Modules de Drinfeld de rang 2 sur un corps Fini

Mohamed Saadbouh Mohamed Ahmed

Table des matières

0.1 Introduction 4
0.2 Notations 15

1 Courbes Elliptiques et Notions Générales 16
1.1 Courbes Elliptiques 16
1.1.1 Anneau d'Endomorphismes 18
1.1.2 Classes d'isogénies 19
1.1.3 Structure de $E(\mathsf{F}_q)$ 20
1.1.4 Théorème de Deuring 22
1.1.5 Statistique sur la Cyclicité de Courbes Elliptiques sur les corps finis 23
1.2 Extensions 25
1.3 Ordres 27
1.4 L'anneau des Polynômes d'Ore 28
1.5 Algèbres centrales simples 31

2 Sur l'analogie entre les modules de Drinfeld et les courbes elliptiques 33
2.1 Introduction 34
2.2 Modules de Drinfeld 37
2.2.1 La hauteur et le rang de A-module Φ 40
2.2.2 Morphismes des modules de Drinfeld 42
2.2.3 Norme d'isogènie 45
2.3 Modules de Drinfeld sur un corps fini 46
2.4 Modules de Drinfeld de rang 2 53
2.4.1 Anneaux d'endomorphismes 53
2.4.2 Classes d'isogénies 56
2.4.3 Structure de A-module L^{Φ} 66

3 Statistique sur la Cyclicité de Modules de Drinfeld de Rang 2 sur les Corps Finis **71**

3.1 Préliminaires : 73

3.2 Statistique sur la cyclicité de A-module 74
3.3 Le cas : $d = m = 1$ 80
3.4 Le cas : $m = 1$ et $d = 2$ 83
3.5 Le cas : $m = 2$ et $d = 1$ 85
3.6 $\lim_{q\to\infty} C_0(d, m, q)$ et $\lim_{q\to\infty} C(d, m, q)$ pour $m.d \leq 2$ 87

Bibliographie **89**

Remerciements

Je tiens à remercier le professeur Serge VLADUT, mon directeur de thèse, pour sa patience et son aide régulière et constante qui furent nécessaires pour accomplir ce travail, je lui exprime toute ma reconnaissance et ma gratitude.

Je remercie le professeur Bruno ANGLES et le professeur Alexei PANTCHICHKINE d'avoir accepter d'être les rapporteurs de ce travail.

Je tiens particulierement à remercier le professeur Gilles LACHAUD le directeur de l'IML qui fut mon directeur de DEA de m'avoir accueilli au sein de son équipe et d'avoir accepeter de faire partie du jury.

Je remercie Yves AUBRY, Bruno ANGLEZ et Stephen LOUBOUTIN, Francois Blanchard, Christian Mauduit, pour leur aide, écoute et sympathie, et un autre remerciement de plus à Yves d'avoir accepter de faire partie de ce Jury.

Je remercie tous les membres de l'équipe ATI, les Professeurs Robert ROLLAND, Michel LAURENT, et Francois RODIER. Et mes collègues : Redha, Ali, Alain, Frédérique, les Nicolas, Idriss et France BODIN, pour l'ambiance fraternelle et amicale.

En fin j'adresse un remerciement particulier à : Aurelia LOZINGOT, JEAN-BRUNO ERISMANN, Mohamed Fadel, Abdallah, Hamid Oughaddou et à Fabien PELLEGRINI.

0.1 Introduction

Dans [4], V.G. Drinfeld transpose aux corps de fonctions la théorie des représentations l-adique de dimension 2 de $\mathrm{Gal}(\bar{\mathsf{Q}}/\mathsf{Q})$ attachées aux formes modulaires holomorphes sur le demi plan de Poincaré. Autrement, il transpose cette théorie restreinte au cas des formes de poids 2 (dans ce cas, les représentations l-adiques sont construites à partir des points de division des jacobiennes de schémas de modules des courbes elliptiques).

Soit K un corps de fonctions d'une variable sur un corps fini, ∞ une place de K, et A l'anneau des éléments de K entiers sauf au plus en ∞. Le triple (K, ∞, A) est l'analogue de $(\mathsf{Q}, \infty, \mathsf{Z})$.

Une courbe elliptique sur un corps algébriquement clos k peut être définie comme une variété de dimension 1 sur k, munie d'une structure de $\mathsf{Z}-$module, et telle que pour n inversible dans k le noyau de la multiplication par n ait n^2 éléments. Par analogie un module de Drinfeld (module elliptique) de rang r sur un schéma S est un schéma en groupe G sur S, localement isomorphe à G_a et muni d'une structure de A-module telle que le noyau de la multiplication par a soit fini sur S, de degré $\mid A/a \mid^r$. L'action de A sur $\mathrm{Lie}(G)$ définit par $A \to \Theta_S : G$ fait de S un schéma sur $\mathrm{Spec}(A)$. On dispose d'une théorie des points de divisions (par un idéal ρ de A) parallèle à celle des courbes elliptiques, et pour $\rho \neq A$, il existe un schéma de modules de M_ρ pour les modules de Drinfeld de rang r munis d'une structure de niveau $\rho : G_\rho \to (\rho^{-1}/A)^r$.

Plus précisément on prend pour notre corps algébriquement clos k, $\bar{\mathsf{F}}_q$, qui est une clôture algébrique d'un corps fini F_q à $q = p^s$. Une courbe elliptique E sur F_q, est une courbe algébrique projective de genre 1. Par $E(\mathsf{F}_q)$, on note l'ensemble des points de E définis sur

F_q. Cet ensemble est un groupe abélien, avec O comme élément neutre. Un morphisme de courbes elliptiques sur F_q, est une application algébrique $f : E_1 \mapsto E_2$, définie sur F_q, qui respecte la loi de groupe, en particulier $f(O_1) = O_2$. Une isogénie est un morphisme non nul. Pour une courbe elliptique E l'ensemble des morphismes $f : E \mapsto E$ forment un anneau : l'anneau de F_q-endomorphismes de E, cet anneau sera noté $\mathrm{End}_{\mathsf{F}_q}(E)$, de même l'anneau de $\bar{\mathsf{F}}_q$-endomorphismes de E est noté $\mathrm{End}_{\bar{\mathsf{F}}_q}(E)$, dans le cas où l'anneau $\mathrm{End}_{\bar{\mathsf{F}}_q}(E)$ est non commutatif la courbe E est dite supersinguliere, autrement elle est ordinaire. D'après [10], [13], [14] et [16] :

Théorème 1 *Il existe deux possibilités pour l'anneau d'endomorphismes d'une courbe elliptique E sur un corps fini F_q :*

1. *$End_{\mathsf{F}_q}(E) = \mathsf{Z} + c.O_{\max}$, où $c \in \mathsf{Z}_{>0}$, p ne divise pas c, et $O_{\max}$ est l'ordre maximal dans un corps quadratique complexe qui est égal au corps des fractions de $End_{\mathsf{F}_q}(E)$ (c est appelé le conducteur de $End_{\mathsf{F}_q}(E)$);*
2. *$End_{\mathsf{F}_q}(E)$ est un ordre maximal dans l'algèbre de quaternion $\mathsf{Q}_{\infty,p}$.*

A.Weil a prouvé que deux courbes elliptiques E et E_1 sont isogénes si :

Théorème 2 *Deux courbes elliptiques E et E_1, sur F_q, sont isogénes, si et seulement si :*

$$\mid E(\mathsf{F}_q) \mid = \mid E_1(\mathsf{F}_q) \mid .$$

Le nombre $\mid E(\mathsf{F}_q) \mid$ pour une courbe elliptique E sur un corps fini F_q est donnée, d'après [10], [18] et [14], par :

Théorème 3 *Soit E une courbe elliptique sur F_q. Soient φ son endomorphisme de Frobenius dans $End_{\mathsf{F}_q}(E)$ et p la caractéristique de F_q :*

1. *L'endomorphisme φ satisfait une unique équation $\varphi^2 - c\varphi + q = 0$ dans $End_{\mathsf{F}_q}(E)$, où $c \in \mathsf{Z} \subset End_{\mathsf{F}_q}(E)$,*
2. *$\mid c \mid \leq 2\sqrt{q.}$*
3. *$\mid E(\mathsf{F}_q) \mid = q + 1 - c$,*
4. *$p \mid c$, si et seulement si, E est supersingulière.*

L'ensemble des classes d'isogénies d'une courbe elliptique E sur un corps fini F_q, est donné d'après [10], [13] et [14], par :

Théorème 4 *L'ensemble des classes d'isogénies de courbes elliptiques sur un corps fini F_q est en bijection naturelle avec l'ensemble des entiers c tel que $\mid c \mid \leq 2.\sqrt{q}$ et l'une de ces conditions :*

1. *$(c, q) = 1$;*
2. *q est un carré et $c = \pm 2\sqrt{q}$;*
3. *q est un carré, p n'est pas congru à $1 (\mathrm{mod}\, 3)$, et $c = \pm\sqrt{q}$;*
4. *q n'est pas un carré, $p = 2$ ou 3, et $c = \pm\sqrt{p.q}$;*
5. *q n'est pas un carré et $c = 0$; ou q est un carré , p n'est pas congru à $1 (\mathrm{mod}\, 4)$, et $c = 0$.*

Le cas 1 correspond au cas non supersingulier et les autres cas correspondent au cas supersingulier.

En fin la structure de groupe abélien $E(\mathsf{F}_q)$ est bien connu et d'après [10], [13], [14], [16], et [17] elle est de la forme :

Théorème 5 *Soit E une courbe elliptique sur un corps fini F_q d'ordre $N = q+1-c$, alors le groupe abélien $E(\mathsf{F}_q)$ occure comme l'une des structures suivantes :*

1. $E(\mathsf{F}_q) \simeq \mathsf{Z}/A \oplus \mathsf{Z}/B$, *si* $(c,q) = 1$ *et* $\mid c \mid \leq 2.\sqrt{q}$, $B \mid A$, $B \mid c-2$ *et* $A.B = N$,
2. q *est un carré et* $c = \pm 2\sqrt{q}$ *; et* $E(\mathsf{F}_q) \simeq (\mathsf{Z}/A)^2$, *ou* $A = \sqrt{q} \pm 1$;
3. q *est un carré,* p *n'est pas congru à* $1 (\mathrm{mod}\, 3)$, *et* $c = \pm\sqrt{q}$ *et* $E(F_q)$ *est cyclique ;*
4. q *n'est pas un carré,* $p = 2$ *ou* 3, *et* $c = \pm\sqrt{p.q}$; *et* $E(\mathsf{F}_q)$ *est cyclique ;*
   (a) q *n'est pas un carré et* p *n'est pas congru à* $3 (\mathrm{mod}\, 4)$ *; ou* q *est un carré et* p *n'est pas congru à* $1 (\mathrm{mod}\, 4)$, $c = 0$, *et* $E(\mathsf{F}_q)$ *est cyclique ;*
   (b) q *n'est pas un carré et* $p \equiv 3 (\mathrm{mod}\, 4)$ *;* $c = 0$, *et* $E(\mathsf{F}_q)$ *soit est cyclique soit* $E(\mathsf{F}_q) \simeq \mathsf{Z}/M\mathsf{Z} \oplus \mathsf{Z}/2\mathsf{Z}$, $M = \frac{q+1}{2}$.

Le cas 1 correspond à une courbe elliptique non supersingulière, et les autres correspondent au cas supersingulier.

Et enfin, et comme dernier point d'analogie, on se livre à une statistique concernant le rapport de courbes elliptiques pour lesquels la structure $E(\mathsf{F}_q)$ est cyclique sur le nombre des classes de F_q-endomorphismes de courbes elliptiques sur le corps fini F_q, un tel rapport dépendra de q et sera noté $c(q)$, et on a :

$$c(q) = \frac{\#\{E,\, E(\mathsf{F}_q) \text{ cyclique}\}}{\#\{E\}},$$

où $\#\{E\}$ est le nombre des classes de F_q-endomorphismes de courbes eliptiques sur le corps fini F_q, et on sait, d'après [18] :

Théorème 6 *$c(q) = 1$ si et seulement si $q = 2^l$ où $l \neq 2$ est un nombre premier (ou $l = 1$) et on a l'une de ces conditions :*

1) $q - 1$ est premier, $q \neq 4$ (le cas $q = 2$ est inclus, donc 1 est considéré premier) ;

2) $q - 1 = l_1 l_2$ tels que les premiers l_1 et l_2 sont pas des " petits " diviseurs de $q - 1$;

3) $q - 1 = l_1 l_2 l_3$ tels que les premiers l_1, l_2 et l_3 sont pas des " petits " diviseurs de $q - 1$.

Le cas $l_1 = l_2$ n'est pas exclu.

En général, le nombre $c(q)$ est donné, dans [18], par :

Théorème 7 *Soit $\varepsilon > 0$ on a :*

$$c(q) = \prod_l (1 - \frac{1}{l(l-1)}) + O(q^{-1/2+\varepsilon}),$$

où le produit est pris sur tous les diviseurs premiers de $q - 1$.

Les notions définies précédemment pour les courbes elliptiques sur les corps finis (anneaux d'endomorphismes $\mathrm{End}_{\mathsf{F}_q}(E)$, classes d'isogénies, et structure de groupe $E(\mathsf{F}_q)$ ainsi que le rapport $c(q)$) sont analogues à d'autres notions qu'on trouve pour les modules de Drinfeld, qu'on définissent ici rapidement : soit K un corps global de caractéristique p non nulle (c'est à dire un corps de fractions rationnelles d'une variables sur un corps fini) de corps des constantes le corps fini F_q. On fixe une place de K, notée ∞ et on appelle A l'anneau des éléments de K réguliers en dehors de la place ∞. Soit L un corps de caractéristique p. On note $L\{\tau\}$ l'anneau des polynômes d'Ore, c'est à dire l'anneau des polynômes en τ, le Frobenius F_q, muni de l'addition usuelle et dont le produit est donné par la règle : pour tout λ de L, $\tau\ \lambda = \lambda^q\ \tau$. Un A-module de Drinfeld est la donnée d'un homomorphisme d'anneaux $\Phi : A \to L\{\tau\}$ tel que pour tout élément a de A non inversible on ait :

$\deg_\tau \Phi_a > 0$. Soit $\gamma : A \to L$ l'application qui à un élément a de A associé le terme constant de Φ_a, c'est un homomorphisme d'anneaux et son noyau P s'appelle la A-caractéristique de L. Les propriétés d'un A-module de Drinfeld dépendra d'un entier r positif appelé le rang de A-module. On se limite pour prouver ces analogies au module de Drinfled de rang 2 . Cette thèse est composée de trois chapitres, dans le premier chapitre, on se contentera de donner des rappels concernants les courbes elliptiques, plus particulierement des rappels concernants les notions d'analogies avec les modules de Drinfeld, et nous finissons par des définitions de quelques notions générales, pour le deuxième chapitre on donne les analogies correspondantes aux notions précédemment données pour les courbes elliptiques selon l'ordre de présentation des résultats analogues pour les courbes elliptiques, on s'intéressera d'abord à l'anneau des endomorphismes, et on prouvera que, pour $A = \mathsf{F}_q[T]$:

Proposition 8 *Soit $\Delta = c^2 - 4\mu P^m$, le discriminant du P_F, le polynôme caractéristique de F, le Frobenius de corps fini L, qui est $P_F(X) = X^2 - cX + \mu P^m$, et soit $O_{K(F)}$ le A-ordre maximal de l'algèbre $K(F)$.*

1. *Pour tout $g \in A$ tel que $\Delta = g^2 .\omega$, il existe un A-module de Drinfeld Φ sur L de rang 2, ordinaire, tels que : $O_{K(F)} = A[\sqrt{\omega}]$ et :*

$$End_L\Phi = A + g.O_{K(F)}.$$

2. *Il n'existe pas des polynômes g de A tels que g^2 divise Δ, alors : il existe un A-module de Drinfeld Φ sur L de rang 2, ordinaire, tel que $End_L\Phi = O_{K(F)}$*

En suite, on définit la notion de classe d'isogénie d'un A-module de Drinfeld de rang 2, et on aboutira, d'après [12], à un analogue du Théorème 4, prouvant que :

Proposition 9 *L'injection :*

$$\{\textit{classes d'isogénies de } A\textit{-module de Drinfeld de rang 2 sur } L\} \hookrightarrow W_2,$$

est une bijection.

Où W_2 désigne l'ensemble des nombres de Weil de rang 2, qui sont des éléments $F \in \overline{K}$, intégraux sur A ; et tels que Il existe une unique place de $K(F)$ qui s'annule pour F, Il existe une unique place de $K(F)$ en dessous de la place ∞, et $\mid F \mid_\infty = \mid L \mid^{\frac{1}{2}}$, où $\mid \mid_\infty$est l'unique extension à $K(F)$ de la valuation : valeur absolue normalisée de K correspondante à ∞, et en fin $[K(F) : K] \mid 2$.

Puisque dans le cas de A-module de Drinfeld de rang 2, sur un corps fini L, le Frobenius F de L est un nombre de Weil de rang 2, et vu la correspondance entre ce Frobenius et son polynôme caractéristique P_Φ dans une classe d'isogénie, on a :

Proposition 10 $\#\{$*classes d'isogénies*$\} = \#\{P_\Phi\}$ *où* P_Φ *est le polynôme caractéristique de Frobenius* F *de* L.

Les polynômes caractéristiques d'un A-module de Drinfeld de rang 2, P_Φ, sont donnés dans [11], par :

Proposition 11 *Soit* Φ *un* A*-module de Drinfeld de rang* 2 *sur le corps fini* $L = \mathsf{F}_{q^n}$ *et soit* P *la caractéristique de* L. *On pose* $m = [L : A/P]$ *et* $d =$*deg* P. *Le polynôme caractéristique* P_Φ *est de la forme :*

1)$P_\Phi(X) = X^2 - cX + \mu P^m$, *où* $c^2 - 4\mu P^m$ *est imaginaire (c-a-d :* 2 *deg* $c <$ deg $P.m$ *ou* $2 \deg c =$*deg*$P.m$ *et* $X^2 - c_0 X + \mu$ *est irréductible sur* L *où* c_0 *est le coefficient de plus grande*

puissance de c), $c \in A$, $(c, P) = 1$ et $\mu \in \mathsf{F}_q^*$; si Φ est ordinaire et dans le cas supersingulier elle est l'une de trois cas suivants :

2)$P_\Phi(X) = X^2 + \mu P^m$, avec $\mu \in \mathsf{F}_q^*$, si m est impaire,

3) $P_\Phi(X) = X^2 + c_0 X + \mu P^m$, si m est paire et d est impaire, $\mu \in \mathsf{F}_q^*$ et $c_0 \in \mathsf{F}_q$.

4)$P_\Phi(X) = (X + \mu P^{\frac{m}{2}})^2$, si m est paire.

