{R}}(z)S(z)$.

Démonstration. Par définition il existe $D_1, \ldots, D_r \in E_\rho$ tels que

$$(\Phi_1\rho_z, \ldots, \Phi_r\rho_z) = (\Phi_1, \ldots, \Phi_r)\phi_{\mathcal{R}}(z) + (D_1, \ldots, D_r).$$

Si l'on prend en compte des formules (3.5.4) et (3.5.5) alors on obtient

$$\begin{aligned}(Q_1, \ldots, Q_r) \;=\; & (\Phi_1, \ldots, \Phi_r)[M(z) + \phi_{\mathcal{R}}(z)S] + (G_1\rho_z, \ldots, G_r\rho_z) + (T_1, \ldots, T_r) \\ & +(D_1, \ldots, D_r)S.\end{aligned} \tag{3.5.6}$$

La décomposition (3.5.1) implique alors que $M(z) + \phi_{\mathcal{R}}(z)S(z) = 0$. □

Lemme 3.5.4. *Supposons que* $(P_1(\lambda), ..., P_{s-1}(\lambda), Q_1(\lambda), ..., Q_r(\lambda))$ *est une famille génératrice de* $H_A^*\Lambda_{\mathfrak{m}}$. *Soit* $\theta : (H_A^*)^r \longrightarrow (H_A^*)^r$ *l'application linéaire définie par* $\theta(V) = M_{\mathcal{R}}(z)V^t$, *pour tout* $V = (b_1, \ldots, b_r) \in (H_A^*)^r$. *Alors on a*

$$rank_B(B\Lambda_{\mathfrak{m}}) = \deg(\mathfrak{m}) - \dim_{H_A^*}(\ker(\theta)). \tag{3.5.7}$$

Démonstration. On définit un diagramme exact commutatif comme suit

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \ker(\theta) & \longrightarrow & (H_A^*)^r & \xrightarrow{\theta} & Im(\theta) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle D} & & \downarrow{\scriptstyle D} & & \downarrow & & \\ 0 & \longrightarrow & \ker(\widetilde{\theta}) & \longrightarrow & \Sigma_d \times (H_A^*)^r & \xrightarrow{\widetilde{\theta}} & H_A^*\Lambda_{\mathfrak{m}} & \longrightarrow & 0, \end{array} \tag{3.5.8}$$

où $\Sigma_\rho = E_\rho \cap V_d$ et $D : (H_A^*)^r \longrightarrow \Sigma_d \times (H_A^*)^r$ est l'application linéaire définie par $D(V) = (-\sum_{j=1}^{r} b_j T_j, V)$ pour tout $V = (b_1, \ldots, b_r) \in (H_A^*)^r$. Si $(P, b_1, \ldots, b_r) \in \Sigma_d \times (H_A^*)^r$, alors on pose

$\widetilde{\theta}(P, b_1, \ldots, b_r) = P(\lambda) + \sum_{j=1}^{r} b_j Q_j(\lambda)$. L'inclusion $D(\ker(\theta)) \subset \ker(\widetilde{\theta})$ est immédiate d'après les relations (3.5.4) et (3.5.5). Soit $(P, b_1, \ldots, b_r) \in \ker(\widetilde{\theta})$ et notons $V = (b_1, \ldots, b_r)$. d'après le Lemme 3.4.1 il existe $U \in H_A^*[\tau]$ tel que $P + \sum_{j=1}^{r} b_j Q_j = U\rho_z$. d'après les relations (3.5.4) et (3.5.5) on a

$$P + \sum_{j=1}^{r} b_j Q_j = P + \sum_{j=1}^{r} b_j g_j \rho_z + \sum_{j=1}^{r} b_j \left(\sum_{i=1}^{r} a_i^{(j)}(z)\Phi_i \right) + \sum_{j=1}^{r} b_j T_j.$$

Des deux égalités précédentes on déduit que

$$P + \sum_{j=1}^{r} b_j \left(\sum_{i=1}^{r} a_i^{(j)}(z)\Phi_i \right) + \sum_{j=1}^{r} b_j T_j = (U - (\sum_{j=1}^{r} b_j g_j))\rho_z.$$

