Torsion des modules de Drinfeld à coefficients entiers

Alexander Gewirtz *

Prépublication de l'Institut Fourier n° 600 (2003)[1]
http ://www-fourier.ujf-grenoble.fr/prepublications.html

Abstract

Let φ be a Drinfeld $A = \mathbb{F}_q[T]$- module. When φ is defined over A, it induces a new A-module structure on A. We show that for this structure, the set A^{φ}_{tor} of A-rational torsion points is isomorphic to one of the following : $\{0\}$, $A/(T-\alpha)$ ($\alpha \in \mathbb{F}_q$), or $A/(T(T+1))$ (if $q=2$). Next, we prove that if $n \geq 1$, then for all ring B which is integral and of finite type over A, whose field of fractions is an extension of $\mathbb{F}_q(T)$ of degree $\leq n$, and for all Drinfeld A-module defined over B, the set of B-rational torsion points has cardinality $\leq q^{\frac{qn}{q-1}}$.

Résumé

Soit φ un module de Drinfeld défini sur $A = \mathbb{F}_q[T]$. On montre que pour la structure de A-module sur A induite par φ, A^{φ}_{tor} (points de torsion) est borné uniformément en le rang r de φ et qu'il est isomorphe en tant que A-module à l'un des modules suivants : $\{0\}$, $A/(T-\alpha)$ (avec $\alpha \in \mathbb{F}_q$), ou $A/(T(T+1))$ (si $q=2$). Nous démontrons que si $n \geq 1$ est fixé, alors pour tout anneau B entier et de type fini sur A dont le corps de fractions est une extension de $\mathbb{F}_q(T)$ de degré $\leq n$, le cardinal de points de torsion B-rationnels d'un A-module de Drinfeld B-rationnel est majoré par $q^{\frac{qn}{q-1}}$. Enfin, nous retrouvons et précisons dans un contexte plus restreint un résultat de Poonen.

1 Introduction

Soit A une variété abélienne définie sur un corps de nombres K. Le théorème de Mordell-Weil [4] établit que $A(K)$ est un groupe abélien de type fini, c'est-à-dire que $A(K) \simeq A(K)_{tor} \times \mathbb{Z}^r$, où $A(K)_{tor}$ est le groupe fini des points de

*Université Joseph Fourier, UFR de Mathématiques, 100, rue des Maths - B.P. 74, 38402, Saint Martin d'Hères Cedex, France. Email: Alexander.Gewirtz@ujf-grenoble.fr

[1]Mots clés : Module de Drinfeld, torsion, borne uniforme.
Classification mathématique : 11G09

torsion K-rationnels et r un entier ≥ 0. De nombreuses questions restent encore ouvertes. Par exemple, si on fixe la dimension g, et le corps de nombres K, existe-t-il des variétés abéliennes A, définies sur K et de dimension g, de rang arbitraire ? Même pour $g = 1$ et $K = \mathbb{Q}$ ou $\mathbb{Q}(t)$, on ne dispose pas de réponse définitive. Les résultats dans cette direction ont été initiés par Néron [20], mais surtout Mestre [16, 17, 18], puis Fermigier [5], Nagao [19] (voir également [10, 13]).

En ce qui concerne la torsion, la conjecture de la borne uniforme affirme la chose suivante : soient d, g des entiers ≥ 1, alors il existe un entier $B(d, g) \geq 1$ tel que pour toute variété abélienne A de dimension g définie sur un corps de nombres K de degré d, $\mid A(K)_{tor} \mid \leq \ B(d, g)$.

Pour $g \geq 2$, cette conjecture est encore ouverte, et l'on ne dispose essentiellement que de résultats montrant que certains groupes sont des groupes de torsion de Jacobiennes de courbes de genre g [6, 11, 21].

En revanche, pour $g = 1$, qui correspond au cas des courbes elliptiques, cette conjecture est maintenant un théorème, dû à Merel ([15] ; voir également [3, 23] ainsi que [12] pour des résultats sur la p-torsion).

Pour d petit, on dispose de résultats précis sur le groupe des points rationnels de torsion d'une courbe elliptique E définie sur un corps de nombres de degré d, et qui ont été obtenus historiquement avant ceux de Merel. En particulier, pour $d = 1$ (pour $d = 2$, voir les résultats de Kamienny [9]), le théorème de Mazur [14] donne la liste des quinze groupes $E(\mathbb{Q})_{tor}$ possibles.