Le cas 1, correspond au cas ordinaire et les autres cas correspondent aux cas supersingulier. Donc le nombre des classes d'isogénie est donné par :

Proposition 12 *Soit Φ un A-module de Drinfeld de rang 2 sur le corps fini $L = F_{q^n}$ et soit P la A-caractéristique de L. On pose $m = [L : A/P]$ et $d =$deg P :*

1. *m est impaire et d est impaire :*

$$\#\{P_\Phi, \Phi : ordinaire(1)\} = (q-1)(q^{[\frac{m}{2}d]+1} - q^{[\frac{m-2}{2}d]+1} + 1).$$

2. *m est paire et d est impaire :*

$$\#\{P_\Phi\} = (q-1)[\frac{q-1}{2} q^{\frac{m}{2}d} - q^{\frac{m-2}{2}d+1} + q].$$

3. *m est paire et d est paire :*

$$\#\{P_\Phi\} = (q-1)[\frac{q-1}{2} q^{\frac{m}{2}d} - q^{\frac{m-2}{2}d} + 1].$$

On s'interéssera en suite à la structure de A-module induite par Φ sur L, selon le A-homomorphisme :

$$\begin{aligned} L \times A &\rightarrow L, \\ (l, a) &\rightarrow l.a := \Phi_a(l) \ . \end{aligned}$$

Ce A-module, noté L^{Φ}, est le parfait analogue, pour les courbes elliptiques à $E(\mathsf{F}_q)$, et on prouvera que, dans le cas ordinaire, elle est de la forme :

Proposition 13 *Le A-module L^{Φ} est de la forme $\frac{A}{I_1} \oplus \frac{A}{I_2}$, où $I_1 = (i_1)$ et $I_2 = (i_2)$ ($i_2 \mid i_1$) sont deux idéaux de A. Et si Φ est ordinaire, alors $i_2 \mid c - 2$, $c \in A$.*

On prouvera qu'inversement, chaque structure de la forme $\frac{A}{I_1} \oplus \frac{A}{I_2}$, tels que $i_2 \mid c-2$ et $i_2 \mid i_1$, est une structure de A-module de Drinfeld, et on prouvera le théorème suivant qui est le parfait analogue du théorème 5, dans son cas ordinaire :

Théorème 14 *Soient $M = \frac{A}{I_1} \oplus \frac{A}{I_2}$, $I_1 = (i_1)$ et $I_2 = (i_2)$, tels que : $i_2 \mid i_1$, $i_2 \mid (c-2)$. Alors il existe un A-module de Drinfeld Φ sur L de rang 2 ordinaire, tel que :*

$$L^{\Phi} \simeq M.$$

En fin, dans le troisième chapitre on s'intéressera à la statistique des A-modules de Drinfeld ordinaires dont les A-modules L^{Φ} sont cycliques, on note alors par $C(d, m, q)$ la proportion des A-modules de Drinfeld, ordinairs et de rang 2 (modulo isomorphisme) dont les structures des A-modules L^{Φ} sont cycliques, autrement dit :

si on note par $\#\{\Phi$, isomorphisme, ordinaire$\}$ le nombre des classes de L-isomorphismes des modules de Drinfeld de rang 2, ordinaires, on a :

$$C(d,m,q)=\frac{\#\{\Phi, L^{\Phi}\text{ cyclique}\}}{\#\{\Phi\text{, isomorphisme, ordinaire}\}},$$

et on note par $C_0(d,m,q)$ la proportion des A-modules de Drinfeld, ordinaires de rang 2 (modulo les classes d'isogénies) dont les A-modules L^{Φ} sont cycliques, autrement dit, si on note par $\#\{\Phi$, isogénie, ordinaire$\}$ le nombre de classes d'isogénie, des modules de Drinfeld de rang 2, ordinaires, on a :

$$C_0(d,m,q)=\frac{\#\{\text{Classe d'isogénie de }\Phi,\ L^{\Phi}\text{ cyclique}\}}{\#\{\Phi\text{, isogénie, ordinaire}\}}.$$

Bien sûre ce nombre dépendra de q et aussi de d,m.

Un de nos résultats dans ce chapitre consiste à dire que :

Proposition 15 *$C(d,m,q)=C_0(d,m,q)=1$, si et seulement si, $m=d=1$.*

Autrement dit, pour avoir un A-module cyclique il faut que l'extension L soit triviale, nous donnons aussi d'autres valeurs de $C(d,m,q)$ et $C_0(d,m,q)$ dans des cas précis selon la valeur de d et m, comme par exemple pour le cas :

Proposition 16 *On pose $d=2$ et $m=1$. Soit $H(O(D))$ le nombre des classes de Hurwitz pour un ordre O dont le déterminant imaginaire est D :*

$$C_0(2,1,q)=\frac{q(q-1)-5}{q(q-1)-2},$$

$$C(2,1,q)=\frac{q^3-q^2-q+1-[\frac{q-1}{2}\sum_{P_\Phi}\sum_{i_2,\, i_2^2\Vdash 4-4\mu P}H(O(\frac{4-4\mu P}{i_2^2})+(q-1)\sum_{P_\Phi}\sum_{i_2,\, i_2^2\Vdash c^2-4\mu P}H(O(\frac{c^2-4\mu P}{i_2^2})]}{q^3-q^2-q+1}.$$

Et nous laissons penser, en forme de conjecture, que pour q grand les valeurs $C(d, m, q)$ et $C_0(d, m, q)$ tendront vers 1.

0.2 Notations

F_q : désignera toujours un corps fini à $q = p^s$ éléments, p étant sa caractéristique.

K : corps global de caractéristique $p > 0$ contenant F_q, le corps fini F_q étant algébriquement fermé dans K (par exemple et c'est le cas que nous utilisons dans cette thèse, si T est un élément transcendant sur F_q, $K = \mathsf{F}_q(T)$).

∞ : une place fixée de K.

A : l'anneau des éléments de K réguliers en dehors de ∞, c'est un anneau de Dedekind et $K = \text{frac}\ (A)$. Le cas que nous considérons pour prouver nos résultats est le cas $K = \mathsf{F}_q(T)$, ∞ correspond à la valuation $\frac{1}{T}$-adique sur K, et $A = \mathsf{F}_q[T]$.

On désigne par v_∞ la valuation normalisée sur K correspondant à la place ∞.

Si H est un corps global de caractéristique $p > 0$, et si P est une place de H, on notera H_P le complété de H à la place P.

De même, si R est un anneau de Dedekind, et si Q est un premier non nul de R, on notera R_Q le complété Q-adique de R.

Le mot "corps" signifie corps commutatif.

Chapitre 1

Courbes Elliptiques et Notions Générales

Dans cet chapitre, on rappelle quelques propriétés basiques des courbes elliptiques sur les corps finis, pour preuve et plus de détails voir [13], [14] et [17].

1.1 Courbes Elliptiques

Définition 17 *Soit* F_q *un corps fini à* q *éléments. Une courbe elliptique* E *sur* F_q *est une courbe algébrique projective, non singuliére de genre* 1, *définie sur* F_q, *munie d'un point* O *de* E, *défini sur* F_q.

Soit $\bar{\mathsf{F}}_q$ une clôture algébrique de F_q. Par $E(\bar{\mathsf{F}}_q)$, on note l'ensemble des points de E définis sur $\bar{\mathsf{F}}_q$. Cet ensemble est un groupe abélien, avec O comme élément neutre.

L'ensemble $E(\mathsf{F}_q)$ des points de E qui sont définis sur F_q, est un sous-groupe de $E(\bar{\mathsf{F}}_q)$. On note par $\mid E(\mathsf{F}_q) \mid$ le cardinal de l'ensemble $E(\mathsf{F}_q)$.

Définition 18 *Un morphisme de courbes elliptiques sur F_q, est une application algébrique $f : E_1 \mapsto E_2$, définie sur F_q, qui respecte la loi de groupe, en particulier $f(O_1) = O_2$. Un isomorphisme est un morphisme inversible. Une isogénie est un morphisme non nul. Pour une courbe elliptique E l'ensemble de morphisme $f : E \mapsto E$ forme un anneau : l'anneau de F_q-endomorphismes de E, cet anneau sera noté $End_{\mathsf{F}_q}(E)$.*

Définition 19 *On dit que E et E_1 sont isogénes s'il existe une isogénie entre E et E_1.*

Théorème 20 *Deux courbes elliptiques E et $\bar{E}$ sont isogénes, si et seulement, si :*

$$\mid E(\mathsf{F}_q) \mid = \mid \bar{E}(\mathsf{F}_q) \mid .$$

Définition 21 *Un ordre quadratique complexe O est un sous anneau, d'indice fini, de l'anneau des entiers d'un corps des nombres quadratique complexe .*

Soit K un corps de nombres quadratique complexe. Par $O_{\max}$ on note l'anneau des entiers de K. Pour chaque $k \in \mathsf{Z}_{>0}$, l'anneau $O_{\max}$ a précisément un sous anneau O d'index k. Le discriminant de cet ordre est $\Delta(O_{\max})k^2$. Ce qui implique que les ordres quadratiques complexes sont caractérisés par leur discriminant. Par $O(\Delta)$ on note l'ordre quadratique complexe de discriminant Δ.

Lemme 22 *Si α est un nombre algébrique, pour lequel $O = \mathsf{Z}[\alpha]$ est un ordre quadratique complexe, alors $\Delta(O)$ est égal au discriminant de polynôme minimal de α.*

Définition 23 *Soit $p = char(\mathsf{F}_q)$. On note par $\mathsf{Q}_{\infty,p}$ l'unique algèbre de Quaternion sur Q ramifiée seulement sur p et ∞.*

Proposition 24 *Les ordres maximaux dans cette algèbre sont des anneaux non commutatifs de rang 4 sur Z.*

Soit E une courbe elliptique sur F_q, les anneaux $\mathrm{End}_{\mathsf{F}_q}(E)$ et $\mathrm{End}_{\bar{\mathsf{F}}_q}(E)$ sont soit des ordres quadratiques complexes ou des ordres maximaux dans $\mathsf{Q}_{\infty,p}$.

Remarque 25 *Il peut arriver que $End_{\mathsf{F}_q}(E)$ soit quadratique complexe et $End_{\bar{F}_q}(E)$ ne le soit pas.*

Définition 26 *On définit la norme et la trace sur $End_{\bar{F}_q}(E)$ par : soit $\alpha \in \mathsf{Z}$ ou $\mathsf{Z}[\alpha]$ est un ordre quadratique complexe, on injecte $\mathsf{Z}[\alpha]$ dans C et on pose $T(\alpha) = \alpha + \bar{\alpha}$, $N(\alpha) = \alpha\bar{\alpha}$ qui sont deux éléments de Z.*

Définition 27 *Une courbe elliptique E sur F_q est dite supersinguliére si $End_{\bar{\mathsf{F}}_q}(E)$ est non commutatif.*

On peut remarquer que la super singularité des courbes elliptiques dépend seulement de E sur $\bar{\mathsf{F}}_q$.

1.1.1 Anneau d'Endomorphismes

Pour l'anneau d'endomorphismes on peut le caractériser par le théorème suivant :

Théorème 28 *Il existe deux possibilités pour l'anneau d'endomorphismes d'une courbe elliptique :*

1. $End_{\mathsf{F}_q}(E) = \mathsf{Z} + c.O_{\max}$, *où* $c \in \mathsf{Z}$, *p ne divisant pas* $c, O_{\max}$ *est l'ordre maximal dans un corps quadratique complexe qui est égal au corps des fractions de* $End_{\mathsf{F}_q}(E)$*(c est appelé le conducteur de* $End_{\mathsf{F}_q}(E)$*)*;
2. $End_{\mathsf{F}_q}(E)$ *est un ordre maximal dans l'algèbre de quaternion* $\mathsf{Q}_{\infty,p}$.

Le cas 2 correspond au cas supersingulier.

1.1.2 Classes d'isogénies

Le calcul du nombre de classes d'isogénies peut découler du théorème suivant :

Théorème 29 *L'ensemble de classes d'isogénies de courbes elliptiques sur un corps fini* F_q *est en bijection naturelle avec l'ensemble des entiers c tel que* $\mid c \mid \leq 2.\sqrt{q}$ *et l'une de ces conditions :*

1. $(c, q) = 1$;
2. q *est un carré et* $c = \pm 2\sqrt{q}$;
3. q *est un carré,* p *n'est pas congru à* $1 (\mathrm{mod}\, 3)$, *et* $c = \pm\sqrt{q}$;
4. q *n'est pas un carré ,* $p = 2$ *ou* 3, *et* $c = \pm\sqrt{p.q}$;
5. q *n'est pas un carré et* $c = 0$ *; ou* q *est un carré,* p *n'est pas congru à* $1 (\mathrm{mod}\, 4)$, *et* $c = 0$.

1.1.3 Structure de $E(\mathsf{F}_q)$

On commence par décrire la structure de $E(\bar{\mathsf{F}}_q)$ comme un groupe abélien :

Définition 30 *Soit A un groupe abélien et soit $n \in \mathsf{Z}$ on note par $A[n]$ le sous-groupe de torsion : $A[n] = \{a \in A : n.a = 0\}$.*

Proposition 31 *Soit F_q un corps fini de caractéristique p, et soit E une courbe elliptique sur F_q :*

1. *Le groupe $E(\bar{\mathsf{F}}_q)$ est un groupe de torsion,*
2. *Si p ne divise pas n, alors $E(\bar{\mathsf{F}}_q)[n] = \mathsf{Z}/n\mathsf{Z} \oplus \mathsf{Z}/n\mathsf{Z}$ est un groupe abélien,*
3. *Si n est une puissance de p on a : $E(\bar{\mathsf{F}}_q)[n] = 0$ si E est supersingulière et $\mathsf{Z}/n\mathsf{Z}$ autrement.*

Définition 32 *Soit E une courbe elliptique sur F_q. L'endomorphisme de Frobenius $\varphi \in End_{\mathsf{F}_q}(E)$ est l'endomorphisme de E qui agit sur $E(\mathsf{F}_q)$ en élevant les composantes d'un point à la puissance q : $\varphi(x : y : z) = (x^q : y^q : z^q)$.*

Théorème 33 *Soit E une courbe elliptique sur F_q. Soient φ son endomorphisme de Frobenius dans $End_{\mathsf{F}_q}(E)$ et p la caractéristique de F_q :*

1. *L'endomorphisme φ satisfait une unique équation $\varphi^2 - c\varphi + q = 0$ dans $End_{\mathsf{F}_q}(E)$, où $c \in \mathsf{Z} \subset End_{\mathsf{F}_q}(E)$,*
2. *$\mid c \mid \leq 2\sqrt{q.}$*
3. *$\#E(\mathsf{F}_q) = N(\varphi - 1) = q + 1 - c$,*

4. $p \mid c$, si et seulement si, E est supersingulière.

Remarque 34

1) L'endomorphisme $\varphi - 1 \in \mathrm{End}_{\mathsf{F}_q}(E)$ et $\mathrm{Ker}(\varphi - 1)(E(\mathsf{F}_q))$ est exactement $E(\mathsf{F}_q)$.

2) L'entier c est la trace de φ ($c = \mathrm{Tr}(\varphi)$).

On est alors en mesure de donner les conditions nécessaires et suffisantes pour la non cyclicité de la structure de $E(\mathsf{F}_q)$ il suffit pour cela de donner les conditions pour qu'on puisse injecter un ordre non cyclique dans cette structure, nous annonçons le résultat suivant :

Proposition 35 *Soit E une courbe elliptique sur un corps fini F_q. Soient p la caractéristique de F_q ; $n \in \mathsf{Z}_{>1}$ où p - n et c la trace de l'endomorphisme de Frobenius φ de E. Les assertions suivantes sont équivalentes :*

1. $E(\bar{\mathsf{F}}_q)[n] \subset E(\mathsf{F}_q)$;

2. $n^2 \mid q + 1 - c$, $n \mid q - 1$ et soit $\varphi \in \mathsf{Z}$ ou $O(\frac{c^2-4q}{n^2}) \subset End_{\mathsf{F}_q}(E)$.

Maintenant on est en mesure de donner la structure ou les structures possibles pour $E(\mathsf{F}_q)$:

Théorème 36 *Soit E une courbe elliptique ordinaire sur un corps fini F_q d'ordre $N = q + 1 - c$, alors le groupe abélien $E(\mathsf{F}_q)$ occure comme l'une des structures suivantes :*

1. $E(\mathsf{F}_q) \simeq \mathsf{Z}/A \oplus \mathsf{Z}/B$, si $(c, q) = 1$ et $\mid c \mid \leq 2.\sqrt{q}$ et $B \mid A$, $B \mid c - 2$ et $A.B = N$,

2. q est un carré et $c = \pm 2\sqrt{q}$; et $E(\mathsf{F}_q) \simeq (\mathsf{Z}/A)^2$, ou $A = \sqrt{q} \pm 1$;

3. q est un carré, p n'est pas congru à $1(\mathrm{mod}\,3)$, et $c = \pm\sqrt{q}$ et $E(F_q)$ est cyclique ;

4. q n'est pas un carré, $p = 2$ ou 3, et $c = \pm\sqrt{p.q}$; et $E(\mathsf{F}_q)$ est cyclique ;

(a) q n'est pas un carré et p n'est pas congru à $3(\mathrm{mod}\,4)$; où q est un carré et p n'est pas congru à $1(\mathrm{mod}\,4)$, $c = 0$, et $E(\mathsf{F}_q)$ est cyclique ;

(b) q n'est pas un carré et $p \equiv 3(\mathrm{mod}\,4)$; $c = 0$, et $E(\mathsf{F}_q)$ ou cyclique ou égal à $\mathsf{Z}/M\mathsf{Z} \oplus \mathsf{Z}/2\mathsf{Z}$, $M = \frac{q+1}{2}$.

Le cas 1 correspond au cas ordinaire et les autres au cas supersingulier.

1.1.4 Théorème de Deuring

Le théorème suivant, prouvé par Max-Deuring dans [13] et [17] est utilisé pour la démonstration de l'analogue de notre résultat principal qui est le théorème précédent dans le cas ordinaire :

Théorème 37 *Soit E_0 une courbe elliptique sur un corps fini de caractéristique p, avec un endomorphisme F_0 non trivial. Alors il existe une courbe elliptique E définie sur un corps des nombres, et il existe un endomorphisme F de E tels que E_0 est isomorphe à $\overline{E}$ et F_0 correspond à F sous cette isomorphisme.*

Du théorème précédent, on peut déduire le théorème suivant :

Théorème 38 *Soient $N \in \mathsf{N}$, $M = \begin{pmatrix} a & b \\ a_1 & b_1 \end{pmatrix} \in \mathsf{M}_2(\mathsf{Z}/N\mathsf{Z})$ et F_q un corps fini à q éléments, on suppose :*

1. $(det\ M) = q(\mathrm{mod}\, N)$;

2. $\mid a + b_1 \mid \leq 2.\sqrt{q}$.

Il existe alors un Endomorphisme de Frobenius F qui vérifie : $F^2 - cF + q = 0$ (mod N), tel que $c = a + b_1$ et dont la matrice $M_F \in \mathsf{M}_2(\mathsf{Z}/N\mathsf{Z})$ est exactement M.

Ce théorème est utlisé pour prouver le théorème suivant :

Théorème 39 *Soient* $M = \begin{pmatrix} c-1 & -A \\ B & 1 \end{pmatrix} \in \mathsf{M}_2(\mathsf{Z}/N\mathsf{Z})$ *et* F_q *un corps fini à q éléments, tel que :* $\mid c \mid \leq 2.\sqrt{q}$, $B \mid A$, $B \mid c-2$ *et* $A.B = N = q + 1 - c$, *on suppose :* $(c, q) = 1$. *Il existe alors, une courbe elliptique E sur F_q, ordinaire, tel que :*

$$E(\mathsf{F}_q) \simeq \mathsf{Z}/A \oplus \mathsf{Z}/B.$$

1.1.5 Statistique sur la Cyclicité de Courbes Elliptiques sur les corps finis

Soient F_q un corps fini à q éléments, E une courbe elliptique sur F_q. Par $E(\mathsf{F}_q)$, on note l'ensemble des points de E définis sur F_q. Cet ensemble est un groupe abélien.

Le rapport de la cyclicité du groupe abélien $E(\mathsf{F}_q)$, noté $c(q)$ vu sa dépendance de q est :

$$c(q) = \frac{\#\{E,\ E(\mathsf{F}_q) \text{ cyclique}\}}{\#\{E\}},$$

où $\#\{E\}$ est le nombre des classes de F_q-endomorphismes de courbes eliptiques sur le corps fini F_q.

Serge Vladut dans [18] a prouvé qu'un cas important, concernant la cyclicité de $E(\mathsf{F}_q)$, consiste à savoir pour quelle q, le nombre $c(q)$ est égal à 1, et on a :

Théorème 40 *$c(q) = 1$ si et seulement si $q = 2^l$ où $l \neq 2$ est un nombre premier (ou $l = 1$) et on a l'une de ces conditions :*

1. $q-1$ est premier, $q \neq 4$ (le cas $q = 2$ est inclus et 1 est considéré premier) ;
2. $q - 1 = l_1 l_2$ tels que les premiers $l_1$et l_2 sont pas des " petits " diviseurs de $q - 1$;
3. $q-1 = l_1 l_2 l_3$ tels que les premiers l_1, l_2 et l_3 sont pas des " petits " diviseurs de $q-1$.

Le cas $c(q) = 1$ est intéressant pour beaucoup des applications, voir [18].

Et généralement le nombre $c(q)$ est donné, dans [18], par :

Théorème 41 *Soit $\varepsilon > 0$ on a :*

$$c(q) = \prod_l (1 - \frac{1}{l(l-1)}) + O(q^{-1/2+\varepsilon}),$$

où le produit est pris sur tous les diviseurs premiers de $q - 1$.

1.2 Extensions

Dans tout ce paragraphe, on se donne un corps K et une extension de degré fini L de K ; son degré $[L : K]$ sera noté n.

Soit A un anneau noethérien et intégralement clos, de corps des fractions K. On note B la fermeture intégrale de A dans L (c'est à dire l'ensemble des éléments de L qui sont entiers sur A). On a : $K.B = L$, et le corps des fractions de B est L. On suppose que l'anneau B est un A-module de type fini, donc B est un anneau nothérien intégralement clos.