Puisque le polynôme à gauche de l'égalité ci-dessus a un degré en τ inférieur ou égal à $\deg(z)$, on déduit que $U - (\sum_{j=1}^{r} b_j g_j) \in H_A^*$. Soit $\alpha = U - (\sum_{j=1}^{r} b_j g_j) \in H_A^*$, alors on a

$$M_{\mathcal{R}}(z)V^t = 0 \quad et \quad P + \sum_{j=1}^{r} b_j T_j = \alpha\rho_z,$$

grâce à la relation (3.5.1). Cela prouve la décomposition

$$\ker(\widetilde{\theta}) = D(\ker(\theta)) \oplus \Big(< \rho_z >_{H_A^*} \times \{(0, \ldots, 0)\} \Big).$$

Puisque D est injective, on déduit du diagramme exact (3.5.8) que

$$rank_B(B\Lambda_{\mathfrak{m}}) = s + r - \dim_{H_A^*}(\ker(\widetilde{\theta})) = \deg(\mathfrak{m}) - \dim_{H_A^*}(\ker(\theta)),$$

comme le dit le lemme. □

La première assertion du Théorème 3.5.2 est une conséquence immédiate du Lemme 3.5.3 et du Lemme 3.5.4. Pour prouver la seconde assertion du Théorème 3.5.2 nous supposons que $r = g$. Cela signifie notamment que $E_\rho \cap V_d = E_d$. Par conséquent, nous pouvons choisir $(P_1, ..., P_{s-1}, P_s)$ sous la forme de $(\rho_{e_1}, \ldots, \rho_{e_{s-1}}, \rho_{e_s})$, où $e_s = z$ et $(e_1, \ldots, e_s)$ est une $\mathbb{F}_q$-base de $\mathcal{L}(d\infty)$. Nous laissons au lecteur le soin de vérifier que $(e_1, \ldots, e_{s-1})$ est libre modulo $\mathfrak{m}$. Soient $f_1, ..., f_g$ des éléments de A tels que $(e_1, ..., e_{s-1}, f_1, ..., f_g)$ est une $\mathbb{F}_q$-base de $A/\mathfrak{m}$. Puis le système $(\rho_{e_1}(\lambda), ..., \rho_{e_{s-1}}(\lambda), \rho_{f_1}(\lambda), ..., \rho_{f_g}(\lambda))$ est une famille génératrice de $H_A^*\Lambda_{\mathfrak{m}}$. Posons $Q_j = \rho_{f_j}$, pour $j = 1, \ldots, g$.

Lemme 3.5.5. *Supposons que* $\dim_{H_A^*} \mathcal{R} = g$. *On prend* $P_i = \rho_{e_i}$ *et* $Q_j = \rho_{f_j}$, *pour* $i = 1, \ldots, s-1$ *et* $j = 1 \ldots, g$, *où* e_i *et* f_j *sont comme au-dessus. Alors la matrice associée* S *est inversible.*

Démonstration. Soit $V = (b_1, \ldots, b_g) \in (H_A^*)^g$ tel que $SV^t = 0$. d'après l'équation (3.5.6) et le Lemme 3.5.3 on a

$$\sum_{j=1}^{g} b_j Q_j = \sum_{j=1}^{g} b_j G_j \rho_z + \sum_{j=1}^{g} b_j T_j.$$

Par hypothéses, il existe $c_1, \ldots, c_s \in H_A^*$ tels que $\sum_{j=1}^{g} b_j T_j = \sum_{i=1}^{s} c_i \rho_{e_i}$. Écrivons chaque G_j comme une somme finie $G_j = \sum_{x \in E_j} c_x^{(j)} \rho_x$, où E_j est un sous-ensemble fini de A et $c_x^{(j)} \in H_A^*$. d'après le Corollaire 3.4.9 l'application linéaire surjective

$$\Xi : H_A^* \otimes_{\mathbb{F}_q} A \longrightarrow E_\rho,$$

qui à chaque somme finie $\sum a_i \otimes v_i$ on lui associe $\sum a_i \rho_{v_i}$, est un isomorphisme. Ainsi on a

$$\sum_{j=1}^{g} b_j \otimes f_j = \sum_{j=1}^{g} b_j \Big(\sum_{x \in E_j} c_x^{(j)} \otimes xz \Big) + \sum_{i=1}^{s} c_i \otimes e_i.$$