Cet article s'attache à certaines de ces questions. Dans la deuxième partie, nous rappelons le concept de module de Drinfeld, l'analogie avec les courbes elliptiques, ainsi que certains résultats. Dans la troisième partie, nous précisons la structure induite par un module de Drinfeld. Dans la quatrième partie, nous étudions la torsion d'un module de Drinfeld et obtenons un analogue du théorème de Mazur et donc de la conjecture de la borne uniforme dans ce cas. Plus précisement, nous montrons que pour un $\mathbb{F}_q[T]$-module de Drinfeld rationnel, le module des points de torsion sur $\mathbb{F}_q[T]$ est isomorphe à l'un des modules suivants :

- (i) Si $q = 2$: $\{0\}$, $\mathbb{F}_q[T]/(T)$, $\mathbb{F}_q[T]/(T + 1)$, $\mathbb{F}_q[T]/(T^2 + T)$.
- (ii) Si $q > 2$, $\{0\}$, $\mathbb{F}_q[T]/(T - a)$, pour $a \in \mathbb{F}_q$.

Enfin, dans la dernière partie, nous obtenons d'une part un analogue du théorème de Merel et d'autre part nous retrouvons et précisons dans un cadre plus restreint un résultat de Poonen [24]. Plus précisement, nous montrons que si $n \geq 1$ est fixé, il existe une constante $C(q, n)$ ne dépendant que de q et n telle que, pour tout anneau B entier et de type fini sur $\mathbb{F}_q[T]$ vérifiant $[L : \mathbb{F}_q(T)] \leq n$, où L désigne le corps des fractions de B, et pour tout $\mathbb{F}_q[T]$-module de Drinfeld B-rationnel, le module des points de torsion B-rationnels est de cardinal $\leq C(q, n)$. Nous montrons qu'une valeur convenable pour $C(q, n)$ est $q^{\frac{nq}{q-1}}$.

Remerciements : je tiens à remercier Franck Leprévost et Alexeï Pantchichkine pour les nombreuses discussions que nous avons eues ainsi que pour les conseils qu'ils m'ont donnés.

2 Rappels sur les modules de Drinfeld

Soit p un nombre premier, m un entier ≥ 1, et $q = p^m$. On considère $A = \mathbb{F}_q[T]$, $k = \mathbb{F}_q(T)$, $k_\infty = \mathbb{F}_q((T^{-1}))$ (la complétion de k par rapport à la valeur absolue définie par $| \frac{f}{g} |_\infty = q^{\deg f - \deg g}$). Soit également $\Omega = \hat{\bar{k}}_\infty$ (la complétion d'une clôture algébrique fixée de k_∞). On peut alors formuler l'analogie suivante entre courbes elliptiques définies sur un corps de nombres et modules de Drinfeld :

$$
\begin{array}{rcl}
\mathbb{Z} & \longleftrightarrow & A = \mathbb{F}_q[T] \\
\mathbb{Q} & \longleftrightarrow & k = \mathrm{Frac}(A) = \mathbb{F}_q(T) \\
\mathbb{R} & \longleftrightarrow & k_\infty = \mathbb{F}_q((T^{-1})) \\
\mathbb{C} & \longleftrightarrow & \Omega = \hat{\bar{k}}_\infty \\
\mathbb{Z} - \text{module} & \longleftrightarrow & A - \text{module} \\
E \text{ (courbe elliptique)} & \longleftrightarrow & \varphi \text{ (module de Drinfeld sur A)} \\
K \text{ corps de nombres} & \longleftrightarrow & L \text{ extension finie de } k \\
E \text{ définie sur } K & \longleftrightarrow & \varphi \text{ défini sur } L \\
\text{groupe abélien } \mathrm{Hom}(E, E') & \longleftrightarrow & A - \text{module } \mathrm{Hom}(\varphi, \psi) \\
\text{anneau } \mathrm{End}_{\mathbb{Q}}(E) & \longleftrightarrow & \text{anneau } \mathrm{End}_k(\varphi) \\
\text{algèbre } \mathrm{End}_{\mathbb{Q}}(E) \otimes \mathbb{Q} & \longleftrightarrow & \text{algèbre } \mathrm{End}_k(\varphi) \otimes_A k \\
\Lambda \text{ réseau de } \mathbb{C} & \longleftrightarrow & A - \text{module libre et discret } \Lambda
\end{array}
$$

De manière formelle, soit τ l'endomorphisme de Frobienus défini sur Ω par $\tau(x) = x^q$. Dans toute la suite, on identifiera un élément de $a \in \Omega$ avec l'endomorphisme de multiplication par a.