Proposition 42 *Si A est Dedekind, B est de Dedekind.*

On sait que B est nothérien intégralement clos. Il nous suffit donc de montrer que B est de dimension ≤ 1.

Soit $\beta_0 \subset \beta_1 \subset \beta_2$ une chaîne d'idéaux premiers distincts de B.

Le lemme suivant montre que les β_i sont distincts (ce qui contredit le fait que A de dimension ≤ 1) :

Lemme 43 *Soient A et B deux anneaux, avec $A \subset B$, et B entier sur A. Si $\beta \subset O$ sont deux idéaux premiers de B tels que $\beta \cap A = O \cap A$, on a $\beta = O$.*

Soit β un idéal premier non nul de B, et si $\rho = \beta \cap A$, on dira que β divise ρ (ou que β est au dessus de ρ) et on écrira $\beta \ / \ \rho$.

Cette relation équivaut aussi à dire que β contient l'idéal $\rho\ B$ de B engendré par ρ. On notera e_β l'exposant de β dans la décomposition en idéaux premiers de $\rho\ B$. On a donc :

$e_\beta = v_\beta(\rho B), \rho B = \pi_{\beta/\rho}\ \beta^{e_\beta}$.

L'entier e_β est appelé l'indice de ramification de β dans l'extension L/K.

D'autre part, si β divise ρ, le corps $B/\ \beta$ est une extension du corps A/ρ. Comme B est de type fini sur $A, B/\ \beta$ est une extension de degré fini de A/ρ. Le degré de cette extension est appelé résiduel de β dans l'extension L/K, noté f_β.

Lorsqu'il y a un seul idéal premier de β qui divise ρ, et que $f_\beta = 1$, on dit que L/K est totalement ramifiée en ρ .

Lorsque $e_\beta = 1$ et que $B/\ \beta$ est séparable sur A/ρ, on dit que L/K est non ramifiée en β. Si L/K est non ramifiée pour tous les idéaux premiers β divisant ρ, on dit que L/K est non ramifiée au dessus de ρ (ou en ρ).

Lemme 44 *Soit L une extension finie d'un corps complet K par une valuation v et soit K' la clôture algébrique de K. Donc on peut prolonger v à une valuation v' sur K'.*

On note par O_K l'anneau de valuation de la valuation v et par P_K l'idéal maximal de O_K.

Soit $\overline{O_K} = O_K/\ P_K$ le corps résiduel, et soit $f(T) \in O_{K[T]}$. On suppose que dans $\overline{O}_{K[T]}$ il y'a la factorisation $\overline{f(T)} = u(T)w(T)$, où $u(T)$ est monique et $u(T)$, $w(T)$ relativement premiers. Donc il existe une factorisation dans $O_{K[T]}$: $f(T) = g(T)h(T)$, telle que g est monique et $\overline{g} = u, \overline{h} = w$.

Puisque L est une extension non ramifiée de K si $e(L/K) = 1$ et $\overline{O}_L$ est une extension séparable de O_K. Alors : l'étude des extensions non ramifiées se réduit à l'étude des extensions séparables de corps résiduels :

1. Soit L une extension non ramifiée de K. Il existe une bijection entre l'ensemble des

corps L tel que $K \subset L \subset K\prime$ et l'ensemble des corps G , fini et séparable sur $\overline{O}_K$. Cette correspondance attribue à chaque corps L le corps G donné par $G = \overline{O}_L$.

2. Si $L = K(a)$, où a est une racine d'un polynôme monique $f(T) \in O_{K[T]}$ telle que $\overline{a}$ est une racine simple de $\overline{f}(T)$, donc L est non ramifiée sur K, et $O_L = O_{K[a]}$, $O_L = \overline{O}_K(\overline{a})$, $(L : K) = (\overline{O}_L : \overline{O}_K)$. Inversement, chaque extension non ramifiée L de K est de cette forme.

1.3 Ordres

Soit A un domaine intégral noethérien, et soit V un espace vectoriel sur un corps K. Un A-réseau dans V est un A-sous-module fini M dans V tel que $K.M = V$, où

$$K.M = \{\sum \alpha_i m_i \text{ (somme fini)} : \alpha_i \in K,\, m_i \in M\}.$$

Définition 45 *Un A-ordre dans une K-algèbre R est un sous anneau N de R, qui a le même élément unité que R et tel que N est un A-réseau dans R.*

1) Soit A un anneau de Dedekind et soit L une extension séparable finie de K. On note par S la clôture intégrale de A dans L. Alors : S est un A-ordre dans L.

2) Soit $R = M_r(K)$ l'algèbre des matrices $r \times r$ sur K. On pose $\Lambda = M_r(R)$, alors Λ est un A-ordre dans R.

3) Soit $a \in R$ un élément intégral sur A, qui est racine d'un polynôme monique sur A. Alors l'anneau $A[a]$ est un A-ordre dans la K-algèbre $K[a]$.

Théorème 46 *Chaque A-ordre dans R est contenu dans un A-ordre maximal dans R.*

1.4 L'anneau des Polynômes d'Ore

Définition 47 *Soit L une extension finie d'un corps fini F_q, et soit τ le Frobenius de F_q, alors l'anneau des polynômes en τ de coefficients dans L, noté $L\{\tau\}$, est un anneau non commutatif sous la composition.*

Soit $\{f(\tau), g(\tau)\} \subset L\{\tau\}$. On remarque que $f(\tau).g(\tau) = 0$ implique que $f(\tau)$ ou $g(\tau)$ est nulle. En particulier, la multiplication dans $L\{\tau\}$ a les propriétés suivantes :

si $f(\tau)g(\tau) = f(\tau)h(\tau)$, alors $g(\tau) = h(\tau)$ et aussi si $g(\tau)f(\tau) = h(\tau)f(\tau)$, alors $g(\tau) = h(\tau)$.

Définition 48 *1-On dit que $f(\tau)$ est divisible à droite par $g(\tau)$ s'il existe $h(\tau) \in L\{\tau\}$ tel que :*

$$f(\tau) = h(\tau).g(\tau).$$

2- On dit que $f(\tau)$ est divisible à gauche par $g(\tau)$ s' il existe $m(\tau) \in L\{\tau\}$ tel que :

$$f(\tau = g(\tau).m(\tau).$$

Proposition 49 *Soient $\{f(\tau), g(\tau)\} \subset L\{\tau\}$ avec $g(\tau) \neq 0$. Alors ils existent $\{h(\tau), r(\tau)\} \subset L\{\tau\}$, avec deg $r(\tau) <$ deg $g(\tau)$, tel que :*

$$f(\tau) = h(\tau)g(\tau) + r(\tau).$$

En plus, $h(\tau)$ et $r(\tau)$ sont uniques.

Corollaire 50 *Chaque idéal gauche de $L\{\tau\}$ est principal.*

Définition 51 *On dit que L est parfait si et seulement si $\tau(L) = L$.*

Proposition 52 *Soit L un corps parfait, et soient $\{f(\tau), g(\tau)\} \subset L\{\tau\}$ avec $g(\tau) \neq 0$. Alors ils existent $\{h(\tau), r(\tau)\} \subset L\{\tau\}$, avec*

$\deg r(\tau) < \deg g(\tau)$, tel que : $f(\tau) = g(\tau).\ h(\tau) + r(\tau)$. En plus, $h(\tau)$ et $r(\tau)$ sont uniques.

Corollaire 53 *Si L est parfait, alors chaque idéal de $L\{\tau\}$ est principal.*

Exemple 54 *Soit $L = F_q(T)$. On pose $f(T) = \tau^2 - \tau$ et $g(T) = \tau - T\tau^0$. Alors*

$$\tau^2 - \tau = (\tau + (T^q - 1)\tau^0)(\tau - T\tau^0) + T(T^q - 1)\tau^0.$$

Puisque l'anneau de polynôme d'Ore $L\{\tau\}$ n'est pas un anneau commutatif, il n'est pas évident de le plonger dans un anneau de division des fractions, mais heureusement, l'anneau $L\{\tau\}$ vérifie une propriété importante, qui est :

Soit $f(\tau), g(\tau) \in L\{\tau\}$ deux éléments non nuls. On peut trouver le plus petit multiple commun droite $h(\tau)$ entre f et g. Et donc :

$$h(\tau) = a(\tau)f(\tau) = b(\tau)g(\tau) \text{ pour } a, b \in L\{\tau\}, \text{ non nuls.}$$

Et c'est exactement ce dont nous aurons besoin, d'après la condition d'Ore, nécessaire pour le passage aux anneaux de division des fractions pour les anneaux non commutatifs :

Définition 55 *Soit R un anneau unitaire, non commutatif. On dit que R satisfait la condition d'Ore gauche, si et seulement si, étant donné deux éléments non nuls $a, b \in R$, il existe deux éléments non nuls $a', b' \in R$, tel que $a'a = b'b$.*

Et puisque L est parfait, $L\{\tau\}$ satisfait la condition d'Ore droite et les deux anneaux des fractions gauche et droite sont donc isomorphes.

Soit $H = F_q((T))$ le corps des séries formelles de Laurent définies sur F_q avec l'anneau des entiers $O_L = F_q[[T]]$, et soit L une extension finie de F_q de degré n, et soit $O_D = L\{\tau\}$ l'anneau des séries non commutatives sur L (le variable est τ) avec la règle de commutativité $\tau\ a = a^q\ \tau$ pour $a \in L$. On injecte la F_q-algèbre O_L dans O_D par l'injection $T \hookrightarrow \tau^n$ qui identifie O_L avec le centre de O_D. Donc le produit tensorielle $D := O_D \otimes_{O_H} H$ est bien définie et il s'accorde avec le corps non commutatif de séries de Laurent $L((\tau))$ qui est central sur H.

On pose maintenant $H = F_q(T)$ le corps des fonctions rationnelles avec l'anneau des entiers $O_H = F_q[T]$. Soit $O_D = L\{\tau\}$ l'anneau des polynômes en τ.

L'application $T \hookrightarrow \tau^n$ identifie O_H avec le centre de O_D, et $D := O_D \otimes_{O_H} H$ est le corps non commutatif $L(\tau)$ de fonctions rationnelles en τ.

En prenant la complétion T-adique, c'est à dire en appliquant $\otimes_{OH}\hat{O}_H$, où

$$\hat{O}_H\ = Lim_r(O_H/T^r O_H) = F_q[[T]]),$$

on retourne à la situation de $H = F_q((T))$ vue précédemment.

Soit maintenant H local et D/H algèbre de division central de dimension n^2.

La valuation $v : H^* \mapsto \mathsf{Z}$, peut être prolongée à la valuation $v_D : D^* \to \frac{1}{n}\mathsf{Z}$.

L'anneau $O_D = \{x \in D\ /\ v_D(x) \geq 0\}$ est composé des éléments de D qui sont intégraux sur l'anneau des entiers O_H de H et on a $v_D(f) = \frac{1}{n}\ ord_\tau(f)$ pour $f \in O_D$.

1.5 Algèbres centrales simples

Pour preuve et plus des détails voir [3] :

Définition 56 *Soit M un anneau unitaire. M est simple, si et seulement si, M n'admet pas des idéaux triviaux non nuls.*

Le centre D de R, est défini par :

$$D = \{\alpha \in M \mid \alpha m = m\alpha, \forall m \in M\}.$$

Définition 57 *Soit M un anneau unitaire. Alors M est Artinien (à gauche) si et seulement si, chaque chaine décroissante d'idéaux (gauches) de M est stationnaire (à partir d'un certain rang).*

On note que D est un sous anneau commutatif de M. Le théorème suivant s'apelle le théorème de Wedderburn, voir [3] :

Théorème 58 *Soit M simple et Artinien. Alors M est isomorphe à l'anneau $\mathsf{M}_n(D)$ des matrices $n \times n$ sur l'anneau D.*

Définition 59 *Soit M un anneau et H un corps arbitraire. Donc M est une H-algèbre, si et seulement si, il existe un homomorphisme d'anneau de H vers D, le centre de M.*

L'exemple basique d'une H-algèbre est $\mathsf{M}_n(H)$, l'ensemble des matrices $n \times n$ sur H.

Définition 60 *On dit que la H-algèbre M est centrale simple sur H, si et seulement si, M est simple, et $D = H$ (donc M est centrale sur H).*

On appelle D le Noyau de Brauer de l'algèbre M, et on a :

Théorème 61 *Deux algèbres simples centrales M et M' sont équivalentes si leurs noyeau de Brauer D et D' sont isomorphes. L'ensemble $\{[M]\}$ des classes d'équivalences forment un groupe appelé le groupe de Brauer $Br(H)$ de H, par : $[M].[M'] = [M \otimes_H M']$.*

L'élément neutre de ce groupe est $[H]$, l'inverse de $[M]$ est la classe de l'algèbre opposée M^{op}.

Soit S une sous-algèbre simple de M. On défini le centralisateur de S, $C(S)$, par :

$$C(S) = \{m \in M \mid ms = sm, \forall s \in S\}.$$

Le centralisateur $C(S)$ est simple aussi, et on a :

$$(dim_H S)(dim_H C(S) = dim_H M$$

et,

$$C(C(S)) = S.$$

Proposition 62 *Soit R une algèbre simple centrale sur H. Donc $dim_H(A)$ est un carré, soit d^2. Si $R = D$ est un anneau de division, alors les sous corps maximaux de D sont excactement d-dimensionelle et égaux à leur centralisateurs.*

Théorème 63 *Soit D une algèbre simple centrale sur H. Alors ils existent des sous corps maximaux de D qui sont aussi separable sur H.*

Chapitre 2

Sur l'analogie entre les modules de Drinfeld et les courbes elliptiques

Résumé :

Soit Φ un $\mathsf{F}_q[T]$-module de Drinfeld de rang 2, sur un corps fini L, une extension de degré n d'un corps fini à q éléments F_q. Soit P_Φ le polynôme caractéristique, de Frobenius F de L. Soient m le degré de l'extension L sur le corps $\mathsf{F}_q[T]/P$, P est la $\mathsf{F}_q[T]$-caractéristique de L , d le degré de polynôme P, et μ un élément non nul de F_q. On abordera quatre points d'analogie avec les courbes elliptiques. On commencera par l'anneaux d'endomorphismes d'un $\mathsf{F}_q[T]$-module de Drinfeld de rang 2, $\mathrm{End}_L\Phi$, et on spécifiera les conditions de sa maximalité et non maximalité en tant que $\mathsf{F}_q[T]$-ordre dans l'anneau de division $\mathrm{End}_L\Phi \otimes_{\mathsf{F}_q[T]} \mathsf{F}_q(T)$, on s'intéressera ensuite aux polynôme caractéristique d'un module de Drinfeld de rang 2 et par son intermédiaire on calculera le nombre de classes d'iogénies, qui est égal dans le cas ordinaire à :

$(q-1)(q^{[\frac{m}{2}d]+1} - q^{[\frac{m-2}{2}d]+1} + 1)$ où [.] est la partie entière, on s'intéressera en suite à l'idéal caractéristique d'Euler-poincaré χ_Φ. Enfin on s'intéressera à la structure de $\mathsf{F}_q[T]$-module fini L^Φ et on prouvera notre résultat principal qui est : soit $M = \frac{\mathsf{F}_q[T]}{I_1} \oplus \frac{\mathsf{F}_q[T]}{I_2}$, où $I_1 = (i_1)$, $I_2 = (i_2)$ (i_1, i_2 deux polynômes de $\mathsf{F}_q[T]$) et tel que : $i_2 \mid (c-2)$. Alors il existe un $\mathsf{F}_q[T]$–module de Drinfeld Φ sur L de rang 2, ordinaire, tel que : $L^\Phi \simeq M$.

2.1 Introduction

Soit E une courbe Elliptique sur un corps fini F_q, on sait d'après [10], [13], [14] et [17] que l'anneau d'endomorphismes de E, $\mathrm{End}_{\mathsf{F}_q}E$, est un $\mathsf{Z}-$ordre dans une algèbre de division qui est soit : Q et dans ce cas $\mathrm{End}_{\mathsf{F}_q}E = \mathsf{Z}$, soit un corps quadratique complexe et dans ce cas : $\mathrm{End}_{\mathsf{F}_q}E = \mathsf{Z} + c\ O_K$ où c est un élément de Z et O_K est le $\mathsf{Z}-$ordre maximal de ce corps quadratique complexe, ou soit une algèbre de quaternion sur Q et dans un tel cas $\mathrm{End}_{F_q}E$ est un ordre maximal dans cette algèbre de quaternion. On pose $E(\mathsf{F}_q)$ le groupe abélien de points F_q-rationnels de E. Le cardinal de ce groupe abélien est égal à $N = q + 1 - c$, et d'après Hasse-Weil $\mid c \mid \leq 2.\sqrt{q}$. La structure de ce groupe dans le cas ordinaire est de la forme :

$$E(\mathsf{F}_q) \simeq \mathsf{Z}/A \oplus \mathsf{Z}/B, \text{ si } (c,q) = 1 \text{ et } B \mid A,\ \ B \mid (c-2) \quad \text{et } A.B = N \tag{1}$$

inversement pour tout groupe abélien de la forme $\mathsf{Z}/A \oplus \mathsf{Z}/B$, avec $B \mid A$, $B \mid (c-2)$ et $A.B = N$, il existe une courbe elliptique E tel que : $E(\mathsf{F}_q) \simeq \mathsf{Z}/A \oplus \mathsf{Z}/B$, on note que dans le cas supersingulier cette structure est aussi connue, voir [13].

Notre but ici sera de donner un analogue de ces résultat dans le cas de module de Drinfeld (de rang 2).

Rappelons brièvement de quoi il s'agit : soit K un corps global de caractéristique p non nulle (c'est à dire un corps de fonctions rationnelles d'une variable sur un corps fini) de corps des constants le corps fini F_q à p^s éléments. On fixe une place de K, notée ∞ et on appelle A l'anneau des éléments de K réguliers en dehors de la place ∞. Soit L un corps commutatif de caractéristique p, soit le A-homomorphisme d'anneau $\gamma : A \to L$, le noyau de cet homomorphisme est noté P et m =$[L, A/P]$ est le degré de l'extension L sur A/P.

On note $L\{\tau\}$ l'anneau des polynômes d'Ore c'est à dire l'anneau des polynômes en τ, τ étant le Frobenius de F_q, muni de l'addition usuelle et dont le produit est donné par la règle : pour tout élément λ de L, $\tau\lambda = \lambda^p\tau$. On appelle un A-module de Drinfeld Φ un homomorphisme d'anneaux, non trivial, de A vers $L\{\tau\}$ qui est différent de γ. Cet homomorphisme Φ, une fois défini, induit une structure de A-module sur le A-corps L, notée L^Φ, d'où l'appellation A-module de Drinfeld pour l'homomorphisme Φ. Cette structure de A-module dépend de Φ et spécialement de son rang .

Soit χ la caractéristique d'Euler-Poincaré (c'est un idéal de A), on peut alors parler de l'idéale $\chi(L^\Phi)$, qui sera noté χ_Φ, qui est par définition un diviseur de A, correspondant dans le cas des courbes elliptiques au nombre des poins de la variété sur son corps de base.

On va travailler dans le cas particulier $K = \mathsf{F}_q(T)$, $A = \mathsf{F}_q[T]$ et $P_\Phi(X)$: le polynôme caractéristique de A-module Φ, qui est aussi le polynôme caractéristique de Frobenius F de L. On peut démontrer que ce polynôme peut être écrit dans le cas de rang

2, sous la forme : $P_\Phi(X) = X^2 - cX + \mu P^m$, tel que $\mu \in \mathsf{F}_q^*$, $c \in A$ et $\deg c \leq \frac{md}{2}$, l'analogue de Hasse-Weil dans ce cas.

On s'intéresse à la structure de A-module L^Φ dans le cas de rang 2, on prouve que pour un $\mathsf{F}_q[T]$-module de Drinfeld ordinaire, cette structure est toujours la somme de deux $\mathsf{F}_q[T]$-modules finis et cycliques : $\frac{A}{I_1} \oplus \frac{A}{I_2}$ avec $I_1 = (i_1)$ et $I_2 = (i_2)$, où $i_1$et i_2 deux idéaux de A, qui vérifient $i_2 \mid i_1$. On démontre que $\chi_\Phi = I_1 I_2 = (P_\Phi(1))$. Soit $i = \text{pgcd}(i_1, i_2)$, alors : $i^2 \mid P_\Phi(1)$. On donne quelques aperçus des résultats que nous prouvons dans ce chapitre :

Proposition 64 *Avec les notations précédentes, on a :* $L^\Phi \simeq \frac{A}{I_1} \oplus \frac{A}{I_2}$. *En plus si* Φ *est ordinaire, alors :* $i_2 \mid (c-2)$.