Mais nous avons supposé que la famille $(e_1, \ldots, e_{s-1}, e_s, f_1, \ldots, f_g)$ est libre sur $\mathbb{F}_q$. Cela implique que $b_j = 0$ pour tout $j = 1, \ldots, g$. □

La deuxième assertion du Théorème 3.5.2 découle de Lemme 3.5.3, Lemme 3.5.4 et Lemme 3.5.5. □

Remarque. Lorsque k est un corps de fonctions rationnelles, nous avons $\dim_{H_A^*}(\mathcal{R}) = 0$, et le Théorème 3.5.2 implique que $rank_B(B\Lambda_{\mathfrak{m}}) = \deg(\mathfrak{m})$, pour tout idéal non nul $\mathfrak{m}$ de A ayant la propriété (**P**). En d'autres termes, nous avons $\mathfrak{m}_\rho = A$.

3.6 Le cas $d_\infty = g = 1$

Dans cette section, on suppose que k est un corps de fonctions de genre $g = 1$ et que $d_\infty = \deg(\infty) = 1$. D'après le Théorème de Riemman-Roch, on a $\dim_{\mathbb{F}_q} \mathcal{L}(n.\infty) = n$ pour tout entier positif n. En prennant $n = 2$ et $n = 3$, on voit qu'il existe deux fonctions $x \in \mathcal{L}(2.\infty)$ et $y \in \mathcal{L}(3.\infty)$ dont le pôle diviseurs est respectivement $2.\infty$ et $3.\infty$.

Lemme 3.6.1. *On a* $A = \mathbb{F}_q[x, y]$.

Démonstration. On prend $e_0 = 1$, pour tout entier n strictement positif on prend $e_{2n} = x^n$ et $e_{2n+1} = x^{n-1}y$. Donc la famille $(e_0, e_2, e_3, ..., e_n)$ est une $\mathbb{F}_q$-base de $\mathcal{L}(n.\infty)$, puisque $\deg(e_i) = i$ et $\dim_{\mathbb{F}_q} \mathcal{L}(n.\infty) = n$. Cela implique que $A = \bigcup_{n\in\mathbb{N}} \mathcal{L}(n.\infty) = \mathbb{F}_q[x, y]$. □

Comme indiqué dans la remarque 3.4.2, pour tout entier strictement positif n on a $\mathcal{R} \oplus E_n = V_n$, où $\mathcal{R} =< \tau >_{H_A^*}$. Pour tout $z \in A$, il existe $\phi_{\mathcal{R}}(z) \in H_A^*$ tel que $\Phi_{\mathcal{R}}(z)(\tau) = \phi_{\mathcal{R}}(z)\tau$. L'application $\phi_{\mathcal{R}} : A \longrightarrow H_A^*$ est un morphisme d'anneaux

Proposition 3.6.2. *Supposons qu'on a $d_\infty = g = 1$, alors l'homomorphisme d'anneaux $\phi_{\mathcal{R}} : A \longrightarrow H_A^*$ est injectif. En particulier on a $\mathfrak{m}_\rho = A$.*

Démonstration. Puisque $d_\infty = 1$ on a $sgn(x), sgn(y) \in \mathbb{F}_q$. Donc on peut supposer que $sgn(x) = sgn(y) = 1$. On écrit

$$\rho_x = \tau^2 + a\tau + x\tau^0 \quad et \quad \rho_y = \tau^3 + c\tau^2 + b\tau + y\tau^0,$$

où $a, b, c \in H_A^*$. En fait, $a, b, c \in B$, grâce au Corollaire [16, Corollary 7.4]. Remarquons d'abord que

$$E_3 = H_A^*\tau^0 \oplus H_A^*\rho_x \oplus H_A^*\rho_y \quad et \quad E_4 = H_A^*\tau^0 \oplus H_A^*\rho_x \oplus H_A^*\rho_y \oplus H_A^*\rho_{x^2}.$$

En appliquant les décompositions $\mathcal{R} \oplus E_n = V_n$ pour $n = 3$ et $n = 4$, en posant $s = -\phi_{\mathcal{R}}(x)$ et $t = -\phi_{\mathcal{R}}(y)$, on obtient les équations

$$\rho_y = (\tau + \alpha\tau^0)\rho_x + s\tau + A_0\tau^0 \tag{3.6.1}$$

et

$$\rho_{x^2} = (\tau + \beta\tau^0)\rho_y + t\tau + B_0\tau^0 + B_1\rho_x, \tag{3.6.2}$$