On appelle module de Drinfeld (voir [22] ; pour une définition plus générale, voir [2, 8]) de rang d sur Ω toute application φ de A dans $\Omega\{\tau\}$ vérifiant les conditions suivantes :

- (i) φ est un morphisme d'anneaux
- (ii) $\deg_\tau \varphi(T) = d$
- (iii) $\forall a \in A, D\varphi(a)(z) = az$ où $D\varphi_a(z)$ désigne la partie linéaire

Dans le cas des courbes elliptiques, le théorème d'uniformisation de Riemann établit une correspondance entre courbes elliptiques sur $\mathbb{C}$ et réseaux de $\mathbb{C}$. Le cas des modules de Drinfeld est tout à fait analogue :

Théorème 2.1 [7, 22] *Soit φ un module de Drinfeld de rang d. Alors :*

- (1) *Il existe une unique fonction entière $e(z) = \sum_{n \geq 0} a_n z^{q^n}$ avec $a_0 = 1$ sur Ω telle que $\forall a \in A, \forall z \in \Omega, e(az) = \varphi_a(e(z))$*
- (2) *$\Lambda = Ker(e) = \{z \in \Omega, e(z) = 0\}$ est un A-module libre de rang d et discret*

La fonction e ici est l'analogue de la fonction $\mathcal{P}$ de Weierstrass pour les courbes elliptiques.

Corollaire 2.2 [7] *Si $a \in A \setminus \{0\}$, alors $E_a = ker\varphi_a$ est un $A/(a)$-module libre de rang d (pour l'action via φ de A sur E_a)*

Dans le cas d'une courbe elliptique E définie sur $\mathbb{C}$, si $n \geq 2$, alors le groupe des points de n-torsion $E(\mathbb{C})[n]$ est isomorphe à $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Ce corollaire met en évidence les similitudes entre courbes elliptiques et modules de Drinfeld.

Réciproquement, à tout A-réseau de Ω on peut associer un module de Drinfeld :

Théorème 2.3 [7, 22] *Soit Λ un sous-A-module libre de rang d discret de Ω. Alors :*

- *(i) L'application e_Λ de Ω dans Ω définie par $e_\Lambda(z) = z\prod_{a\in\Lambda\setminus\{0\}}(1-\frac{z}{a})$ définit une fonction entière $\mathbb{F}_q$-linéaire sur Ω.*
- *(ii) $\forall a \in A, e_\Lambda(az) = ae(z)\prod_{0\neq\alpha\in a^{-1}\Lambda/\Lambda}\left(1-\frac{e_\Lambda(z)}{e_\Lambda(\alpha)}\right)$*
- *(iii) Pour tout $a \in A$, il existe un unique polynôme $\mathbb{F}_q$-linéaire φ_a tel que $\forall z \in \Omega, e_\Lambda(az) = \varphi_a(e_\Lambda(z))$*
- *(iv) L'application φ qui à un élément $a \in A$ associe le polynôme φ_a est un module de Drinfeld de rang d.*

3 Groupe de Mordell-Weil d'un module de Drinfeld

On se place ici dans le cas où $\varphi : A \to A\{\tau\}$ et on considère la nouvelle structure de A-module sur A induite par φ :

$$\begin{array}{rcl} A \times A & \to & A \\ (a, x) & \to & a.x = \varphi_a(x) \end{array}$$

A^φ désignera dans ce qui suit l'ensemble A muni de cette structure de A-module : c'est l'analogue du groupe de Mordell-Weil pour les variétés abéliennes. A^φ_{tor} désignera le A-module de torsion.

Dans la première section, on a vu que si l'on considère un module de Drinfeld à valeurs dans $\Omega\{\tau\}$, alors pour tout $a \in A$ non nul, les points de a-torsion forment un $A/(a)$-module libre de rang r. En particulier, on a une infinité de points de torsion. Dans le cas présent, c'est-à-dire le cas où φ est à valeurs dans $A\{\tau\}$ (φ est A-rationnel), on peut remarquer les deux choses suivantes :

Proposition 3.1 *Soit $\varphi : A \to A\{\tau\}$ un module de Drinfeld de rang r. Alors :*

- *(1) A^φ_{tor} est fini.*
- *(2) A^φ n'est pas de type fini sur A.*

Remarque : Nous proposons ici une démonstration élémentaire et constructive, différente de celle de [1, 25, 26], où ces résultats sont établis dans un cadre plus général.

Notons $\varphi_T = b_0 + b_1\tau + \cdots + b_r\tau^r$ où $b_0 = T$, $b_i \in A$ pour $i \geq 1$ et $b_r \neq 0$. Lorsque $a \in A$ est de degré suffisamment élevé, on a $\deg(\varphi_T(a)) = \deg(b_r) + q^r\deg(a)$. Ce qui montre que a n'est pas de torsion. Ceci établit le premier point : à savoir que A^{φ}_{tor} est fini.

Montrons à présent que A^{φ} n'est pas de type fini. Pour cela, on va exhiber une famille infinie d'éléments de A qui soit A-libre.

On note $b = \deg(b_r)$, $b \geq 0$ puisque φ est de rang r. Considérons alors la suite d'entiers i_n définie par $i_0 = b - 1 + \lambda q$ (où λ est un entier tel que T^{i_0} ne soit pas de torsion), et $i_{n+1} = i_n + q$.