Proposition 65 *Soit* Φ *un* A*-module de Drinfeld , ordinaire , de rang* 2 *et soit* ρ *un idéal premier de* A *différent de la* A*-caractéristique* P *de* L, *tel que* $\rho^2 \mid P_\Phi(1)$ *et* $\rho \mid (c-2)$. *Alors* $\Phi(\rho) \subset L^\Phi$ *si et seulement si le* A*-ordre* $O(\Delta/\rho^2) \subset End_L\Phi$.

Nous aboutissons en fin à notre résultat principal, qui est le parfait analogue au résultat correspondant pour les Courbes elliptiques (1) :

Théorème 66 *Soit* $M = \frac{A}{I_1} \oplus \frac{A}{I_2}$, *où* $I_1 = (i_1)$, $I_2 = (i_2)$ *et tel que :* $i_2 \mid i_1$, $i_2 \mid (c-2)$. *Alors il existe un* A*-module de Drinfeld* Φ *sur* L *de rang* 2, *ordinaire, tel que :* $L^\Phi \simeq M$.

2.2 Modules de Drinfeld

Sur k on définit l'anneau $\mathsf{k}\{\tau\}$, où τ est le Frobenius de F_q.

Définition 67 *Soit R l'ensemble des polynômes k-linéaires à coefficient dans k, c'est à dire de la forme :*

$$Q(x) = \sum_{K>0} l_K x^{q^K},$$

où $l_K \in \mathsf{k}$ pour tout $K > 0$, seul un nombre fini l_k est non nul. L'anneau R est un anneau pour l'addition et la composition des polynômes.

Lemme 68 *$\mathsf{k}\{\tau\}$ et R sont des anneaux isomorphes.*

Preuve. Considérons l'application suivante :

$$\theta : \mathsf{k}\{\tau\} \mapsto R$$

$$\sum f_i \tau^i \mapsto \sum_{i\geq 0} l_i x^{qi}$$

On voit que θ est un morphisme de groupes additifs et une bijection. Prouvons que θ est un morphisme d'anneaux. Soit $l \in \mathsf{k}$,

$$\theta(\tau^j l \tau^i) = \theta(l^{q^j} \tau^{i+j}) = l^{q^j} X^{q^{i+j}} = (lX^{q^i})^{q^j} = \theta(\tau^j) \circ \theta(l\tau^i) \ . \ \blacksquare$$

Si on pose $A = \mathsf{F}_q[T]$, $f(\tau) = \sum_{i=0}^{v} a_i \tau^i \in \mathsf{k}\{\tau\}$ *et* $Df := \mathsf{a}_0 = f'(\tau)$.

Il est claire que l'application :

$$\mathsf{k}\{\tau\} \mapsto \mathsf{k}$$

$$f \mapsto Df,$$

est un morphisme de F_q-algèbres.

Définition 69 *Un A-corps* k *est un corps* k *muni d'un morphisme fixe* $\gamma : A \mapsto \mathsf{k}$. *L'idéal* $P = Ker\,\gamma$ *est appelé la caractéristique de* k. *On dit que* k *est de caractéristique générique si et seulement si* $P = (0)$ *; autrement (c.a.d* $P \neq (0)$ *)* k *est de caractéristique finie.*

On a alors la définition fondamentale suivante :

Définition 70 *Soit* $\Phi : A \mapsto \mathsf{k}\{\tau\}$ *un homomorphisme d'algèbre. Donc* Φ *est un A-module de Drinfeld sur un A-corps* k*, si et seulement si :*

1. $D \circ \Phi = \gamma$;
2. Pour un certain $a \in A, \Phi_a \neq \gamma(a)\tau^0$.

Remarque 71 *1. La normalisation numéro 2 de la définition précédente est analogue à la normalisation utilisée pour la multiplication complexe de courbes elliptiques.*

2. Via Φ*, toute extension* L *de* k *devient un A-module par :*

$$\begin{aligned} L \times A &\rightarrow L, \\ (l, a) &\rightarrow l.a := \Phi_a(l)\ . \end{aligned}$$

On notera cet A-module par L^{Φ}.

Soient $\overline{\mathsf{k}}$ une clôture algébrique fixe de k et Φ un module de Drinfeld sur k et I un idéal de A . Comme A est un domaine de Dedekind, on sait que I peut-être généré par (au plus) deux éléments $\{i_1\ ,\ i_2\} \subset I$.

Puisque $\mathsf{k}\{\tau\}$ a un algorithme de division droite, il existe un plus grand commun diviseur dans $\mathsf{k}\{\tau\}$. C'est le générateur unitaire de l'idéal gauche de $\mathsf{k}\{\tau\}$ généré par : Φ_{i_1}et Φ_{i_2}.

Définition 72 *On note par* Φ_I *le générateur unitaire de l'idéal gauche de* $\mathsf{k}\{\tau\}$ *généré par* Φ_{i_1} *et* Φ_{i_2}.

Définition 73 *Soient* L *une extension de* k *et* I *un idéal de* A. *On définit par :* $\Phi[I](\mathsf{k})$ *le sous groupe fini de* $\Phi[\overline{L}]$, *formé par les racines de* Φ_I *dans* $\overline{\mathsf{k}}$.

Si $a \in A$, on pose $\Phi[a] := \Phi[(a)]$.

On peut voir $\Phi[a] = \{$ l'ensemble des racines de $\Phi(a)$ dans $\overline{\mathsf{k}}\}$, et $\Phi_I = \cap_{a\in I}\Phi[a]$. Donc :

$$\Phi_a(\overline{\mathsf{k}}) := \Phi[a](\overline{\mathsf{k}}) = \{x \in \overline{\mathsf{k}}, \Phi_a(x) = 0\}$$

et pour tout idéal $Q \subset A$,

$$\Phi_Q(\overline{\mathsf{k}}) := \Phi_Q(\overline{\mathsf{k}}) = \cap_{a\in Q}\Phi_a(\overline{\mathsf{k}}).$$

Remarque 74 *Les groupes : $\Phi[I](\mathsf{k})$ et $\Phi[I](\overline{\mathsf{k}})$ sont clairement stables par $\{\Phi_a\}_{a\in A}$.*

Définition 75 *Soit Φ un A-module de Drinfeld sur un A-Corps K. On dit que Φ est supersingulier, si et seulement si, le A-module constitué par les points de P-division $\Phi_P(\overline{K})$ est trivial.*

2.2.1 La hauteur et le rang de A-module Φ

Soit Φ un A-module de Drinfeld sur le A-corps k. On note aussi $\deg_\tau$ le degré en l'indéterminée τ.

Définition 76 *Un élément de $\mathsf{k}\{\tau\}$ est dit séparable, si son coefficient constant est non nul. Il est purement inséparable s'il est de la forme $\lambda\tau^n$, $n>1$ et $\lambda\in\mathsf{k}$, $\lambda\neq 0$.*

Soit H un corps global de caractéristique $p>0$, et soit ∞ une place (un idéal premier en général) de H, on notera H_∞ le complété de H à la place ∞.

On définit la fonction degré sur A par :

Définition 77 *Soit $a\in A$, deg $a=\dim_{F_q}\frac{A}{aA}$ si $a\neq 0$ et $\deg 0=-\infty$.*

On étend alors deg à K en posant deg x = deg a−deg b si $0 \neq x = \frac{a}{b} \in K$.

Si $A = \mathsf{F}_q[T]$, alors la fonction deg est le degré usuel des polynômes. Soit Q un idéal non nul de A, on définit le degré de l'idéal Q, noté deg Q, par :

$$\deg Q = \dim_{F_q} \frac{A}{Q}.$$

Lemme 78 *Il existe un nombre rationnel r tel que :*

$$deg_\tau \Phi_a = r \ dega.$$

Preuve. Il est facile de voir que Φ est une injection, sinon comme $\mathsf{k}\{\tau\}$ est intègre, Ker Φ est un idéal premier non nul, donc maximal dans A et par conséquent Im Φ est un corps, ce qui entraînerait $\Phi = \gamma$. Puisque $-\deg_\tau$ définit une valuation non triviale sur Frac($\Phi(A)$) (le corps des fractions de $\Phi(A)$) qui est isomorphe à K, donc $-\deg_\tau$ et $-\deg$ sont des valuations équivalentes sur K. Il existe alors un nombre rationnel $r > 0$, tel que : r deg=$\deg_\tau$. ■

Corollaire 79 *Soit $\Phi : A \mapsto \mathsf{k}\{\tau\}$ un A-module de Drinfeld, alors Φ est injective.*

Proposition 80 *Le nombre r est un entier positif.*

Définition 81 *L'entier r est appelé le rang de A-module de Drinfeld Φ.*

Par exemple si $A = \mathsf{F}_q[T]$, un A-module de Drinfeld de rang r est de la forme : $\Phi(T) = a_1 + a_2\tau + ... + a_r\tau^r$, où $a_i \in \mathsf{k}$, $1 \leq i \leq r-1$ et $a_r \in \mathsf{k}^*$.

Dans le cas où char K= $P \neq (0)$ on peut définir la notion de hauteur d'un module de Drinfeld Φ.

Pour cela, soit $v_P : K \mapsto \mathsf{Z}$, la valuation normalisée associée à P, c'est à dire, si $a \in k$ a une racine sur P d'ordre t, on a $v_P(a) = t$.

Pour tout $a \in A$, soit $w(a)$ le plus petit entier $t > 0$, où τ^t occure en Φ_a avec un coefficient non nul.

Lemme 82 *Il existe un nombre rationnel h tel que :*

$$w(a) = hv_P(a) \deg P.$$

Proposition 83 *Le nombre h est un entier positif.*

Définition 84 *L'entier h est appelé la hauteur de Φ.*

Par exemple, si $A = \mathsf{F}_q[T]$, un A-module de Drinfeld :

$\Phi(T) = \gamma(T) + a_h\tau^h + ... + a_r\tau^r$ est de hauteur h (si $\gamma(T) = 0$) et de rang r où $a_i \in \mathsf{k}$, $h \leq i \leq r-1$ et $a_r \in \mathsf{k}^*$. Si $\gamma(T) \neq 0$, la hauteur est 0 par définition.

2.2.2 Morphismes des modules de Drinfeld

Soit k un A-corps et soit $\overline{\mathsf{k}}$ une clôture algébrique fixe. Soient Φ et Ψ deux modules de Drinfeld sur k de rang $r > 0$. On définit un morphisme de Φ vers Ψ sur k par :

Définition 85 *Soient Φ et Ψ deux modules de Drinfeld sur un A-corps k. Un morphisme de Φ vers Ψ sur k est un élément $p(\tau) \in \mathsf{k}\{\tau\}$ tel que :*

$$p\ \Phi_a = \Psi_a\ p, \forall a \in A.$$

Un morphisme non nul est appelé une isogénie. Notons qu'une isogénie n'est possible qu'entre deux modules de Drinfeld de même rang.

Une isogénie u inversible (i.e : $\deg_\tau u = 0$) est appelée isomorphisme et les modules sont appelés isomorphes.

L'ensemble des ces morphismes forment un A-module noté $\mathrm{Hom}_{\mathsf{k}}(\Phi, \Psi)$.

On peut voir cette structure par le fait que si Φ et Ψ sont deux A-modules de Drinfeld sur k. Un morphisme (ou k-morphisme) $p : \Phi \mapsto \Psi$ de Φ dans Ψ est un morphisme de A-module p : (k,Φ)$\mapsto$ (k,Ψ) où (k,Φ) (respectivement (k,Ψ)) désigne k muni de la structure de A-module donnée par Φ (resp Ψ).

Un tel morphisme est en particulier un morphisme du groupe additif de k. On peut voir facilement que $\mathsf{k}\{\tau\}$ est un $\mathsf{k}[F]-$module de type fini et par conséquence $\mathsf{k}\{\tau\}$ est entier sur $\mathsf{k}[F]$. Ceci entraîne que :

$$\mathsf{k}(\tau) = \mathsf{k}\{\tau\} \otimes_{\mathsf{k}[F]} \mathsf{k}(F) = \mathsf{k}\{\tau\} \otimes_A K,$$

L'anneau des fractions de $\mathsf{k}\{\tau\}$ est noté $\mathsf{k}(\tau)$ ($\mathsf{k}(\tau)$ est un corps non commutatif qui est appelé corps gauche des fractions de $\mathsf{k}\{\tau\}$).

En particulier si $\Phi = \Psi$, l'anneau de k-endomorphismes de Φ ($\mathrm{End}_{\mathsf{k}}\Phi = \mathrm{Hom}_{\mathsf{k}}(\Phi, \Phi)$ est un sous anneau de $\mathsf{k}\{\tau\}$ et un A-module sans torsion contenant $\Phi(A)$:

$$\mathrm{End}_{\mathsf{k}}\Phi = \{u \in \mathsf{k}\{\tau\} / \forall a \in A, u\Phi_a = \Psi_a u\}.$$

Puisque Φ est une injection, Φ se prolonge naturellement à une injection

$\Phi : K \mapsto \mathsf{k}(\tau)$. Par cette injection on identifie dans $\mathsf{k}(\tau)$, A et $\Phi(A)$ ainsi K et $\Phi(K)$.

Soit F le Frobenius de k on a : $\Phi\ (A) \subset\ \mathrm{End}_{\mathsf{k}}\Phi$, $F \in \mathrm{End}_{\mathsf{k}}\Phi$.

On peut s'appuyer sur le théorème de Wedderburn pour avoir une décomposition générale de $\mathrm{End}_{\mathsf{k}}\Phi \otimes_A K$:

$$\mathrm{End}_{\mathsf{k}}\Phi \otimes_A K = M_{n_1}(D_1) \oplus ... \oplus M_{n_l}(D_l),$$

où D_K , pour $1 < k < l$, sont des corps gauches, de centres C_K et $M_{n_k}(D_k)$ sont les anneaux des matrices carrées d'ordre n_k sur D_k.

Pour démonstration on renvoie à [2] et [3].

Définition 86 *Soient Φ et Ψ deux A-modules de Drinfeld sur un A-corps k et p une isogénie sur k de Φ vers Ψ.*

1. On dit que l'isogénie p est séparable si et seulement si $p(\tau)$ est séparable.
2. On dit que p est purement inséparable si et seulement si $p(\tau) = \tau^j$ pour un certain $j > 0$.

Théorème 87 *$End_{\mathsf{k}}\Phi$ est un A-module projectif de rang $\leq r^2$.*

Corollaire 88 *$End_{\mathsf{k}}\Phi \otimes_A K$ est une algèbre de division finie dimensionnelle sur K et centrale sur $K(F)$.*

Proposition 89 *Soit $p : \Phi \mapsto \Psi$ une isogénie. Alors $End_{\mathsf{k}}\Phi$ et $End_{\mathsf{k}}\Psi$ ont le même rang sur A.*

2.2.3 Norme d'isogènie

Définition 90 *Soit F un élément entier sur un anneau A, de corps des fractions K. On note par $N_{K/K(F)}$ le déterminant de l'application K-linéaire multiplication par F dans $K(F)$ (c'est la norme usuelle si l'extension $K(F)/K$ est séparable.*

On peut voir qu'il y'a un morphisme $N_{K/K(F)} : I_{\overline{A}} \to I_A$ du groupe des idéaux fractionnaires de $\overline{A}$ dans celui des idéaux fractionnaires de A, par ce morphisme on a :

Proposition 91 *La norme d'une isogénie est un idéal principal.*

Proposition 92 *Soit $M_{fin}(A)$ la catégorie des idéaux premiers de A et soit $D(A)$ le monoïde des ideaux entiers de A. Il existe une unique fonction :*

$$\chi : M_{fin}(A) \mapsto D(A),$$

multiplicative sur les suites exactes et telle que $\chi(0) = 1$ et $\chi(A/\wp\ ) = \wp$ pour tout idéal premier $\wp$ de A.

Définition 93 *La fonction χ est appelée la caractéristique d'Euler-Poincaré.*

On peut regarder $\chi(\mathsf{k}^{\Phi})$ et on le note par χ_{Φ}.

Proposition 94 *Les idéaux χ_{Φ} et P^m sont principaux (dans A), et plus précisement $\chi_{\Phi} = (P_{\Phi}(1))$ et $P^m = P_{\Phi}(0)$.*

Remarque 95

1. On sait que la norme d'une isogénie est un idéal principal, en effet $N(F) = P_\Phi(0)$ et $N(1-F) = (P_\Phi(1))$ puisque F et $1-F$ sont deux k-isogénies.
2. On peut appeler χ_Φ le diviseur de k-points, ce diviseur est analogue au nombre de k-points pour les courbes elliptiques.
3. χ_Φ est l'annulateur de A-module k^Φ. On peut en déduire que : $\mathsf{k}^\Phi \subset (\frac{A}{\chi_\Phi})^r$.
4. La structure de A-module k^Φ est stable par l'endomorphisme de Frobenius F.

Corollaire 96 *S'il existe un A-module de Drinfeld Φ, sur un corps k, de caractéristique P et de degré m sur A/P, alors l'idéal P^m est un idéal principal.*

Remarque 97 *Ce corollaire nous montre qu'il y'a une restriction pour l'existence de A-module de Drinfeld.*

2.3 Modules de Drinfeld sur un corps fini

Soit L une extension finie de degré n d'un corps fini F_q à q éléments. Le Frobenius F de L est alors $F = \tau^n$, donc $\mathsf{F}_q[F]$ est le centre de $L\{\tau\}$. On pose $m = [L : A/P]$ et $d = \deg P$, alors $n = m.d$. La fonction $-\deg$ définie une valuation sur K. Soit $\tau : x \mapsto x^p$ le Frobenius de F_q et soit L une extension finie de F_q. On notera $L\{\tau\}$ l'anneau des polynômes en τ muni de l'addition usuelle et de la multiplication définie par :

$$\forall l \in L,\ \tau l = l^q \tau.$$

Un A-module de Drinfeld Φ sur L donne donc une structure de A-module sur le groupe additif L, cette structure sera notée L^{Φ}. Soit γ l'application de A dans L qui à un élément a de A associe le terme constant de Φ_a, alors il est facile de voir que γ est un endomorphisme d'anneaux, et que Φ et γ coïncident sur l'ensemble $A^* = \mathsf{F}_q^*$ des éléments inversibles de A qui égal à celui de F_q.

