

Algebra & Number Theory

Volume 6

2012

No. 6

**Torsion des modules de Drinfeld de rang 2 et
formes modulaires de Drinfeld**

Cécile Armana



mathematical sciences publishers

Torsion des modules de Drinfeld de rang 2 et formes modulaires de Drinfeld

Cécile Armana

On donne des résultats de non-existence pour les points rationnels de la courbe modulaire de Drinfeld affine $Y_1(\mathfrak{p})$ avec \mathfrak{p} idéal premier de $\mathbb{F}_q[T]$. Cette courbe classe les modules de Drinfeld de rang 2 munis d'un point de torsion d'ordre \mathfrak{p} . Le premier énoncé concerne les points définis sur les extensions de $\mathbb{F}_q(T)$ quadratiques pour \mathfrak{p} de degré 3 et cubiques pour \mathfrak{p} de degré 4 et $q \geq 7$. Le deuxième, conditionné à une dualité entre algèbre de Hecke et formes modulaires de Drinfeld, concerne les points sur les extensions de degré $\leq q$ pour $\deg \mathfrak{p}$ suffisamment grand. Comme conséquence, on déduit, sous la même condition, une borne uniforme pour la torsion des modules de Drinfeld de rang 2 définis sur les extensions de $\mathbb{F}_q(T)$ de degré $\leq q$, prédite par Poonen.

We give nonexistence results for rational points on the affine Drinfeld modular curve $Y_1(\mathfrak{p})$ with \mathfrak{p} a prime ideal of $\mathbb{F}_q[T]$. This curve classifies Drinfeld modules of rank 2 with a torsion point of order \mathfrak{p} . The first statement concerns points defined over quadratic extensions of $\mathbb{F}_q(T)$ for \mathfrak{p} of degree 3 and cubic extensions of $\mathbb{F}_q(T)$ for \mathfrak{p} of degree 4 and $q \geq 7$. The second statement is valid under a duality condition between Hecke algebra and Drinfeld modular forms, and concerns points over extensions of degree $\leq q$ whenever $\deg \mathfrak{p}$ is sufficiently large. As a consequence we derive, under the same condition, a uniform bound for the torsion of rank-2 Drinfeld modules defined over extensions of $\mathbb{F}_q(T)$ of degree $\leq q$, as predicted by Poonen.

1. Introduction

L'objet de ce travail est d'exclure certaines structures de torsion sur les modules de Drinfeld de rang 2. Soit \mathbb{F}_q un corps fini à q éléments, A l'anneau $\mathbb{F}_q[T]$ et K le corps des fractions rationnelles $\mathbb{F}_q(T)$ en l'indéterminée T . Considérons les couples donnés par un A -module de Drinfeld de rang 2 avec un point de torsion d'ordre n , pour n idéal non nul de A (on renvoie aux rappels de la section 3). La courbe modulaire de Drinfeld $Y_1(n)$ est une courbe algébrique affine sur K ainsi

MSC2010 : primary 11G09; secondary 11F52, 11G18, 14G05.

Mots-clefs : torsion of Drinfeld modules, Drinfeld modular forms, Drinfeld modular curves.

qu'un schéma de modules pour ces objets. En règle générale, on ne s'attend pas à ce qu'elle ait de points rationnels.

Conjecture 1.1 [Poonen 1997]. *Fixons q puissance d'un nombre premier et d un entier ≥ 1 . Il existe une constante $C > 0$ telle que, si \mathfrak{n} est de degré $\geq C$ et si L est une extension de K de degré $\leq d$, la courbe $Y_1(\mathfrak{n})$ n'a pas de point L -rationnel. Autrement dit, il existe une constante $C' > 0$ telle que, si L/K est de degré $\leq d$, tout A -module de Drinfeld de rang 2 sur L ait au plus C' points de torsion dans L .*

Les constantes C et C' dépendent de q et d . Il s'agit de la conjecture 2 de [Poonen 1997] dans le cas des $\mathbb{F}_q[T]$ -modules de Drinfeld de rang 2 (une version plus faible avait été proposée auparavant par Denis [1995, problème 3]). À la lumière des fortes analogies entre courbes elliptiques et modules de Drinfeld de rang 2, cette conjecture s'apparente au théorème de borne uniforme pour la torsion des courbes elliptiques sur les corps de nombres de Merel [1996], après des travaux de Mazur [1977] notamment. Si on s'intéresse uniquement aux points K -rationnels, Schweizer a prédit un résultat plus précis :

Conjecture 1.2 (conséquence de [Schweizer 2003, conjecture 1]). *Si \mathfrak{p} est un idéal premier de A de degré ≥ 3 , la courbe $Y_1(\mathfrak{p})$ n'a pas de point K -rationnel.*

À l'heure actuelle, les résultats connus en direction de ces conjectures sont partiels et assez peu nombreux. Les plus avancés sont dus à Schweizer et Pál.

Théorème 1.3. *La courbe $Y_1(\mathfrak{n})$ n'a pas de point $\mathbb{F}_q(T)$ -rationnel pour les idéaux \mathfrak{n} suivants de $\mathbb{F}_q[T]$:*

- (i) \mathfrak{n} idéal premier de degré ≥ 3 de $\mathbb{F}_2[T]$. En particulier la conjecture 1.1 est vérifiée pour $L = K = \mathbb{F}_2(T)$ (i.e., $q = 2$, $d = 1$) [Pál 2010, théorèmes 1.2 et 1.4].
- (ii) $\mathfrak{n} \in \{(T^2 + T + 1)^2, T(T^2 + T + 1), T^3, (T^2(T + 1))\}$ dans $\mathbb{F}_2[T]$ [Pál 2010, théorème 10.8; Schweizer 2003, lemme 1.3].
- (iii) $\mathfrak{n} \in \{T(T - 1)(T + 1), T^2(T - 1)\}$ dans $\mathbb{F}_3[T]$ [Schweizer 2011, page 297].
- (iv) \mathfrak{n} produit de trois facteurs linéaires distincts dans $\mathbb{F}_4[T]$ [Schweizer 2011, proposition 3.2].

Pour les idéaux de cet énoncé, hormis $(T^2 + T + 1)^2 \in \mathbb{F}_2[T]$, le résultat est en fait établi pour la courbe modulaire de Drinfeld $Y_0(\mathfrak{n})$ qui paramètre les modules de Drinfeld de rang 2 munis d'une isogénie cyclique d'ordre \mathfrak{n} .

En ce qui concerne la conjecture 1.1, Poonen [1997, théorème 6] et Schweizer [2003, théorème 2.4] ont aussi obtenu une borne uniforme sur la composante \mathfrak{p} -primaire de la torsion, à rapprocher des énoncés de Manin [1969] et de Kamienny et Mazur [1995] pour les courbes elliptiques. Mentionnons enfin une preuve de

Nguyen et Yamada de la conjecture 1.1 en 2001 qui s'est avérée fautive (voir [Schweizer 2003] pour les détails).

Dans ce travail, on détermine les points rationnels de $Y_1(\mathfrak{p})$ pour certains premiers \mathfrak{p} en suivant l'approche de Mazur et Merel pour les courbes modulaires classiques. Dans le cas des corps de fonctions, il s'avère que la propriété d'immersion formelle requise par Mazur [1978] est loin d'être évidente. L'objet principal de cet article, issu de la thèse [Armana 2008] débutée en 2003, est d'explicitier cette difficulté, ce qui n'avait pas été fait dans la littérature, et de détailler les liens entre immersion formelle, formes modulaires de Drinfeld et symboles modulaires. Ainsi ce travail s'appuie en partie sur [Armana 2011b]. Précisons que l'approche de Mazur a aussi été employée par Pál [2010] : la différence réside dans le choix d'une place auxiliaire de réduction ($\infty = (1/T)$ pour Pál, place l distincte de ∞ ici).

D'autres outils nécessaires à la mise en place de la méthode de Mazur sur les corps de fonctions sont développés dans ce travail. Un premier est le quotient d'enroulement de la jacobienne $J_0(\mathfrak{p})$ de la courbe modulaire de Drinfeld compactifiée $X_0(\mathfrak{p})$. C'est le plus grand quotient de $J_0(\mathfrak{p})$ de rang analytique nul et il fait l'objet de la section 4. Pour établir les théorèmes principaux, on utilisera aussi une borne effective sur le degré de la torsion des modules de Drinfeld de rang 2 à bonne réduction potentielle (proposition 5.2).

Lorsque \mathfrak{p} est premier de petit degré, la situation se trouve simplifiée. Le quotient d'enroulement est alors essentiellement la jacobienne $J_0(\mathfrak{p})$ ou son quotient sur lequel l'involution d'Atkin–Lehner opère comme -1 , d'après la connaissance du degré de la fonction L de $J_0(\mathfrak{p})$. L'immersion formelle pour les puissances symétriques de $X_0(\mathfrak{p})$ provient alors d'un argument de point de Weierstrass ou de gonalgité (section 7D1). Cela fournit l'énoncé suivant, résultat non trivial en direction de la conjecture 1.2. Comparé au théorème 1.3, il a l'avantage d'être sans condition forte sur le cardinal q du corps fini de base et d'autoriser des extensions de K de degré > 1 .

Théorème 1.4. *Soit \mathfrak{p} un idéal premier.*

- (i) *Si \mathfrak{p} est de degré 3, la courbe $Y_1(\mathfrak{p})$ n'a pas de point L -rationnel pour toute extension L/K de degré ≤ 2 .*
- (ii) *Supposons \mathfrak{p} de degré 4 et $d = 1$ si q quelconque, $d = 2$ si $q = 5$, $d = 3$ si $q \geq 7$. Alors la courbe $Y_1(\mathfrak{p})$ n'a pas de point L -rationnel pour toute extension L/K de degré $\leq d$.*

En d'autres termes, pour de tels q , \mathfrak{p} et L , il n'existe pas de A -module de Drinfeld de rang 2 sur L ayant un point de torsion dans L d'ordre \mathfrak{p} .

Il se déduit du théorème 7.5, plus général, qui concerne les niveaux \mathfrak{p} tels que toute forme primitive associée est de rang analytique ≤ 1 . Considérons l'espace

$H_p(\mathbb{C})$ des cochaînes harmoniques paraboliques pour $\Gamma_0(p) \subset GL_2(A)$ à valeurs complexes. D'après Drinfeld, elles s'identifient naturellement à des formes automorphes paraboliques pour GL_2 sur les adèles de K . L'algèbre de Hecke \mathbb{T} est la sous \mathbb{Z} -algèbre commutative de $\text{End}(H_p(\mathbb{C}))$ engendrée par les opérateurs de Hecke. Le théorème 7.5(ii) est alors valable pour les premiers p tels que la fonction L de toute forme primitive de $H_p(\mathbb{C})$ pour Hecke s'annule à l'ordre ≤ 1 au centre de symétrie (on dira que p satisfait la condition \mathcal{C}). Signalons aussi le théorème 7.8 qui donne $Y_0(p)(K) = \emptyset$ pour $q \geq 5$ et p de degré ≥ 5 vérifiant \mathcal{C} . La condition \mathcal{C} présente l'avantage d'être testable sur machine, par exemple à l'aide des symboles modulaires pour $\mathbb{F}_q(T)$ [Teitelbaum 1992]. On l'a ainsi vérifiée pour tous les premiers de degré 5 dans $\mathbb{F}_2[T]$ (déjà couverts par le théorème 1.3(i)) et, par exemple, pour les premiers suivants de $\mathbb{F}_3[T]$: $(T^5 + T^3 - T^2 - T + 1)$, $(T^5 + T^4 + T^3 - T^2 + T - 1)$, $(T^5 - T^4 - T^2 - 1)$. L'ensemble $Y_1(p)(K)$ est donc vide pour de tels p .

Cette condition \mathcal{C} n'est certainement pas vérifiée par tout idéal premier p . En effet, d'après Ulmer [2002] il existe des courbes elliptiques non-isotriviales sur $\mathbb{F}_q(T)$, pour q premier, de rang arithmétique arbitrairement grand. Par le théorème de modularité pour les courbes elliptiques sur K (corollaire des travaux de Grothendieck, Deligne, Jacquet–Langlands et Drinfeld, voir [Gekeler et Reversat 1996]) et en supposant la conjecture de Birch et Swinnerton-Dyer pour ces courbes, on voit que la condition \mathcal{C} n'est pas satisfaite pour tout p . Cependant, on s'attend à ce qu'elle le soit assez fréquemment car une philosophie courante prédit que les courbes elliptiques de rangs élevés (≥ 2) sont rares. Heath-Brown, Young et récemment Bhargava et Shankar ont obtenu des résultats en ce sens pour les courbes elliptiques sur \mathbb{Q} . De façon générale, déterminer la densité d'idéaux p vérifiant \mathcal{C} semble être un problème délicat.

Le deuxième énoncé relie l'existence de points rationnels sur $Y_1(p)$ aux formes modulaires de Drinfeld, en exploitant la méthode de Mazur dans le cas général. Commençons par des notations. Soit S_p le $A[1/p]$ -module des différentielles relatives globales de degré 1 de $X_0(p)$ sur $A[1/p]$. Ce sont des formes modulaires de Drinfeld algébriques doublement paraboliques de poids 2 pour $\Gamma_0(p)$. Pour \mathfrak{l} un idéal premier non nul de A et distinct de p , notons $\mathbb{F}_{\mathfrak{l}}$ le corps fini A/\mathfrak{l} et $S_p(\mathbb{F}_{\mathfrak{l}}) = S_p \otimes_{A[1/p]} \mathbb{F}_{\mathfrak{l}}$. L'algèbre \mathbb{T} agit sur $S_p(\mathbb{F}_{\mathfrak{l}})$ via son quotient $\mathbb{T}/p\mathbb{T}$ où p désigne la caractéristique de \mathbb{F}_q . De plus, tout élément f de $S_p(\mathbb{F}_{\mathfrak{l}})$ possède un développement de la forme $\sum_{i \geq 1} b_i(f)t^{1+i(q-1)} \in \mathbb{F}_{\mathfrak{l}}[[t]]$ en la pointe infinie de $X_0(p)$ (voir section 6).

Dans [Armana 2011b], on a défini un symbole modulaire parabolique \mathbf{e} relativement à $\Gamma_0(p)$ au sens de Teitelbaum [1992]. C'est l'analogue de l'élément d'enroulement de Mazur [1977]. L'algèbre de Hecke \mathbb{T} agit aussi sur les symboles modulaires pour $\mathbb{F}_q(T)$. Soient $I_{\mathbf{e}}$ et $\tilde{I}_{\mathbf{e}}$ les idéaux annulateurs dans \mathbb{T} de \mathbf{e} et

($e \bmod p$) respectivement (sections 4A et 4D). On note $S_p(\mathbb{F}_l)[\tilde{I}_e]$ le sous-espace de $S_p(\mathbb{F}_l)$ annulé par \tilde{I}_e .

Théorème 1.5. *Soit p premier de degré ≥ 3 . Supposons qu'il existe :*

- *Un idéal saturé I de \mathbb{T} , d'annulateur noté \hat{I} , vérifiant $I_e \subset I \subset \tilde{I}_e$ et $\hat{I} + \tilde{I}_e = \mathbb{T}$.*
- *Un idéal \mathfrak{l} de A de degré 1 tel que l'application \mathbb{F}_l -linéaire*

$$\Phi_{\mathfrak{l}} : (\mathbb{T}/\tilde{I}_e) \otimes_{\mathbb{Z}} \mathbb{F}_l \longrightarrow \text{Hom}(S_p(\mathbb{F}_l)[\tilde{I}_e], \mathbb{F}_l),$$

qui envoie la classe de $u \in \mathbb{T}$ sur la forme linéaire $f \mapsto b_1(uf)$, est un isomorphisme.

Alors

- (i) *si $\deg p \geq \max(q + 1, 5)$, la courbe $Y_1(p)$ n'a de point L -rationnel pour toute extension L/K de degré $\leq q$;*
- (ii) *si $\deg p \geq 3$, la courbe $Y_1(p)$ n'a pas de point K -rationnel.*

L'hypothèse sur l'existence de l'idéal I est vraisemblablement de nature technique. Elle évite un problème lié au passage de suites exactes de variétés abéliennes sur K aux espaces cotangents de leur modèles de Néron. De fait, elle permet la construction d'un raffinement du quotient d'enroulement possédant de bonnes propriétés (sections 4D et 7E2). On démontre que I_e vérifie cette hypothèse pour tout p de degré 3, ou de degré 4 avec $p \neq 2$ (proposition 4.12). Un critère est aussi donné en section 4D2.

L'hypothèse sur $\Phi_{\mathfrak{l}}$ est certainement plus profonde. Elle permet de traduire l'immersion formelle (critère de Kamienny) en une indépendance linéaire de symboles modulaires sur les corps de fonctions, qui a fait l'objet d'un travail précédent [Armana 2011b]. Si on supprime l'idéal \tilde{I}_e de sa formulation, l'hypothèse s'apparente à un accouplement entre formes modulaires de Drinfeld et algèbre de Hecke, qui entraînerait un énoncé de multiplicité un dans $S_p(\mathbb{F}_l)$. Depuis [Goss 1980a], on sait que des formes modulaires de Drinfeld pour $GL_2(A)$ de poids distincts peuvent avoir les mêmes valeurs propres de Hecke en caractéristique générique. Cependant, le problème de multiplicité un, dans S_p ou $S_p(\mathbb{F}_l)$ à p fixé, est semble-t-il ouvert à l'heure actuelle. Ici, on démontre notre hypothèse sur $\Phi_{\mathfrak{l}}$, a priori plus faible, ainsi que la multiplicité un, dans le cas où p est de degré 3 avec \mathfrak{l} quelconque (proposition 7.14). Le cas général requerrait une étude plus approfondie.

Quant à la condition sur le degré de l'extension L/K du théorème 1.5, elle provient de relations entre coefficients du développement des formes modulaires de Drinfeld et opérateurs de Hecke de degré 1 (théorème 6.15 et proposition 7.14).

À nouveau, le théorème 1.5 est sans hypothèse sur q , autorise des extensions non triviales de K et va dans le sens de la conjecture 1.2. Il contient même le résultat de Pál sur $Y_1(p)$ (théorème 1.3(i)) si les hypothèses peuvent être levées.

Remarquons que, pour \mathfrak{p} de degré 3, on retrouve $Y_1(\mathfrak{p})(K) = \emptyset$ de façon inconditionnelle (théorème 1.4(i)). Comme conséquence du théorème 1.5 et du travail de Schweizer [2003], on obtient une borne uniforme conditionnelle sur la torsion des modules de Drinfeld de rang 2.

Corollaire 1.6. *Fixons q . Supposons qu'il existe une constante $B_q > 0$ telle que pour tout premier \mathfrak{p} de degré $\geq B_q$ on peut trouver des idéaux I de \mathbb{T} et \mathfrak{l} de A comme dans l'énoncé du théorème 1.5. Alors la conjecture 1.1 est vraie pour les A -modules de Drinfeld de rang 2 sur les extensions de K de degré $1 \leq d \leq q$.*

2. Notations

Soient q une puissance d'un nombre premier p , \mathbb{F}_q (respectivement \mathbb{F}_p) un corps fini à q (respectivement p) éléments, $A = \mathbb{F}_q[T]$ l'anneau en T indéterminée et $K = \mathbb{F}_q(T)$ son corps des fractions. On note \deg le degré usuel sur A avec la convention $\deg 0 = -\infty$. Le degré d'un idéal non nul de A est celui de l'un de ses générateurs. Pour P, Q dans A , on note (P) l'idéal engendré par P et $P \mid Q$ si P divise Q .