Lemme 3.2 *La suite $(T^{i_n})_{n\in\mathbb{N}}$ est une famille A-libre de A^{φ}.*

On raisonne par l'absurde. Supposons que $\sum_{m=0}^{n} A_m.T^{i_m} = 0$ où $A_i \in A$ (non tous nuls). Par définition de A^{φ}, ceci équivaut à : $\sum_{m=0}^{n} \varphi_{A_m}(T^{i_m}) = 0$ Mais par construction, T^i_m n'est pas de torsion pour tout entier m. D'après ce qui précède, on a donc pour tout indice m apparaissant dans la somme pour lequel $A_m \neq 0$, en posant $a_m = \deg(A_m)$: $\deg(\varphi_{A_m}(T^{i_m})) = \frac{q^{a_m r}-1}{q^r-1}b + q^{a_m r}i_m$ Montrons alors que ces degrés sont deux à deux distincts. Ceci permettra de conclure puisque dans ce cas le degré de la somme sera non nul (puisque au moins A_m est non nul), ce qui contredit la nullité de cette même somme. On suppose donc que : $\frac{q^{a_m r}-1}{q^r-1}b + q^{a_m r}i_m = \frac{q^{a_l r}-1}{q^r-1}b + q^{a_l r}i_l$. En multipliant cette expression par $q^r - 1$ (qui est non nul), on obtient : $q^{a_m r}b - b + (q^r-1)q^{a_m r}i_m = q^{a_l r}b - b + (q^r-1)q^{a_l r}i_l$. Soit encore :

$$((q^r-1)i_m + b)\, q^{a_m r} = ((q^r-1)i_l + b)\, q^{a_l r}$$

On distingue alors deux cas :

- $a_m = a_l$: dans ce cas, on a $i_m = i_l$, ce qui n'est pas possible pour deux indices l et m distincts.
- $a_m \neq a_l$: quitte à échanger les indices, on peut supposer $a_m < a_l$. Dans ce cas, l'équation précédente peut s'écrire sous la forme :

  $$(q^r-1)i_m + b = ((q^r-1)i_l + b)\, q^{(a_l - a_m)r}$$

  Mais le membre de gauche de la dernière égalité est congru à zéro modulo q (puisque $a_l - a_m > 0$) alors que le membre de droite vérifie :

  $$(q^r-1)i_m + b \equiv -i_m + b \bmod q \equiv 1 \bmod q$$

  Ce qui est impossible. Ceci montre bien que les degrés sont deux à deux distincts et achève la preuve du lemme.

4 Borne uniforme et structure de A^{φ}_{tor}

Dans ce paragraphe, nous étudions le A-module A^{φ}_{tor} qui est fini d'après ce qui précède. En appliquant la méthode précédente (consistant à évaluer le degré de $\varphi_T(a)$ en fonction du degré de a), on peut montrer que pour $r = 1$, la torsion est majorée par q si $q \neq 2$ et par 4 si $q = 2$. En revanche, il est facile de vérifier

que pour $r = 2$ la torsion est majorée par q. En étudiant de manière précise le comportement du degré de $\varphi_T(a)$ en fonction du degré de a, on peut montrer que la torsion est majorée par $q^{\mathrm{Max}(2,r)}$.

Mais la borne précédente n'étant pas optimale (pour $r = 2$ par exemple) on cherche à l'améliorer. Dans ce paragraphe, nous montrons d'abord que la borne uniforme est indépendante de r et nous donnons les structures possibles de A^{φ}_{tor}. Le théorème suivant est une sorte d'analogue (beaucoup plus élémentaire) du théorème de Mazur évoqué dans l'introduction.

Théorème 4.1 *Pour tout module de Drinfeld A-rationnel de rang r, on a :*

- *(1) Si $q = 2$, alors $\mid A^{\varphi}_{tor} \mid \leq q^2$.*
  De plus A^{φ}_{tor} est isomorphe (en tant que A-module) à l'un des modules suivants :
  $$\{0\}\ ,\ A/(T)\ ,\ A/(T+1)\ ,\ A/(T(T+1))$$

- *(2) Si $q > 2$, alors $\mid A^{\varphi}_{tor} \mid \leq q$.*
  De plus A^{φ}_{tor} est isomorphe (en tant que A-module) à l'un des modules suivants :
  $$\{0\}\ ,\ A/(T-\alpha)\ \text{avec}\ \alpha \in \mathbb{F}_q$$

- *(3) Enfin, si l'on fixe $r \geq 1$ ($r \neq 2$ si $q = 2$) et B l'un des modules cycliques précédents, il existe un module de Drinfeld de rang r dont la torsion est isomorphe à B.*

On commence par démontrer deux lemmes :

Lemme 4.2 *Soit f un polynôme non constant et P un point de f-torsion pour φ (de rang r quelconque). Alors :*

$$P \neq 0 \Rightarrow P^{q-1} \mid f^s$$

pour un entier $s \geq 1$.