$\alpha, \beta, A_0, B_0, B_1 \in B$. De la formule (3.6.1) on tire

$$\alpha x + A_0 = y. \tag{3.6.3}$$

Nous pouvons également utiliser la formule (3.6.1) pour reécrire la formule (3.6.2) comme suit

$$\left(\rho_x - \left((\tau + \beta\tau^0)(\tau + \alpha\tau^0) + B_1\tau^0\right)\right)\rho_x = \left(s^q\tau^2 + (\beta s + A_0^q + t)\tau + (\beta A_0 + B_0)\tau^0\right)$$

Puisque $\rho_x(\tau)$ est unitaire de degré 2 on déduit

$$s^q\rho_x(\tau) = \left(s^q\tau^2 + (\beta s + A_0^q + t)\tau + (\beta A_0 + B_0)\tau^0\right)$$

$$\rho_x(\tau) = (\tau + \beta\tau^0)(\tau + \alpha\tau^0) + (B_1 + s^q)\tau^0 = \tau^2 + (\alpha^q + \beta)\tau + (\alpha\beta + B_1 + s^q)\tau^0$$

$$s^q a = \beta s + A_0^q + t. \tag{3.6.4}$$

$$a = \alpha^q + \beta. \tag{3.6.5}$$

Supposons maintenent que $\Phi_{\mathcal{R}}$ est non injective. Alors $\ker(\Phi_{\mathcal{R}}) = \ker(\phi_{\mathcal{R}})$ est un idéal non nul de A, donc $A/\ker(\phi_{\mathcal{R}})$ est corps fini. Puisque $\ker(\phi_{\mathcal{R}}) \neq A$ alors le quotient $A/\ker(\phi_{\mathcal{R}})$ est isomorphe à un sous-corps fini de H_A^*. Or $\mathbb{F}_q$ est le corps des constantes de H_A^*, donc nécessairement on a $s, t \in \mathbb{F}_q$. Ainsi, on tire de la formule (3.6.5) et de la formule (3.6.4) la relation

$$s\alpha^q = A_0^q + t$$

En utilisant la formule (3.6.3) on obtient la relation $s\alpha^q = (y - \alpha x)^q + t$ qu'on peut l'écrire sous la forme $(s\alpha - t)^q = (y - \alpha x)^q$, par conséquent on a

$$\alpha(s + x) = y + t$$

Cela implique que $\alpha \in B \cap k = A$. De plus, on a $v_\infty(\alpha) = v_\infty(y + t/x + s) = -1$, ce qui est absurde. □

Bibliographie

[1] n.H.Abel. *Oeuvres Complètes.*Tome 2, Grondahl, Son, Christiania, 1881.

[2] Abhyankar S S and Sundaram G S. *Galois theory of Moore-Carlitz-Drinfeld modules*. C. R. Acad. Sci. Paris 325. I Math. 325 (1997), no. 4, 349-353.

[3] Breuer, Florian *Explicit Drinfeld moduli schemes and Abhyankar's generalized iteration conjecture*. J. Number Theory 160 (2016), 432-450.

[4] Broche, Osnel ; del Río, Ángel, *Polynomials defining many units*. Math. Z. 283 (2016), no. 3-4, 1195-1200.

[5] Carlitz, Leonard, *A class of polynomials*. Trans. Amer. Math. Soc. 43 (1938), no. 2, 167-182.

[6] R. F. Coleman, *On the Galois groups of the exponential Taylor polynomials*. Enseign. Math. (2) 33 (1987), no. 3-4, 183-189.

[7] El Kati, Mohamed ; Oukhaba, Hassan, *Polynomials defining many units in function field*. Acta Arith. 190 (2019), no. 4, 351-361

[8] El Kati, Mohamed ; Oukhaba, Hassan, *Remarks on rank one Drinfeld modules and their torsion elements*. À paraître dans Functiones et Approximatio commentarii mathematici.

[9] El Kati, Mohamed ; Oukhaba, Hassan, *Laguerre type polynomials for rational function fields and applications*. À paraître dans Mediterranean journal of mathematics.

[10] Evertse, J.-H. ; Győry, K. ; Stewart, C. L. ; Tijdeman, R., *S-unit equations and their applications*. New advances in transcendence theory (Durham, 1986), 110-174, Cambridge Univ. Press, Cambridge, 1988.