Les lettres gothiques désigneront des idéaux de A . En particulier, \mathfrak{p} désignera un premier (c'est-à-dire un idéal premier non nul) de A . Le corps fini A/\mathfrak{p} est noté $\mathbb{F}_{\mathfrak{p}}$. Pour un idéal \mathfrak{n} , le sous-groupe $\Gamma_0(\mathfrak{n})$ de $\mathrm{GL}_2(A)$ est formé des matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ avec $c \in \mathfrak{n}$.

Pour un corps F , on désigne par F^{alg} une clôture algébrique et F^{sep} une clôture séparable. Le cardinal d'un ensemble fini S est noté $\#S$.

3. Rappels

3A. Courbes modulaires de Drinfeld. Soit L un A -corps c'est-à-dire un corps L muni d'un homomorphisme d'anneaux $\iota : A \rightarrow L$. Soit $L\{\tau\}$ l'anneau des polynômes tordus sur L avec multiplication donnée par $\tau l = l^q \tau$ ($l \in L$). Fixons $r \geq 1$ entier. Un A -module de Drinfeld (on abrègera en module de Drinfeld) de rang r sur L est un homomorphisme d'anneaux

$$\phi : A \longrightarrow L\{\tau\}, \quad a \longmapsto \phi_a,$$

tel que le terme constant de ϕ_a est $\iota(a)$ et $\deg_{\tau} \phi_a = r \deg a$. Si ϕ est de rang 2, il est déterminé de façon unique par l'image de $T : \phi_T = \iota(T)\tau^0 + g\tau + \Delta\tau^2$ avec $g \in L$ et $\Delta \in L^{\times}$. En identifiant τ à l'automorphisme $x \mapsto x^q$ de L , on identifie $L\{\tau\}$ à l'anneau des polynômes (additifs) combinaisons linéaires de $\{x^{q^i}\}_{i \geq 0}$ à coefficients dans L , avec pour loi de multiplication la composition. En faisant agir un élément a de A sur $x \in L$ par $\phi_a(x)$, on obtient une nouvelle structure de A -module sur le corps L , notée ${}^{\phi}L$.

Soit \mathfrak{a} un idéal de A . On fixe un générateur a de \mathfrak{a} . Les *points de \mathfrak{a} -torsion* de ϕ dans une extension F/L sont les éléments du A -module

$$\phi[\mathfrak{a}](F) = (\ker \phi_a)(F) \subset {}^\phi F$$

(il ne dépend pas du choix de a). Les points de torsion dans F forment le A -module $({}^\phi F)_{\text{tors}}$, le sous-module de torsion de ${}^\phi F$. L'ordre d'un élément de $({}^\phi F)_{\text{tors}}$ est son idéal annulateur dans A . On pose $\phi[\mathfrak{a}] = \phi[\mathfrak{a}](L^{\text{alg}})$. Si le noyau de ι ne contient pas \mathfrak{a} , le polynôme ϕ_a est alors séparable et le A -module $\phi[\mathfrak{a}]$ est en fait contenu dans $({}^\phi L^{\text{sep}})_{\text{tors}}$.

Un *homomorphisme* de modules de Drinfeld $u : \phi \rightarrow \psi$ sur L est un élément $u \in L\{\tau\}$ tel que $\phi_a u = u \psi_a$ pour tout $a \in A$. C'est un *isomorphisme* si $u \in L^\times$. Une *isogénie* est un homomorphisme non nul ; il n'en existe qu'entre modules de Drinfeld de même rang. Une isogénie est *cyclique d'ordre α* si $\deg_\tau u = \deg \alpha$ et si son noyau $C = (\ker u)(L^{\text{alg}})$ est un sous-module de $({}^\phi L^{\text{alg}})_{\text{tors}}$ isomorphe à A/α . On note alors ϕ/C le module de Drinfeld ψ isogène à ϕ . Il y a une bijection entre l'ensemble des isogénies L -rationnelles (*i.e.*, définies sur L) cycliques d'ordre α de ϕ et les sous-modules C de $({}^\phi L^{\text{alg}})_{\text{tors}}$ stables par $\text{Gal}(L^{\text{sep}}/L)$ et isomorphes à A/α comme A -modules.

On peut étendre la notion de module de Drinfeld d'un A -corps à un A -schéma quelconque S [Drinfeld 1974]. Soit \mathfrak{n} un idéal non nul de A . Considérons le foncteur qui associe à S l'ensemble des classes d'isomorphisme de couples (ϕ, C) , où ϕ est un module de Drinfeld de rang 2 sur S et C est un sous-groupe cyclique de ϕ d'ordre \mathfrak{n} au sens de Katz–Mazur. Il possède un schéma de modules grossier $\mathcal{Y}_0(\mathfrak{n})$ sur A . De même, en considérant les classes d'isomorphisme de couples (ϕ, P) où P est un point de ϕ d'ordre \mathfrak{n} , on obtient un schéma de modules grossier $\mathcal{Y}_1(\mathfrak{n})$ sur A . Les schémas $\mathcal{Y}_0(\mathfrak{n})$ et $\mathcal{Y}_1(\mathfrak{n})$ sont affines, de type fini sur A et de dimension relative pure 1.

On définit les courbes $Y_0(\mathfrak{n}) = \mathcal{Y}_0(\mathfrak{n}) \times_A K$ et $Y_1(\mathfrak{n}) = \mathcal{Y}_1(\mathfrak{n}) \times_A K$. Pour L une extension de K , les points L -rationnels de $Y_0(\mathfrak{n})$ (respectivement $Y_1(\mathfrak{n})$) sont en bijection avec les classes d'isomorphisme sur L^{alg} de modules de Drinfeld de rang 2 sur L munis d'une isogénie L -rationnelle cyclique d'ordre \mathfrak{n} (respectivement d'un point de torsion d'ordre \mathfrak{n} défini sur L).

Pour mémoire, rappelons le versant analytique de ces courbes. On désigne par \mathbb{C}_∞ le complété d'une clôture algébrique de $\mathbb{F}_q((1/T))$. Les analytifiées de $Y_0(\mathfrak{n})$ et $Y_1(\mathfrak{n})$ sur \mathbb{C}_∞ sont alors les espaces analytiques rigides obtenus comme quotients du demi-plan de Drinfeld $\mathbb{C}_\infty - \mathbb{F}_q((1/T))$ par l'action de certains sous-groupes de congruence de $\text{GL}_2(A)$ [Drinfeld 1974, section 6].

On a une compactification canonique $\mathcal{X}_0(\mathfrak{n})$ de $\mathcal{Y}_0(\mathfrak{n})$ et $\mathcal{X}_1(\mathfrak{n})$ de $\mathcal{Y}_1(\mathfrak{n})$ sur $\text{Spec}(A)$ [Drinfeld 1974, section 9 ; Gekeler 1986] et un homomorphisme canonique $\mathcal{X}_1(\mathfrak{n}) \rightarrow \mathcal{X}_0(\mathfrak{n})$. L'énoncé suivant se déduit de [Drinfeld 1974].

Théorème 3.1. *Soit $i \in \{0, 1\}$.*

- (i) *Le schéma $\mathcal{X}_i(\mathfrak{n})$ est propre, normal, plat et irréductible de dimension relative pure 1 sur A .*
- (ii) *Le morphisme structurel $\mathcal{X}_i(\mathfrak{n}) \rightarrow \text{Spec } A[1/\mathfrak{n}]$ est lisse et propre.*
- (iii) *La courbe $X_i(\mathfrak{n}) = \mathcal{X}_i(\mathfrak{n}) \times_A K$ est lisse, propre et géométriquement connexe sur K .*

D’après Drinfeld, on sait aussi que l’ensemble $X_0(\mathfrak{n})(K^{\text{alg}}) - Y_0(\mathfrak{n})(K^{\text{alg}})$ est fini. Ses éléments sont appelés les *pointes* de $X_0(\mathfrak{n})$. Elles sont en bijection avec l’ensemble quotient $\Gamma_0(\mathfrak{n}) \backslash \mathbb{P}^1(K)$ (on a fait opérer le groupe $\Gamma_0(\mathfrak{n})$ par homographies sur $\mathbb{P}^1(K)$). En particulier, pour $\mathfrak{n} = \mathfrak{p}$ premier, la courbe $X_0(\mathfrak{p})$ possède exactement deux pointes notées 0 et ∞ et elles sont K -rationnelles.

Gekeler a donné des formules pour le genre $g(X_0(\mathfrak{n}))$ [Gekeler 1980, 3.4.18 ; Gekeler et Nonnengardt 1995], dont l’énoncé suivant est un cas particulier.

Proposition 3.2. *Pour \mathfrak{p} de degré d , le genre de $X_0(\mathfrak{p})$ est*

$$g(X_0(\mathfrak{p})) = \begin{cases} \frac{q^d - q^2}{q^2 - 1} & \text{si } d \text{ est pair,} \\ \frac{q^d - q}{q^2 - 1} & \text{si } d \text{ est impair.} \end{cases}$$

La courbe $X_0(\mathfrak{n})$ est munie de correspondances de Hecke [Gekeler 1986, 5.3 ; Gekeler et Reversat 1996, 4.12 ; Gekeler 1997a, section 7]. Pour \mathfrak{m} idéal non nul, la correspondance $T_{\mathfrak{m}}$ est définie sur le problème de modules par

$$(\phi, C) \mapsto \sum_{D \cap C = \{0\}} (\phi/D, (C + D)/D),$$

la somme portant sur les sous-modules cycliques D de ϕ d’ordre \mathfrak{m} . De même, pour un idéal \mathfrak{m} divisant \mathfrak{n} et premier à $\mathfrak{n}/\mathfrak{m}$, l’involutions $w_{\mathfrak{m}}$ de $X_0(\mathfrak{n})$ est définie par $(\phi, C) \mapsto (\phi/C, \phi[\mathfrak{m}]/C)$. Ces correspondances stabilisent l’ensemble des pointes de $X_0(\mathfrak{n})$. Si $\mathfrak{n} = \mathfrak{p}$ premier, $w_{\mathfrak{p}}$ échange 0 et ∞ et $T_{\mathfrak{m}}$ opère par multiplication par $(1 + q^{\text{deg } \mathfrak{m}})$ sur chaque pointe, pour \mathfrak{m} étranger à \mathfrak{p} .

La jacobienne $J_0(\mathfrak{n})$ de $X_0(\mathfrak{n})$ est une variété abélienne sur K de dimension $g(X_0(\mathfrak{n}))$. Elle a bonne réduction en-dehors de $\mathfrak{n} \cdot (\infty)$ et, pour $\mathfrak{n} = \mathfrak{p}$, réduction torique en \mathfrak{p} . La structure de la fibre spéciale de $\mathcal{X}_0(\mathfrak{p})$ et le groupe des composantes de $J_0(\mathfrak{p})$ en \mathfrak{p} ont été déterminés par Gekeler [1986].

3B. Cochaînes harmoniques. Les cochaînes harmoniques paraboliques pour $\Gamma_0(\mathfrak{p})$ à valeurs dans \mathbb{Z} sont des fonctions sur les arêtes de l’arbre de Bruhat–Tits de $\text{PGL}_2(\mathbb{F}_q((1/T)))$ (on se réfère à [Gekeler et Reversat 1996] pour leurs définitions et propriétés). Elles forment un \mathbb{Z} -module libre de rang $g(X_0(\mathfrak{p}))$, noté $H_{\mathfrak{p}}$. Soit

$H_{\mathfrak{p}}(\mathbb{C}) = H_{\mathfrak{p}} \otimes_{\mathbb{Z}} \mathbb{C}$ le \mathbb{C} -espace vectoriel des cochaînes paraboliques à valeurs dans \mathbb{C} . La plupart du temps, on omettra la dépendance en \mathfrak{p} et on notera H et $H(\mathbb{C})$. D'après Drinfeld et le théorème d'approximation faible, $H(\mathbb{C})$ s'identifie à un espace de formes automorphes paraboliques pour GL_2 sur les adèles de K . Toute cochaîne de $H(\mathbb{C})$ admet un développement de Fourier indexé par les idéaux de A (voir [Weil 1971 ; Tan 1993 ; Gekeler 1980 ; 1995b] pour différents points de vue).

Pour \mathfrak{m} idéal non nul de A , on définit l'opérateur de Hecke $T_{\mathfrak{m}}$ comme l'endomorphisme de $H(\mathbb{C})$ provenant de l'action à gauche des matrices $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ (a, b, d dans A , $(ad) = \mathfrak{m}$, $(a) + \mathfrak{p} = A$, $\deg b < \deg d$, a et d unitaires) sur les arêtes de l'arbre. Soit $w_{\mathfrak{p}}$ l'involution de $H(\mathbb{C})$ induite par l'action de $\begin{pmatrix} 0 & -1 \\ P & 0 \end{pmatrix}$ où P désigne le générateur unitaire de l'idéal \mathfrak{p} . Le lien avec les correspondances $T_{\mathfrak{m}}$ et $w_{\mathfrak{p}}$ sera explicité en section 3D. Soit \mathbb{T} la sous-algèbre commutative de $\text{End } H(\mathbb{C})$ engendrée sur \mathbb{Z} par $w_{\mathfrak{p}}$ et les $T_{\mathfrak{m}}$ pour \mathfrak{m} et \mathfrak{p} étrangers. Ces opérateurs sont hermitiens pour le produit de Petersson sur $H(\mathbb{C})$ induit par celui sur les formes automorphes. On a $w_{\mathfrak{p}} = -T_{\mathfrak{p}}$. L'algèbre de Hecke \mathbb{T} stabilise la structure entière H . Le \mathbb{Z} -module \mathbb{T} est libre de type fini car il en est de même de H .

Par le théorème spectral, il existe une base de $H(\mathbb{C})$ constituée de formes propres pour tous les opérateurs de Hecke et normalisées (*i.e.*, le coefficient de Fourier associé à l'idéal A est 1). On les appelle *formes primitives*. Elles sont propres pour $w_{\mathfrak{p}}$ de valeur propre $+1$ ou -1 .

La fonction $L(F, s)$ est la série de Dirichlet associée aux coefficients de Fourier de $F \in H(\mathbb{C})$ (s variable complexe). Cette fonction s'écrit aussi comme transformée de Mellin de F . Pour $L(F, s)$, on en déduit un prolongement holomorphe à \mathbb{C} , l'équation fonctionnelle

$$L(F, s) = -q^{(\deg(\mathfrak{p})-3)(1-s)} L(w_{\mathfrak{p}}F, 2-s) \quad (s \in \mathbb{C}) \quad (1)$$

et la propriété que $L(F, s)$ est un polynôme non nul en q^{-s} de degré $\leq \deg(\mathfrak{p}) - 3$ (voir [Tan 1993], proposition 2, équation (3.4) et le corollaire à la page 305 pour ces affirmations). En particulier, en $s = 1$, la fonction $L(F, s)$ a un zéro d'ordre impair si $w_{\mathfrak{p}}F = +F$ et un zéro d'ordre pair (ou pas de zéro) si $w_{\mathfrak{p}}F = -F$. On complète ces rappels par des propriétés élémentaires.

Lemme 3.3. *Soit F primitive dans $H_{\mathfrak{p}}(\mathbb{C})$.*

- (i) *La fonction $L(F, s)$ est un polynôme en q^{-s} de degré $\deg(\mathfrak{p}) - 3$ et de terme constant 1.*
- (ii) *Supposons que l'ordre d'annulation de $L(F, s)$ en $s = 1$ est ≤ 1 (c'est le cas si $\deg \mathfrak{p} \leq 4$). Alors*

$$w_{\mathfrak{p}}F = -F \iff L(F, 1) \neq 0.$$

Démonstration. (i) Voir [Tan 1993, page 305].

(ii) La condition est vérifiée si $\deg \mathfrak{p} \leq 4$ car la fonction L est alors un polynôme en q^{-s} de degré ≤ 1 . D'après (1), on a $L(F, 1) = -L(w_{\mathfrak{p}}F, 1)$. Donc $L(F, 1) \neq 0$ entraîne $w_{\mathfrak{p}}F = -F$, sans condition sur l'ordre d'annulation. Réciproquement, supposons $w_{\mathfrak{p}}F = -F$. Alors l'ordre d'annulation est pair ≥ 2 ou bien $L(F, 1) \neq 0$. Comme $L(F, s)$ s'annule à l'ordre ≤ 1 , seul le deuxième cas est possible. \square

Soit \mathcal{F} l'ensemble des formes primitives de $H_{\mathfrak{p}}(\mathbb{C})$. Le groupe de Galois absolu de \mathbb{Q} opère sur \mathcal{F} via son action sur les coefficients de Fourier. Notons \mathcal{O} l'ensemble des orbites, $[F]$ l'orbite de $F \in \mathcal{F}$ et $a_{[F]}$ l'idéal annulateur de F dans \mathbb{T} . L'application $[F] \mapsto a_{[F]}$ est une bijection entre \mathcal{O} et l'ensemble des idéaux premiers minimaux de \mathbb{T} .

Soit K_F le corps de nombres totalement réel engendré par les coefficients de Fourier de F . Son degré sur \mathbb{Q} est le cardinal de $[F]$. L'application $u \mapsto uF/F$ de \mathbb{T} dans K_F induit un isomorphisme de \mathbb{Q} -algèbres $(\mathbb{T}/a_{[F]}) \otimes_{\mathbb{Z}} \mathbb{Q} \simeq K_F$. La \mathbb{Q} -algèbre $\mathbb{T} \otimes_{\mathbb{Z}} \mathbb{Q}$ est alors semi-simple : elle est isomorphe au produit des K_F pour $[F] \in \mathcal{O}$. Le rang de \mathbb{T} sur \mathbb{Z} est donc $g(X_0(\mathfrak{p}))$.

La variété abélienne $J_{[F]}$ est définie comme le quotient de $J_0(\mathfrak{p})$ par la sous-variété abélienne $a_{[F]}J_0(\mathfrak{p})$. Elle est simple sur K et sa dimension est $\#[F]$. Sa fonction L de Hasse–Weil se factorise en

$$L(J_{[F]}, s) = \prod_{G \in [F]} L(G, s) \quad (s \in \mathbb{C}), \quad (2)$$

l'égalité étant valable pour les facteurs locaux. (Pour les places étrangères à \mathfrak{p} , cela provient d'une relation d'Eichler et Shimura ; dans le cas général, de [Deligne 1973; Drinfeld 1984, théorème A et remarque 2]. Voir aussi [Tamagawa 1995, (3.3)].)