En effet, soit $n = \deg(f)$ et $s \geq 1$. Il existe $c_1, \ldots, c_{nrs} \in A$ tels que :

$$\varphi_{f^s} = f^s + \sum_{i=0}^{nrs} c_i \tau^i$$

Maintenant, si P est un point de f-torsion non nul, alors il existe un s tel que :

$$0 = \varphi_{f^s}(P) = f^s P + \textstyle\sum_{i=0}^{nsr} c_i P^{q^i} = P(f^s + \sum_{i=0}^{nrs} c_i P^{q^i-1})$$

P étant non nul et A intègre, on en déduit que :

$$f^s = -\textstyle\sum_{i=0}^{nsr} c_i P^{q^i-1} = P^{q^{i_0}-1}(-\sum_{i=i_0}^{nsr} c_i P^{q^i-q^{i_0}})$$

où i_0 est le plus petit entier tel que $c_{i_0} \neq 0$ (un tel entier existe puisque c_{nrs} est non nul).

Il s'ensuit que P^{q-1} divise f^s (puisque $(q-1)$ divise $(q^{i_0}-1)$) et le lemme est démontré.

Lemme 4.3 *Soit $f \in A$ unitaire irréductible et $A^\varphi[f]$ le A-module des points de f-torsion (i.e. annulés par une puissance de f). Alors*

$$dim_{\mathbb{F}_q}(A^\varphi[f]) \leq 1$$

Tout d'abord, notons que, φ_a étant $\mathbb{F}_q$-linéaire pour tout $a \in A$, les points de f-torsion forment bien un $\mathbb{F}_q$-espace vectoriel.

Supposons que $\dim_{\mathbb{F}_q}(A^\varphi[f]) \geq 2$. Soit alors (P_1, P_2) une famille $\mathbb{F}_q$-libre de $A^\varphi[f]$. Quitte à les multiplier par une constante non nulle, on peut les supposer unitaires. Pour $i \in \{1,2\}$, P_i est un point de f-torsion donc d'après le lemme précédent, on en déduit que P_i^{q-1} divise f^{α_i} pour un entier $\alpha_i \geq 1$. P_i étant unitaire et f unitaire irréductible, il s'ensuit que $P_i = f^{a_i}$ où a_i est un entier vérifiant $(q-1)a_i \leq \alpha_i$. On distingue alors deux cas :

- Si $a_1 = a_2$ alors $P_1 = P_2$ ce qui contredit le fait que (P_1, P_2) est une famille $\mathbb{F}_q$-libre.
- Sinon, quitte à échanger les indices $a_1 < a_2$. Mais alors

$$P_1 + P_2 = f^{a_1}(1 + f^{a_2 - a_1})$$

  Or $P_1 + P_2$ est également un point de f-torsion donc divise une puissance de f d'après le lemme précédent, ce qui est contradictoire avec la dernière égalité.

Ceci achève la preuve du lemme. Terminons à présent la preuve du théorème : on désigne par S l'ensemble A^φ_{tor} muni de sa structure de $\mathbb{F}_q$-espace vectoriel. De plus, A^φ_{tor} étant fini, il est a fortiori de dimension finie sur $\mathbb{F}_q$: soit n cette dimension. Par ailleurs, soit $\Phi \in \mathrm{End}_{\mathbb{F}_q}(S)$ défini par $\Phi(P) = \varphi_T(P)$, M_Φ son polynôme minimal et $M_\Phi = f_1^{\alpha_1} \dots f_s^{\alpha_s}$ la décomposition de M_Φ en facteurs irréductibles. Alors :

$$S \simeq \bigoplus_{i=1}^{s} A^\varphi[f_i]$$

En effet, A^φ_{tor} est la somme directe des modules de f-torsion (la somme étant prise sur tous les polynômes irréductibles unitaires) mais si f est irréductible et distinct des f_i ,$1 \leq i \leq s$, alors il existe $u, v \in A$ tels que $uf + vM_\Phi = 1$. En appliquant cette égalité à Φ, on en déduit donc que $\varphi_u \varphi_f = \mathrm{Id}_S$. Par suite, $A^\varphi[f]$ est réduit à zéro. En regardant alors les dimensions, il vient :

$$n = \dim_{\mathbb{F}_q}(S) = \dim_{\mathbb{F}_q}(\bigoplus_{i=1}^{s} A^\varphi[f_i]) = \sum_{i=1}^{s} \dim_{\mathbb{F}_q}(A^\varphi[f_i]) \leq \sum_{i=1}^{s} 1 \leq s$$

Mais l'inégalité inverse découle du fait que le degré de M_Φ est inférieur ou égal à n (Cayley-Hamilton). Par suite, $s = n$, $\forall i \in \{1, \dots, n\}$, $\alpha_i = 1$, $\deg(f_i) = 1$ et $\dim_{\mathbb{F}_q}(A^\varphi[f_i]) = 1$.