Théorème 98 *Soit Φ un A-module de Drinfeld de rang r, $K(F)$ le sous corps de $End_L\Phi\otimes_A K$ de degré r_1, donc $r_2 = \frac{r}{r_1}$ est un entier et il existe une unique place ω de $K(F)$ qui divise F. Les invariants de $End_L\Phi\otimes_A K$ sont $\frac{1}{r_2}$ en $\omega, -\frac{1}{r_2}$ en $\infty_{K(F)}$ ($\infty_{K(F)}$ est le prolongement de la place ∞ de $\mathsf{F}_q(F)$ à $K(F)$).*

Théorème 99 *Soit Φ un A-module de Drinfeld de rang r sur un corps fini L. On pose $r_1 = [K(F) : K]$ et r_2^2 le degré du corps gauche $End_L\Phi \otimes_A K$ sur son centre $K(F)$. Alors on a :*

$$r = r_1.r_2.$$

Preuve. Soient $K(F)_\infty$, $K_\infty et(F)_\infty$, les complétés de $K(F), K$ et $L(F)$ à la place ∞ (la place ∞ restreinte à $L(F)$ est la place $\frac{1}{F}$). On a :

$$[K(F) : K] = \ [K(F)_\infty, K_\infty] = e_\infty.f_\infty = r_1,$$

où e_∞ et f_∞ sont l'indice de ramification et le degré résiduel en ∞ de l'extension $K(F)/K$. De même :

$$[K(F),\ L(F)] = [K(F)_\infty,\ L(F)_\infty] = e'_\infty.f'_\infty,$$

avec $f'_\infty = f_\infty.d_\infty$, $e'_\infty = e_\infty.d_\infty$, où e'_∞ et f'_∞ sont l'indice de ramification et degré résiduel

en ∞ pour l'extension $K(F)/L(F)$.Or sur K , on a : $e'_\infty = \frac{n}{rd_\infty} e_\infty$, ainsi :

$$\frac{[K(F), L(F)]}{[K(F) : K]} = \frac{e'_\infty . f'_\infty}{e_\infty . f_\infty} = \frac{n}{r},$$

et $[K(F) : K] = \frac{n}{r} r_1 = \frac{n}{r_2}$; d'où $r = r_1 r_2$. ■

Définition 100 *Soit Φ un A-module de Drinfeld sur le corps fini L. On note par $M_\Phi(X)$ le polynôme minimal unitaire de F sur K .*

Proposition 101 *Avec les notations précédentes : $M_\Phi(X)$ est un élément de $A[X]$, égal à $P_\Phi^{\frac{1}{r_2}}$.*

Corollaire 102 *Pour deux A-modules de Drinfeld Φ et Ψ, de rang r sur le corps fini L, les assertions suivantes sont équivalentes :*

1. *Φ et Ψ sont isogènes,*
2. *$M_\Phi(X) = M_\Psi(X)$,*
3. *$P_\Phi = P_\Psi$.*

Proposition 103 *Soit L une extension finie de degré n du corps fini F_q, soit F le Frobenius de L. Alors $L(\tau)$ est une algèbre de division centrale sur $\mathsf{F}_q(F)$ de dimension n^2.*

Définition 104 *Tout élément $u \in L\{\tau\}$ peut s'écrire sous la forme $u = \tau^h u'$ (car L est un corps parfait) où $u' \in L\{\tau\}$ séparable. L'entier h est appelé la hauteur de u et noté ht u.*

Dans le cas de corps fini, on peut voir la hauteur d'un A-module de Drinfeld Φ sur un corps finis L, l'entier H_Φ comme étant :

$$H_\Phi = \frac{1}{\deg P} \inf\{\text{ht } \Phi_a, 0 \neq a \in P\}.$$

Remarque 105 *Il est facile de voir que H_Φ est invariant par isogénie et que*

$$1 \leq H_\Phi \leq r.$$

Proposition 106 *Soit Φ un A-module de Drinfeld de rang r sur un corps fini L, les assertions suivantes sont équivalentes :*

1. *Il existe une extension finie L' de L, telle que l'anneau de division $End_{L'}\Phi \otimes_A K$, a une dimension r^2 sur K.*
2. *Certaines puissances de l'endomorphisme de Frobenius F de L appartiennent à A.*
3. *Φ est supersingulier.*
4. *Le corps $K(F)$ a une seule place au dessus de P.*

Proposition 107 *Soit Φ un A-module de Drinfeld de rang r et soit Q un idéal de A premier avec P, alors :*

$$\Phi_Q(\overline{L}) = (\frac{A}{Q})^r.$$

Preuve. On distingue deux étapes :

Première étape : On suppose A principal. Dans ce cas, il existe $a \in A$, $a \neq 0$, tel que $Q = aA$. Pour tout $b \in A$ on pose $M(b) = \Phi_b(\overline{L})$. On remarque que si $b \in A$ est premier P, alors $\Phi_b(X)' = \gamma(b) \neq 0$ (Φ_b est considéré ici comme un élément de R) et donc :

$$\#M(b) = deg_X \Phi_b(X) = q^{r \deg b}.$$

Soit $a = \Pi_{i=0}\pi_i^{n_i}$, la décomposition de a en facteurs irréductibles, alors on a :

$$A/aA \simeq \Pi_{i=0}(\frac{A}{\pi_i^{n_i}A})$$

et

$$M(a) = \oplus_{i=0} M(\pi_i^{n_i}).$$

Soit donc π un élément irréductible de A premier avec P et soit s un entier ≥ 1.

D'après la structure des modules de π-torsion sur un anneau principal, il existe des éléments $d_1, ..., d_n$ de N tels que : $M(\pi^s) \simeq (\frac{A}{\pi^s A})^{d_s} \oplus ... \oplus (\frac{A}{\pi A})^d$ où $\text{long}_A M(\pi^s) = sd_s \oplus ... \oplus d_1$.

Comme l'action de π^{s-1} est triviale sur les composantes indexées de :

1 à $s-1$, et comme $\pi A/A\pi^s \simeq A/\pi^{s-1}A$, on a :

$M(\pi^{s-1}) \simeq (\frac{A}{\pi^{s-1}A})^{d_s+d_{s-1}} \oplus ... \oplus (\frac{A}{\pi A})^{d_1}$ et

$\text{long}_A M(\pi^{s-1}) = (s-1)(d_s + d_{s-1}) \oplus ... \oplus d_1$.

Ainsi $\text{long}_A M(\pi^s) - long_A M(\pi^{s-1}) = d_{s-1}$.

Or $\text{long}_A M(\pi^s) = \dim_{A/\pi A} M(\pi^s) \quad = \frac{log_q \# M(\pi^s)}{log_q \#(A/\pi A)} \; = \frac{rs \deg \pi}{\deg \pi} \; = rs$, et de même $\text{long}_A M(\pi^{s-1}) = r(s-1)$. D'où $r = d_s, d_{s-1} = d_{s-2} = ... = d_1 = 0$.

Ainsi : $M(\pi^s) \simeq (A/\pi^s A)^r$, et donc :

$$M(a) \simeq (A/\pi A)^r.$$

Deuxième étape : On ne suppose plus A principal. Pour tout idéal Q de A on pose $M(Q) = \Phi_Q(\overline{L})$. Comme A est un anneau de Dedekind, on a la décomposition :

$$Q \quad = \Pi_{\rho \in Spec(A)} \rho^{s_\rho}.$$

Ainsi $A/Q = \Pi_{\rho \in Spec(A)} A/\rho^{s_\rho}$ et

$$M(Q) = \oplus_\rho M(\rho^{s_\rho}).$$

Soit $\rho \in Spec(A)$ distinct de P et soit s un entier ≥ 1. On pose $M = M(\rho^s)$. Soit A_ρ le localisé de A en ρ et soit $\pi \in A$ premier avec ρ tel que $\pi A_\rho = \rho A_\rho . M \simeq M_\rho$ comme A-modules où M_ρ est le localisé de M en ρ et donc on a un isomorphisme de A_ρ-modules : $M \simeq M(\pi^{sn})$ où $M(\pi^s)$ est le A-module des points de π^s-torsion. Comme A_ρ est un anneau principal, on peut utiliser la première étape $M(\pi^s) \simeq (A_\rho/\rho^s A_\rho)^r \simeq (A/\rho^s)^r$. ■

Corollaire 108 *On peut en déduire, alors que :* $\Phi_P(\overline{L}) = (\frac{A}{P})^{r-H_\Phi}$.

On peut en déduire un résultat important, caractérisant la super singularité :

Proposition 109 *Le A-module Φ est supersingulier ($\Phi_P(\overline{L}) = 0$) si et seulement si $r = H_\Phi$.*

Définition 110 *On dit que le corps L est assez grand si tout les endomorphismes qui sont définis sur $\overline{L}$ sont aussi définis sur L, c.a.d : $End_{\overline{L}}\Phi = End_L\Phi$.*

Le résultat suivant est prouvé dans [7] :

Proposition 111 *Soit Φ un A-module de Drinfeld sur un corps fini L. Si Φ est supersingulier et L assez grand, alors l'anneau d'endomorphismes $End_L\Phi$ est un A-ordre maximal dans l'algèbre $End_L\Phi \otimes_A K$.*

Par exemple, si $A = \mathsf{F}_q[T]$ et $L = \mathsf{F}_{q^n}$,

Un A-module de Drinfeld sur L de rang r est un homomorphisme $\Phi : A \mapsto L\{\tau\}$, cet homomorphisme est déterminé par :

$$\Phi_T = \gamma(T) + c_1\tau + ... + c_r\tau^r,$$

où $c_1, ..., c_{r-1} \in L$ et $c_r \in L^*$.

De plus, tout choix de c_1,..., c_r définit un module de Drinfeld sur L.

Deux modules de Drinfeld Φ et Ψ sont isomorphes, si et seulement si, il existe un $a \in L$ tel que : $a^{-1}\Phi_a = \Psi_a a$.

Lemme 112 *Soit Φ un A-module de Drinfeld de rang r, sur un corps fini L, de caractéristique P. Le polynôme caractéristique de l'endomorphisme de Frobenius F est de la forme :*

$$P_\Phi(X) = X^r + c_1X^{r-1} + ... + c_{r-1}X + \mu P^m, c_1, ...c_{r-1} \in A \text{ et } \mu \in \mathsf{F}_q^*.$$

Remarque 113 *le fait que le coefficient constant de polynôme caractéristique est μP^m vient du fait que $P_\Phi(0) = P^m$ dans A.*

La proposition suivante est l'analogue de l'hypothèse de Riemann pour les courbes elliptiques :

Proposition 114 *Soit Φ un A-module de Drinfeld de rang r sur un corps fini L qui est une extension de degré n de F_q. Alors deg $(w) = \frac{n}{r}$, pour toute racine w du polynôme caractéristique $P_\Phi(X)$.*

Le résultat suivant est l'analogue de Hasse-Weil pour les courbes elliptiques :

Corollaire 115 *Soit* $P_\Phi(X) = X^r + c_1X^{r-1} + ... + c_rX + \mu P^m$, *le polynôme caractéristique d'un module de Drinfeld* Φ, *de rang* r, *sur un corps fini* L. *Alors :*

$$\forall \ \ 1 \leq i \leq r-1, \qquad \deg\, c_i \leq \frac{i}{r} m \deg P.$$

Preuve. La preuve découle immédiatement de la proposition 114. ■

2.4 Modules de Drinfeld de rang 2

Dans tout ce qui suit, on considéra Φ un A-module de Drinfeld de rang 2 et $A = \mathsf{F}_q[T]$, pour les démonstrations voir [1], [12] et [6].

Notre intérêt pour l'arithmétique de tels modules nous amène à s'intéresser à leurs anneaux d'endomorphismes, à leurs classes d'isogènies, et aussi à la structure de A-module fini induite par ces modules sur le A-corps fini L.

2.4.1 Anneaux d'endomorphismes

On commence par annoncer les résultat suivants caractérisant les anneaux d'endomorphismes d'un A-module de Drinfeld de rang 2, pour preuve voir [12] :

Proposition 116 *Soit* O *un* A*-ordre dans une extension quadratique* $K(F)$, *et soit* $O_{K(F)}$ *le* A*-ordre maximal dans* $K(F)$, *alors tout* A*-ordre* O *de* $K(F)$ *est de la forme :*

$$O = A + g.O_{K(F)},$$

où g *est un élément unitaire de* A.

Définition 117 *L'élément g de A dans la proposition précédente est appelé le conducteur de A-ordre O.*

Proposition 118 *Soit Φ un A-module de Drinfeld de rang 2, sur un corps fini L, de degré m, sur A/P et de Frobenius F, où P est la A-caractéristique de L et soit D_P le complété à la place P de l'algèbre $End_L\Phi \otimes_A K$.*

1. *Si F est de la forme $kP^{\frac{m}{2}} (k \in F_q^*)$, alors l'anneau $End_L\Phi$ peut être identifié avec un A-ordre maximal dans $_{D_P}$, et tout ordre maximal dans D_P peut-être obtenu de cette façon.*
2. *Autrement, l'anneau $End_L\Phi$ peut être identifié avec un A-ordre dans le corps quadratique imaginaire $K(F)$. Un A-ordre O de $K(F)$ occure de cette façon, si et seulement si, $F \in O$, de plus le conducteur de O est premier avec P dans les deux cas suivants :*
   (a) *F est de la forme $\sqrt{\mu P^m}$ avec $\mu \in F_q^*$ si m est impaire et $\sqrt{\mu P^m}$ est imaginaire quadratique ,*
   (b) *F est de la forme $\frac{k_2}{k} P^{\frac{m}{2}}$ si m est paire et deg P est impaire.*

Corollaire 119 *Si le conducteur de O est premier avec P, alors O est un A-ordre maximal dans l'algèbre $End_L\Phi \otimes_A K$.*

Pour des modules de Drinfeld de rang 2, on est en mesure de spécifier l'algèbre $\mathrm{End}_L\Phi \otimes_A K$ comme étant tout simplement, dans le cas ordinaire, égale à $K(F)$.

Proposition 120 *Soit Φ un A-module de Drinfeld de rang 2 sur L :*

1. *Soit Φ est supersingulier,*
2. *Soit $End_L\Phi \otimes_A K = K(F)$.*

Preuve. Soient $r_1 = [K(F) : K]$ et r_2^2 le degré du corps gauche $\mathrm{End}_L\Phi \otimes_A K$ sur son centre $K(F)$. Puisque $2 = r_1.r_1$, on a deux cas : ($r_1 = 1$ et $r_2 = 2$) ou ($r_1 = 2$ et $r_2 = 1$), alors dans le cas où ($r_1 = 1$ et $r_2 = 2$) on a un module de Drinfeld supersingulier, car : $r_1 = [K(F) : K] = 1$ et :

$$F \in \overline{A^{K(F)}} = \overline{A^K} = A.$$

Autrement (c.a.d : $r_1 = 2$ et $r_2 = 1$), nous aurons $\mathrm{End}_L\Phi \otimes_A K = K(F)$ et $\mathrm{End}_L\Phi$ est un A-ordre dans le corps quadratique $K(F)$. ■

Remarque 121 *Le résultat précédent montre que dans le cas ordinaire, et puisque $End_L\Phi$ est un A-ordre contenant toujours $A[F]$, on peut se contenter, pour définir ou étudier la maximalité de $End_L\Phi$, d'étudier l'existence de A-ordre contenant $A[F]$ et contenu dans le A-ordre maximal $O_{K(F)}$ de l'algèbre $K(F)$.*

On se met maintenant dans le cas non supersingulier et $O_{K(F)}$ est toujours le A-ordre maximal dans l'algèbre $K(F)$, on s'intéresse à savoir : l'existence d'un A-ordre O tel que :

$$A[F] \subset O \subset O_{K(F)} \,?$$

Pour répondre à cette question, on a le résultat suivant :

Proposition 122 *Soit $\Delta = c^2 - 4\mu P^m$, le discriminant du P_F, le polynôme caractéristique de F le Frobenius de corps fini L, qui est $P_F(X) = X^2 - cX + \mu P^m$, et soit $O_{K(F)}$ le A-ordre maximal de l'algèbre $K(F)$.*

1. *Pour tout $g \in A$ tel que $\Delta = g^2 .\omega$, il existe un A-module de Drinfeld Φ sur L de rang 2, tel que : $O_{K(F)} = A[\sqrt{\omega}]$ et :*

$$End_L\Phi = A + g.O_{K(F)}.$$

2. *Il n'existe pas des polynômes g de A tels que g^2 divise Δ, alors : il existe un A-module de Drinfeld Φ sur L de rang 2, ordinaire et tel que $End_L\Phi = O_{K(F)}$.*

Preuve. 1) On suppose qu'il existe $g \in A$, tel que $\Delta = g^2.\omega$, où F étant une racine de polynôme caractéristique P_Φ, on peut poser alors :

$F = -c/2 + \sqrt{\Delta}/2 = -c/2 + g.\sqrt{\omega}/2$, donc $A[F] = A[-c/2 + g.\sqrt{\omega}/2] =$

$A[\ g\sqrt{\omega}/2] \sqsubseteq A + g.A[\sqrt{\omega}]$ et on peut voir facilement dans ce cas que le A-ordre $O_{K(F)} = A[\sqrt{\omega}]$ est un A-ordre maximal, et d'après la proposition 118, il existe un A-module de Drinfeld Φ tel que : $\mathrm{End}_L\Phi = A + g.O_{K(F)}$.

2)Dans l'autre cas : s'il 'existe pas $g \in A$ tel que $g^2 \mid \Delta$, et d'après la proposition 118, il existe un A-module de Drinfeld Φ tel que le A-ordre $\mathrm{End}_L\Phi$ ne peut pas être de la forme $A+g.O_{K(F)}$ et dans ce cas il sera certainement égal à $O_{K(F)}$.

2.4.2 Classes d'isogénies

Soit Φ un A-module de Drinfeld de rang 2 sur un corps fini L de A-caractéristique P, et soit $m = \deg P$. Le polynôme caractéristique P_Φ peut être donné par l'intermédiaire

de polynôme minimale unitaire de F dans $A[X]$, M_Φ, et avec la relation $P_\Phi = M_\Phi^{r_2}$, r_2 étant la racine du degré de corps gauche $\mathrm{End}_L\Phi \otimes_A K$ sur son centre $K(F)$.

Soient $\overline{K}$ une clôture algébrique de K, et ∞ une place de K divisant $\frac{1}{T}$, et soient $K_\infty = F_q((\frac{1}{T}))$, et C_∞ le completé d'une clôture algébrique de K_∞.

On fixe un plongement $\bar{K} \hookrightarrow \mathsf{C}_\infty$.

Pour tout $\alpha \in \mathsf{C}_\infty$, $\mid \alpha \mid_\infty$est la valeur normalisée de α ($\mid \frac{1}{T} \mid_\infty = \frac{1}{q}$).

Soit $\theta \in \bar{K}$, on dit que θ est un nombre de Weil ordinaire si :

1. θ est entier sur A,
2. $\mid \theta \mid_\infty = q^{\frac{md}{2}}$
3. $K(\theta)/K$ est imaginaire, et $[K(\theta), K] = 2$;
4. il existe une unique place de $K(\theta)$ divisant θ et $\mathrm{Tr}_{K(\theta)/K}(\theta) \neq 0(P)$.

Soit θ un nombre de Weil ordinaire alors $\forall \sigma \in \mathrm{col}(\bar{K}/K)$, θ^σ est aussi un nombre de Weil ordinaire. Notons W^{ord} l'ensemble des classes de conjugaison des nombress de Weil ordinaires. Alors :

Théorème 123 *Il y'a une bijection entre W^{ord} et l'ensemble des classes d'isogénies des A-module de Drinfeld de rang 2 ordinaires définies sur L.*

Soit θ un nombre de Weil ordinaire, posons :

$$P(x) = Hr(\theta, K; x).$$

Alors par (1), (2), (3) et (4) :

$$P(x) = x^2 - cx + \mu P^m,$$

avec $\mu \in \mathsf{F}_q^*$ et $c \in A$, $c \neq 0(P)$, et $\deg_T c \leq \frac{md}{2}$.

Psonos $\Gamma = \{c \in A,\ c \neq 0(P),\ \deg_T c \leq \frac{md}{2}\}$.

Lemme 124 *Soient $\mu \in \mathsf{F}_q^*$ et $c \in \Gamma$.*

Soit E le corps de décomposition de $P(x) = x^2 - cx + \mu P^m$ sur K. Soit θ une racine de $P(x)$. Alors θ verifie (1), (2), et (4) et $[K(\theta), K]$ =2.

Preuve. Soit B la fermeture intégrale de A dans E. Supposons qu'il existe θ racine de $P(x)$ avec $\theta \in B^*$. Comme le coefficient constant de $P(x)$ est μP^m, on a : $\theta \in \mathsf{F}_q^*$. Mais alors : $v_\infty(\theta^2 - c\theta) = -\deg_T c > -md$, et $\theta^2 - c\theta = -\mu P^m$ d'où une contradiction. Fixons donc θ une racine de $P(x)$, on a $\theta \notin B^*$ et $(\theta - c) \notin B^*$. Or $\theta(\theta - c) = -\mu P^m$. Comme $c \neq 0(P)$.Il existe exactement deux premiers β_1, β_2 de B au dessus de P et $\beta_1 \mid \theta$, $\beta_2 \mid \theta - c$. En particulier $[E : K] = 2$. On travaille dans C_∞, on a :

$$v_\infty(\theta) + v_\infty(\theta - c) = -md.$$

Comme $v_\infty(c) = -\deg_T c \geq \frac{-md}{2}$, on a $v_\infty(\theta) < 0$. Supposons que $v_\infty(\theta)$ ou $v_\infty(\theta - c) \neq \frac{-md}{2}$. Quitte à remplacer θ par $\theta - c$, on peut supposer :

$$v_\infty(\theta) < \frac{-md}{2}.$$

Donc :

$$v_\infty(\theta - c) = \inf(v_\infty(\theta), v_\infty(c)) = v_\infty(\theta).$$

D'où la contradiction. ■

Corollaire 125 *1) Soient $\mu \in \mathsf{F}_q^*$ et $c \in \Gamma$, alors si θ est une racine de $x^2 - cx + \mu P^m$, θ est un nombre de Weil ordinaire, si et seulement si $K(\theta)/K$ est imaginaire.*

2)Si $md \equiv 1(2)$, alors $\forall \mu \in \mathsf{F}_q^*$ et $\forall c \in \Gamma$, les racines de $x^2 - cx + \mu P^m$ sont des nombres de Weil.

Pour simplifier notre propos, on suppose $p \neq 2$. Dorenevant $md \equiv 0(2)$.