3C. Symboles modulaires pour $\mathbb{F}_q(T)$. Les rappels suivants sur la théorie de Teitelbaum se basent sur [Teitelbaum 1992], auquel on renvoie pour les détails. Les symboles modulaires paraboliques pour $\mathbb{F}_q(T)$ à valeurs dans \mathbb{Z} relativement au sous-groupe $\Gamma_0(\mathfrak{p})$ forment un \mathbb{Z} -module qu'on note $M_{\mathfrak{p}}^0$ ou encore M^0 . Il est de type fini et de rang $g(X_0(\mathfrak{p}))$. On note qu'il peut avoir une torsion non nulle. Soit $M^0(\mathbb{Q}) = M^0 \otimes_{\mathbb{Z}} \mathbb{Q}$ (respectivement $M^0(\mathbb{C}) = M^0 \otimes_{\mathbb{Z}} \mathbb{C}$) l'espace vectoriel des symboles modulaires paraboliques à valeurs dans \mathbb{Q} (respectivement \mathbb{C}).

Comme auparavant, les matrices

$$\left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \right\}_{a,b,d} \quad \text{et} \quad \begin{pmatrix} 0 & -1 \\ P & 0 \end{pmatrix}$$

définissent des éléments de $\text{End } M^0(\mathbb{C})$ notés T_m et $w_{\mathfrak{p}}$. Par ailleurs, Teitelbaum a défini un accouplement parfait $\langle \cdot, \cdot \rangle : M^0(\mathbb{C}) \times H(\mathbb{C}) \rightarrow \mathbb{C}$. Il est compatible aux opérateurs de Hecke et parfait sur $M^0(\mathbb{Q}) \times H(\mathbb{Q})$ où $H(\mathbb{Q}) = H \otimes_{\mathbb{Z}} \mathbb{Q}$. Il permet donc d'identifier \mathbb{T} à la sous-algèbre de $\text{End } M^0(\mathbb{C})$ engendrée sur \mathbb{Z} par les

opérateurs d'indice étranger à p . On désigne encore par \mathbb{T} cette algèbre. À nouveau, elle stabilise la structure entière M^0 .

Lemme 3.4. *Le $(\mathbb{T} \otimes_{\mathbb{Z}} \mathbb{Q})$ -module $M^0(\mathbb{Q})$ est libre de rang 1.*

Démonstration. Pour $F \in H$, on note $c_A(F)$ le coefficient de Fourier de F associé à l'idéal A . On a un accouplement de groupes abéliens

$$\mathbb{T} \times H \rightarrow \mathbb{Z}, \quad (u, F) \mapsto c_A(uF),$$

qui est équivariant par \mathbb{T} . D'après le théorème 3.17 de [Gekeler 1995a], l'accouplement est parfait après extension des scalaires à $\mathbb{Z}[1/p]$. Ainsi $H(\mathbb{Q})$ est un $(\mathbb{T} \otimes_{\mathbb{Z}} \mathbb{Q})$ -module libre de rang 1. Par l'accouplement $\langle \cdot, \cdot \rangle$ de Teitelbaum, on sait que $H(\mathbb{Q})$ et $M^0(\mathbb{Q})$ sont des $(\mathbb{T} \otimes_{\mathbb{Z}} \mathbb{Q})$ -modules isomorphes, ce qui permet de conclure. \square

3D. Compatibilité de l'action de Hecke. Les correspondances de Hecke sur la courbe $X_0(p)$ induisent des endomorphismes de $J_0(p)$ définis sur K . Considérons la sous-algèbre de $\text{End}_K J_0(p)$ engendrée sur \mathbb{Z} par w_p et les T_m pour m étranger à p . Un théorème fondamental de Drinfeld [1974, théorème 2] permet de l'identifier à l'algèbre de Hecke $\mathbb{T} \subset \text{End } H_p(\mathbb{C})$. Cette compatibilité peut aussi se déduire de la construction explicite de $J_0(p)$, en tant que variété analytique rigide sur \mathbb{C}_{∞} , comme tore modulo le réseau des périodes de certaines fonctions thêta d'après [Gekeler et Reversat 1996, sections 5 à 9; Gekeler 1997a, 7.6]. L'algèbre de Hecke \mathbb{T} agit ainsi de façon fidèle et compatible sur plusieurs objets : la jacobienne $J_0(p)$, les structures entières H_p de cochaînes et M_p^0 de symboles modulaires.

4. Le quotient d'enroulement de $J_0(p)$

4A. Définition et groupe de Mordell–Weil. Par l'accouplement $\langle \cdot, \cdot \rangle$, la forme linéaire $F \mapsto (q-1)L(F, 1)$ définit un élément \mathbf{e} de $M^0(\mathbb{Q})$ appelé *élément d'enroulement* [Armana 2011b, définition 7.1].

Définition 4.1. Notons $I_{\mathbf{e}}$ l'idéal annulateur de \mathbf{e} dans \mathbb{T} et $I_{\mathbf{e}}J_0(p)$ la sous-variété abélienne de $J_0(p)$ engendrée par ux pour $u \in I_{\mathbf{e}}$ et $x \in J_0(p)$. Le *quotient d'enroulement* $J_{\mathbf{e}}(p)$ est la variété abélienne $J_0(p)/I_{\mathbf{e}}J_0(p)$, définie sur K .

Cette construction est similaire à celle de Merel [1996] pour la courbe modulaire classique. On commence par donner deux propriétés de $I_{\mathbf{e}}$ qui serviront pour l'étude de $J_{\mathbf{e}}(p)$.

Lemme 4.2. (i) *On a*

$$I_{\mathbf{e}} = \bigcap_{\substack{[F] \in \mathbb{C} \\ L(F, 1) \neq 0}} a_{[F]}. \tag{3}$$

(ii) *Soit $F \in H(\mathbb{C})$ une cochaîne propre pour \mathbb{T} et non nulle. Alors*

$$I_{\mathbf{e}}F = 0 \iff L(F, 1) \neq 0.$$

Démonstration. (i) Voir la preuve du lemme 7.12 de [Armana 2011b].

(ii) Si $L(F, 1) \neq 0$, l'idéal I_e est contenu dans $a_{[F]}$ d'après (3). Cela démontre un sens de l'équivalence. Passons à l'autre. Le $(\mathbb{T} \otimes_{\mathbb{Z}} \mathbb{Q})$ -module $M^0(\mathbb{Q})$ est semi-simple, par semi-simplicité de $\mathbb{T} \otimes_{\mathbb{Z}} \mathbb{Q}$, et libre de rang 1 par le lemme 3.4. On a donc décomposition en somme directe $M^0(\mathbb{Q}) = (\mathbb{T} \otimes_{\mathbb{Z}} \mathbb{Q})\mathbf{e} \oplus I_e M^0(\mathbb{Q})$. Soit F non nulle dans $H(\mathbb{C})$, propre pour \mathbb{T} et annulée par I_e . Elle est orthogonale à la seconde composante de $M^0(\mathbb{Q})$ pour $\langle \cdot, \cdot \rangle$. Cet accouplement étant non dégénéré, il existe $u \in \mathbb{T} \otimes_{\mathbb{Z}} \mathbb{Q}$ tel que $0 \neq \langle u\mathbf{e}, F \rangle = \langle \mathbf{e}, uF \rangle$. Comme F est propre, on obtient $\langle \mathbf{e}, F \rangle \neq 0$. Cela revient à dire $L(F, 1) \neq 0$. \square

Si F est primitive avec $L(F, 1) \neq 0$, on a $(1 + w_p) \in a_{[F]}$ d'après l'équation (1). Donc par le lemme 4.2, l'idéal I_e contient $(1 + w_p)$. En posant

$$J_0(\mathfrak{p})^- = J_0(\mathfrak{p}) / (1 + w_p)J_0(\mathfrak{p})$$

on a alors un homomorphisme canonique surjectif $J_0(\mathfrak{p})^- \rightarrow J_e(\mathfrak{p})$.

Proposition 4.3. *La variété abélienne $J_e(\mathfrak{p})$ est isogène sur K au produit de variétés abéliennes simples*

$$\prod_{\substack{[F] \in \mathcal{C} \\ L(F, 1) \neq 0}} J_{[F]}.$$

On a donc, pour $s \in \mathbb{C}$,

$$L(J_e(\mathfrak{p}), s) = \prod_{\substack{F \in \mathcal{F} \\ L(F, 1) \neq 0}} L(F, s). \tag{4}$$

Le groupe de Mordell–Weil $J_e(\mathfrak{p})(K)$ est fini.

Démonstration. D'après la théorie d'Eichler–Shimura, due dans ce cadre à Drinfeld [1974], les variétés abéliennes $J_e(\mathfrak{p})$ et $\prod_{[F] \in \mathcal{C}, I_e \subset a_{[F]}} J_{[F]}$ sont isogènes sur K (c'est un cas particulier du lemme 4.1 de [Tamagawa 1995]). Donc leurs fonctions L de Hasse–Weil coïncident. D'après le lemme 4.2, on peut remplacer la condition $I_e \subset a_{[F]}$ par $L(F, 1) \neq 0$. En combinant à (2), on obtient l'égalité (4) pour tout $s \in \mathbb{C}$. En particulier, $L(J_e(\mathfrak{p}), 1)$ est non nul. Par une inégalité connue dans la conjecture de Birch et Swinnerton-Dyer pour les variétés abéliennes sur K (théorème 11(i) de [Schneider 1982]), le groupe de Mordell–Weil $J_e(\mathfrak{p})(K)$ est alors fini. \square

Pál [2010, définition 5.10] a construit un objet qui coïncide probablement avec notre quotient d'enroulement. Il est possible de montrer que $J_e(\mathfrak{p})$ est le plus grand quotient optimal de $J_0(\mathfrak{p})$ dont la fonction L ne s'annule pas en $s = 1$, en suivant les lignes de la proposition 5.11(iii) de [Pál 2010]. Selon la conjecture de Birch et

Swinerton-Dyer, $J_e(\mathfrak{p})$ serait alors le plus grand quotient optimal de $J_0(\mathfrak{p})$ n'ayant qu'un nombre fini de points K -rationnels.

Dans la situation classique, il résulte de travaux de Mazur que l'homomorphisme canonique induit une bijection entre le groupe des points \mathbb{Q} -rationnels d'ordre fini de la jacobienne et le groupe des points \mathbb{Q} -rationnels du quotient d'enroulement (conséquence du corollaire III/1.4 et du théorème II/8.10 de [Mazur 1977]). Par analogie, on s'attend ici à une bijection naturelle entre $J_0(\mathfrak{p})(K)_{\text{tors}}$ et $J_e(\mathfrak{p})(K)$.

4B. Étude pour \mathfrak{p} de petit degré. En nous appuyant sur des résultats de Schweizer, on décrit le quotient d'enroulement lorsque le premier \mathfrak{p} est de degré 3 ou 4.

4B1. Quotients d'enroulement triviaux.

Proposition 4.4. *On a $J_e(\mathfrak{p}) = J_0(\mathfrak{p})$ si et seulement si \mathfrak{p} est de degré 3. Dans cette situation, on a les propriétés suivantes :*

- L'idéal I_e est nul.
- La fonction $L(J_e(\mathfrak{p}), s)$ est constante égale à 1.
- Le groupe $J_0(\mathfrak{p})(K)$ est cyclique d'ordre $q^2 + q + 1$.
- Le groupe de Tate–Shafarevich de $J_0(\mathfrak{p})$ est trivial.

Démonstration. Supposons $J_e(\mathfrak{p}) = J_0(\mathfrak{p})$. Comme l'idéal I_e contient $(1 + w_{\mathfrak{p}})$, l'involution $w_{\mathfrak{p}}$ agit comme -1 sur la jacobienne. Cela signifie que la courbe $X_0(\mathfrak{p})$ est hyperelliptique. Or, d'après Schweizer (théorème 20 de [Schweizer 1997]), les seuls premiers \mathfrak{p} pour lesquels $X_0(\mathfrak{p})$ est hyperelliptique sont ceux de degré 3.

Réciproquement, supposons \mathfrak{p} premier de degré 3. Alors d'après le lemme 3.3, la fonction L de toute forme primitive est constante égale à 1. Par le lemme 4.2, on en déduit $I_e = \bigcap_{[F] \in \mathcal{O}} a_{[F]} = \{0\}$. Donc la sous-variété abélienne $I_e J_0(\mathfrak{p})$ est nulle et $J_e(\mathfrak{p}) = J_0(\mathfrak{p})$. Avec la proposition 4.3, on obtient $L(J_e(\mathfrak{p}), s) = 1$ et $J_0(\mathfrak{p})(K)$ est fini.

Par ailleurs, le théorème 1.2 de [Pál 2005] dit que le sous-groupe de torsion de $J_0(\mathfrak{p})(K)$ est cyclique (pour \mathfrak{p} premier quelconque) et, si \mathfrak{p} est de degré 3, d'ordre $q^2 + q + 1$. Donc ici $J_0(\mathfrak{p})(K)$ est cyclique d'ordre $q^2 + q + 1$.

On constate que le rang de $J_0(\mathfrak{p})(K)$ coïncide avec l'ordre d'annulation en $s = 1$ de $L(J_0(\mathfrak{p}), s)$, car ils sont tous deux nuls. D'après le théorème de Kato et Trihan [2003], la formulation forte de la conjecture de Birch et Swinerton-Dyer est vérifiée pour $J_0(\mathfrak{p})$, donc

$$L(J_0(\mathfrak{p}), 1) = \frac{S c_{\mathfrak{p}} c_{\infty}}{(\#J_0(\mathfrak{p})(K))^2},$$

où S est l'ordre du groupe de Tate–Shafarevich de $J_0(\mathfrak{p})$ (il est alors fini), $c_{\mathfrak{p}}$ et c_{∞} sont les ordres du groupe des composantes du modèle de Néron de $J_0(\mathfrak{p})$ en \mathfrak{p} et $\infty = (1/T)$, respectivement (ce sont les seules places de mauvaise réduction de $J_0(\mathfrak{p})$). On a vu précédemment que $\#J_0(\mathfrak{p})(K) = q^2 + q + 1$. De plus, d'après

Gekeler, on a $c_p = q^2 + q + 1$ [1986, lemme 5.9 et proposition 5.10] et $c_\infty = q^2 + q + 1$ [1997b, 6.3(ii)]. On trouve donc $S = 1$. \square

4B2. Exemples en degré supérieur. Soit I un idéal de \mathbb{T} . On rappelle qu'il est dit saturé si le groupe abélien \mathbb{T}/I est sans torsion. On note I^{sat} le plus petit idéal saturé de \mathbb{T} contenant I .

Une cochaîne de $H(\mathbb{C})$ sera dite de *rang analytique* r si sa fonction L s'annule à l'ordre r en $s = 1$.

Proposition 4.5. Soit \mathfrak{p} un premier tel que toute forme primitive de $H_{\mathfrak{p}}(\mathbb{C})$ est de rang analytique ≤ 1 (c'est le cas si $\deg \mathfrak{p} = 4$). Alors $I_{\mathfrak{e}} = (1 + w_{\mathfrak{p}})^{\text{sat}}$ et la variété abélienne $J_{\mathfrak{e}}(\mathfrak{p})$ est isogène à $J_0(\mathfrak{p})^-$ sur K . Notons $d = \deg \mathfrak{p}$ et P le générateur unitaire de \mathfrak{p} .

– Si q est impair : soient $h(\sqrt{f})$ le nombre de classes d'idéaux de l'ordre $\mathbb{F}_q[T, \sqrt{f}]$ pour $f \in A$ et α un élément qui n'est pas un carré de \mathbb{F}_q^\times . Alors

$$\dim J_{\mathfrak{e}}(\mathfrak{p}) = \begin{cases} \frac{1}{2} \left(\frac{q^d - q^2}{q^2 - 1} + \frac{h(\sqrt{\alpha P})}{2} - 1 \right) & \text{si } d \text{ est pair,} \\ \frac{1}{2} \left(\frac{q^d - q}{q^2 - 1} + \frac{h(\sqrt{P}) + h(\sqrt{\alpha P})}{2} - 1 \right) & \text{si } d \text{ est impair.} \end{cases}$$

– Si q est pair : soit (S, R) l'unique couple de $A \times A$ tel que $P = S^2 + TR^2$. Posons $Q = \prod_a a^{\text{ord}_a(R)}$, le produit fini portant sur les polynômes unitaires irréductibles de A . Alors

$$\dim J_{\mathfrak{e}}(\mathfrak{p}) = \begin{cases} \frac{1}{2} \left(\frac{q^d - q^2}{q^2 - 1} + \sum_{f|Q} q^{\deg f} - 1 \right) & \text{si } d \text{ est pair,} \\ \frac{1}{2} \left(\frac{q^d - q}{q^2 - 1} + \sum_{f|Q} q^{\deg f} - 1 \right) & \text{si } d \text{ est impair.} \end{cases}$$

Démonstration. On a vu que $(1 + w_{\mathfrak{p}}) \subset I_{\mathfrak{e}}$, donc $(1 + w_{\mathfrak{p}})^{\text{sat}} \subset I_{\mathfrak{e}}$ car $I_{\mathfrak{e}}$ est saturé. Passons à l'inclusion réciproque. Soit $[F] \in \mathbb{C}$ tel que $(1 + w_{\mathfrak{p}})^{\text{sat}} \in a_{[F]}$. L'idéal $a_{[F]}$ contenant $(1 + w_{\mathfrak{p}})$, on a $w_{\mathfrak{p}}F = -F$. Par l'hypothèse sur l'ordre d'annulation et le lemme 3.3, $L(F, 1)$ est non nul. Par ailleurs, la description de $I_{\mathfrak{e}}$ donnée en (3) assure que $a_{[F]}$ contient $I_{\mathfrak{e}}$. L'idéal $(1 + w_{\mathfrak{p}})^{\text{sat}}$ étant saturé, il est l'intersection des idéaux premiers minimaux de \mathbb{T} le contenant. Donc $I_{\mathfrak{e}} \subset (1 + w_{\mathfrak{p}})^{\text{sat}}$.

Posons $I = (1 + w_{\mathfrak{p}})$, $J = J_0(\mathfrak{p})$ et montrons que les variétés abéliennes $J/I^{\text{sat}}J$ et J/IJ sont isogènes. Le \mathbb{Z} -module I^{sat}/I est de torsion et de type fini (pour la dernière affirmation, car I^{sat} est de type fini comme sous-module de \mathbb{T}). Donc I^{sat}/I est fini. La surjection canonique $J \rightarrow J/I^{\text{sat}}J$ induit un homomorphisme surjectif de variétés abéliennes $J/IJ \rightarrow J/I^{\text{sat}}J$. Son noyau $I^{\text{sat}}J/IJ$ est fini par ce qui précède. Cet homomorphisme est donc l'isogénie cherchée.