Ceci entraîne donc que

$$A_{tor}^{\varphi} \simeq \bigoplus_{i=1}^{n} A/(T-a_i)$$

où l'on a posé $f_i = T - a_i$ pour tout entier $1 \leq i \leq n$. On distingue maintenant deux cas :

- Si $q > 2$
  Pour $1 \leq i \leq n$, soit P_i un générateur de $A^{\varphi}[f_i]$, alors d'après le lemme, $P_i^{q-1} \mid (T-a_i)$. Par suite, P_i est constant donc $A_{tor}^{\varphi} \subset \mathbb{F}_q$ et $n \leq 1$. De plus, si $n = 1$, alors $A_{tor}^{\varphi} \simeq A/(T-\alpha)$ pour $\alpha \in \mathbb{F}_q$. Ce qui démontre le point (2) du théorème.

- Si $q = 2$
  Le même raisonnement montre que les générateurs de $A^{\varphi}[f_i]$ sont de degré inférieur ou égal à un. Par suite $n \leq 2$.
  De plus, si $n = 1$, alors d'après la décomposition de S trouvée ci-dessus, les points de torsions sont isomorphes au quotient de A par un polynôme de degré 1, i.e. par T ou $T+1$ (car $q = 2$).
  Enfin, si $n = 2$, A_{tor}^{φ} est isomorphe $A/(T-a) \oplus A/(T-b)$. Mais ces facteurs sont premiers entre eux (ce sont les facteurs irréductibles de M_{Φ}). Par suite, $A_{tor}^{\varphi} \simeq A/((T+1)T)$ (puisque $q = 2$). Ce qui démontre le point (1) du théorème.

En ce qui concerne le point (3), il est facile de vérifier que :

- Si $q > 2$ alors pour tout $r \geq 1$
  - pour $\varphi_T = T + (\alpha - T)\tau^r$, $A_{tor}^{\varphi} \simeq A/(T-\alpha)$.
  - pour $\varphi_T = T + \tau^r$, $A_{tor}^{\varphi} = \{0\}$.

- Si $q = 2$ et $r \geq 3$:
  - pour $\varphi_T = T + (T^{2^r-2}+1)\tau + \tau^r$ alors $A_{tor}^{\varphi} \simeq A/(T)$.
  - pour $\varphi_T = T + T\tau + \tau^r$ alors $A_{tor}^{\varphi} \simeq A/(T+1)$.
  - pour $\varphi_T = T + g_r\tau + g_r\tau^2 + \tau^r$ où l'on a posé $g_r = \sum_{i=0}^{2^{r-1}-2} T^i$ alors $A_{tor}^{\varphi} \simeq A/(T(T+1))$.

Ce qui achève la démonstration du théorème.

5 Borne uniforme pour les extensions entières finies de A

Dans ce dernier paragraphe, nous démontrons l'analogue du théorème de Merel évoqué dans l'introduction.

Théorème 5.1 *Soit $n \geq 1$ fixé. Alors pour tout anneau B entier et de type fini sur A vérifiant $[L : k] \leq n$ (où L désigne le corps de fractions de B) et pour tout module de Drinfeld B-rationnel φ,*

$$\mid B_{tor}^{\varphi} \mid \leq \; q^{\frac{nq}{q-1}}$$

Preuve :

Soit B comme dans l'énoncé du théorème et φ un module de Drinfeld A-rationnel de rang $r \geq 1$. On a alors par définition, $\varphi_T = b_0 + b_1\tau + \cdots + b_r\tau^r$ où $b_0 = T$, $b_i \in A$ pour $1 \leq i \leq r$ et $b_r \neq 0$. Considérons ω la valuation discrète de k associée au polynôme T et soit ν une valuation discrète de L au-dessus de ω. On note O_ω (resp. O_ν) l'anneau de valuation de ω (resp. ν) et π_ω (resp. π_ν) une uniformisante pour ω (resp. ν). On notera par la suite $e = e(\nu/\omega)$ l'indice de ramification de ν par rapport à ω, et $f = f(\nu/\omega)$ le degré résiduel.