Lemme 126 *Soit $\mu \in \mathsf{F}_q^*$ et $c \in \Gamma$avec $deg_T\ c \leq \frac{md}{2}$. Soit θ une racine de $x^2 - cx + \mu P^m$. Alors θ est un nombre de Weil, si et seulement si, $-\mu \notin (\mathsf{F}_q^*)^2$.*

Preuve. Par le lemme de Hensel : $P^m \in (K_\infty^*)^2$. On a :

$$v_\infty(\frac{c}{\sqrt{P^m}}\ ) \quad = \frac{md}{2}\ - deg_T\ c > 0.$$

Or $\frac{\theta}{\sqrt{P^m}}$ est racine de :

$$x^2 - \frac{c}{\sqrt{P^m}}x + \mu = 0.$$

Or : $x^2 - \frac{c}{\sqrt{P^m}}x + \mu \equiv x^2 + \mu \quad (\frac{1}{T}\mathsf{F}_q[[\frac{1}{T}]])$.

Par le lemme de Hensel $\theta \notin (\mathsf{F}_q^*)^2 \Leftrightarrow -\mu \notin (\mathsf{F}_q^*)^2$. ■

Lemme 127 *Soit $\mu \in \mathsf{F}_q^*$ et $c \in \Gamma$avec $deg_T\ c = \frac{md}{2}$, et notons c_0 le terme de plus haut degré de c. On suppose $c_0^2 \neq -4\mu$. Soit θ une racine de $x^2 - cx + \mu P^m$. Alors θ est un nombre de Weil, si et seulement si, $x^2 - c_0 x + \mu$ est irréductible dans $\mathsf{F}_q[X]$.*

Preuve. Cette fois ci, on choisit $\sqrt{P^m}$ tel que :

$$\sqrt{P^m}(\frac{1}{T})^{\frac{md}{2}} \equiv 1(\frac{1}{T})$$

Alors : $\frac{c}{\sqrt{P^m}} \equiv 0(\frac{1}{T})$. Donc :

$$x^2 - \frac{c}{\sqrt{P^m}}x + \mu \equiv x^2 - c_0 x + \mu \ \ (\frac{1}{T}).$$

On applique le lemme de Hensel car $x^2 - c_0 x + \mu$ a deux racines simples. ■

Si $c_0^2 = -4\mu$, posons $\Delta = c^2 - 4\mu$. Alors θ est un nombre de Weil, si et seulement si $\deg_T \Delta \equiv 1(2)$ oubien $\deg_T \Delta \equiv 0(2)$ et le terme de plus haut degré de Δ n'est pas un carré dans F_q^*.

On notes quelques remarques sur les nombres de Weil :

1. Les nombres de Weil sont définis pour tous les rangs, ainsi que la bijection précédente.
2. La bijection permet d'avoir le nombre de classes d'isogénies par l'intermédiaire de celui des racines de polynôme caractéristique de Frobenius F de L.
3. Le Frobenius F de L est un nombre de Weil.

Maintenant, on sait d'après [7] et [12] que le polynôme caractéristique P_Φ d'un A-module de Drinfeld de rang 2, s'écrit de quatre façons :

Proposition 128 *Soit Φ un A-module de Drinfeld de rang 2 sur le corps fini $L = \mathsf{F}_{q^n}$ et soit P la caractéristique de L. On pose $m = [L : A/P]$ et $d =$deg P. Le polynôme caractéristique P_Φ est de la forme :*

1)$P_\Phi(X) = X^2 - cX + \mu P^m$, où $c^2 - 4\mu P^m$ est imaginaire, $c \in A$, $(c, P) = 1$ et $\mu \in \mathsf{F}_q^*$; si Φ est ordinaire et dans le cas supersingulier elle est l'un des trois cas suivants :

2)$P_\Phi(X) = X^2 + \mu P^m$, avec $\mu \in \mathsf{F}_q^*$, si m est impaire,

3) $P_\Phi(X) = X^2 + c_0X + \mu P^m$, *si* m *est paire et* $d = \deg P$ *est impaire,* $\mu \in \mathsf{F}_q^*$ *et* $c_0 \in \mathsf{F}_q$.

4)$P_\Phi(X) = (X + \mu P^{\frac{m}{2}})^2$, *si* m *est paire.*

Le cas 1, dans le théorème précédent, correspond à un A-module de Drinfeld ordinaire et les trois autres correspondent aux cas supersinguliers.

On peut tout résumer dans les trois cas suivant :

1. Pour le cas ordinaire, le polynôme caractéristique est de la forme :

$$P_\Phi(X) = X^2 - cX + \mu P^m,$$

tel que : $2 \deg c < \deg P.m$ ou $2 \deg c = \deg P.m$ et $X^2 - a_0X + \mu$ est irréductible sur F_{q^n} où a_0 est le coefficient de plus grande puissance de c. Pour le cas supersingulier on a les deux cas suivants :

2. $\deg P$ est paire ou $-\mu \notin (\mathsf{F}_q^*)^2$.
3. $X^2 + c_0X + \mu$ est irréductible sur F_q.

On est en mesure maintenant de calculer le nombre de ces polynômes caractéristiques qui correspond à celui des classes d'isogénies :

Lemme 129

$$\#\{\textit{classes d'isogénies}\} = \#\{P_\Phi\}.$$

On commence par calculer le cas ordinaire. Le résultat (dans le cas1) nous permet de calculer le nombre général de c, qui correspond au nombre de classes d'isogénies des modules de Drinfeld non supersinguliers, et de calculer autrement le nombre de classes d'isogénies des modules de Drinfeld supersinguliers dans le cas 2,3 et 4.

En effet dans le cas 1, la condition principale qu'on a sur c, autre que sa primalité avec P, est la condition de Riemann qui certifie que le discriminant $c^2-4\mu P^m$ est imaginaire ce qui peut se traduire par : $\deg c \leq \frac{m.d}{2}$.

On distingue, alors deux cas :

1) Le cas où le nombre $m.d$ est impaire, ce qui veut dire que m et d sont impaires. Nous aurons $q^{[\frac{m}{2}d]+1}$ polynômes de degré inférieur ou égal à $[\frac{m}{2}.d]$(où [..] désigne la partie entière). En suite, on élimine les polynômes c qui sont pas premiers avec P autrement dit divisibles par P. On peut remarquer que pour chaque c divisible par P, il existe un polynôme Q tel que $c = Q.P$ alors le cardinal des polynômes c qui sont divisibles par P est égal au cardinal de l'ensemble de Q qui est de l'ordre de $q^{\frac{m-2}{2}d+1}$(car $\deg Q \leq \frac{m-2}{2}d$). En tenant compte du fait que $\mu \in \mathsf{F}_q^*$, nous aurons :

$$\#\{P_\Phi, \Phi : \text{ordinaire}(1)\} = (q-1)(q^{[\frac{m}{2}d]+1} - q^{[\frac{m-2}{2}d]+1}).$$

2) Pour le cas où le nombre $\frac{m}{2}.d$ est paire ce qui veut dire qu'au moins l'un de m ou de d est paire nous serons amenés à écarter le cas où les polynômes minimaux associés aux modules correspondants ne sont pas irréductibles et la condition sur c devient alors :

$\deg c < m.\frac{d}{2}$ et le polynôme $X^2 - a_0X + c$ est irréductible où a_0 est le coefficient de plus grand degré de c, avec la condition de la primalité de c et P nous aurons alors dans ce cas :

$$\#\{P_\Phi \text{ , } \Phi \text{ ordinaire (1)}\} = (q-1)(\tfrac{(q-1)}{2}q^{\frac{m}{2}d} - q^{\frac{m-2}{2}d+1}).$$

Pour le cas où le polynôme caractéristique est de la forme :

$P_\Phi(X) = X^2 + \mu P^m$, où $\mu \in F_{q^n}$ si m est paire. Nous aurons $q-1$ possibilités, et $q^2 - q$ possibilités pour le cas 3, et enfin nous aurons $q-1$ possibilités pour le cas 4.

Ainsi nous sommes en mesure de calculer le cardinal de la classe d'isogénies d'un module de Drinfeld de rang 2 :

Proposition 130 *Soit Φ un A-module de Drinfeld de rang 2 sur le corps fini $L = F_{q^n}$ et soit P la A-caractéristique de L. On pose $m = [L : A/P]$ et $d =$deg P :*

1. *m est impaire et d est impaire :*

$$\#\{P_\Phi, \Phi : ordinaire(1)\} = (q-1)(q^{[\frac{m}{2}d]+1} - q^{[\frac{m-2}{2}d]+1} + 1).$$

2. *m est paire et d est impaire :*

$$\#\{P_\Phi\} = (q-1)[\frac{q-1}{2}q^{\frac{m}{2}d} - q^{\frac{m-2}{2}d+1} + q].$$

3. *m est paire et d est paire :*

$$\#\{P_\Phi\} = (q-1)[\frac{q-1}{2}q^{\frac{m}{2}d} - q^{\frac{m-2}{2}d} + 1].$$

Charactéristique d'Euler-Poincaré

Soit Φ un A-module de Drinfeld de rang 2, sur un corps fini $L = \mathsf{F}_{q^n}$ et de polynôme caractéristique P_Φ. On a vu précédemment que $\chi_\Phi = (P_\Phi(1))$ ce qui nous permet de déduire que si Ψ est un autre A-module de Drinfeld de rang 2, sur le corps fini L de caractéristique P_Ψ et de caractéristique d'Euler-Poincaré χ_Ψ, alors :

$$\chi_\Phi = \chi_\Psi \Longleftrightarrow \exists \lambda \in F_{q^n}^* : P_\Phi(1) = \lambda P_\Psi(1).$$

Ce qui veut dire que le cardinal de l'ensemble de caractéristique d'Euler-Poincaré, peut être déduit de celui des classes d'isogénies et on a la majoration :

$$\#\{\chi_\Phi\} \quad \leq \quad \frac{\#\{P_\Phi\}}{q^n - 1}.$$

Remarque 131

1. La caractéristique d'Euler-Poincaré représente pour un A-module de Drinfeld de rang 2, ce que représente le nombre des points d'une courbe elliptique sur un corps fini.
2. Pour deux courbes elliptiques, il est suffisant d'avoir le même nombre de points pour que les deux courbes soit isogénes, ce qui est plus le cas, pour deux A-modules de Drinfeld car il n'est pas suffisant pour deux A-module de Drinfeld d'avoir la même caractéristique d'Euler-Poincaré pour qu'ils soient isogénes. En effet on sait que deux modules de Drinfeld Φ et Ψ sont isogénes, si et seulement si, $P_\Phi = P_\Psi$, or le fait que $\chi_\Phi = \chi_\Psi$ et équivalent seulement à dire qu'il existe un $\lambda \in F_{q^n}^*$ tel que :

$$P_\Phi(1) = \lambda P_\Psi(1).$$

On peut alors avoir une formule pour le cardinal de l'ensemble des caractéristiques d'Euler-Poincaré :

Proposition 132 *Soit Φ un A-module de Drinfeld de rang 2 sur le corps fini $L = \mathsf{F}_{q^n}$ et soit P la caractéristique de L. On pose $m = [L : A/P]$ et $d =$deg P. Ils existent H, $B \in \mathsf{Z}_{>0}$, tels que :*

$$\#\{\chi_\Phi\} = H + B\ ;$$

où H et B vérifient :

$$\#\{P_\Phi\} = (q-1)H + (q-2)B.$$

Preuve. Soient Φ et Ψ, deux A-modules de Drinfeld sur F_{q^n}, $P_\Phi(1) = 1-c+\mu P^m$ et $P_\Psi(1) = 1-c'+\mu' P^m$. Alors $\chi_\Phi = \chi_\Psi$, si et seulement si il existe $\lambda \in F_{q^n}$, tel que $P_\Phi(1) = \lambda P_\Psi(1)$ donc : $1-c+\mu P^m = \lambda - \lambda c' + \lambda\mu' P^m$. Ce qui nous ramène à : $\mu = \mu'$ et $c' = \lambda^{-1}(1-c+\lambda)$, ce qui veut dire que ces λ sont de l'ordre de $q-2$ (car $\lambda \in F_q - \{0,1\}$) . En plus de la condition de la non primalité avec P, nous aurons, si un tel diviseur Q existe, $Q.P = 1+\lambda+\lambda c'$ et donc $\deg Q = -d + \deg c' \leq \frac{(m-2}{2})d$. Alors le cardinal de ces Q est égal au cardinal de ces c', qui est $q^{[\frac{m}{2}d]+1} - q^{[\frac{m-2}{2}d]+1}$, et qui n'est rien d'autre que le B cherché, donc les couples (λ, t') sont d'ordre $(q-2)(q^{[\frac{m}{2}d]+1} - q^{\frac{[m-2}{2}d]+1})$. On peut avoir H facilement à partir de l'équation : $\#\{P_\Phi\} = (q-1)H + (q-2)B \Longrightarrow H = \frac{1}{q-1}(\#\{P_\Phi\} - (q-2)B)$:

on commence par le cas : 1) m est impaire et d est impaire :

$$H = \frac{1}{q-1}q^{[\frac{m}{2}d]+1} - \frac{1}{q-1}q^{\frac{[m-2}{2}d]+1} + 1.$$

2) m est paire et d est impaire :

$$H = \frac{1+2q-q^2}{2q-2}q^{\frac{m}{2}d} - \frac{1}{q-1}q^{\frac{m-2}{2}d+1} + q.$$

3) m est paire et d est paire :

$$H = \frac{1+2q-q^2}{2q-2}q^{\frac{m}{2}d} - \frac{1}{q-1}q^{\frac{m-2}{2}d+1} + 1.$$

■

A la fin, on récupéra la valeur de $\#\{\chi_\Phi\}$:

Proposition 133 *Soit Φ un A-module de Drinfeld de rang 2 sur le corps fini $L = \mathsf{F}_{q^n}$ et soit P le A- caractéristique de L. On pose $m = [L : A/P]$ et $d =$deg P :*

1. *m est impaire et d est impaire :*

$$\#\{\chi_\Phi\} = \frac{q}{q-1}q^{[\frac{m}{2}d]+1} - \frac{q}{q-1}q^{[\frac{m-2}{2}d]+1} + 1$$

2. *m est paire et d est impaire :*

$$\#\{\chi_\Phi\} = \frac{q^2+1}{2q-2}q^{\frac{m}{2}d} - \frac{q}{q-1}q^{\frac{m-2}{2}d+1} + q$$

3. *m est paire et d est paire :*

$$\#\{\chi_\Phi\} = \frac{q^2+1}{2q-2}q^{\frac{m}{2}d} - \frac{q}{q-1}q^{\frac{m-2}{2}d+1} + 1.$$

2.4.3 Structure de A-module L^Φ

Soit Φ un A-module de Drinfeld de rang 2, sur un corps fini L et de caractéristique P. Pour la structure de A-module L^Φ, on a le résultat suivant :

Proposition 134 *Le A-module de Drinfeld Φ induit une structure de A-module fini L^Φ, qui est de la forme $\frac{A}{I_1} \oplus \frac{A}{I_2}$ où I_1 et I_2 sont deux idéaux de A, tels que : $\chi_\Phi = I_1 I_2$.*

Preuve. Puisque le A-module L^Φ est un sous module de l'A-module :

$\Phi(\chi_\Phi) \simeq \frac{A}{\chi_\Phi} \oplus \frac{A}{\chi_\Phi}$, ils existent donc I_1 et I_2 dans A tels que : $L^\Phi \simeq \frac{A}{I_1} \oplus \frac{A}{I_2}$ et vu le fait que la caractéristique d'Euler-Poincaré est multiplicative sur les suites exactes nous aurons $\chi_\Phi = I_1 I_2$. ■

On pose $I_1 = (i_1)$ et $I_2 = (i_2)$ (i_1 et i_2 deux polynômes unitaires en A).

Soit $i = \text{pgcd}\,(i_1, i_2)$ il est évident d'après le lemme chinois, que la non cyclicité de l'A-module L^Φ, nécessite que I_1 et I_2 ne soient pas premiers entre eux ce qui veut dire que $i \neq 1$, et vu la relation $\chi_\Phi = I_1 I_2$, nous aurons : $i^2 \mid P_\Phi(1)$ $(\chi_\Phi = (P_\Phi(1)))$.

Désormais cette condition sera supposée vérifiée dans le reste, et plus particulièrement on suppose $I_2 \mid I_1$ (i.e : $i_2 \mid i_1$), autrement L^Φ est un A-module cyclique qui s'écrit sous la forme A/χ_Φ.

Proposition 135 *Si* $L^\Phi \simeq \frac{A}{I_1} \oplus \frac{A}{I_2}$ *, alors* $i_2 \mid c-2$.

Preuve. On sait que la structure de A-module L^Φ est stable par l'endomorphisme de Frobenius F de L. On choisit alors une base pour A/χ_Φ, dans la quelle le A-module L^Φ sera engendré par $(i_1, 0)$ et $(0, i_2)$. Soit $M_F \in \mathsf{M}_2(A/\chi_\Phi)$ la matrice de l'endomorphisme de Frobenius F dans cette base. Donc $M_F = \begin{pmatrix} a & b \\ a_1 & b_1 \end{pmatrix}$, où $a, b, a_1, b_1 \in A/\chi_\Phi$. Cependant puisque : Tr $M_F = a + b_1 = c$ et $M_F(i_1, 0) = (i_1, 0)$ et $M_F(0, i_2) = (0, i_2)$, nous aurons $a.i_1 \simeq i_1 (\text{mod}\, \chi_\Phi)$ et donc $a - 1$ est divisible par i_1, de même $b_1.i_2 \simeq i_2 (\text{mod}\, \chi_\Phi)$, ce qui veut dire que $b_1 - 1$ est divisible par i_2 et donc : $c - 2 = a - 1 + b_1 - 1$ est divisible par i_2 (car on a toujours $i_2 \mid i_1$). ■

Soit ρ un idéal premier de A, différent de la A-caractéristique P, on définit le A-module fini $\Phi(\rho)$ comme étant le A-module $(A/\rho)^2$.

Le A-ordre $A + g.O_{K(F)}$, a pour discriminant $\Delta.g^2$, où Δ est le discriminant du polynôme caractéristique $P_\Phi(X) = X^2 - cX + \mu P^m$. Ainsi chaque ordre est défini par son

discriminant et peut être noté par $O($ disc). Il est claire, d'après la proposition 114, que l'inclusion $\Phi(\rho) \subset L^{\Phi}$ implique que $\rho^2 \mid P_{\Phi}(1)$ et $\rho \mid c-2$.

Proposition 136 *Soit Φ un A-module de Drinfeld ordinair, de rang 2, et soit ρ un idéal de A différent de la A-caractéristique P de L, tel que $\rho^2 \mid P_{\Phi}(1)$ et $\rho \mid c-2$. Alors $\Phi(\rho) \subset L^{\Phi}$, si et seulement si, le A-ordre $O(\Delta/\rho^2) \subset End_L\Phi$.*

Pour prouver cette proposition, on a besoin du lemme suivant :

Lemme 137 $\Phi(\rho) \subset L^{\Phi}$ *est équivalent à* $\frac{F-1}{\varrho} \in End_L\Phi$.

Preuve. Puisque $L^{\Phi} = \mathrm{Ker}(F-1)$ et $\Phi(\rho) = \mathrm{Ker}(\rho)$ (on confond par commodité l'idéal ρ avec son générateur dans A) et on sait d'après [3], proposition 4.7.9, que pour deux isogènies, par exemple $F-1$ et ρ , on a $\mathrm{Ker}(F-1) \subset \mathrm{Ker}(\rho)$, si et seulement si, il existe un élément $g \in \mathrm{End}_L\Phi$ tel que $F-1 = g.\rho$ et donc $\Phi(\rho) \subset L^{\Phi}$, si et seulement si, $\frac{F-1}{\varrho} = g \in \mathrm{End}_L\Phi$. ■

On prouve maintenant la proposition 115 :

Preuve. Soit $N(\frac{F-1}{\rho})$ la norme de l'isogénie $\frac{F-1}{\rho}$, qui est un idéal principal engendré par $\frac{P_{\Phi}(1)}{\rho^2}$, et la trace (Tr) de cette isogénie est $\frac{c-2}{\rho}$ donc on est en mesure de calculer le discriminant de A-module $A[\frac{F-1}{\rho}]$ par :

$\mathrm{disc}A([\frac{F-1}{\rho}]) = Tr(\frac{F-1}{\rho})^2 - 4N(\frac{F-1}{\varrho}) = \frac{c^2-4\mu P^m}{\rho^2} = \Delta/\rho^2$, donc :

$O(\Delta/\rho^2) \subset \mathrm{End}_L\Phi$.