[11] M. Filaseta, T.-Y. Lam, *On the irreducibility of the Generalized Laguerre polynomials*. Acta Arith. 105 (2002), no. 2, 177-182.

[12] M. Filaseta, R. L. Williams, Jr, *On the irreducibility of a certain class of Laguerre polynomials*. J. Number Theory 100 (2003), no. 2, 229-250.

[13] Goss, David, *Basic structures of function field arithmetic*. Springer-Verlag, Berlin, 1996. xiv+422 pp.

[14] R. Gow, *Some Generalized Laguerre polynomials whose Galois groups are the Alternating groups*. J. Number Theory 31 (1989), no. 2, 201-207.

[15] F. Q. Gouvêa, *p-adic numbers. Second edition*. Springer, Berlin, 1997.

[16] Hayes, David R., *Explicit class field theory for rational function fields*. Trans. Amer. Math. Soc. 189 (1974), 77-91.

[17] Hayes, David R., *Explicit class field theory in global function fields*. G.C. Rota (ed.), Studies in Algebra and Number Theory. New York : (Academic Press) (1979) 173-217.

[18] Hayes, David R, *Stickelberger elements in function fields*. Compositio Math. 55 (1985), no. 2, 209-239.

[19] F. Hajir, *Some A_n-extensions obtained from Generalized Laguerre polynomials*. J. Number Theory 50 (1995), no. 2, 206-212.

[20] F. Hajir, *Algebraic properties of a family of Generalized Laguerre Polynomials*. Preprint, 2004, 19pp.

[21] F. Hajir, S. Wong, *Specializations of one-parameter families of polynomials*. Ann. Inst. Fourier (Grenoble), to appear, 26pp.

[22] F. Hajir, S. Wong, *On the Galois group of generalized Laguerre polynomials*. Journal de Théorie des Nombresde Bordeaux 17 (2005).517-525.

[23] E. Laguerre, *Sur l'intègrale* $\displaystyle\int_0^{+\infty} \frac{e^{-x}dx}{x}$. Bull. Soc. math. France 7 (1879) 72Ű81. Reprinted in Oeuvres, Vol. 1. New York : Chelsea, 428-437, 1971.

[24] Jacobson, Nathan, *The Theory of Rings*. American Mathematical Society Mathematical Surveys, vol. II. American Mathematical Society, New York, 1943.

[25] G. Pólya, G. Szegő, *Problems and theorems in analysis*. Vol. II. Revised and enlarged translation by C. E. Billigheimer of the fourth German edition, Springer Study Edition, Springer, New York, 1976.

[26] Rosen, Michael, *Number theory in function fields*. Graduate Texts in Mathematics, 210. Springer-Verlag, New York, 2002

[27] Stichtenoth, H., *Algebraic function fields and codes*, Graduate Texts in Mathematics 254,© Springer-Verlag Berlin Heidelberg 2009.

[28] Harbater, David *Mock covers and Galois extensions*. J. Algebra 91 (1984), no. 2, 281-293.

[29] Iwasawa, Kenkichi *Local class field theory*. Oxford Science Publications. Oxford Mathematical Monographs. The Clarendon Press, Oxford University Press, New York, 1986. viii+155 pp. ISBN : 0-19-504030-9

[30] Malle, Gunter ; Matzat, B. Heinrich Inverse *Galois theory*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 1999. xvi+436 pp. ISBN : 3-540-62890-8

[31] Moore, Eliakim Hastings *A two-fold generalization of Fermat's theorem*. Bull. Amer. Math. Soc. 2 (1896), no. 7, 189-199.

[32] Ore, Oystein *On a special class of polynomials*. Trans. Amer. Math. Soc. 35 (1933), no. 3, 559-584.

[33] Oukhaba, Hassan *On local fields generated by division values of formal Drinfeld modules*. Glasg. Math. J. 62 (2020), no. 2, 459-472.

[34] Schur. I. *Gleichungen Ohne Affekt (1930)*. In : Gesammelte Abhandlungen. Band III, Springer-Verlag, Berlin, 1973, pp. 191-197.

[35] Zbigniew Marciniak and Sudarshan K. Sehgal *Generic units in abelian group rings*. In : J. Group Theory 8 (2005), 777-799