Notons g la dimension de J et g^+ celle de IJ . La suite exacte de variétés abéliennes $0 \rightarrow IJ \rightarrow J \rightarrow J/IJ \rightarrow 0$ donne $\dim J_{\mathfrak{e}}(\mathfrak{p}) = \dim(J/IJ) = g - g^+$. Avec la formule de Riemann–Hurwitz, Schweizer [1997, proposition 7] a établi

des expressions pour g^+ . On en déduit

$$\dim J_{\mathfrak{e}}(\mathfrak{p}) = \begin{cases} \frac{1}{2}(g - 1 + \frac{n}{2}) & \text{si } q \text{ est impair,} \\ \frac{1}{2}(g - 1 + n) & \text{si } q \text{ est pair,} \end{cases}$$

où n est le nombre de points fixes de l'involution $w_{\mathfrak{p}}$ sur $X_0(\mathfrak{p})$. Ces points fixes sont dénombrés dans [Schweizer 1997, proposition 11 et lemme 12] :

$$n = \begin{cases} h(\sqrt{\alpha P}) & \text{si } q \text{ est impair et } \deg \mathfrak{p} \text{ pair.} \\ h(\sqrt{P}) + h(\sqrt{\alpha P}) & \text{si } q \text{ est impair et } \deg \mathfrak{p} \text{ impair.} \\ \sum_{f|Q} q^{\deg f} & \text{si } q \text{ est pair.} \end{cases}$$

En substituant la formule pour g (proposition 3.2), on trouve les dimensions annoncées. □

4C. Minoration de la dimension. La dimension de $J_{\mathfrak{e}}(\mathfrak{p})$ est, d'après la proposition 4.3,

$$\dim J_{\mathfrak{e}}(\mathfrak{p}) = \sum_{\substack{[F] \in \mathbb{C} \\ L(F,1) \neq 0}} \dim J_{[F]} = \sum_{\substack{[F] \in \mathbb{C} \\ L(F,1) \neq 0}} \#[F] = \#\{F \in \mathcal{F} \mid L(F, 1) \neq 0\}.$$

Dans [Armana 2011b], on a minoré cette quantité *via* une indépendance linéaire dans $\mathbb{T}\mathfrak{e}$.

Théorème 4.6 (reformulation du théorème 1.3 de [Armana 2011b]). *Si \mathfrak{p} est premier de degré ≥ 3 et r est la partie entière de $(\deg(\mathfrak{p}) - 3)/2$, on a*

$$\dim J_{\mathfrak{e}}(\mathfrak{p}) \geq \frac{q^{r+1} - 1}{q - 1} \geq \frac{(q^2 - 1)^{1/2}}{q^2} (\dim J_0(\mathfrak{p}))^{1/2}.$$

Cette estimation est meilleure que celle obtenue pour le quotient d'enroulement classique par une approche similaire (liberté d'une famille de symboles modulaires). En effet, Parent [1999, remarque page 89] et VanderKam [2000] obtiennent des minorants en $(\dim J_0(p^n))^{1/6}$ et $\dim(J_0(p))^{1/2+\varepsilon}$ pour tout $\varepsilon > 0$, pour les jacobiniennes de courbes modulaires classiques $X_0(p^n)$ et $X_0(p)$ respectivement. Toujours dans le cas classique, des méthodes de théorie analytique des nombres fournissent même des estimations linéaires en la dimension de la jacobienne : $(\frac{1}{6} + o(1)) \dim J_0(p)$ chez Kowalski et Michel [1999, théorème 3], amélioré en $(\frac{1}{4} + o(1)) \dim J_0(p)$ par Iwaniec et Sarnak [2000, corollaire 13]. Sur $\mathbb{F}_q(T)$, on pourrait s'attendre à une borne linéaire.

Corollaire 4.7. *Les propriétés suivantes sont équivalentes pour un premier \mathfrak{p} :*

- (i) *La variété abélienne $J_{\mathfrak{e}}(\mathfrak{p})$ est non nulle.*
- (ii) $\deg \mathfrak{p} \geq 3$.
- (iii) $g(X_0(\mathfrak{p})) > 0$.

Démonstration. L'équivalence des deux dernières affirmations provient des formules pour le genre (proposition 3.2). Si le genre est nul, la variété jacobienne est nulle, et de même pour $J_e(\mathfrak{p})$. Enfin, si $\text{deg } \mathfrak{p} \geq 3$, le théorème 4.6 assure que la variété abélienne $J_e(\mathfrak{p})$ est de dimension > 0 , donc n'est pas la variété abélienne nulle. \square

4D. Une version raffinée de $J_e(\mathfrak{p})$.

4D1. Construction. Notons $\overline{M^0}$ le quotient maximal sans torsion $M^0/(M^0)_{\text{tors}}$. Il s'identifie à un sous \mathbb{Z} -module de $M^0(\mathbb{Q})$. L'élément d'enroulement e étant défini sur \mathbb{Q} , il possède un dénominateur d_e qui est le plus petit entier strictement positif n tel que $ne \in \overline{M^0}$. Dans [Armana 2011b, proposition 7.5], on a vu que d_e est premier à p .

Notation 4.8. On note \tilde{e} la classe de $d_e e$ dans $\overline{M^0}/p\overline{M^0}$. Soit \tilde{I}_e l'annulateur de \tilde{e} dans \mathbb{T} c'est-à-dire l'ensemble des $u \in \mathbb{T}$ tels que $d_e u e \in p\overline{M^0}$. Il contient $I_e + p\mathbb{T}$. Si I est un idéal de \mathbb{T} , on note \hat{I} l'idéal annulateur de I dans \mathbb{T} .

Dans la section 7E, nous serons amenés à considérer une variante du quotient d'enroulement. *Jusqu'à la fin de section 4D1, nous faisons l'hypothèse suivante afin de construire cette variante.*

Hypothèse 4.9. *Il existe un idéal saturé I de \mathbb{T} vérifiant :*

- (J1) $I_e \subset I$.
- (J2) $I \subset \tilde{I}_e$.
- (J3) $\hat{I} + \tilde{I}_e = \mathbb{T}$.

Définition 4.10. Soit $I J_0(\mathfrak{p})$ la sous-variété abélienne de $J_0(\mathfrak{p})$ engendrée par ux pour $u \in I$ et $x \in J_0(\mathfrak{p})$. Le *quotient raffiné* $J'_e(\mathfrak{p})$ relatif à I est la variété abélienne quotient $J_0(\mathfrak{p})/I J_0(\mathfrak{p})$, définie sur K .

Il satisfait des propriétés analogues à celles du quotient d'enroulement.

Proposition 4.11. (i) *Le groupe abélien $J'_e(\mathfrak{p})(K)$ est fini.*

(ii) *Soient \mathfrak{p} premier de degré $d \geq 3$ et r la partie entière de $(d - 3)/2$. On a*

$$\dim J'_e(\mathfrak{p}) \geq \frac{q^{r+1} - 1}{q - 1}.$$

En particulier, la variété abélienne $J'_e(\mathfrak{p})$ est non nulle.

Démonstration. (i) Par le lemme 4.10 de [Tamagawa 1995], la variété abélienne $J'_e(\mathfrak{p})$ est isogène sur K à

$$\prod_{\substack{[F] \in \mathbb{C} \\ IF=0}} J_{[F]}.$$

La propriété (J1) assure que toute forme primitive F annihilée par I l'est aussi par I_e , donc vérifie $L(F, 1) \neq 0$ par le lemme 4.2. On conclut comme dans la preuve de la proposition 4.3.

(ii) D'après l'isogénie évoquée précédemment, la dimension de $J'_e(\mathfrak{p})$ est

$$\sum_{\substack{[F] \in \mathcal{O} \\ IF=0}} \dim J_{[F]} = \sum_{\substack{[F] \in \mathcal{O} \\ I \subset a_{[F]}}} \dim_{\mathbb{Q}}((\mathbb{T}/a_{[F]}) \otimes_{\mathbb{Z}} \mathbb{Q}).$$

La projection canonique donne un isomorphisme $\mathbb{T}/I \rightarrow \prod_{I \subset a_{[F]}} \mathbb{T}/a_{[F]}$ car l'idéal I est saturé. Donc la dimension de $J'_e(\mathfrak{p})$ est égale au rang du \mathbb{Z} -module libre \mathbb{T}/I . Elle est minorée par le rang de \mathbb{T}/\tilde{I}_e , puisque \tilde{I}_e contient I (propriété (J2)). Par ailleurs, on trouve dans [Armana 2011b, théorème 7.10(ii)] l'énoncé suivant dans $\mathbb{T}\tilde{e}$: les symboles modulaires $T_m\tilde{e}$, pour m de degré $\leq r$, sont libres sur \mathbb{F}_p . Le rang sur \mathbb{Z} de \mathbb{T}/\tilde{I}_e , qui coïncide avec sa dimension comme \mathbb{F}_p -espace vectoriel, est donc $\geq (q^{r+1} - 1)/(q - 1)$. Donc $\dim J'_e(\mathfrak{p}) \geq (q^{r+1} - 1)/(q - 1) > 0$. \square

4D2. Des situations dans lesquelles l'hypothèse 4.9 est vérifiée. On commence par vérifier l'hypothèse pour l'idéal I_e avec \mathfrak{p} de petit degré. De manière générale, l'idéal I_e est saturé et vérifie les propriétés (J1) et (J2); il vérifie (J3) dès que $I_e + \hat{I}_e + p\mathbb{T} = \mathbb{T}$.

Proposition 4.12. *Supposons que \mathfrak{p} vérifie l'une des deux conditions suivantes :*

- (i) \mathfrak{p} est de degré 3.
- (ii) $p \neq 2$ et toute forme primitive de $H_{\mathfrak{p}}(\mathbb{C})$ est de rang analytique ≤ 1 (c'est le cas si $\deg \mathfrak{p} = 4$).

Alors l'idéal I_e vérifie l'hypothèse 4.9.

Démonstration. (i) Si \mathfrak{p} est de degré 3, l'idéal I_e est nul d'après la proposition 4.4. Donc son annulateur est \mathbb{T} et les trois propriétés de l'hypothèse 4.9 sont satisfaites.

(ii) Soit \mathfrak{p} comme dans l'énoncé. Par la proposition 4.5, on a $I_e = (1 + w_{\mathfrak{p}})^{\text{sat}}$. De $(1 - w_{\mathfrak{p}})(1 + w_{\mathfrak{p}}) = 0$, on déduit $(1 - w_{\mathfrak{p}})I_e = 0$. Ainsi, $I_e + \hat{I}_e$ contient l'idéal $(1 + w_{\mathfrak{p}})\mathbb{T} + (1 - w_{\mathfrak{p}})\mathbb{T}$ et donc $2\mathbb{T}$. On obtient les inclusions

$$2\mathbb{T} + p\mathbb{T} \subset I_e + \hat{I}_e + p\mathbb{T} \subset \mathbb{T}.$$

Comme 2 et p sont premiers entre eux, ces inclusions sont des égalités. \square

On définit maintenant un idéal I'_e qui vérifie les propriétés (J2) et (J3) et on donne une condition pour qu'il vérifie (J1).

Notation 4.13. On note \mathcal{P} l'ensemble des idéaux premiers minimaux de \mathbb{T} et \mathcal{P}' l'ensemble des $\mathfrak{q} \in \mathcal{P}$ tels qu'il existe un idéal maximal \mathfrak{m} de \mathbb{T} contenant \mathfrak{q} et \tilde{I}_e . Enfin, I'_e désigne l'idéal $\bigcap_{\mathfrak{q} \in \mathcal{P}'} \mathfrak{q}$ de \mathbb{T} .

L'idéal I'_e est donc l'intersection des idéaux premiers minimaux \mathfrak{q} de \mathbb{T} tels que l'inclusion $\mathfrak{q} + \tilde{I}_e \subset \mathbb{T}$ est stricte.

Lemme 4.14. *On a $\prod_{\mathfrak{q} \notin \mathcal{P}'} \mathfrak{q} \subset \hat{I}'_e$.*

Démonstration. Il suffit de voir que les générateurs $\prod_{\mathfrak{q} \notin \mathcal{P}'} x_{\mathfrak{q}}$ (avec $x_{\mathfrak{q}} \in \mathfrak{q}$) de l'idéal produit annulent I'_e . Posons $y = u \prod_{\mathfrak{q} \notin \mathcal{P}'} x_{\mathfrak{q}}$ avec $u \in I'_e$. Soit \mathfrak{m} un idéal premier minimal de \mathbb{T} . Si $\mathfrak{m} \notin \mathcal{P}'$ alors $x_{\mathfrak{m}}$ appartient à \mathfrak{m} , donc y aussi. Si $\mathfrak{m} \in \mathcal{P}'$ alors $I'_e \subset \mathfrak{m}$, donc u appartient à \mathfrak{m} et il en est de même de y . Ainsi, y est dans l'intersection des idéaux premiers minimaux de \mathbb{T} . Donc y est nul. \square

Proposition 4.15. (i) *L'idéal I'_e est saturé.*

(ii) *On a $I'_e = \bigcap_{k \geq 1} (\tilde{I}_e)^k$. En particulier, I'_e est contenu dans \tilde{I}_e .*

(iii) *On a $\hat{I}'_e + \tilde{I}_e = \mathbb{T}$.*

Démonstration. (i) Supposons qu'on ait $nu \in I'_e$ avec $u \in \mathbb{T}$ et n non nul dans \mathbb{Z} . Soit \mathfrak{q} un idéal de \mathcal{P}' . Alors nu appartient à \mathfrak{q} par définition de I'_e . Si $n \in \mathfrak{q}$, on aurait $nF = 0$ pour une forme primitive F dans l'orbite correspondant à \mathfrak{q} , donc $F = 0$, ce qui est exclu. Comme l'idéal \mathfrak{q} est premier, u appartient donc à \mathfrak{q} . Cela prouve que u est dans I'_e .

(ii) C'est une conséquence de l'énoncé d'algèbre commutative suivant. Soient R un anneau noethérien et J un idéal de R . Soit \mathcal{P} l'ensemble des idéaux premiers minimaux de R . Alors on a

$$\bigcap_{\substack{\mathfrak{q} \in \mathcal{P} \\ J + \mathfrak{q} \neq R}} \mathfrak{q} = \bigcap_{k \geq 1} J^k. \tag{5}$$

En effet, soit $R_{\mathfrak{m}}$ le localisé de R par rapport à la partie multiplicative $R - \mathfrak{m}$ pour un idéal maximal \mathfrak{m} de R . Comme R est noethérien, le théorème de Krull donne $\bigcap_{k \geq 1} J^k = \bigcap_{\mathfrak{m}, J \subset \mathfrak{m}} \ker(R \rightarrow R_{\mathfrak{m}})$ [Atiyah et Macdonald 1969, exercice 10/3]. Par ailleurs, le noyau de $R \rightarrow R_{\mathfrak{m}}$ est $\bigcap_{\mathfrak{q} \in \mathcal{P}, \mathfrak{q} \subset \mathfrak{m}} \mathfrak{q}$ [ibid, corollaire 10.21]. En combinant ces observations, on obtient l'égalité (5).

(ii) Supposons que $\hat{I}'_e + \tilde{I}_e \neq \mathbb{T}$. Alors il existe un idéal maximal \mathfrak{m} de \mathbb{T} contenant \hat{I}'_e et \tilde{I}_e . Le lemme 4.14 permet d'exhiber un idéal premier minimal $\mathfrak{q} \notin \mathcal{P}'$ contenu dans \mathfrak{m} . Comme $\tilde{I}_e \subset \mathfrak{m}$, l'idéal \mathfrak{q} appartient alors à \mathcal{P}' par définition de cet ensemble. C'est impossible. \square

Proposition 4.16. *Si $d_e e$ engendre le \mathbb{T} -module $\overline{M^0} / I'_e \overline{M^0}$, on a $I_e \subset I'_e$, et donc I'_e vérifie (J1).*

Démonstration. L'idéal I'_e étant saturé, il est l'intersection des idéaux premiers minimaux de \mathbb{T} le contenant. Soient \mathfrak{q} un tel idéal et F une forme primitive de l'orbite correspondant à \mathfrak{q} . Pour montrer que $I_e \subset I'_e$, il s'agit d'établir $uF = 0$ pour tout $u \in I_e$. L'accouplement entre $M^0(\mathbb{C})$ et $H(\mathbb{C})$ étant parfait, cela revient à

prouver que uF est orthogonal à $\overline{M^0}(\mathbb{C})$. Comme $d_e \mathbf{e}$ engendre $\overline{M^0}/I'_e \overline{M^0}$, on a la décomposition en sous \mathbb{T} -modules $\overline{M^0} = \mathbb{T} d_e \mathbf{e} + I'_e \overline{M^0}$. Par extension des scalaires, on en déduit

$$M^0(\mathbb{C}) = (\mathbb{T} \otimes_{\mathbb{Z}} \mathbb{C}) \mathbf{e} + (I'_e \otimes_{\mathbb{Z}} \mathbb{C}) M^0(\mathbb{C}).$$

On utilise ensuite l'équivariance de l'accouplement par Hecke. L'élément u annihilant \mathbf{e} , il reste à montrer que uF est orthogonal à $(I'_e \otimes_{\mathbb{Z}} \mathbb{C}) M^0(\mathbb{C})$. Mais c'est le cas puisque I'_e annule F . \square

5. L'uniformisation et le module de Tate–Drinfeld

5A. Uniformisation de Tate–Drinfeld.

5A1. Réduction des modules de Drinfeld. D'après [Drinfeld 1974, proposition 7.1], tout module de Drinfeld ϕ sur un A -corps local L a réduction potentiellement stable. En d'autres termes, il existe un module de Drinfeld ϕ' sur une extension F/L , à coefficients dans l'anneau de valuation \mathbb{O} de F , tel que ϕ est isomorphe à ϕ' sur F et la réduction $\overline{\phi'}$ de ϕ' est un module de Drinfeld sur le corps résiduel. On appellera un tel ϕ' un *modèle potentiellement stable* de ϕ .

Supposons ϕ de rang 2. Alors ϕ a bonne réduction potentielle (*i.e.*, $\overline{\phi'}$ est de rang 2) ou réduction potentiellement stable de rang 1 ($\overline{\phi'}$ est de rang 1). Si ϕ est muni d'un point $x \in {}^\phi L$, on obtient par l'isomorphisme un point y de ${}^{\phi'} F$. Si on part d'un point x entier (*i.e.*, dans l'anneau de valuation de L), y n'est pas nécessairement dans \mathbb{O} . Cependant, si y est dans \mathbb{O} , on peut vérifier que l'image de x dans tout autre modèle potentiellement stable de ϕ est encore dans \mathbb{O} .

5A2. Uniformisation de Tate–Drinfeld. C'est l'analogue de l'uniformisation de Tate pour les courbes elliptiques à réduction multiplicative. Soit L un A -corps local dont l'anneau de valuation discrète \mathbb{O} est complet. Si ψ est un module de Drinfeld sur L , un ψ -réseau de rang 1 est un sous A -module projectif, discret, de rang 1 et invariant par $\text{Gal}(L^{\text{sep}}/L)$ de ${}^\psi L^{\text{sep}}$. D'après [Drinfeld 1974, paragraphe 7], il existe une bijection entre les ensembles de classes d'isomorphisme sur L de

- modules de Drinfeld ϕ de rang 2 sur L à réduction potentiellement stable de rang 1,
- couples (ψ, Γ) où ψ est un module de Drinfeld de rang 1 sur L et Γ est un ψ -réseau de rang 1,

respectivement. L'uniformisation permet aussi de décrire les points de torsion de ϕ . Soit e la fonction exponentielle associée au réseau Γ (voir [Drinfeld 1974] pour sa définition). Soit \mathfrak{a} un idéal non nul de A , dont on fixe un générateur a . Par construction, on a $\phi_a e = e \psi_a$ et l'isomorphisme de A -modules

$$e : \psi_a^{-1}(\Gamma) / \Gamma \xrightarrow{\sim} \phi[\mathfrak{a}], \quad (6)$$

où $\psi_a^{-1}(\Gamma)$ est l'image réciproque de Γ par ψ_a . Supposons ϕ à coefficients dans \mathbb{C} . Alors ψ est à coefficients dans \mathbb{C} et on a des A -modules $\phi_{\mathbb{C}}$ et $\psi_{\mathbb{C}}$ induits par ϕ et ψ respectivement.