On suppose maintenant que : $O(\Delta/\rho^2) \subset \mathrm{End}_L\Phi$ et on prouve que $\Phi(\rho) \subset L^{\Phi}$. L'ordre de discriminant Δ/ρ^2 est $A[\frac{F-1}{\rho}]$ ce qui veut dire que : $\frac{F-1}{\varrho} \in \mathrm{End}_L\Phi$ et donc, d'après le lemme 116 : $\Phi(\rho) \subset L^{\Phi}$. ■

Corollaire 138 *Si* $O(\Delta/\rho^2) \subset \ End_L\Phi$, *alors* L^Φ *est non cyclique .*

Preuve. On sait que $\Phi(\rho)$ est non cyclique (car c'est un A-module de rang 2), et donc les conditions nécessaires et suffisantes pour la non cyclicité du A-module L^Φ sont équivalentes aux conditions nécessaires et suffisantes pour avoir $\Phi(\rho) \subset L^\Phi$. ■

On est alors en mesure de prouver le théorème important suivant :

Théorème 139 *Soient* $M = \frac{A}{I_1} \oplus \frac{A}{I_2}$, $I_1 = (i_1)$ *et* $I_2 = (i_2)$ *, tels que :* $i_2 \mid i_1$, $i_2 \mid (c-2)$. *Alors il existe un* A*-module de Drinfeld* Φ *sur* L *de rang* 2 *ordinaire, tel que :*

$$L^\Phi \simeq M.$$

Preuve. En effet, si on considère le A-module de Drinfeld Φ, pour lequel la caractéristique d'Euler-Poincaré est donnée par $\chi_\Phi = I_1.I_2$ et l'anneau d'endomorphismes est $O(\Delta/i_2^2)$ où Δ est toujours le discriminant du polynôme caractéristique de F. On rappelle que $\Phi(\rho) \subset L^\Phi$ pour tout ρ idéal de A, différent de P et qui vérifie $\rho^2 \mid P_\Phi(1)$ et $\rho \mid (c-2)$, si et seulement si, le A-ordre $O(\Delta/\rho^2) \subset \ \mathrm{End}_L\Phi = A[F]$. Soit maintenant $\rho = i_2$, alors $\Phi(i_2) \simeq (A/i_2)^2 \subset L^\Phi$, si et seulement si, le A-ordre $O(\Delta/i_2^2) \subset \mathrm{End}_L\Phi$ ce qui est vrai par construction. On sait que le A-module L^Φ est inclus ou égal à $\Phi(\chi_\Phi) \simeq \frac{A}{\chi_\Phi} \oplus \frac{A}{\chi_\Phi}$, nous aurons certainement : $L^\Phi = \frac{A}{I_1} \oplus \frac{A}{I_2}$. ■

Le théorème précédent va dans le sens de la conjecture suivante :

Conjecture 140 *Soient* $M \in \mathsf{M}_2(A/\chi_\Phi)$, $\overline{P} = P(\mathrm{mod}\,\chi_\Phi)$. *On suppose :* $(det\ M) = \overline{P}^m$, $Tr\ (M) = c$ *et* c - P. *Il existe alors, un* A*-module de Drinfeld sur* L *de rang* 2*, ordinaire, dont la matrice de Frobenius,* F*, est* M_F*, et tel que :*

$$M_F = M \in \mathsf{M}_2(A/\chi_\Phi).$$

En appliquant la conjecture précédente, on choisit la matrice :

$$M_F = \begin{pmatrix} c-1 & i_1 \\ \\ i_2 & -1 \end{pmatrix} \in \mathsf{M}_2(A/\chi_\Phi).$$

On peut voir facilement que les trois conditions de la conjecture précédente sont vérifiées, il exsite alors un A-module de Drinfeld Φ sur L de rang 2 ordinaire, tel que $L^\Phi \simeq M$.

Chapitre 3

Statistique sur la Cyclicité de Modules de Drinfeld de Rang 2 sur les Corps Finis

Introduction :

A la lumière du travail effectué par S.Vladut dans [18] et qui est motivé par l'intérêt des courbes elliptiques sur les corps fini, dont les points rationnels forment un groupe cyclique, vu l'importance de tels modules dans beaucoup d'applications (voir [18]) et dans le cadre de l'analogie entre les courbes elliptiques sur les corps finis et les modules de Drinfeld de rang 2 sur un corps fini, on essaye ici de faire un travail analogue, à savoir faire une statistique sur les modules de Drinfeld de rang 2, ordinaires (vu le fait que le nombre des modules ordinaires est largement supérieur à celui des modules supersinguliers) sur un corps fini L qui est une extension de degré n d'un corps fini F_q à q éléments, pour lesquels

le A-module induit par Φ sur L et noté L^{Φ}, est un A-module cyclique.

Pour cela : soit $A = \mathsf{F}_q[T]$ et γ le A-homomorphisme d'anneau de $A \to L$, le noyau de cet homomorphisme est noté P et $m = [L, A/P]$ est le degré de l'extension L sur A/P, on note par $C(d, m, q)$, la proportion de A-module de Drinfeld, de rang 2, ordinaire (modulo isomorphisme) dont la structure L^{Φ} est cyclique, et par $C_0(d, m, q)$ la proportion des A-modules de Drinfeld, de rang 2, ordinaires (modulo isogénie) dont les A-modules L^{Φ} sont cycliques, bien sûre ce nombre dépendra de q et aussi de d, m.Un de nos résultats dans ce chapitre consiste à dire que :

$C(d, m, q) = C_0(d, m, q) = 1$, si et seulement si, $m = d = 1$, autrement dit pour avoir un module cyclique il faut que l'extension L soit triviale, nous donnons aussi d'autres valeurs de $C(d, m, q)$ et $C_0(d, m, q)$ dans des cas précis selon la valeur de d et m, par exemple si on note par $H(D)$ le nombre des classes de Hurwitz pour un déterminant imaginaire D (voir [11]) et $P_{\Phi}(X) = X^2 - cX + \mu P^m$, $c \in A$, $\mu \in F_q^*$ le polynôme caractéristique de l'endomorphisme de Frobenius $\mathsf{F} = \tau^n$, on a ces valeurs de $C(d, m, q)$ et $C_0(d, m, q)$ dans le cas où $d = 2$ et $m = 1$:

$$C_0(2, 1,\ q) = \frac{q(q-1) - 5}{q(q-1) - 2},$$

$$C(2, 1,\ q) = \frac{q^3 - q^2 - q + 1 - [\frac{q-1}{2} \sum_{P_{\Phi}} \sum_{i_2, i_2^2 \nmid 4 - 4\mu P} H(O(\frac{4-4\mu P}{i_2^2}) + (q-1) \sum_{P_{\Phi}} \sum_{i_2, i_2^2 \nmid c^2 - 4\mu P} H(O(\frac{c^2 - 4\mu P}{i_2^2})]}{q^3 - q^2 - q + 1}.$$

3.1 Préliminaires :

Dans tout ce chapitre, tous les A-modules de Drinfeld sont ordinaires et de rang 2.

Soient L une extension finie de degré n d'un corps fini F_q à q éléments, $A = \mathsf{F}_q[T]$ et K son corps des fractions .

Soit le A-homomorphisme d'anneau $\gamma : A \to L$ dont le noyau est P et appelé la A-caractéristique de L.

On pose $m = [L : A/P]$ et $d =$deg P, alors $n = m.d$.

Soit $\tau : x \mapsto x^p$ le Frobenius de F_q. Le Frobenius de L est alors $F = \tau^n$, donc $\mathsf{F}_q[F]$ est le centre de $L\{\tau\}$, l'anneau de polynôme d'Ore.

Le polynôme caractéristique de l'endomorphisme de Frobenius $\mathsf{F} = \tau^n$ est de la forme $P_\Phi(X) = X^2 - cX + \mu P^m$, $\mu \in F_q^*$.

Soit $\Delta = c^2 - 4\mu P^m$ le discriminant de ce polynôme caractéristique.

Dans notre cas $A = \mathsf{F}_q[T]$ et un A-module de Drinfeld de rang 2 est de la forme : $\Phi(T) = \gamma(T) + a_1\tau + a_2\tau^2$, $a_1 \in L$ et $a_2 \in L^*$.

Via Φ, l'extension L de F_q devient un A-module par :

$$\begin{aligned} L \times A &\to L, \\ (l, a) &\to l.a := \Phi_a(l) \ . \end{aligned}$$

On notera cet A-module par L^Φ.

On pose $I_1 = (i_1)$ et $I_2 = (i_2)$ (i_1 et i_2 deux polynômes unitaires de A).

On s'intéresse dans ce chapitre à faire quelques statistiques concernant la cyclicité ou la non cyclicité de la structure L^{Φ}, pour un A-module de Drinfeld Φ ordinaire, de rang 2, en utilisant notre résultat principal du chapitre précédent que nous rappelons ici :

Théorème 141 *Soient* $M = \frac{A}{I_1} \oplus \frac{A}{I_2}$, $I_1 = (i_1)$ *et* $I_2 = (i_2)$, *tels que :* $i_2 \mid i_1$, $i_2 \mid (c-2)$. *Alors il existe un* A*-module de Drinfeld* Φ *sur* L *de rang* 2 *ordinaire, tel que :* $L^{\Phi} \simeq M$.

Soit $i = \text{pgcd}(i_1, i_2)$, il est évident d'après le lemme chinois, que la non cyclicité de A-module L^{Φ}, nécessite que I_1et I_2 ne soient pas premiers entre eux ce qui veut dire que $i \neq 1$, et vu la relation $\chi_{\Phi} = I_1 I_2$, nous aurons forcement : $i^2 \mid P_{\Phi}(1)$ $(\chi_{\Phi} = (P_{\Phi}(1)))$.

3.2 Statistique sur la cyclicité de A-module

Du théorème précédent on va faire des statistiques sur les modules de Drinfeld de rang 2, qui ont une structure L^{Φ} cyclique, pour cela nous définissons $C(d, m, q)$ comme étant le rapport de modules de Drinfeld de rang 2 dont la structure L^{Φ} est cyclique sur le nombre des classes de L-isomorphismes de module de Drinfeld de rang 2, ordinaire qu'on note $\#\{\Phi$, isomorphisme, ordinaire$\}$:

$$C(d, m, q) = \frac{\#\{\Phi, L^{\Phi} \text{ cyclique}\}}{\#\{\Phi, \text{ isomorphisme, ordinaire}\}},$$

on définie aussi $N(d, m, q)$ comme étant le rapport de modules de Drinfeld de rang 2 dont la structure L^{Φ} est non cyclique sur le nombre des classes de L-isomorphismes de

module de Drinfeld de rang 2 :

$$N(d,m,q) = \frac{\#\{\Phi, L^{\Phi} \text{ non cyclique}\}}{\#\{\Phi, \text{ isomorphisme, ordinaire}\}}.$$

On remarque que : $0 \leq C(d,m,q),\ N(d,m,q) \leq 1$.

Puisque la cyclicité de la structure L^{Φ} nécessite le fait que $i^2 \mid P_{\Phi}(1)$ et $i_2 \mid (c-2)$, il est naturel d'introduire i (en occurrence i_2) dans le calcule de $C(d,m,q)$ et $N(d,m,q)$.

On fixe le polynôme caractéristique P_{Φ}, c'est à dire la classe d'isogènie de Φ, et on définit :

Définition 142 *On note par* $n(P_{\Phi}, i_2) = \#\{\Phi : L^{\Phi} = \frac{A}{(i_1)} \oplus \frac{A}{(i_2)}\}$.

Remarque 143 *Le nombre* $n(P_{\Phi}, i_2)$ *égal alors au nombre des classes d'isomorphismes* Φ, *dont les A-module* $L^{\Phi} \simeq \frac{A}{(i_1)} \oplus \frac{A}{(i_2)}$, *dans une classe d'isogènie, d'où la correspondance de* Φ *à* i_2.

Pour $n(P_{\Phi}, i_2)$ on a, d'après le théorème 144 :

Lemme 144 *Soit* $P_{\Phi}(X) = X^2 - cX + \mu P^m$, *le polynôme caractéristique d'un A-module de Drinfeld de rang 2, ordinaire et soit* i_2 *un polynôme unitaire de A. Alors : si* $i_2 \mid c-2$ *on a :* $n(P_{\Phi}, i_2) \geq 1$, *sinon* $n(P_{\Phi}, i_2) = 0$.

On peut en déduire :

Corollaire 145 *Avec les notations précédentes :*

$$\#\{\Phi, L^{\Phi} \text{ non cyclique}\} = \sum_{P_{\Phi}} \sum_{i_2, i_2^2 \mid P_{\Phi}(1)} n(P_{\Phi}, i_2).\#\{i_2, i_2^2 \mid P_{\Phi}(1) \text{ et } i_2 \mid (c-2)\},$$

$$\#\{\Phi, L^{\Phi} \text{ cyclique}\} = \sum_{P_\Phi} \sum_{i_2, i_2^2 | P_\Phi(1)} n(P_\Phi, i_2).\#\{i_2, i_2^2 \text{ - } P_\Phi(1) \text{ et } \ i_2 \mid (c-2)\}\,;$$

et si on note par $n_0(P_\Phi, i_2) = \#\{\text{classe d'isogénie de } \Phi : L^{\Phi} = \frac{A}{(i_1)} \oplus \frac{A}{(i_2)}\}$, on a :

$$n_0(P_\Phi, i_2) = 1.$$

On note maintenant par $\#\{\Phi$, isogénie, ordinaire$\}$ le nombre des classes d'isogénies, pour un module Φ ordinaire, on définit alors :

$$N_0(d, m, q) = \frac{\#\{\text{classes d'isogénie de } \Phi,\ L^{\Phi} \text{ non cyclique}\}}{\#\{\Phi, \text{isogénie, ordinaire}\}},$$

de même

$$C_0(d, m, q) = \frac{\#\{\text{Classes d'isogénie de } \Phi,\ L^{\Phi} \text{ cyclique}\}}{\#\{\Phi, \text{isogénie, ordinaire}\}},$$

On peut alors annoncer le lemme :

Lemme 146 *Avec les notations précédentes, on a :*

$$\begin{aligned} N_0(d, m, q) &= \frac{\#\{i_2, i_2^2 \mid P_\Phi(1) \ et\ i_2 \mid (c-2)\}}{\#\{\Phi,\ isogénie,\ ordinaire\}}, \\ N(d, m, q) &= \frac{\displaystyle\sum_{P_\Phi} \sum_{i_2, i_2^2 | P_\Phi(1)} n(\Phi, i_2).\#\{i_2, i_2^2 \mid P_\Phi(1) \ et\ i_2 \mid (c-2)\}}{\#\{\Phi,\ isomorphisme,\ ordinaire\}}, \end{aligned}$$

$$C_0(d, m, q) = \frac{\#\{i_2, i_2^2 \text{ - } P_\Phi(1) \text{ et } i_2 \mid (c-2)\}}{\#\{\Phi, \text{ isogénie, ordinaire}\}},$$

$$C(d, m, q) = \frac{\displaystyle\sum_{P_\Phi} \sum_{i_2, i_2^2 \text{-} P_\Phi(1)} n(\Phi, i_2).\#\{i_2, i_2^2 \text{ - } P_\Phi(1) \text{ et } i_2 \mid (c-2)\}}{\#\{\Phi, \text{ isomorphisme, ordinaire}\}},$$

et $N(d,m,q)+C(d,m,q)=1$, $N_0(d,m,q)+C_0(d,m,q)=1$.

Le calcul de $\#\{\Phi$, isogéne, ordinaire$\}$, pour un A-module Φ ordinaire, a été fait dans le chapitre précédent, comme étant :

Proposition 147 *Soient $L=F_{q^n}$ et P la A-caractéristique de L.*

On pose $m=[L:A/P]$ et $d=$deg P :

1. m est impaire et d est impaire :

$$\#\{\Phi,\ \text{isogénie, ordinaire}\}=(q-1)(q^{[\frac{m}{2}d]+1}-q^{[\frac{m-2}{2}d]+1}+1).$$

2. $m.d$ est paire :

$$\#\{\Phi,\ \text{isogénie, ordinaire}\}=(q-1)(\frac{(q-1)}{2}q^{\frac{m}{2}d}-q^{\frac{m-2}{2}d}+1).$$

Quant au nombre des classes de L-isomorphismes, nous aurons besoin des résultats suivants, pour preuve et détails de la proposition suivante voir [7] :

Proposition 148 *Soit L une extension finie de degré n sur F_q, alors le nombre des classes de L-isomorphismes d'un A-module de Drinfeld de rang 2 sur L est $(q-1)q^n$ si n est impaire et $q^{n+1}-q^n+q^2-q$ sinon.*

Et pour calculer le nombre des classes de L-isomorphismes pour des modules de Drinfeld ordinaires, nous aurons besoin de calculer celui de nombres des classes de L-isomorphismes de Modules de Drinfeld supersinguliers et le soustraire du nombre des classes de L-isomorphismes général calculé précédemment, pour cela, on a d'après [8] :

Proposition 149 *Soit L une extension finie de degré n sur F_q, alors le nombre des classes de L-isomorphismes d'un A-module de Drinfeld de rang 2, supersingulier sur L est $(q^{n_2}-1)$, où $n_2 = pgcd(2,n)$.*

Le calcul de $C(d,m,q)$ sera fait en fonction de la valeur de d et m qui sont deux valeurs majeures pour la détermination de c car deg $c \leq \frac{m.d}{2}$, aussi :

dans le cas $c \neq 2$, $i_2 \mid (c-2) \Rightarrow \deg i_2 \leq \deg c \leq \frac{m.d}{2}$.

Et pour calculer les nombres des classes de L-isomorphismes qui existent dans chaque classe d'isogénie, on a la définition suivante, pour plus de détails voir [11].

Définition 150 *Soit L une extension finie de degré n sur F_q, on définit $W(F)$ comme étant :*

$$W(F) = \sum_{\Phi,\ F=Frobenius(\Phi)} Poid(\Phi)$$

où :

$$Poid(\Phi) = \frac{q-1}{\#Aut_L\Phi}.$$

$W(F)$ est la somme des poids (noté Poid(Φ)) de nombres des classes de L-isomorphismes existants dans chaque classe d'isogénie des modules Φ dont le Frobenius est F.

Pour calculer $\#\mathrm{Aut}_L\Phi$ on a le lemme suivant, pour preuve voir chapitre 2 :

Lemme 151 *Soit Φ un A-module de Drinfeld, ordinaire, de rang 2, sur un corps fini $L = F_{q^n}$, alors : $\#Aut_L\Phi = q-1$.*

En tenant compte du lemme précédent on voit que $\mathrm{Poid}(\Phi) = \frac{q-1}{\#\mathrm{Aut}_L\Phi} = 1$, ce qui veut dire que :

Corollaire 152 *Dans le cas de modules de Drinfeld ordinaires de rang 2, $W(F)$ est le nombre des classes de L-isomorphismes qui existent dans chaque classe d'isogénie.*

Définition 153 *Soit D un discriminant imaginaire et soit l un polynôme dont le carré divise D et soit $h(\frac{D}{l^2})$ le nombre des classes d'un ordre dont le discriminant est $\frac{D}{l^2}$. On définit le nombre des classes de Hurwitz pour un déterminant imaginaire D, noté $H(D)$ par :*

$$H(D) = \sum_{l} \sum_{l^2 \| D} h(\frac{D}{l^2}).$$

Pour d'autres définitions et plus de détails concernant le nombre des classes de Hurwitz, voir [11] et [18].

Lemme 154 *Si α est élément algébrique sur A, pour lequel $O = A[\alpha]$ est un A-ordre , alors disc$(A[\alpha])$ est égal au discriminant du polynôme minimal de α.*

Ce qui nous intéresse est de calculer le $\mathrm{disc}(A[F])$ et d'après le lemme précédent, $\mathrm{disc}(A[F]) = \mathrm{disc}(P_\Phi)$.

Pour calculer le nombre des classes $W(F)$, on a le résultat suivant pour preuve voir [11].