On remarque alors pour commencer que d'une part, $A \subset O_\omega$, et d'autre part $B \subset O_\nu$ (puisque B est entier sur A). On distingue alors deux cas :

- 1er cas : $\forall i \in \{1, \ldots, r\}$, $\nu(b_i) \geq e$
  Il est alors facile de constater que $B_{tor}^\varphi \subset O_\nu^\star$. Or, $\mathbb{F}_q \simeq O_\omega/\pi_\omega$ et donc $[O_\nu/\pi_\nu : \mathbb{F}_q] = f$. Par suite, $\dim_{\mathbb{F}_q}(B_{tor}^\varphi) \leq f \leq n$.
- 2ème cas : $\exists i \in \{1, \ldots, r\}$, $\nu(b_i) < e$
  Dans ce cas, on a :

$$\nu(b) > \frac{e}{q-1} \quad \Rightarrow \quad \nu(\varphi_T(b)) = \nu(b) + e$$

  Ceci montre que les points de torsion sont de valuation comprise entre 0 et $\frac{e}{q-1}$. Soit N la partie entière de $\frac{e}{q-1}$ et $B_i = B_{tor}^\varphi \cap \{x \in L, \nu(x) \geq i\}$ pour $0 \leq i \leq N$. On constate alors d'une part que $\dim_{\mathbb{F}_q}(B_N) \leq f$, et d'autre part que pour tout $0 \leq i \leq N-1$, $\dim_{\mathbb{F}_q}(B_i/B_{i+1}) \leq f$. Par suite,

$$\dim_{\mathbb{F}_q}(B_{tor}^\varphi) = \sum_{i=0}^{N-1} \dim_{\mathbb{F}_q}(B_i/B_{i+1}) + \dim_{\mathbb{F}_q}(B_N) \leq (N+1)f$$

  On en déduit donc que $\mid B_{tor}^\varphi \mid \ \leq q^{(N+1)f} \leq q^{\frac{ef}{q-1}+f} \leq q^{\frac{qn}{q-1}}$

Ceci achève la preuve du théorème.

D'autre part, jusqu'ici nous nous sommes intéréssés aux modules de Drinfeld à coefficients entiers. Il est naturel de se demander si ces résultats s'étendent au cas des extensions finies de $\mathbb{F}_q(T)$. On ne peut cependant pas s'attendre à trouver des bornes identiques. En effet, nous avons démontré que la torsion des modules de Drinfeld à coefficients entiers est borné uniformément, indépendament du rang. Ceci n'est plus vrai lorsque les coefficients ne sont plus entiers. En effet, si W est un sous-espace vectoriel de dimension finie r de $k = \mathbb{F}_q(T)$, alors $P = \prod_{w \in W}(X - w)$ est un polynôme $\mathbb{F}_q$-linéaire, donc de la forme $P_0 x + ... + P_r x^{q^r}$. En considérant $\varphi_T = T + ... + \frac{P_r}{P_0}\tau^r$, on constate que la torsion contient W, donc est de cardinal au moins q^r.

Parmi les questions ouvertes, citons les conjectures suivantes [24] :

Conjecture 5.2 *Soit $r \geq 1$ et L une extension finie de $k = Frac(A)$ fixés. Alors il existe une constante $B(r, L)$ telle que pour tout module de Drinfeld L-rationnel de rang r, le cardinal de L_{tor}^φ soit majoré par $B(r, L)$.*

Conjecture 5.3 *Soit $r \geq 1$ et $d \geq 1$ fixés. Alors il existe une constante $B(r,d)$ telle que pour toute extension finie de k de degré inférieur ou égal à d et pour tout module de Drinfeld rationnel de rang r, le cardinal de L_{tor}^{φ} soit majoré par $B(r,d)$.*

Poonen [24] a démontré que la conjecture 5.3 est vraie pour $r = 1$ dans un cadre plus général : à savoir lorsque A désigne l'anneau des fonctions régulières d'une courbe affine obtenue en retirant un point fermé "∞" d'une courbe projective lisse X définie sur $\mathbb{F}_q$.

La méthode précédente permet de retrouver et de préciser ce résultat lorsque $A = \mathbb{F}_q[T]$:

Corollaire 5.4 *Soit $n \geq 1$ alors pour toute extension finie L de k de degré $\leq n$ et pour tout module de Drinfeld de rang 1 L-rationnel, le cardinal de L_{tor}^{φ} est majoré par $q^{\frac{nq}{q-1}}$.*

Soit L/k une extension de degré $\leq n$ et φ un A-module de Drinfeld L-rationnel de rang 1. Notons $\varphi_T = T + B\tau$ où $B \in L^\star$. Soit ω la valuation normalisée de k associée au polynôme T et ν un prolongement de ω à L. On note e (respectivement f) l'indice de ramification (resp. le degré résiduel) de ν par rapport à ω. De même que précédement, on remarque que :

$$\begin{aligned} \nu(x) > \frac{e - \nu(B)}{q-1} &\quad \Rightarrow \quad \nu(\varphi_T(x)) = \nu(x) + 1 \\ \nu(x) < \frac{-\nu(B)}{q-1} &\quad \Rightarrow \quad \nu(\varphi_T(x)) < \nu(x) \end{aligned}$$

On en déduit donc que les points de torsion L-rationnels sont de valuation comprise entre $\frac{-\nu(B)}{q-1}$ et $\frac{e-\nu(B)}{q-1}$. Mais ν est à valeurs entières. Par suite, il y a au plus $\frac{e}{q-1} + 1$ valeurs de $\nu(x)$ pour lesquelles x peut être un point de torsion. Le même raisonnement que précédement permet alors de conclure que $\dim_{\mathbb{F}_q}(L_{tor}^{\varphi}) \leq f(\frac{e}{q-1} + 1) \leq \frac{nq}{q-1}$, ce qui achève la preuve du corollaire.