Lemme 5.1. *Si ϕ est à coefficients dans \mathbb{C} , on a pour tout $a \in A - \{0\}$,*

$$\phi[\mathfrak{a}](\mathbb{C}) = e(\psi[\mathfrak{a}](\mathbb{C})).$$

Démonstration. C'est une adaptation d'arguments de Rosen. On esquisse la preuve et renvoie à [Rosen 2003, lemme 5.3 et théorème 5.4] pour les détails. D'abord, l'inclusion \supset est immédiate car e et ψ sont à coefficients dans \mathbb{C} . Passons à l'autre inclusion. Fixons une racine primitive λ_a de ψ_a dans L^{alg} (*primitive* signifiant : λ_a engendre $\psi[\mathfrak{a}]$ comme A -module). D'après l'uniformisation de Tate–Drinfeld, le réseau Γ est le noyau de e et il est de la forme $\psi_A(\gamma) = \{\psi_b(\gamma) \mid b \in A\}$ pour un $\gamma \in \Gamma$. Fixons aussi une racine γ_a de $\psi_a(x) = \gamma$ dans L^{alg} . On note w l'unique prolongement de la valuation de L à L^{alg} . L'ensemble $\psi_a^{-1}(\Gamma)/\Gamma$ a pour système de représentants :

$$\{\psi_c(\lambda_a) + \psi_d(\gamma_a) \mid (c, d) \in A \times A, \deg c < \deg a, \deg d < \deg a\} \subset \psi_a^{-1}(\Gamma).$$

De plus, pour un tel (c, d) avec $d \neq 0$, on a $w(\psi_c(\lambda_a)) \geq 0$ et $w(\psi_d(\gamma_a)) < 0$. On en déduit $w(e(\psi_c(\lambda_a))) \geq 0$ et $w(e(\psi_d(\gamma_a))) < 0$. Par linéarité de e et l'isomorphisme (6), on a alors $\phi[\mathfrak{a}](\mathbb{C}) \subset e(\psi[\mathfrak{a}])$. En raisonnant comme à la page 254 de [Rosen 2003], on voit que $\phi[\mathfrak{a}](\mathbb{C})$ est en fait contenu dans $e(\psi[\mathfrak{a}](L))$. Mais tout élément de $\psi[\mathfrak{a}](L)$ est dans \mathbb{C} , car il est racine du polynôme ψ_a dont le coefficient dominant est inversible dans \mathbb{C} . Finalement, on obtient $\phi[\mathfrak{a}](\mathbb{C}) \subset e(\psi[\mathfrak{a}](\mathbb{C}))$. \square

5B. Estimation locale pour la torsion. Par un argument local, Poonen a donné un résultat quantitatif sur la torsion des modules de Drinfeld de rang quelconque à bonne réduction potentielle (théorèmes 5 et 7 de [Poonen 1997]). La borne qu'il obtient peut être rendue explicite, mais est loin d'être optimale en rang 2. On raffine l'estimation dans le cas des modules de Drinfeld de rang 2.

Proposition 5.2. *Soit $K_{\mathfrak{l}}$ la complétion de K en un premier \mathfrak{l} . Soient L une extension de $K_{\mathfrak{l}}$ de degré $\leq d$, ϕ un module de Drinfeld de rang 2 sur L et x un point de $(\phi L)_{\text{tors}}$ d'ordre \mathfrak{n} avec $\mathfrak{n} \neq A$ et $\mathfrak{l} \nmid \mathfrak{n}$. Supposons vérifiée l'une des conditions suivantes :*

- (i) ϕ a bonne réduction potentielle.
- (ii) ϕ a réduction potentiellement stable de rang 1 et x donne un point entier d'un modèle potentiellement stable de ϕ .

Alors on a $\deg \mathfrak{n} \leq d \deg \mathfrak{l}$.

Démonstration. Notons $r = 2$ dans le premier cas, $r = 1$ dans le deuxième. Le module de Drinfeld ϕ est défini par $\phi_T = T\tau^0 + g\tau + \Delta\tau^2 \in L\{\tau\}$ avec $g \in L$

et $\Delta \in L^\times$. Notons v la valuation de L et P une uniformisante. Le polynôme $X^{q^r-1} - P$ est d'Eisenstein donc irréductible dans $L[X]$. Soit α une racine de ce polynôme et $F = L(\alpha)$. L'extension F/L est séparable et totalement ramifiée de degré $q^r - 1$. Notons O l'anneau de valuation de F et w l'unique valuation de F prolongeant v . Supposons vérifiée l'assertion :

Il existe un module de Drinfeld ψ de rang r sur F , à coefficients dans O et à bonne réduction, et un point y de $(\psi O)_{\text{tors}}$ d'ordre n .

Soit B le sous A -module de $(\psi F)_{\text{tors}}$ engendré par y (en fait, B est contenu dans ψO). Soit $\pi : B \rightarrow k$ l'homomorphisme de groupes additifs donné par la réduction sur le corps résiduel k de F . Démontrons qu'il est injectif. Un élément z de B est de n -torsion pour ψ , donc si N est un générateur de \mathfrak{n} , on a

$$\psi_N(z) = Nz + \sum_{i=1}^{r \deg N} l_i z^{q^i} = 0,$$

avec $l_1, \dots, l_{r \deg N} \in O$ et $l_{r \deg N} \in O^\times$ (car ψ a bonne réduction). S'il existe z non nul dans le noyau de π , on aurait $N + \sum_{1 \leq i \leq r \deg N} l_i z^{q^i-1} = 0$. De $w(z) > 0$, on déduirait $w(N) > 0$, ce qui contredit $l \nmid n$. Donc π est injectif.

Comme F/L est totalement ramifiée, les corps résiduels de F et L sont égaux. De plus, celui de L est une extension de degré au plus d de \mathbb{F}_l . En combinant ce qui précède, on trouve $\#B \leq (\#\mathbb{F}_l)^d \leq q^{d \deg l}$. Par ailleurs, y est d'ordre n dans ψO , donc B est isomorphe à A/\mathfrak{n} comme A -module. On en déduit $\#B = q^{\deg n}$. Ainsi on a l'inégalité $\deg n \leq d \deg l$. Maintenant, démontrons l'assertion.

Supposons la condition (i) vérifiée. Posons $u = \alpha^{-v(\Delta)}$ dans F^\times de sorte que $w(u) = -v(\Delta)/(q^2 - 1)$. Le module de Drinfeld ϕ ayant bonne réduction potentielle, son invariant modulaire $j = g^{q+1}/\Delta$ est entier, donc $v(\Delta) \leq (q + 1)v(g)$. Ainsi, on a $w(u) \geq -v(g)/(q - 1)$. On définit le module de Drinfeld ρ de rang 2 sur F par $\rho_T = T\tau^0 + u^{q-1}g\tau + u^{q^2-1}\Delta\tau^2$. Il est isomorphe à ϕ sur F et, par construction, à coefficients dans O et de terme dominant dans O^\times . Par l'isomorphisme avec ϕ , le point x de $(\phi L)_{\text{tors}}$ définit un point y de $(\psi F)_{\text{tors}}$ d'ordre n . De plus, y est racine du polynôme $\psi_N(z)$ qui est à coefficients dans O et de terme dominant inversible (car ψ est de rang 2 et a bonne réduction). Donc y est dans O .

Supposons la condition (ii) vérifiée. Posons $u = \alpha^{-v(g)}$ dans F^\times de sorte que $w(u) = -v(g)/(q - 1)$. Le module de Drinfeld ϕ n'ayant pas bonne réduction potentielle, on a $(q + 1)w(g) < w(\Delta)$ d'où $w(u^{q^2-1}\Delta) > 0$. Soit φ le module de Drinfeld sur F de rang 2 défini par $\varphi_T = T\tau^0 + u^{q-1}g\tau + u^{q^2-1}\Delta\tau^2$. Il est isomorphe à ϕ sur F , à coefficients dans O et sa réduction est de rang 1. C'est un modèle potentiellement stable de ϕ sur F . Par hypothèse sur x , on a un point x' de $(\varphi O)_{\text{tors}}$ d'ordre n . Considérons une uniformisation de Tate-Drinfeld (ρ, Γ) de φ sur F . Le module de Drinfeld ρ est de rang 1, à coefficients dans O et a bonne

réduction. Par le lemme 5.1, il existe $y \in \rho[n](O)$ tel que $x' = e(y)$. Comme x' est d'ordre n , on en déduit que l'ordre de y dans ${}^{\rho}O$ est aussi n . \square

5C. Le module de Tate–Drinfeld. Ce nom désigne l'objet analogue à la courbe de Tate classique dans le cadre de Drinfeld. Il a été étudié par Goss [1980b, définitions 1.51 et 1.54], Gekeler [1988, paragraphe 11.3], Böckle [2002, sections 2.2 à 2.4] et van der Heiden [2006, section 6]. Nous rappelons les résultats adaptés à notre situation.

5C1. Construction. Soit $K((t))$ le corps des séries de Laurent formelles sur K en l'indéterminée t . Considérons le module de Carlitz $\rho : A \rightarrow K((t))\{\tau\}$ de rang 1 défini par $\rho_T = T\tau^0 + \tau$. Posons $\Gamma = \rho_A(1/t) = \{\rho_a(1/t) \mid a \in A\} \subset A((t))$. Ce sous A -module de ${}^{\rho}K((t))^{\text{sep}}$ est projectif, de rang 1, discret et invariant par le groupe de Galois absolu de $K((t))$. D'après l'uniformisation de Tate–Drinfeld, la donnée de (ρ, Γ) définit un module de Drinfeld TD sur $K((t))$ de rang 2 et à réduction potentiellement stable de rang 1. On appelle TD le *module de Tate–Drinfeld*. Si $e_{\Gamma} \in K((t))\{\tau\}$ désigne l'exponentielle de Γ , on a alors

$$\text{TD}_a e_{\Gamma} = e_{\Gamma} \rho_a \quad (a \in A).$$

De plus, les réductions modulo (t) de TD et ρ coïncident. En fait, TD est un module de Drinfeld de rang 2 sur $A((t))$ à coefficients dans $A[[t]]$ (voir par exemple les lemmes 6.5 de [van der Heiden 2006] et 2.10 de [Böckle 2002]). Le polynôme TD_T est donc de la forme $T\tau^0 + g^*(t)\tau + \Delta^*(t)\tau^2$ avec $g^*(t)$ dans $A[[t]]^{\times}$ et $\Delta^*(t)$ dans $A((t))^{\times} \cap tA[[t]]$.

La construction précédente est inchangée si on remplace $\rho_A(1/t)$ par $\rho_A(1/(\lambda t))$ pour $\lambda \in \mathbb{F}_q^{\times}$: en effet, l'uniformisation de Tate–Drinfeld fournit alors un module de Drinfeld qui est isomorphe à TD sur \mathbb{F}_q , donc égal à TD. On en déduit que les séries formelles $g^*(t)$ et $\Delta^*(t)$ sont en fait dans $A((t^{q-1}))$ et TD est un module de Drinfeld de rang 2 sur $A((t^{q-1}))$ à coefficients dans $A[[t^{q-1}]]$.

Ces séries $g^*(t)$ et $\Delta^*(t)$ peuvent être vues comme développements formels des formes modulaires de Drinfeld g et Δ au voisinage de l'infini (voir [Goss 1980b] ou [Gekeler 1988] pour leur définition). Plus précisément, par la théorie analytique des modules de Drinfeld, le module de Carlitz sur \mathbb{C}_{∞} correspond à un réseau de \mathbb{C}_{∞} de rang 1 de la forme $\bar{\pi}A$, où la période fondamentale $\bar{\pi} \in \mathbb{C}_{\infty}^{\times}$ est définie à multiplication près par un élément de \mathbb{F}_q^{\times} . Dorénavant, on fixe un tel choix de $\bar{\pi}$. Notons e_A l'exponentielle associée au réseau A de rang 1 de \mathbb{C}_{∞} . Suivant la convention de [Gekeler 1988, 4.1], on pose $t(z) = \bar{\pi}^{-1}/e_A(z)$ pour $z \in \mathbb{C}_{\infty} - A$. En substituant $t(z)$ à t dans TD, on obtient un module de Drinfeld $\text{TD}(z)$. On peut voir que c'est aussi le module de Drinfeld de rang 2 sur \mathbb{C}_{∞} associé au réseau $\bar{\pi}Az \oplus \bar{\pi}A$ de rang 2. Ses coefficients sont reliés à g et Δ par $g^*(t(z)) = \bar{\pi}^{1-q}g(z)$

et $\Delta^*(t(z)) = \bar{\pi}^{1-q^2} \Delta(z)$ (les formes modulaires g et Δ sont de poids $q - 1$ et $q^2 - 1$, respectivement).

5C2. Points de torsion.

Notation 5.3. Pour tout $a \in A$, on fixe :

- Une racine primitive λ_a de ρ_a dans K^{alg} .
- Une racine γ_a de l'équation $\rho_a(x) = 1/t$ dans $K((t))^{\text{alg}}$.

Notons N le générateur unitaire d'un idéal non nul \mathfrak{n} . D'après (6), l'ensemble des points de \mathfrak{n} -torsion du module de Tate–Drinfeld est

$$\text{TD}[\mathfrak{n}] = e_{\Gamma}(\rho_N^{-1}(\Gamma)/\Gamma) = \{e_{\Gamma}(\rho_c(\lambda_N) + \rho_d(\gamma_N)) \mid (c, d) \in A/\mathfrak{n} \times A/\mathfrak{n}\},$$

le dernier ensemble étant bien défini et indépendant des choix de λ_N et γ_N . Donc les sous A -modules de $\text{TD}(K((t))^{\text{sep}})_{\text{tors}}$ isomorphes à A/\mathfrak{n} et stables par le groupe de Galois absolu de $K((t))$ sont :

$$\text{TD}_A e_{\Gamma}(\rho_c(\lambda_N) + \rho_d(\gamma_N)) \quad \text{avec } (c, d) \text{ d'ordre } \mathfrak{n} \text{ dans } (A/\mathfrak{n} \times A/\mathfrak{n})/(A/\mathfrak{n})^{\times}$$

(on fait agir $(A/\mathfrak{n})^{\times}$ diagonalement sur $A/\mathfrak{n} \times A/\mathfrak{n}$). Cet ensemble est en bijection naturelle avec la droite projective $\mathbb{P}^1(A/\mathfrak{n})$, donc avec l'ensemble $\Gamma_0(\mathfrak{n}) \backslash \mathbb{P}^1(K)$ des pointes de $\mathcal{X}_0(\mathfrak{n})$.

5C3. Interprétation modulaire. Soit $C_{\mathfrak{n}}$ le sous-module de TD correspondant à $(1 : 0) = \infty$ dans $\mathbb{P}^1(A/\mathfrak{n})$, i.e., $C_{\mathfrak{n}} = \text{TD}_A e_{\Gamma}(\lambda_N)$. Le module de Tate–Drinfeld TD muni de $C_{\mathfrak{n}}$ définit, par interprétation modulaire, une section

$$\mathbf{s} : \text{Spec } A[1/\mathfrak{n}][[t^{q-1}]] \rightarrow \mathcal{Y}_0(\mathfrak{n})$$

du morphisme structurel. Soit $r : \text{Spec } A[1/\mathfrak{n}] \rightarrow \text{Spec } A[1/\mathfrak{n}][[t^{q-1}]]$ le morphisme de schémas induit par $t^{q-1} \mapsto 0$ sur les anneaux.

Proposition 5.4. *Le morphisme \mathbf{s} se prolonge en un morphisme*

$$\mathbf{s} : \text{Spec } A[1/\mathfrak{n}][[t^{q-1}]] \rightarrow \mathcal{X}_0(\mathfrak{n}),$$

qui vérifie $\mathbf{s} \circ r = \infty$. De plus, \mathbf{s} induit un isomorphisme entre le spectre formel de $A[1/\mathfrak{n}][[t^{q-1}]]$ et le complété formel de $\mathcal{X}_0(\mathfrak{n})$ le long de la section ∞ .

Démonstration. Pour le prolongement, on se réfère à la démonstration du lemme 9.3 de [van der Heiden 2006]. Les autres assertions se déduisent de la proposition 9.1 et des théorèmes 9.2 et 10.3 de [loc.cit]. □

Le module de Tate–Drinfeld satisfait une propriété universelle : par changement de base, il décrit les modules de Drinfeld de rang 2 à réduction potentiellement stable de rang 1 *via* l'uniformisation de Tate–Drinfeld (théorème 7.8 de [van der Heiden 2006]). Conjointement à la proposition 5.4 et au lemme 5.1, cela amène au résultat suivant concernant l'interprétation modulaire de la pointe ∞ .

Proposition 5.5. *Soit L une extension finie de K , d'anneau des entiers \mathbb{O}_L . Soit ϕ un module de Drinfeld de rang 2 sur L et P un point de $(\phi L)_{\text{tors}}$ d'ordre n . En prenant ϕ et le sous-module cyclique engendré par P on définit un point de $X_0(n)(L)$ qui se prolonge de façon unique en une section $x : \text{Spec } \mathbb{O}_L \rightarrow X_0(n)$. Supposons que ϕ a réduction potentiellement stable de rang 1 en une place \mathfrak{L} de L . Alors la section x se spécialise comme ∞ en \mathfrak{L} si et seulement si P donne un point entier d'un modèle potentiellement stable de ϕ .*

6. Formes modulaires de Drinfeld

6A. Formes modulaires de Drinfeld algébriques de poids 2. Les formes modulaires pour $\mathbb{F}_q[T]$, ou formes modulaires de Drinfeld, ont été introduites par Goss [1980a; 1980b] puis étudiées notamment par Gekeler [1988]. Dans cette section on présente un point de vue algébrique sur les formes modulaires de Drinfeld doublement paraboliques de poids 2 et de type 1 pour $\Gamma_0(n)$, sans supposer n premier.

Pour les formes modulaires classiques, on dispose de plusieurs constructions algébriques à la Serre, Katz [1973] ou encore Deligne et Rapoport [1973]. Elles ont été comparées notamment dans [Mazur 1977, section II.4] en poids 2 pour $\Gamma_0(n) \subset \text{SL}_2(\mathbb{Z})$. Pour les formes modulaires de Drinfeld, on trouve dans la littérature les théories algébriques suivantes. Gekeler [1988, section 12] a donné un point de vue à la Serre des formes modulaires pour $\text{GL}_2(A)$ modulo un idéal premier. Pour les formes modulaires de niveau $\Gamma(n)$, Goss [1980b] a mis en place une théorie à la Katz. Nous présentons ici un point de vue algébrique pour $\Gamma_0(n)$ *via* les sections du faisceau des différentielles relatives, qui couvrira nos besoins. Toutefois, il resterait à faire le lien entre cette approche et celles de Gekeler et Goss.