Proposition 155 *Soient L une extension finie de degré n d'un corps F_q et F le Frobenius de L, alors :*

$$W(F) = H(\mathrm{disc}(A[F])).$$

Il nous reste juste de calculer $n(\Phi, i_2)$:

Lemme 156 *Soit P_Φ le polynôme caractéristique d'un A-module de Drinfeld de rang 2, ordinaire, sur un corps fini L tel que $L^\Phi = \frac{A}{(i_1)} \oplus \frac{A}{(i_2)}$, et soit Δ le discriminant du polynôme caractéristique de Frobenius F, alors :*

$$n(P_\Phi, i_2) = H(O(\Delta/i_2^2)).$$

Preuve. On sait que pour avoir $L^\Phi = \frac{A}{(i_1)} \oplus \frac{A}{(i_2)}$, on a certainement :

$\Phi(i_2) \simeq (A/i_2)^2 \subset L^\Phi$, ce qui est équivalent à dire, d'après le chapitre 2, Proposition 136, que le A-ordre $O(\Delta/i_2^2) \subset \mathrm{End}_L\Phi$ où Δ est toujours le discriminant du polynôme caractéristique de F, P_Φ, et que :

$$n(P_\Phi, i_2) = H(O(\Delta/i_2^2)).$$

■

On est alors en mesure de calculer la valeur $C(d, m, q)$ pour certain d et m :

3.3 Le cas : $d = m = 1$

Dans ce cas $L = A/P = \mathsf{F}_q$, le A-module $L^\Phi = A/P$, donc cyclique, ce qui veut dire que $C(1, 1, q) = 1$.

Ce résultat on va le prouver d'une façon plus explicite :

Proposition 157 *Soient $L = F_{q^n}$ et P la A-caractéristique de L, $m = [L, A/P]$, $d = degP$. On suppose $m = d = 1$. Alors :*

$$C(1,1,q) = C_0(1,1,q) = 1.$$

Preuve. $P_\Phi(1) = 1 - c + \mu P^m = 1 - c + \mu P$, le fait que : $i_2^2 \mid P_\Phi(1) \Rightarrow i_2$ est un constant non nul, donc un élément de F_q^*, alors $(i_2) = A$ et $\frac{A}{I_1} \oplus \frac{A}{I_2} = \frac{A}{I_1}$, donc L^Φ est cyclique, ce qui veut dire que $C(1,1,q) = 1 \Rightarrow N(1,1,q) = 0$.

Pour calculer $\#\{i_2, i_2^2 \mid P_\Phi(1) \text{ et } i_2 \mid (c-2)\}$, on doit avoir i_2 un élément de F_q^* et $\deg i_2 > 0 \Rightarrow$

$\#\{i_2, i_2^2 \mid P_\Phi(1) \text{ et } i_2 \mid (c-2)\} = 0$ et donc :

$$N_0(1,1,q) = \frac{\#\{i_2, i_2^2 \mid P_\Phi(1) \text{ et } i_2 \mid (c-2)\}}{\#\{\Phi, \text{ isogénie, ordinaire}\}} = 0$$

$\Rightarrow C_0(1,1,q) = 1$. ■

D'une façon plus précise, on peut annoncer :

Théorème 158 *Soient $L = F_{q^n}$ et P la A-caractéristique de L, $m = [L, A/P]$, $d = degP$. Alors :*

$$C_0(d,m,q) = C(d,m,q) = 1 \Leftrightarrow m = d = 1.$$

Preuve. On vient de voir que $C_0(1,1,q) = C(1,1,q) = 1$.

Inversement et par l'absurde : on suppose : $m.d > 1$ (c'est à dire $m.d \geq 2$), on prend par exemple $m = 1$ et $d = 2$.

Pour avoir $C_0(d, m, q) = C(d, m, q) = 1$, il faut que

$\#\{i_2, i_2^2 \mid P_\Phi(1) \text{ et } i_2 \mid (c-2)\} = 0$, ce qui est pas vrai, car si $c = aT + b$, où $a \in \mathsf{F}_q^*$ et $b \in \mathsf{F}_q$, il suffit d'avoir un i_2 unitaire et tel que : $i_2 \mid (c-2)$, pour cela, on prend : $i_2 = a^{-1}(c-2)$ ce qui reste compatible avec le fait que : $a^{-2}(c-2)^2 \mid 1 - c + \mu P$, car ils existent des solutions pour l'équation en i_2, c-a-d en a et b :

$$a^{-2}(c-2)^2 \mid 1 - c + \mu P \Rightarrow a^{-2}(aT + b - 2)^2 \mid 1 - aT - b + \mu(T^2 + pT + p_0)$$

d'où les équations : $2a^{-1}\mu(b-2) = \mu p_1 - a$ et $\mu[a^{-1}(b-2)]^2 = 1 - b + \mu p_0 \Rightarrow 2^{-1}[\mu p_1 - a] = 1 - b + \mu p_0$ ce qui donne une valeur de a pour chaque valeur de b, d'où plusieurs possibilités de i_2, par exemple $i_2 = T - (\mu(2p_0 - p_1))^{-1}$,

alors $\#\{i_2, i_2^2 \mid P_\Phi(1) \text{ et } i_2 \mid (c-2)\} > 0$ et donc $C(d, m, q) \neq 1$ et $C_0(d, m, q) \neq 1$. Alors :

$$C_0(d, m, q) = C(d, m, q) = 1 \Rightarrow m = d = 1.$$

En tenant compte du fait que pour $m.d > 2$, trouver un i_2, tel que : $i_2^2 \mid P_\Phi(1)$ et $i_2 \mid (c-2)$, devient plus facile.

Ce qui complète la preuve. ■

Remarque 159 *Puisque $n = m.d$, le résultat précédent donne un résultat important concernant la cyclicité de A-module L^Φ en limitant la possibilité de la définition de ces modules, dont le A-module L^Φ est cyclique, sur le corps fini F_q, c'est à dire sur une extension triviale.*

3.4 Le cas : $m = 1$ et $d = 2$

Dans ce cas $n = m.d = 2$, et $n_2 = 2 \Rightarrow \#\{\Phi$, isomorphisme, ordinaire$\} =$

$q^3 - q - (q^2 - 1) = q^3 - q^2 - q + 1$.

Proposition 160 *Soient $L = F_{q^n}$ et P la A-caractéristique de L, $m = [L, A/P]$, $d = degP$. On suppose $m = 1$ et $d = 2$. Alors :*

$$C_0(2, 1, q) = \frac{q(q-1) - 5}{q(q-1) - 2},$$

$$C(2, 1, q) = \frac{q^3 - q^2 - q + 1 - [\frac{q-1}{2} \sum_{P_\Phi} \sum_{i_2, i_2^2 \mid 4 - 4\mu P} H(O(\frac{4-4\mu P}{i_2^2}) + (q-1) \sum_{P_\Phi} \sum_{i_2, i_2^2 \mid c^2 - 4\mu P} H(O(\frac{c^2-4\mu P}{i_2^2})]}{q^3 - q^2 - q + 1}.$$

Preuve. On commence par calculer

$$\frac{\#\{i_2, i_2^2 \mid P_\Phi(1)\}}{\#\{\Phi\,;\, \text{isogénie}\}}.$$

Pour cela, on distingue entre deux cas, le cas où $c = 2$ et le cas où $c \neq 2$.

Alors pour $c = 2$: $i_2^2 \mid P_\Phi(1) \Rightarrow i_2^2 \mid \mu P^m - 1$ ce qui implique que si on pose $i_2 = T + j_2$, $j_2 \in \mathsf{F}_q$ et $P(T) = T^2 + p_1 T + p_0$ où p_1, $p_0 \in \mathsf{F}_q$, irréductibles, nous aurons $p_1 = 2j_2$ et $\mu p_0 - 1 = \mu j_2^2$ nous aurons alors l'équation $\mu[p_0 - \frac{p_1^2}{4}] = 1 \Rightarrow \mu(p_1^2 - 4p_0) = -4$, vu le fait que $p_1^2 - 4p_0$ n'est pas carré car P est irréductible dans A, nous aurons -μ non carré, ce qui veut dire que le nombre de ces μ possibles est $\frac{q-1}{2}$, en tenant compte du fait que p_0, p_1soient fixes, nous aurons $\frac{(q-1)}{2}$ solutions, il reste alors de calculer pour le cas $c \neq 2$,

pour cela , on pose : $i_2 = T + j_2$, $j_2 \in \mathsf{F}_q$ et $c = aT + b$ où $a \in \mathsf{F}_q^*$ et $b \in \mathsf{F}_q$. le fait que $i_2 \mid (c-2) \Rightarrow j_2 = \frac{b-2}{a}$ et puisque $i_2^2 \mid P_\Phi(1)$ nous aurons : $1-(aT+b)+\mu(T^2+p_1T+p_0) = \mu(T+j_2)^2 \Rightarrow 1-b+\mu p_0 = \mu j_2^2$ et $\mu p_1 - a = 2\mu j_2$, alors : $\mu = \frac{a}{p_1-2j_2} = \frac{a}{p_1-2(\frac{b-2}{a})}$ et donc :

$$\frac{a}{p_1-2(\frac{b-2}{a})}[p_0-(\frac{b-2}{a})^2]+1-b=0.$$

Le nombre des solutions de cette équation en (a,b) (p_0, p_1 étant fixés) nous donne

$\#\{i_2, i_2^2 \mid P_\Phi(1) \text{ et } i_2 \mid (c-2)\}$, nous aurons alors $(q-1)$ cas possibles pour i_2.

Alors :

$$\begin{aligned} N_0(2,1,q) &= \frac{\#\{i_2, i_2^2 \mid P_\Phi(1)\}}{\#\{\Phi,\ \text{isogénie, ordinaire}\}} \\ &= \frac{(q-1)+\frac{(q-1)}{2}}{(q-1)[(\frac{q-1}{2})q-1]} \\ &= \frac{\frac{3(q-1)}{2}}{(q-1)[(\frac{q-1}{2})q-1]} \\ &= \frac{3}{q(q-1)-2} \Rightarrow \end{aligned}$$

$$\begin{aligned} C_0(2,1,q) &= 1-\frac{3}{q(q-1)-2} \\ &= \frac{q(q-1)-5}{q(q-1)-2}. \end{aligned}$$

Et Pour $N(2,1,q)$:

$$N(2,1,q) = \frac{\sum_{P_\Phi}\sum_{i_2} n(\Phi,i_2).\#\{i_2, i_2^2 \mid P_\Phi(1) \text{ et } i_2 \mid (c-2)\}}{\#\{\Phi, \text{ isomorphisme, ordinaire}\}}$$

$$= \frac{\sum_{P_\Phi}\sum_{i_2, i_2^2 \not\equiv 4-4\mu P} H(O(\frac{4-4\mu P}{i_2^2}).\frac{q-1}{2} + \sum_{P_\Phi}\sum_{i_2, i_2^2 \not\equiv c^2-4\mu P} H(O(\frac{c^2-4\mu P}{i_2^2})(q-1)}{q^3-q^2-q+1}$$

$$= \frac{\frac{q-1}{2}\sum_{P_\Phi}\sum_{i_2, i_2^2 \not\equiv 4-4\mu P} H(O(\frac{4-4\mu P}{i_2^2}) + (q-1)\sum_{P_\Phi}\sum_{i_2, i_2^2 \not\equiv c^2-4\mu P} H(O(\frac{c^2-4\mu P}{i_2^2})}{q^3-q^2-q+1}.$$

En fin : $C(2,1,q) = 1 - N(2,1,q) =$

$$1 - \frac{\frac{q-1}{2}\sum_{P_\Phi}\sum_{i_2, i_2^2 \Vdash 4-4\mu P} H(O(\frac{4-4\mu P}{i_2^2}) + (q-1)\sum_{P_\Phi}\sum_{i_2, i_2^2 \Vdash c^2-4\mu P} H(O(\frac{c^2-4\mu P}{i_2^2}))}{q^3-q^2-q+1} =$$

$$\frac{q^3-q^2-q+1-[\frac{q-1}{2}\sum_{P_\Phi}\sum_{i_2, i_2^2 \Vdash 4-4\mu P} H(O(\frac{4-4\mu P}{i_2^2})+(q-1)\sum_{P_\Phi}\sum_{i_2, i_2^2 \Vdash c^2-4\mu P} H(O(\frac{c^2-4\mu P}{i_2^2}))]}{q^3-q^2-q+1}. \blacksquare$$

3.5 Le cas : $m = 2$ et $d = 1$

Dans ce cas aussi $n = m.d = 2$, et $n_2 = 2 \Rightarrow \#\{\Phi$, isomorphisme, ordinaire$\} = q^3 - q - (q^2 - 1) = q^3 - q^2 - q + 1$.

Proposition 161 *Soient $L = F_{q^n}$ et P la A-caractéristique de L, $m = [L, A/P]$, $d = degP$. On suppose $m = 2$ et $d = 1$. Alors :*

$$C_0(1,2,q) = \frac{(q-1)q-4}{(q-1)q-2},$$

$$C(1,2,q) = \frac{q^3-q^2-q+1-\sum_{P_\Phi}\sum_{i_2, i_2^2 \Vdash c^2-4\mu P} H(O(\frac{c^2-4\mu P}{i_2^2})}{q^3-q^2-q+1}.$$

Preuve. On pose $i_2 = T + j_2$, $j_2 \in \mathsf{F}_q$ et $P(T) = T + p$ où $p \in \mathsf{F}_q$. On commence par calculer :

$$N_0(1,2,q) = \frac{\#\{i_2, i_2^2 \mid P_\Phi(1)\}}{\#\{\Phi, \text{ isogénie, ordinaire}\}},$$

dans le cas $c = 2$, $i_2^2 \mid P_\Phi(1) = \mu P^2 - 1$ nous aurons : $2\mu p = 2\mu j_2$ $\mu p^2 - 1 = \mu j_2^2$ ce qui veut dire que $p = j_2$ et $\mu(p^2 - j_2^2) = 1$ contradiction, et donc $\#\{i_2, i_2^2 \mid P_\Phi(1)\} = 0$. Pour $c \neq 2$ on

calcule $\#\{i_2, i_2^2 \mid P_\Phi(1) \text{ et } i_2 \mid (c-2)\}$ et on remarque d'abord que : $i_2 \mid (c-2) \Rightarrow j_2 = \frac{b-2}{a}$ et $i_2^2 \mid P_\Phi(1)$ implique que : $2p\mu - a = 2\mu j_2$ et $p^2 + 1 - b = \mu j_2^2$, finalement nous aurons l'équation :

$$p^2 + 1 - b = \frac{a}{2p - 2(\frac{b-1}{a})}(\frac{b-2}{a})^2$$

qui est une équation en (a, b, p) et qui admet $(q-1)$ solutions, vu le fait que p soit fixe, donc :

$$\begin{aligned} N_0(1,2,q) &= \frac{\#\{i_2, i_2^2 \mid P_\Phi(1)\}}{\#\{\Phi \text{ ; isogénie, ordinaire}\}} \\ &= \frac{q-1}{(q-1)((\frac{q-1}{2})q-1)} \\ &= \frac{1}{(\frac{q-1}{2})q-1}\,; \\ \Rightarrow\ & C_0(1,2,q) = 1 - N_0(1,2,q) \\ &= 1 - \frac{1}{(\frac{q-1}{2})q-1)} \\ &= \frac{(q-1)q-4}{(q-1)q-2}. \end{aligned}$$

Et pour $N(1,2,q)$:

$$N(1,2,q) = \frac{\sum_{P_\Phi}\sum_{i_2} n(\Phi, i_2).\#\{i_2, i_2^2 \mid P_\Phi(1) \text{ et } i_2 \mid (c-2)\}}{\#\{\Phi, \text{ isomorphisme, ordinaire}\}}$$

$$= \frac{\sum_{P_\Phi}\ \sum_{i_2, i_2^2 \nmid c^2-4\mu P} H(O(\frac{c^2-4\mu P}{i_2^2})(q-1)}{q^3-q}$$

$$= \frac{\sum_{P_\Phi}\ \sum_{i_2, i_2^2 \nmid c^2-4\mu P} H(O(\frac{c^2-4\mu P}{i_2^2})}{q(q+1)}.$$

En fin :

$$C(1,2,q) = 1 - \frac{\sum_{P_\Phi} \sum_{i_2, i_2^2 \Vdots c^2-4\mu P} H(O(\frac{c^2-4\mu P}{i_2^2})}{q^3-q^2-q-1} = \frac{q^3-q^2-q+1-\sum_{P_\Phi} \sum_{i_2, i_2^2 \Vdots c^2-4\mu P} H(O(\frac{c^2-4\mu P}{i_2^2})}{q^3-q^2-q+1}.$$

■

3.6 $\lim_{q\to\infty} C_0(d,m,q)$ et $\lim_{q\to\infty} C(d,m,q)$ pour $m.d \leq 2$

En vu des calculs de $C_0(d,m,q)$ et $C(d,m,q)$ pour $m.d \leq 2$, fait précédemment, on a :

Corollaire 162 *Soient $L = F_{q^n}$ et P la A-caractéristique de L, $m = [L, A/P]$, $d = degP$. Alors :*

$$\lim_{q\to\infty} C_0(1,1,q) = \lim_{q\to\infty} C_0(1,2,q) = \lim_{q\to\infty} C_0(2,1,q) = 1,$$

$$\lim_{q\to\infty} C(1,1,q) = \lim_{q\to\infty} C(1,2,q) = \lim_{q\to\infty} C(2,1,q) = 1.$$

Preuve. Puisque : $C_0(1,2,q) = \frac{q(q-1)-4}{q(q-1)-2}$, $C_0(2,1,q) = \frac{q(q-1)-5}{q(q-1)-2}$ et $C_0(1,1,q) = 1$,

d'ou on peut voir que pour : $md \leq 2$, $\lim_{q\to\infty} C_0(d,m,q) = 1$.

D'autre part, puisque $C_0(d,m,q) \leq C(d,m,q) \leq 1$ et en passant à la limite, on a :

$\lim_{q\to\infty} C(d,m,q) = 1$, pour $md \leq 2$. ■

En vue des résultats précédents, on est en mesure d'annoncer la conjecture suivante :

Conjecture 163 *Soient $L = F_{q^n}$ et P la A-caractéristique de L, $m = [L, A/P]$, $d = degP$. Alors :*

$$\lim_{q\to\infty} C(d,m,q) = \lim_{q\to\infty} C_0(d,m,q) = 1.$$

Bibliographie

[1] Bruno Angles. Thèse de Doctorat : Modules de Drinfeld sur les corps finis, Université Paul Sabatier-Toulous III, no d'ordre 1872, (1994).

[2] Bruno Angles. One Some Subring of Ore Polynomilas Connected with Finite Drinfeld Modules, J. Algebra 181 (1996), no.2, 507–522.

[3] David Goss. Basic Structures of Function Field Arithmetic, Volume 35 Ergbnise der Mathematik und ihrer Grenzgebiete, Springer.

[4] V.G. Drinfeld. Modules Elliptiques. Math, USSR Sbornik, 94 (136), 594-627, 656, (1974).

[5] V.G. Drinfeld. Modules Elliptiques II Math, USSR Sbornik, 102 (144), No 2, 182-194,325, (1977).

[6] Ernst-Ulrich Gekeler. On Finite Drinfeld Module. J. Algebra 141, (1991), 187-203.

[7] Ernst-Ulrich Gekeler and Brian A. Snyder. Drinfled Modules Over Finite Fields . Drinfeld Modules, Modular Schemes and Application. Alden-biesen, (1996).

[8] Igor Potemine. Thèse de Doctorat : Arithmétiques des Corps Globaux de Fonctions

et Géométrie des Schémas Modulaires de Drinfeld, de l'Université Joseph Fourier(Grenoble I), (1997)

[9] J.P. Serre. Corps Locaux, Hermann (1968).

[10] Joseph. H. Silverman The Arithmetic of Elliptic Curves. Graduate Texts in Mathematics, 106.

[11] J.K.Yu. A Classe Number Relation Over Functions Fields, J. Number Theory, 54, (1995), 318–340.

[12] J-K. Yu. Isogenis of Drinfeld Modules Over Finite Fields, J. Number of Theory 54 (1995), no 1, 161–171.

[13] M. Deuring. Die Typen der Multiplikatorenringe Ellipticher Funktionenkorper, Abh. Math.sem.Univ.Hamburg, 14 (1941), 197-272.

[14] M. A.Tsfasman-S. G. Vladut. Algebraic-Geometric Codes, Mathematics and Applications, Dordrecht et al, (1991).

[15] R. Shoof. Nonsingular Plane Cubic Curves Over Finite Filelds, Journal of combinatory theory, series A 46, (1987), 183-211.

[16] I. Reiner. Maximal Orders. Academic Presse, (1975).

[17] H.G. Ruck. A Note on Elliptic Curves Over Finite Fields. Math. Comp. 49, no179, (1987), 301–304.

[18] S.G. Vladut. Cyclicity Statistics for Elliptic Curves Over Finite Fields, Finite Fields Appl. 5 (1999), no 4, 354–363.

[19] W. C. Waterhouse. Abelian Varieties Over Finite Fields. Ann. Sci. Ecole Norm. Sup2, (1969), 521-560.