Références

[1] Denis, L. : *Hauteurs canoniques et modules de Drinfeld* (Math. Ann. 294 (1992),p. 213-223)

[2] Drinfeld, D. : *Elliptic modules* (Math. USSR Sb., 23 (1974), p. 561-592)

[3] Edixhoven, B. : *Rational torsion points on elliptic curves over number fields (after Kamienny and Mazur)* (Séminaire Bourbaki 782, Vol. 1993/94, Astérisque No. 227 (1995), Exp No. 782, 4, p. 209-227)

[4] Faltings, G. : *Finiteness theorems for abelian varieties over number fields* (Invent. Math. 73 (1983), no. 3,p. 349-366)

[5] Fermigier, S. : *Une courbe elliptique définie sur $\mathbb{Q}$ de rang ≥ 22* (Acta Arithmetica, LXXXII (1997), 4, p. 359-363)

[6] Flynn, E.V. :*Large rational torsion on abelian varieties* (J. Number Theory 36, p. 257-265)

[7] Goss, D. : *Basic Structures of Function Field Arithmetic* (Springer 1998)

[8] Hayes, D. : *A brief introduction to Drinfeld modules* (The Arithmetic of Function Fields, ed. D. Goss, D.R. Hayes, et M.I. Rosen, de Gruyter, Berlin 1992)

[9] Kamienny, S. : *Torsion points on elliptic curves over all quadratic fields* (Duke Math. J. 53 (1986), no. 3, p. 545-551)

[10] Kihara, S. : *On an elliptic curve over $\mathbb{Q}(t)$ of rank ≥ 14* (Proc. Japan Acad, Ser A, Math. Sci 77 (2001),p. 50-51)

[11] Leprévost, F. : *Sur certains sous-groupes de torsion de jacobiennes de courbes hyperelliptiques de genre $g \geq 2$* (Manuscripta Math. 92 (1997), no. 1, p. 47-63)

[12] Manin, J. : *The p-torsion of elliptic curves is uniformly bounded* (Math. USSR - Izvestija 3 (1969) p. 433-438)

[13] Martin, R. et Mc-Millen, W. : *An Elliptic Curve over $\mathbb{Q}$ with rank ≥ 24* (Number Theory Listserver, May 2000)

[14] Mazur, B. : *Modular curves and the Eisenstein ideal* (IHES Publi. Math. 47 (1977) p. 33-186)

[15] Merel, L. : *Bornes pour la torsion des courbes elliptiques sur les corps de nombres* (Invent. Math. 124 (1996), no.1-3, p. 437-449)

[16] Mestre, J.F. : *Courbes elliptiques de rang ≥ 12 sur $\mathbb{Q}(t)$* (CRAS, t.313, Série I (1991), no. 4, p. 171-174)

[17] Mestre, J.F. :*Courbes elliptiques de rang ≥ 11 sur $\mathbb{Q}(t)$* (CRAS, t.313, Série I (1991), no. 3, p. 139-142)

[18] Mestre, J.F. : *Un exemple de courbe elliptique sur $\mathbb{Q}$ de rang ≥ 15* (CRAS, t.314, Série I (1992),p. 453-455)

[19] Nagao, K.I. : *An example of Elliptic Curve over $\mathbb{Q}$ with rank ≥ 20* (Proc. Jap. Acad. , 69 (1993), Ser A, p. 291-293)

[20] Néron, A. : *Propriétés arithmétiques de certaines familles de courbes elliptiques* (Proc. Int. Cong. Math., Amsterdam (1954), vol III, p. 481-488)

[21] Ogawa, H. : *Curves of genus 2 with a rational torsion divisor of order 23* (Proc. Japan Acad. 70 (1994), Ser A, p. 295-298)

[22] Pantchichkine, A. : *Algorithmes rapides pour factorisation des nombres et des polynômes, tests de primalité, courbes elliptiques et modules de Drinfeld*

[23] Parent, P. : *Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres* (J. Reine Angew. Math. 506 (1999), p. 85-116)

[24] Poonen, B. : *Torsion in rank one Drinfeld modules and the uniform boundedness conjecture* (Math. Ann. 308 (1997) 4, p. 571-586)

[25] Poonen, B. : *Local height functions and the Mordell-Weil theorem for Drinfeld modules* (Compositio Math. 97 (1995), p. 349-368)

[26] Wang, J. : *The Mordell-Weil theorems for Drinfeld modules over finitely generated function fields* (Manuscripta Math. 106 (2001),no. 3, p. 305-314)