6A1. Définition et t -développement. Soit R une algèbre sur $A[1/n]$. Considérons le R -schéma $\mathcal{X}_R = \mathcal{X}_0(n)_R = \mathcal{X}_0(n) \times_A R$ et son faisceau $\Omega_{\mathcal{X}_R/R}^1$ des différentielles relatives de degré 1. On adopte la définition suivante.

Définition 6.1. Soit $S(R)$ le R -module $H^0(\mathcal{X}_R, \Omega_{\mathcal{X}_R/R}^1)$ des sections globales de $\Omega_{\mathcal{X}_R/R}^1$. Un élément de $S(R)$ est appelé une *forme modulaire sur R pour $\Gamma_0(n)$* .

Posons $s = t^{q-1}$ où t désigne encore une indéterminée. Du morphisme

$$\mathbf{s}_R : \text{Spec } R[[s]] \rightarrow \mathcal{X}_R$$

déduit de \mathbf{s} , et de l'inclusion $i : R[[s]] \hookrightarrow R[[t]]$, on déduit un morphisme de schémas

$$\mathbf{t}_R : \text{Spec } R[[t]] \longrightarrow \mathcal{X}_R.$$

Définition 6.2. Soit $f \in S(R)$. Il existe une unique série formelle $F(t) \in t^2 R[[t]]$ telle que le tiré-en-arrière $\mathbf{t}_R^*(f)$ de f par \mathbf{t}_R soit $(F(t)/t^2) dt$. On appelle $F(t)$ le *t -développement de f* (en la pointe ∞).

Le facteur de normalisation $1/t^2$ sera justifié en 6A4.

Lemme 6.3. On a $F(t)/t \in sR[[s]]$.

Démonstration. Comme $\mathbf{t}_R = \mathbf{s}_R \circ \text{Spec}(i)$, on a $\mathbf{t}_R^*(f) = \text{Spec}(i)^*(\mathbf{s}_R^*(f)) = \mathbf{s}_R^*(f)$. Or $ds/s = -dt/t$ en caractéristique p . Donc

$$\mathbf{t}_R^*(f) = \frac{F(t)}{t^2} dt = -\frac{F(t)}{t} \frac{ds}{s}.$$

La conclusion suit. □

Notation 6.4. En vertu du lemme 6.3, le t -développement de f est de la forme $F(t) = \sum_{i \geq 1} a_{1+i(q-1)} t^{1+i(q-1)} \in t^2 R[[t]]$ soit encore, en posant $b_i = a_{1+i(q-1)}$ pour $i \geq 1$,

$$F(t) = \sum_{i \geq 1} b_i t^{1+i(q-1)} = t \sum_{i \geq 1} b_i s^i. \tag{7}$$

Proposition 6.5 (principe du t -développement). *L'homomorphisme de R -modules*

$$S(R) \rightarrow t^2 R[[t]], \quad f \mapsto F(t),$$

est injectif.

Démonstration. La démonstration de [Katz 1973, théorème 1.6.1] est encore valable dans notre contexte, en utilisant le fait que le schéma \mathcal{X}_R est de Cohen–Macaulay, car il est lisse sur R . □

6A2. Changement de base. On pourra comparer l'énoncé suivant à la proposition II.3.3 de [Mazur 1977] pour les formes modulaires classiques.

Proposition 6.6. *Considérons un corps F qui est une extension de K ou le corps \mathbb{F}_ℓ (pour ℓ un premier étranger à n). L'application F -linéaire canonique*

$$S(A[1/n]) \otimes_{A[1/n]} F \xrightarrow{\sim} S(F)$$

est un isomorphisme.

Démonstration. Pour alléger les notations, on pose $\mathcal{X} = \mathcal{X}_0(n)$ et $\Omega = \Omega_{\mathcal{X}_0(n)/A[1/n]}^1$. Toute extension F de K , munie de sa structure canonique de $A[1/n]$ -module, est plate. L'isomorphisme provient alors d'un théorème de changement de base plat pour la cohomologie des faisceaux quasi-cohérents et du fait que la formation de Ω commute aux changements de base sur $\text{Spec } A[1/n]$ [Hartshorne 1977, III.9.3 et II.8.10].

Supposons maintenant $F = \mathbb{F}_\ell$ avec ℓ comme dans l'énoncé. Soit P un générateur de ℓ . Le morphisme structurel $\mathcal{X} \rightarrow \text{Spec } A[1/n]$ étant lisse, le faisceau Ω est inversible. En particulier, il est sans $A[1/n]$ -torsion. Le morphisme de multiplication par P sur Ω est donc injectif. On a la suite exacte de faisceaux cohérents sur \mathcal{X}

$$0 \longrightarrow \Omega \xrightarrow{\cdot P} \Omega \longrightarrow \Omega/P\Omega = \Omega \otimes_{A[1/n]} \mathbb{F}_\ell = \Omega_{\mathcal{X}_{\mathbb{F}_\ell}/\mathbb{F}_\ell}^1 \longrightarrow 0$$

car la formation de Ω commute aux changements de base. On en déduit la suite exacte longue en cohomologie

$$0 \rightarrow H^0(\mathcal{X}, \Omega) \xrightarrow{\cdot P} H^0(\mathcal{X}, \Omega) \rightarrow H^0(\mathcal{X}_{\mathbb{F}_l}, \Omega_{\mathcal{X}_{\mathbb{F}_l}/\mathbb{F}_l}^1) \rightarrow H^1(\mathcal{X}, \Omega) \xrightarrow{\cdot P} H^1(\mathcal{X}, \Omega).$$

L'application canonique

$$H^0(\mathcal{X}, \Omega) \otimes_{A[1/n]} \mathbb{F}_l \longrightarrow H^0(\mathcal{X}_{\mathbb{F}_l}, \Omega_{\mathcal{X}_{\mathbb{F}_l}/\mathbb{F}_l}^1) \tag{8}$$

est donc injective. De plus, son conoyau est le noyau de la multiplication par P sur $H^1(\mathcal{X}, \Omega)$. Le schéma \mathcal{X} est régulier donc son faisceau dualisant est Ω . Par dualité de Grothendieck, $H^1(\mathcal{X}, \Omega)$ est le $A[1/n]$ -dual de $H^0(\mathcal{X}, \mathcal{O}_{\mathcal{X}}) \simeq A[1/n]$. La multiplication par P sur $A[1/n]$ étant injective, l'application (8) est un isomorphisme. □

Proposition 6.7. *Le $A[1/n]$ -module $S(A[1/n])$ est libre de rang $g(X_0(n))$. Si F est comme dans la proposition 6.6, le F -espace vectoriel $S(F)$ est de dimension $g(X_0(n))$.*

Démonstration. Reprenons les notations de la démonstration précédente et notons X la courbe $X_0(n)$ sur K . Le faisceau Ω étant localement libre, le $A[1/n]$ -module $H^0(\mathcal{X}, \Omega)$ est sans torsion, donc libre. Par ailleurs, d'après la proposition 6.6, on a

$$H^0(\mathcal{X}, \Omega) \otimes_{A[1/n]} K \simeq H^0(X, \Omega_{X/K}^1).$$

Donc le rang du $A[1/n]$ -module $S(A[1/n]) = H^0(\mathcal{X}, \Omega)$ est égal à la dimension sur K de $H^0(X, \Omega_{X/K}^1)$ c'est-à-dire au genre géométrique de X . Cela démontre l'énoncé pour $S(A[1/n])$. Celui pour $S(F)$ s'en déduit par changement de base avec la proposition 6.6. □

6A3. Opérateurs de Hecke. On note $\mathcal{F}_0(n)$ le modèle de Néron de $J_0(n)$ sur $A[1/n]$. C'est un schéma abélien sur $A[1/n]$. Si G est un schéma en groupes lisse sur un schéma T , $\text{Cot } G$ désigne l'espace cotangent de G le long de la section nulle. L'énoncé suivant s'inspire de [Mazur 1978, 2e].

Lemme 6.8. *On a un isomorphisme canonique*

$$\text{Cot}(\mathcal{F}_0(n)) \xrightarrow{\sim} S(A[1/n]).$$

Démonstration. On pose $\mathcal{X} = X_0(n)$ et $U = \text{Spec}(A[1/n])$. Comme \mathcal{X} est propre sur U , le foncteur $\text{Pic}_{\mathcal{X}/U}^0$ est représentable par un U -schéma lisse et séparé, noté $\text{Pic}_{\mathcal{X}/U}^0$ [Bosch et al. 1990, théorème 9.4/2]. D'après le théorème 9.5/4 du même livre, le morphisme naturel $\text{Pic}_{\mathcal{X}/U}^0 \rightarrow \mathcal{F}_0(n)$ identifie $\text{Pic}_{\mathcal{X}/U}^0$ à la composante connexe de l'identité de $\mathcal{F}_0(n)$. En passant aux espaces tangents en la section nulle sur U , on obtient l'isomorphisme $H^1(\mathcal{X}, \mathcal{O}_{\mathcal{X}}) \simeq \text{Tan } \mathcal{F}_0(n)$ (théorème 8.4/1 de [Bosch et al. 1990]). Par ailleurs, le schéma \mathcal{X} sur U est régulier donc de Cohen–Macaulay.

Son faisceau dualisant est donc le faisceau $\Omega_{\mathcal{X}/U}^1$ des différentielles relatives de degré 1. La dualité de Grothendieck permet alors de voir $H^0(\mathcal{X}, \Omega_{\mathcal{X}/U}^1)$ comme le \mathbb{O}_U -dual de $H^1(\mathcal{X}, \mathbb{O}_{\mathcal{X}})$. Par ailleurs, $\text{Cot } \mathcal{F}_0(\mathfrak{n})$ est naturellement le \mathbb{O}_U -dual de $\text{Tan } \mathcal{F}_0(\mathfrak{n})$. Par dualité, on obtient l'isomorphisme $H^0(\mathcal{X}, \Omega_{\mathcal{X}/U}^1) \simeq \text{Cot } \mathcal{F}_0(\mathfrak{n})$. \square

On utilise le lemme 6.8 pour faire opérer l'algèbre de Hecke \mathbb{T} sur les formes modulaires de Drinfeld. Soit \mathfrak{m} un idéal non nul de A . Les endomorphismes $T_{\mathfrak{m}}$ et $w_{\mathfrak{m}}$ de la jacobienne $J_0(\mathfrak{n})$ s'étendent en des endomorphismes de $\mathcal{F}_0(\mathfrak{n})$ (par propriété universelle des modèles de Néron), de l'espace cotangent $\text{Cot } \mathcal{F}_0(\mathfrak{n})$ puis de $S(A[1/\mathfrak{n}])$ (par le lemme). Pour F comme dans la proposition 6.6, on obtient des endomorphismes $T_{\mathfrak{m}}$ et $w_{\mathfrak{m}}$ de $S(F)$ par extension des scalaires. Pour $\mathfrak{n} = \mathfrak{p}$ premier, l'espace de formes modulaires $S(F)$ est donc muni d'une action de l'algèbre de Hecke \mathbb{T} , vue comme sous-algèbre de $\text{End}_K J_0(\mathfrak{p})$. Comme F est de caractéristique p , l'algèbre \mathbb{T} agit sur $S(F)$ via son quotient $\mathbb{T}/p\mathbb{T}$. Cette action n'a pas de raison d'être fidèle.

Pour \mathfrak{m} étranger à \mathfrak{n} et $k \geq 0$, on a l'identité $T_{\mathfrak{m}^k} T_{\mathfrak{m}} = T_{\mathfrak{m}^{k+1}}$ dans $\text{End } S(F)$ à cause de la caractéristique positive, comme l'a remarqué Goss [1980b, proposition 3.3]. Ainsi, $T_{\mathfrak{q}\tau} = T_{\mathfrak{q}} T_{\tau}$ pour tous \mathfrak{q} et τ premiers à \mathfrak{n} . C'est une différence importante avec les opérateurs de Hecke sur les formes modulaires classiques et sur les formes automorphes de $H(\mathbb{C})$.

6A4. Lien avec la théorie analytique. Bien que nous n'en ferons usage qu'un usage limité (dans la proposition 7.17), on précise le lien entre les formes modulaires algébriques définies précédemment et les formes modulaires de Drinfeld analytiques. Soit $M_{2,1}^2(\Gamma_0(\mathfrak{n}))$ le \mathbb{C}_{∞} -espace vectoriel des formes modulaires de Drinfeld de poids 2, de type 1 et doublement paraboliques pour $\Gamma_0(\mathfrak{n})$, au sens de [Gekeler et Reversat 1996]. Une telle forme modulaire possède un développement analytique en la pointe ∞ par rapport au paramètre $t(z) = \bar{\pi}^{-1}/e_A(z)$. Comme elle est doublement parabolique, ce développement est de la forme $\sum_{i \geq 2} a_i t(z)^i$, valable pour $|t(z)|$ suffisamment petit ($|\cdot|$ désigne la valeur absolue sur \mathbb{C}_{∞}). Le groupe $\Gamma_0(\mathfrak{n})$ contenant les matrices $\begin{pmatrix} \lambda & 0 \\ 0 & 1 \end{pmatrix}$ pour $\lambda \in \mathbb{F}_q^{\times}$, un calcul élémentaire montre que le développement est en fait de la forme $\sum_{i \geq 2} a_{1+i(q-1)} t(z)^{1+i(q-1)}$.

Proposition 6.9. *Soit $H^0(X_0(\mathfrak{n})^{\text{an}}, \Omega_{\text{an}}^1)$ l'espace des formes différentielles holomorphes sur l'analytifiée $X_0(\mathfrak{n})^{\text{an}}$ de $X_0(\mathfrak{n})$ sur \mathbb{C}_{∞} . On a l'isomorphisme de \mathbb{C}_{∞} -espaces vectoriels*

$$\begin{aligned} M_{2,1}^2(\Gamma_0(\mathfrak{n})) &\xrightarrow{\sim} H^0(X_0(\mathfrak{n})^{\text{an}}, \Omega_{\text{an}}^1) \simeq S(\mathbb{C}_{\infty}) \\ f &\longmapsto -\frac{1}{\pi} f(z) dz. \end{aligned}$$

De plus, si f a pour développement $\sum_{i \geq 2} a_i t(z)^i$, la forme modulaire associée de $S(\mathbb{C}_{\infty})$ a pour t -développement $\sum_{i \geq 2} a_i t^i$.

Démonstration. Pour le premier isomorphisme, on renvoie au paragraphe 2.10 de [Gekeler et Reversat 1996] (leur définition de $t(z)$ diffère par une constante multiplicative). L'apparition des formes *doublément* paraboliques provient de la relation $dz = -\bar{\pi} d(t(z)) / t(z)^2$, remarquée initialement par Goss [1980b]. Enfin, un énoncé de type GAGA identifie les formes différentielles algébriques sur la courbe projective $X_0(n)_{\mathbb{C}_\infty}$ et analytiques sur $X_0(n)^{\text{an}}$. \square

On peut voir que, par l'isomorphisme de la proposition 6.9, l'action de T_m sur $S(\mathbb{C}_\infty)$ correspond à l'endomorphisme de $M_{2,1}^2(\Gamma_0(n))$ défini par

$$T_m(f)(z) = \frac{1}{P} \sum_{\substack{a,b,d \in A \\ \deg b < \deg d \\ a,d \text{ unitaires} \\ (ad)=m, (a)+n=A}} a^k f\left(\frac{az+b}{cz+d}\right),$$

où P est le générateur unitaire de \mathfrak{m} (cette formule diffère de celles de [Goss 1980a, 1980b, Gekeler 1988] par le facteur $1/P$).

6B. Action de Hecke sur le t -développement.

6B1. Polynômes de Goss, opérateurs de Hecke et t -développement. Ces rappels sur les polynômes de Goss sont dans le cas des réseaux finis issus de la torsion du module de Carlitz. Un traitement plus général est donné par Goss [1980b] et Gekeler [1988] pour les réseaux discrets de \mathbb{C}_∞ . On lui substitue une présentation algébrique plus adaptée à notre contexte.

Soit \mathfrak{a} un idéal non nul de A , de générateur unitaire noté a et de degré d . Ici, ρ désigne le module de Carlitz sur K et $\Lambda_a = \rho[\mathfrak{a}]$. Le polynôme $\rho_a(x)$ étant additif, Λ_a est un \mathbb{F}_q -espace vectoriel de dimension finie. En s'inspirant de Goss, on introduit dans $K^{\text{alg}}(X)$ avec une indéterminée X les quantités

$$S_{0,a}(X) = 0, \quad S_{j,a}(X) = \sum_{\lambda \in \Lambda_a} \frac{1}{(X+\lambda)^j}, \quad t_{\Lambda_a}(X) = \sum_{\lambda \in \Lambda_a} \frac{1}{X-\lambda} = \frac{1}{e_{\Lambda_a}(X)},$$

où $j \geq 1$ et $e_{\Lambda_a}(X) = X \prod_{\lambda \in \Lambda_a - \{0\}} (1 - X/\lambda)$ est l'exponentielle associée à Λ_a .

Proposition 6.10 [Goss 1980b, section 2 ; [Gekeler 1988, sections 3.4–3.9]]. *Pour tout entier $j \geq 1$, il existe un unique polynôme $G_{j,a}(X)$ dans $K[X]$ vérifiant $S_{j,a}(X) = G_{j,a}(t_{\Lambda_a}(X))$. Pour $j = 0$, on pose $G_{0,a}(X) = 0$. On a la formule explicite*

$$G_{j,a}(X) = \sum_{0 \leq k < j} \sum_{\underline{i}} \binom{k}{\underline{i}} l^{\underline{i}} a^{-k} X^{k+1}, \tag{9}$$

avec les notations suivantes :

$\underline{i} = (i_0, \dots, i_d)$ parcourt les $(d + 1)$ -uplets d 'entiers naturels vérifiant

$$i_0 + \dots + i_d = k \quad \text{et} \quad i_0 + i_1q + \dots + i_dq^d = j - 1.$$

$\binom{k}{i}$ est le coefficient multinomial $k!/i_0! \cdots i_d!$ évalué dans $\mathbb{F}_p \subset K$.

$l^i = l_0(a)^{i_0} \cdots l_d(a)^{i_d}$ avec $l_j(a) \in A$, défini par $\rho_a = \sum l_j(a)\tau^j \in A\{\tau\}$.

La formule (9) découle de [Gekeler 1988, 3.8] en remarquant que l'exponentielle $e_{\Lambda_a}(X)$ n'est autre que $\rho_a(X)/a$. De (9), on déduit que le polynôme $G_{j,a}(aX)$ est à coefficients dans A .

Notation 6.11. On garde les notations du paragraphe 5C2. Pour d diviseur unitaire de a , et b dans A de degré $< \deg b$, on pose

$$\chi_{a,d,b}(t) = \frac{1}{\rho_b(\lambda_d) + \rho_{a/d}(\gamma_d)} \in K((t))^{\text{alg}}$$

et $\varphi_a(t) = \chi_{a,1,0}(t) = 1/(\rho_a(1/t)) \in A[[t]]$. Noter que $\chi_{a,d,b}(t)$ dépend des choix de λ_d et γ_d .

Lemme 6.12. Pour tout $i \geq 0$, on a l'égalité dans $dA[[t]]$

$$\sum_{\substack{b \in A \\ \deg b < \deg d}} (\chi_{a,d,b}(t))^i = G_{i,d}(d \cdot \varphi_{a/d}(t)). \tag{10}$$

Cette quantité est indépendante des choix de λ_d et γ_d .

Démonstration. L'ensemble $\{\rho_b(\lambda_d) \mid \deg b < \deg d\}$ est le réseau $\Lambda_d = \rho[(d)]$. En utilisant la proposition 6.10, on voit que le membre de gauche de (10) est

$$\sum_{\lambda \in \Lambda_d} (\rho_{a/d}(\gamma_d) + \lambda)^{-i} = S_{i,d}(\rho_{a/d}(\gamma_d)) = G_{i,d}\left(\frac{1}{e_{\Lambda_d}(\rho_{a/d}(\gamma_d))}\right).$$

Par ailleurs, comme $e_{\Lambda_d}(X) = \rho_d(X)/d$, on a

$$d \cdot e_{\Lambda_d}(\rho_{a/d}(\gamma_d)) = \rho_d \rho_{a/d}(\gamma_d) = \rho_{a/d} \rho_d(\gamma_d) = \rho_{a/d}(1/t),$$

d'où l'égalité annoncée. Le membre de droite de (10) est dans $dA[[t]]$, comme remarqué précédemment, et indépendant des choix de λ_d et γ_d . \square

Jusqu'à la fin de la section 6B, la lettre F désigne au choix l'anneau $A[1/n]$, une extension de corps de K ou le corps fini \mathbb{F}_Γ (pour Γ premier étranger à n). L'énoncé qui suit est une généralisation de [Gekeler 1988, 7.3] pour les formes modulaires algébriques et les opérateurs de Hecke d'indice non nécessairement premier. Une version analytique en poids quelconque se trouve dans [Armana 2011a, proposition 5.2].

Proposition 6.13. Soit $f \in S(F)$ de t -développement $\sum_{i \geq 2} a_i t^i$ dans $F[[t]]$. Soit m premier à n , de générateur unitaire M . Alors le t -développement de la forme modulaire $T_m f$ est donné par

$$\sum_{i \geq 2} \sum_{\substack{d \mid M \\ d \text{ unitaire}}} \frac{M}{d^2} a_i G_{i,d}(d \cdot \varphi_{M/d}(t)) \in F[[t]]. \tag{11}$$

Démonstration. L'expression est bien dans $F[[t]]$ d'après le lemme 6.12. Par la proposition 6.6 de changement de base, il suffit d'établir (11) pour tout f dans $S(A[1/n])$.

Explicitons la correspondance T_m . Reprenons les notations de la section 5C. Soit TD le module de Tate–Drinfeld sur $A[[t]]$, construit à partir du module de Carlitz ρ et du réseau $\Gamma = \rho_A(1/t)$, qu'on munit de son A -module C_n . Comme m est premier à n , les sous-groupes cycliques intervenant dans la définition de $T_m(\text{TD}, C_n)$ sont

$$C_m = \text{TD}_A e_\Gamma(\lambda_M) \quad \text{et} \quad C_{d,b} = \text{TD}_A e_\Gamma(\rho_b(\lambda_d) + \rho_{M/d}(\gamma_d)),$$

pour $(d, b) \in A \times A$ avec d diviseur unitaire de M , $d \neq 1$ et $\deg b < \deg d$.

Notons $E_{1,0}$ le module de Drinfeld de rang 2 construit à partir de ρ et du ρ -réseau $\Gamma' = \rho_A(1/\varphi_M(t)) = \rho_m(1/t)$ par uniformisation de Tate–Drinfeld. L'inclusion de réseaux $\Gamma' \subset \Gamma$ définit une isogénie $\text{TD} \rightarrow E_{1,0}$ de noyau C_m . Donc TD/C_m n'est autre que $E_{1,0}$ et $(C_n + C_m)/C_m$ est le A -module $C'_n = (E_{1,0})_A e_{\Gamma'}(\lambda_N)$.

On notera $E_{d,b}$ le module de Drinfeld de rang 2 construit à partir de ρ et du ρ -réseau $\Gamma'' = \rho_A(1/\chi_{M,d,b}(t))$ par uniformisation de Tate–Drinfeld. Nous avons $\rho_d(\Gamma'') = \rho_{(M/d)}(1/t) \subset \Gamma$. Le morphisme injectif et de conoyau fini $\rho_d : \Gamma'' \rightarrow \Gamma$ définit une isogénie $\text{TD} \rightarrow E_{d,b}$ de noyau $C_{d,b}$. Donc $\text{TD}/C_{d,b}$ n'est autre que $E_{d,b}$ et $(C_n + C_{d,b})/C_{d,b}$ est le A -module $C''_n = (E_{d,b})_A e_{\Gamma''}(\lambda_N)$.

On trouve donc

$$T_m(\text{TD}, C_n) = (E_{1,0}, C'_n) + \sum_{d,b} (E_{d,b}, C''_n) = \sum_{(d,b) \in \mathcal{E}} (E_{d,b}, C), \quad (12)$$

avec \mathcal{E} l'ensemble des $(d, b) \in A \times A$ avec d diviseur unitaire de M et $\deg b < \deg d$, et C vaut C'_n si $d = 1$, C''_n sinon.

Soit $\mathbf{t} = \mathbf{t}_{A[1/n]} : \text{Spec } A[1/n][[t]] \rightarrow \mathcal{X}_0(n)$ le morphisme de 6A1. Soit $\chi_{d,b}$ l'homomorphisme d'anneaux $A[1/n][[t]] \rightarrow K^{\text{sep}}((\gamma_d))$ donné par $t \mapsto \chi_{M,d,b}(t)$. En composant $\text{Spec } \chi_{d,b}$ avec \mathbf{t} , on obtient un morphisme de schémas

$$\mathbf{t}_{d,b} : \text{Spec } K^{\text{sep}}((\gamma_d)) \rightarrow \mathcal{X}_0(n).$$

Soit $f \in S(A[1/n])$ de t -développement $F(t)$. D'après (12), le t -développement de $T_m f$ est donné par

$$\mathbf{t}^*(T_m f) = \sum_{(d,b) \in \mathcal{E}} \mathbf{t}_{d,b}^*(f).$$

Un calcul élémentaire donne

$$\frac{d(\chi_{M,d,b}(t))}{\chi_{M,d,b}(t)^2} = \frac{M dt}{d^2 t^2}.$$

Donc $\mathbf{t}^*(T_m f)$ vaut

$$\sum_{(d,b) \in \mathcal{E}} (\text{Spec } \chi_{d,b})^* \mathbf{t}^*(f) = \sum_{(d,b)} (\text{Spec } \chi_{d,b})^* \left(F(t) \frac{dt}{t^2} \right) = \sum_{(d,b)} F(\chi_{M,d,b}(t)) \frac{M dt}{d^2 t^2}.$$

Comme $F(t) = \sum_{i \geq 2} a_i t^i$, le t -développement de $T_m f$ est donné par

$$\sum_{i \geq 2} a_i \sum_{(d,b) \in \mathcal{E}} \frac{M}{d^2} (\chi_{M,d,b}(t))^i = \sum_{i \geq 2} a_i \sum_{\substack{d|M \\ d \text{ unitaire}}} \frac{M}{d^2} \sum_{\deg b < \deg d} (\chi_{M,d,b}(t))^i.$$

On conclut alors à l'aide du lemme 6.12. □

Proposition 6.14. *Soit m étranger à n , de degré d et générateur unitaire M . Soit $f \in S(F)$ une forme modulaire de t -développement $\sum_{i \geq 2} a_i(f) t^i$. Alors le premier coefficient de $T_m f$ est :*

$$b_1(T_m f) = a_q(T_m f) = \sum_{\underline{m}} \binom{q-1}{\underline{m}} l^{\underline{m}} a_{1+m_0+m_1q+\dots+m_dq^d}(f),$$

la somme portant sur les $(d+1)$ -uplets d'entiers naturels (m_0, \dots, m_d) vérifiant $m_0 + \dots + m_d = q-1$. La notation $l^{\underline{m}}$ désigne le produit de coefficients du module de Carlitz : $l_0(M)^{m_0} \dots l_d(M)^{m_d}$.

Démonstration. Cela provient de la proposition 6.13 et de (9) pour les polynômes de Goss. Pour les détails, on renvoie à [Armana 2011a, proposition 5.5]. □

6B2. Opérateurs de Hecke de degré 1 et coefficients du t -développement. Pour m de degré 1, la proposition 6.14 donne

$$a_q(T_m f) = \sum_{i=0}^{q-1} \binom{q-1}{i} M^{q-i-1} a_{q+i(q-1)}(f) \tag{13}$$

(voir [Gekeler 1988, 7.4] pour un résultat similaire sur les formes modulaires de Drinfeld analytiques pour $GL_2(A)$). Remarquons que le coefficient binomial $\binom{q-1}{i}$ est non nul dans \mathbb{F}_p , pour $0 \leq i \leq q-1$, par le théorème de Lucas.

Théorème 6.15. *Considérons les éléments suivants de l'algèbre de Hecke $\mathbb{T} \otimes_{\mathbb{Z}} A$:*

$$\theta_j = - \binom{q-1}{j-1}^{-1} \sum_{\deg m=1} M^{j-1} T_m \quad (1 \leq j \leq q-1).$$

$$\theta_q = - \sum_{\deg m=1} (M^{q-1} - 1) T_m.$$

Supposons que n ne possède pas de diviseur de degré 1. Pour toute forme modulaire $f \in S(F)$ pour $\Gamma_0(n)$, on a

$$b_j(f) = b_1(\theta_j f) \quad (1 \leq j \leq q).$$

Un énoncé sensiblement plus général a été établi dans [Armana 2011a, théorème 7.2] pour les formes modulaires de Drinfeld analytiques de poids quelconque. Par commodité, on donne ici une preuve simplifiée du théorème 6.15.

Démonstration. On pose $a_i = a_i(f)$. Pour $n \geq 0$, notons $s_1(n)$ la somme des puissances n èmes des polynômes de degré 1 de A . À partir de (13), on obtient pour tout $j \geq 0$

$$a_q \left(\sum_{\deg m=1} M^j T_m f \right) = \sum_{i=0}^{q-1} s_1(j+q-i-1) \binom{q-1}{i} a_{q+i(q-1)}. \tag{14}$$

Il est bien connu que $s_1(n)$ vaut -1 pour $n > 0$ divisible par $q-1$, et 0 sinon. Donc pour $0 \leq j \leq q-2$, l'équation (14) se simplifie en

$$\begin{aligned} a_q \left(\sum_{\deg m=1} M^j T_m f \right) &= s_1(q-1) \binom{q-1}{j} a_{q+j(q-1)} \\ &= - \binom{q-1}{j} a_{1+(j+1)(q-1)}, \end{aligned} \tag{15}$$

et pour $j = q-1$, en

$$a_q \left(\sum_{\deg m=1} M^{q-1} T_m f \right) = -a_{q+(q-1)^2} - a_q.$$

En particulier, on trouve $a_{q+(q-1)^2} = a_q(-\sum_{\deg m=1} M^{q-1} T_m f - f)$. Or, pour $j=0$ l'équation (15) donne $a_q(\sum_{\deg m=1} T_m f) = -a_q$, d'où

$$a_{q+(q-1)^2} = a_q \left(\sum_{\deg m=1} (1 - M^{q-1} T_m) f \right) = a_q(\theta_q f). \quad \square$$

6B3. Points de Weierstrass et t -développement. Dans cette section, on suppose $n = \mathfrak{p}$ premier. D'après la proposition 6.5, une forme modulaire de Drinfeld est déterminée de façon unique par son t -développement. Pour savoir combien de coefficients successifs du t -développement suffisent à la déterminer, on s'intéresse aux points de Weierstrass de la courbe $X_0(\mathfrak{p})$ sur K et en spécialisant aux places de bonne réduction.

Soit C une courbe algébrique projective lisse de genre $g \geq 2$ sur un corps k . On rappelle qu'un point x de C est de Weierstrass s'il existe une différentielle régulière non nulle dans $H^0(C, \Omega_{C/k}^1)$ s'annulant à l'ordre $\geq g$ en x . De façon équivalente, par le théorème de Riemann–Roch, cela revient à l'existence d'une fonction rationnelle non nulle sur C régulière en-dehors de x et ayant un pôle d'ordre $\leq g$ en x .

Proposition 6.16 (d'après Ogg, Gekeler, Schweizer). *Soit \mathfrak{p} premier de degré ≥ 3 .*

- (i) *Considérons un point K -rationnel de $X_0(\mathfrak{p})$ dont la réduction modulo \mathfrak{p} n'est pas supersingulière (c'est-à-dire dont le module de Drinfeld de rang 2 sous-jacent n'est pas supersingulier sur $\mathbb{F}_{\mathfrak{p}}^{\text{alg}}$; c'est le cas des pointes 0 et ∞). Alors ce point n'est pas de Weierstrass.*

- (ii) Soient \mathfrak{p} premier de degré 3 et $\mathfrak{l} \neq \mathfrak{p}$ premier. La courbe $X_0(\mathfrak{p})_{\mathbb{F}_\mathfrak{l}} = \mathcal{X}_0(\mathfrak{p}) \times_A \mathbb{F}_\mathfrak{l}$ est hyperelliptique sur $\mathbb{F}_\mathfrak{l}$. Les pointes $0_{\mathbb{F}_\mathfrak{l}}$ et $\infty_{\mathbb{F}_\mathfrak{l}}$ ne sont pas des points de Weierstrass sur cette courbe.

Démonstration. (i) On adapte l'argument géométrique de Ogg [1978] pour les courbes modulaires classiques. Les détails se trouvent dans la preuve du lemme 7.6 de [Armana 2011a]. Ils sont énoncés pour la pointe ∞ mais restent valables pour les points de $X_0(\mathfrak{p})$ à réduction non supersingulière.

- (ii) D'après [Gekeler 1986, corollaire 3.8], la courbe $X_0(\mathfrak{p})$ sur K est hyperelliptique pour $\deg \mathfrak{p} = 3$. On applique alors un argument de spécialisation remarqué par Schweizer [1997, lemme 17] : la courbe $X_0(\mathfrak{p})_{\mathbb{F}_\mathfrak{l}}$ est hyperelliptique sur $\mathbb{F}_\mathfrak{l}$, dès que \mathfrak{l} est distinct de \mathfrak{p} .

On sait que les points de Weierstrass d'une courbe hyperelliptique C sur un corps k sont les points de ramification de son morphisme séparable $C \rightarrow \mathbb{P}_k^1$ de degré 2, c'est-à-dire les points fixes de son involution hyperelliptique (voir par exemple [Liu 2002, exercice 7/4.7]). D'après [Gekeler 1986, corollaire 3.8], l'involution hyperelliptique de $X_0(\mathfrak{p})$ est $w_\mathfrak{p}$ (résultat étendu en niveau non premier par Schweizer [1997, théorème 20]). Donc l'involution hyperelliptique de $X_0(\mathfrak{p})_{\mathbb{F}_\mathfrak{l}}$ est $(w_\mathfrak{p})_{\mathbb{F}_\mathfrak{l}}$. Les pointes $0_{\mathbb{F}_\mathfrak{l}}$ et $\infty_{\mathbb{F}_\mathfrak{l}}$ étant distinctes et échangées par $(w_\mathfrak{p})_{\mathbb{F}_\mathfrak{l}}$, ce ne sont pas des points fixes de $(w_\mathfrak{p})_{\mathbb{F}_\mathfrak{l}}$ ni des points de Weierstrass de $X_0(\mathfrak{p})_{\mathbb{F}_\mathfrak{l}}$. \square

Proposition 6.17. *Supposons l'une des conditions vérifiées :*

- (i) F est une extension de K et $\deg \mathfrak{p} \geq 3$.
 (ii) $F = \mathbb{F}_\mathfrak{l}$ avec \mathfrak{l} premier $\neq \mathfrak{p}$ et $\deg \mathfrak{p} = 3$.

Posons $g = g(X_0(\mathfrak{p}))$. Alors l'application F -linéaire

$$S(F) \rightarrow F^g, \quad f \mapsto (b_1(f), \dots, b_g(f)),$$

est un isomorphisme.

Démonstration. Soit F comme dans l'énoncé. Posons $X_0(\mathfrak{p})_F = \mathcal{X}_0(\mathfrak{p}) \times_A F$. En la section ∞ sur $X_0(\mathfrak{p})$, on a le paramètre formel local $s = t^{q-1}$ (proposition 5.4). D'après l'équation (7), le développement formel d'une différentielle $f \in S(F)$ est alors $\mathbf{t}_F^*(f) = -\sum_{i \geq 1} b_i(f) s^{i-1} ds$. Donc ∞ n'est pas un point de Weierstrass de $X_0(\mathfrak{p})_F$ si et seulement si toute différentielle s'annule à l'ordre $< g(X_0(\mathfrak{p})_F)$ en ∞ , c'est-à-dire si l'application linéaire

$$S(F) \rightarrow F^{g(X_0(\mathfrak{p})_F)}, \quad f \mapsto (b_1(f), \dots, b_{g(X_0(\mathfrak{p})_F)}(f)),$$

est injective.

Le genre de la courbe $X_0(\mathfrak{p})_F$ est g . En effet, si F est une extension de K , c'est une conséquence du théorème de changement de base plat pour les faisceaux

quasi-cohérents (voir par exemple [Liu 2002, corollaire 5/2.27]). Par ailleurs, l'homomorphisme structurel $\mathcal{X}_0(\mathfrak{p}) \rightarrow \text{Spec } A[1/\mathfrak{p}]$ est lisse et projectif, donc le genre arithmétique des fibres est égal au genre arithmétique de $X_0(\mathfrak{p})$. Donc la courbe $X_0(\mathfrak{p})_{\mathbb{F}_l}$ est aussi de genre g .

Par la proposition 6.16, l'application linéaire de l'énoncé est donc injective pour $F = K$ et $F = \mathbb{F}_l$. Comme $S(F)$ est aussi de dimension g (proposition 6.7), c'est un isomorphisme. Si F est une extension de K , on en déduit que $S(F) \rightarrow F^g$ est un isomorphisme en étendant les scalaires de K à F par la proposition 6.6. \square

Remarque 6.18. (i) La preuve montre que ∞ n'est pas un point de Weierstrass de $X_0(\mathfrak{p})_F$ pour toute extension F de K . Cela complète la proposition 6.16.

(ii) On a la conséquence suivante, dont on ne connaît pas d'autre démonstration : sous les hypothèses de la proposition 6.17, il existe une forme modulaire de Drinfeld f dans $S(F)$ avec $b_1(f) \neq 0$.

7. Points rationnels de courbes modulaires de Drinfeld

7A. Spécialisation dans les quotients optimaux de $J_0(\mathfrak{p})$. La méthode de Mazur utilisait un résultat de spécialisation de Raynaud : si G est un schéma en groupes sur \mathbb{Z}_l avec l premier ≥ 3 , tout point d'ordre fini de $G(\mathbb{Z}_l)$ a même ordre que sa spécialisation en l [Mazur 1978, 1c]. Ce n'est plus vrai sur un anneau de valuation discrète de caractéristique p puisqu'on peut y construire des courbes elliptiques ayant un point d'ordre p et de spécialisation nulle. Cependant, on peut contourner cet écueil dans le cas des quotients optimaux de $J_0(\mathfrak{p})$.

Proposition 7.1. *Soit J' un quotient optimal de $J_0(\mathfrak{p})$ sur K c'est-à-dire un quotient de $J_0(\mathfrak{p})$ par une sous-variété abélienne définie sur K .*

- (i) *La composante p -primaire de $J'(K)_{\text{tors}}$ est nulle.*
- (ii) *L'application de réduction $J'(K)_{\text{tors}} \rightarrow J'(\mathbb{F}_l)$ en un premier l distinct de \mathfrak{p} est injective.*

Démonstration. La première affirmation est le lemme 3.4 de [Pál 2010]. Notons \mathcal{J}' le modèle de Néron de J' sur $A[1/\mathfrak{p}]$. L'application de réduction est définie comme suit : par propriété universelle des modèles de Néron, on a un isomorphisme canonique $J'(K) \simeq \mathcal{J}'(A[1/\mathfrak{p}])$ et la spécialisation en $l \neq \mathfrak{p}$ induit $J'(K) \rightarrow J'(\mathbb{F}_l)$. La deuxième affirmation de l'énoncé, qui se déduit de la première, est essentiellement la proposition 9.4 de [Pál 2010] : elle reste valable en remplaçant $W(\mathfrak{p})$ par J' , à condition de restreindre la spécialisation aux points d'ordre fini de $J'(K)$. \square

7B. Gonalité de $X_0(\mathfrak{p})$. On utilisera à plusieurs reprises un résultat de Schweizer sur la gonalité de la courbe modulaire $X_0(\mathfrak{p})$. La gonalité d'une courbe algébrique C sur un corps k est le plus petit degré $\gamma_k(C)$ d'un morphisme k -rationnel dominant

$C \rightarrow \mathbb{P}^1$. Si C a un point rationnel, alors la gonalité est 1 si et seulement si le genre de C est nul, et la gonalité est 2 si et seulement si C est elliptique ou hyperelliptique. Pour une extension k' de k , notons $\gamma_{k'}(C)$ la gonalité de $C_{k'} = C \times_k k'$. On voit facilement que $\gamma_k(C) \geq \gamma_{k'}(C)$.

Proposition 7.2 [Schweizer 2003, lemme 2.2]. *On suppose encore p premier. Si \tilde{K} est une extension finie purement inséparable de K , on a*

$$\gamma_K(X_0(\mathfrak{p})) \geq \gamma_{\tilde{K}}(X_0(\mathfrak{p})) > \frac{q^{\deg p}}{(q^2 + 1)(q + 1)}.$$

7C. Préliminaires.

Notation 7.3. Pour simplifier, on pose dorénavant $\mathcal{X} = \mathcal{X}_0(\mathfrak{p})$, $X = X_0(\mathfrak{p})$, $J = J_0(\mathfrak{p})$ et J' un quotient optimal de J . Soient \mathcal{Y} et \mathcal{Y}' les modèles de Néron de J et J' sur $A[1/p]$.

Soit $d \geq 1$ entier. La puissance symétrique d ème $X^{(d)}$ est une variété lisse sur K [Milne 1986, sections 3–5]. Ses points sur K s'identifient aux diviseurs K -rationnels sur $X_{K^{\text{sep}}}$ (c'est-à-dire invariants par l'action du groupe de Galois absolu de K) et effectifs de degré d . Notons $\infty^{(d)}$ et $0^{(d)}$ les sections $\text{Spec } A[1/p] \rightarrow X^{(d)}$ déduites de ∞ et 0 .

On définit un homomorphisme $\varphi^{(d)} : X^{(d)} \rightarrow J$ en associant à un diviseur effectif D de degré d la classe d'équivalence linéaire de $D - d(\infty)$. En composant avec le morphisme canonique $J \rightarrow J'$, on obtient

$$u^{(d)} : X^{(d)} \rightarrow J'.$$

Considérons un point de $Y_1(\mathfrak{p})$ défini sur une extension L/K de degré d . Son image par l'homomorphisme canonique $X_1(\mathfrak{p}) \rightarrow X$ est un point P de $X(L)$. Notons s et p^e ($e \geq 0$) les degrés séparable et inséparable de l'extension L/K et $\sigma_1, \dots, \sigma_s$ les plongements de L dans K^{alg} fixant K . Le diviseur $\sum_{i=1}^s p^e \sigma_i(P)$ de $X_{K^{\text{sep}}}$ est K -rationnel de degré $p^e s = d$. Il définit donc un point de $X^{(d)}(K)$.

Lemme 7.4. *On suppose $J'(K)$ fini et $d < \deg p$. Notons E l'ensemble des points de $X^{(d)}(K)$ provenant de $Y_1(\mathfrak{p})(L)$ pour L/K une extension de degré d . Alors $u^{(d)}(w_{\mathfrak{p}}(E)) = \{0\}$ dans $J'(K)$.*

Démonstration. Soit $x \in E$. Notons $y \in Y_1(\mathfrak{p})(L)$ et $P \in X(L)$ les points dont il provient. La variété $X^{(d)}$ possède un modèle $\mathcal{X}^{(d)}$ propre sur $A[1/p]$. Donc x se prolonge naturellement en une section du morphisme structural $\mathcal{X}^{(d)} \rightarrow \text{Spec } A[1/p]$ encore notée x . Fixons un premier \mathfrak{l} de degré 1 (en particulier, $\mathfrak{l} \neq \mathfrak{p}$). D'après la proposition 5.2, en toute place \mathfrak{L} de L au-dessus de \mathfrak{l} , le module de Drinfeld sous-jacent à P n'a ni bonne réduction potentielle, ni réduction potentiellement stable de rang 1 avec point entier. Comme il n'a pas bonne réduction potentielle,

la spécialisation de P en \mathcal{L} est nécessairement une pointe, c'est-à-dire 0 ou ∞ . Or, par la proposition 5.5, cette spécialisation est nécessairement 0. Donc x se spécialise comme $0^{(d)}$ en \mathfrak{l} . Posons $x' = w_{\mathfrak{p}}(x)$. L'involution échangeant les pointes, x' et $\infty^{(d)}$ ont même spécialisation. Donc $u^{(d)}(x')$ se spécialise en 0 dans $J'(\mathbb{F}_{\mathfrak{l}})$. Par ailleurs, comme $J'(K)$ est fini, le point $u^{(d)}(x')$ est de torsion dans $J'(K)$. Donc $u^{(d)}(x')$ est nul par le résultat de spécialisation (proposition 7.1(ii)). \square

7D. Points rationnels pour \mathfrak{p} de petit degré.

7D1. Points de $Y_1(\mathfrak{p})$ pour \mathfrak{p} de petit degré.

Théorème 7.5. (i) Soit \mathfrak{p} de degré 3. La courbe $Y_1(\mathfrak{p})$ n'a pas de point L -rationnel pour toute extension L/K de degré ≤ 2 .

(ii) Supposons que \mathfrak{p} est tel que toute forme primitive de $H_{\mathfrak{p}}(\mathbb{C})$ est de rang analytique ≤ 1 . Soit L/K une extension de degré

$$[L : K] < \min \left(\deg \mathfrak{p}, \frac{q^{\deg \mathfrak{p}}}{2(q^2 + 1)(q + 1)} \right).$$

Ces conditions sont vérifiées pour $\deg \mathfrak{p} = 4$ et $[L : K] \leq d$ avec $d = 2$ si $q = 5$, $d = 3$ si $q \geq 7$. Alors la courbe $Y_1(\mathfrak{p})$ n'a pas de point L -rationnel.

(iii) Soit \mathfrak{p} de degré 4. La courbe $Y_1(\mathfrak{p})$ n'a pas de point K -rationnel.

Revenons sur la condition sur le rang analytique des formes primitives de $H_{\mathfrak{p}}(\mathbb{C})$. Elle se reformule ainsi : pour toute orbite $[F] \in \mathbb{C}$, la variété abélienne $J_{[F]}$ est de rang analytique inférieur ou égal à sa dimension sur K . Calculer l'ordre d'annulation des fonctions L de formes primitives de $H_{\mathfrak{p}}(\mathbb{C})$ peut se faire sur machine, par exemple grâce aux symboles modulaires pour $\mathbb{F}_q(T)$. La condition peut être donc testée numériquement. Nous l'avons vérifiée pour tous les idéaux premiers \mathfrak{p} de degré 5 dans $\mathbb{F}_2[T]$ et, par exemple, pour

$$(T^5 + T^3 - T^2 - T + 1), (T^5 + T^4 + T^3 - T^2 + T - 1), (T^5 - T^4 - T^2 - 1) \subset \mathbb{F}_3[T].$$

Comme expliqué dans l'introduction, la condition n'est certainement pas vérifiée de façon systématique, mais on s'attend à ce qu'elle le soit assez fréquemment.

Démonstration. Supposons qu'il existe un point y de $Y_1(\mathfrak{p})(L)$ sur une extension L/K de degré d . Par la construction donnée en 7C, il définit des points $P \in X(L)$ et $x \in X^{(d)}(K)$.

(i) Comme $d \leq 2 < \deg \mathfrak{p}$ et $J(K)$ est fini (proposition 4.4), on peut appliquer le lemme 7.4 à J : le point $z = u^{(d)}(w_{\mathfrak{p}}(x))$ est nul dans $J(K)$. Donc le diviseur $\sum_{i=1}^s p^e \sigma_i(w_{\mathfrak{p}}(P)) - d(\infty)$ est principal sur K^{alg} . L'interprétation modulaire de P assure qu'il est non nul. Notons f une fonction rationnelle non nulle sur X définie sur K^{alg} dont c'est le diviseur. La courbe $X_{K^{\text{alg}}}$ est de genre $g(X_0(\mathfrak{p}))$ qui est,

d'après la proposition 3.2, supérieur ou égal à $\deg(\mathfrak{p}) - 1$ dès que $\deg \mathfrak{p} \geq 3$. Donc la fonction f possède un pôle unique en ∞ d'ordre $d \leq \deg(\mathfrak{p}) - 1 \leq g(X_0(\mathfrak{p}))$ et est régulière ailleurs. Cela contredit le fait que ∞ n'est pas un point de Weierstrass de $X_{K^{\text{alg}}}$ (voir la remarque 6.18).

(ii) D'après l'hypothèse sur \mathfrak{p} , la variété abélienne $J' = J_0(\mathfrak{p})^-$ est de groupe de Mordell–Weil fini sur K (propositions 4.3 et 4.5). Comme $d < \deg \mathfrak{p}$, on peut appliquer le lemme 7.4 à J' : le point $z = u^{(d)}(w_{\mathfrak{p}}(x))$ est nul dans $J'(K)$. Donc $\varphi^{(d)}(w_{\mathfrak{p}}(x))$ appartient à la sous-variété abélienne $(1 + w_{\mathfrak{p}})J$. On en déduit que $(1 - w_{\mathfrak{p}})\varphi^{(d)}(w_{\mathfrak{p}}(x))$ est nul dans $J(K)$. Le diviseur

$$D = w_{\mathfrak{p}}(x) - d(0) - (x) + d(\infty) = \sum_i p^e w_{\mathfrak{p}}(\sigma_i(P)) + d(\infty) - \sum_i p^e \sigma_i(P) - d(0)$$

est principal sur K^{alg} , donc sur une extension finie purement inséparable \tilde{K} de K . De plus, il est non nul : en effet, on a $\infty \neq 0$ et $\sigma_i(P) \neq \infty$ pour tout i , par interprétation modulaire de P . Ainsi, le diviseur D définit un morphisme \tilde{K} -rationnel non constant $X_{\tilde{K}} \rightarrow \mathbb{P}^1$ de degré $p^e s + d = 2d$. La borne de Schweizer pour la gonality (proposition 7.2) donne $2d > q^{\deg \mathfrak{p}} / ((q^2 + 1)(q + 1))$. Cela contredit l'hypothèse de l'énoncé sur d .

(iii) Reprenons l'argument et les notations de (ii) avec $\deg \mathfrak{p} = 4$ et $d = 1$. On obtient un morphisme \tilde{K} -rationnel non constant $X_{\tilde{K}} \rightarrow \mathbb{P}^1$ de degré 2. Donc la courbe $X_{\tilde{K}}$ est rationnelle, elliptique ou hyperelliptique. Par le lemme 6 de [Schweizer 1997], la courbe $X_0(\mathfrak{p})$ a la même propriété sur K . Comme $\deg \mathfrak{p} = 4$, cela contredit la classification de [Schweizer 1997, théorème 20]. \square

7D2. Résultats partiels sur les points de $Y_0(\mathfrak{p})$. Ils sont obtenus par une variante des démonstrations précédentes.

Proposition 7.6. *Soit \mathfrak{p} de degré 3 ou 4. Soit ϕ un module de Drinfeld de rang 2 sur K possédant une isogénie K -rationnelle cyclique d'ordre \mathfrak{p} . Alors ϕ a bonne réduction potentielle en tout idéal premier distinct de \mathfrak{p} .*

Démonstration. On pourra comparer l'argument suivant avec [Mazur 1978, corollaire 4.3]. Un module de Drinfeld comme dans l'énoncé correspond, par l'interprétation modulaire, à un point x de $Y_0(\mathfrak{p})(K)$. Notons encore x son prolongement en une section du morphisme structurel $\mathcal{X} \rightarrow \text{Spec } A[1/\mathfrak{p}]$. Supposons qu'il existe un premier $\mathfrak{l} \neq \mathfrak{p}$ en lequel ϕ n'a pas bonne réduction potentielle. Alors ϕ a réduction potentiellement stable de rang 1. Donc x se spécialise en \mathfrak{l} comme ∞ ou 0. Les pointes étant permutées par $w_{\mathfrak{p}}$, quitte à remplacer x par $w_{\mathfrak{p}}(x)$, on peut supposer que x et ∞ ont même spécialisation. Si \mathfrak{p} est de degré 3 (respectivement de degré 4), on prend pour J' la jacobienne $J = J_0(\mathfrak{p})$ (respectivement le quotient $J_0(\mathfrak{p})^-$). On a vu dans la section 4B que le groupe de Mordell–Weil de ces variétés abéliennes est fini. Comme $u^{(1)}(x)$ se spécialise en \mathfrak{l} comme 0, la proposition 7.1 assure que

$u^{(1)}(x) = 0$ dans J' . On conclut alors comme dans le théorème 7.5 (i) et (iii) pour $d = 1$. □

Lemme 7.7. *Soient $q \geq 5$ et p de degré ≥ 4 . Pour l premier distinct de p , on pose $\eta_l = T_l - (q^{\text{deg } l} + 1)$ dans \mathbb{T} . L'ensemble des éléments x de $X(K)$ tels que $\eta_l(x) = \eta_l(w_p(x))$, comme diviseurs de degré nul sur X , est égal à $\{0, \infty\}$.*

Démonstration. Pour un tel x , on a l'égalité de diviseurs sur X

$$T_l(x) + (q^{\text{deg } l} + 1)(w_p(x)) = T_l(w_p(x)) + (q^{\text{deg } l} + 1)(x). \tag{16}$$

Pour $\text{deg } n \geq 3$ avec n non nécessairement premier, Schweizer [2003, remarque 4.6] a établi la liste des points K -rationnels CM de $X_0(n)$. Lorsque $n = p$ premier, il n'en existe que si $\text{deg } p = 3$. Donc ici x n'est pas un point K -rationnel CM de X , c'est-à-dire $w_p(x) \neq x$. D'après l'équation (16), on en déduit que le diviseur $T_l(x) - (q^{\text{deg } l} + 1)(x)$ est effectif. Par ailleurs, il est de degré nul. Donc $T_l(x) = (q^{\text{deg } l} + 1)(x)$.

La conjecture de Ramanujan–Petersson, démontrée dans ce cadre par Drinfeld [1988], affirme que les valeurs propres de T_l , opérant sur $H(\mathbb{C})$, sont des entiers algébriques de valeur absolue $\leq 2q^{(\text{deg } l)/2}$. Ainsi, les valeurs propres de η_l sont non nulles. Le noyau de η_l , vu comme élément de $\mathbb{T} \otimes_{\mathbb{Z}} \mathbb{Q} \subset \text{End}_K J \otimes \mathbb{Q}$, est alors nul. De $\eta_l(x) = 0 = \eta_l(\infty)$, on déduit $(x) - (\infty) = 0$ dans $J(K) \otimes_{\mathbb{Z}} \mathbb{Q}$. Donc la classe du diviseur $(x) - (\infty)$ appartient à $J(K)_{\text{tors}}$. Par un théorème de Pál [2005, théorème 1.4], ce groupe est égal au sous-groupe cuspidal. Ce dernier étant annulé par $(1 + w_p)$, la classe de $(1 + w_p)((x) - (\infty))$ est donc nulle dans $J(K)$.

Notons X^+ la courbe $w_p \setminus X$ sur K , ∞^+ son unique pointe et J^+ sa jacobienne. On a le diagramme commutatif

$$\begin{array}{ccc} X & \xrightarrow{\varphi} & J \\ \pi \downarrow & & \downarrow \pi_* \\ X^+ & \xrightarrow{\varphi^+} & J^+, \end{array}$$

où π est la projection canonique, π_* le morphisme qui s'en déduit par fonctorialité d'Albanese, $\varphi = \varphi^{(1)}$ l'application d'Abel–Jacobi normalisée par $\varphi(\infty) = 0$, de même pour φ^+ normalisée par $\varphi^+(\infty^+) = 0$. D'après ce qui précède, le diviseur $\pi_*((1 + w_p)((x) - (\infty))) = 2((x^+) - (\infty^+))$ est linéairement équivalent à 0 dans J^+ .

Supposons x^+ distinct de ∞^+ . Alors le diviseur $(x^+) - (\infty^+)$ est non nul et sa classe est d'ordre 1 ou 2 dans $J^+(K)$. Supposons qu'elle soit d'ordre 2. Le diviseur $2((x^+) - (\infty^+))$ étant non nul et principal sur K , il définit un morphisme K -rationnel non constant $X^+ \rightarrow \mathbb{P}^1$ de degré 2. En composant avec $\pi : X \rightarrow X^+$ qui est dominant, on obtient un morphisme K -rationnel dominant $X \rightarrow \mathbb{P}^1$ de degré 4. Donc la gonalgité de X sur K est ≤ 4 . Comme $q \geq 5$ et $\text{deg } p \geq 4$, cela contredit

la minoration de la proposition 7.2. Ainsi, le diviseur $(x^+) - (\infty^+)$ est non nul et linéairement équivalent à 0. Comme précédemment, on en déduit un morphisme K -rationnel dominant $X^+ \rightarrow \mathbb{P}^1$ de degré 1. Donc la courbe X^+ serait de genre nul. En particulier, le morphisme K -rationnel $\pi : X \rightarrow X^+ \simeq \mathbb{P}^1$ est dominant de degré 2. La courbe modulaire X serait rationnelle, elliptique ou hyperelliptique. Mais comme $\deg \mathfrak{p} \geq 4$, elle est de genre > 1 et n'est pas hyperelliptique d'après [Schweizer 1997, théorème 20]. En conclusion on a $x^+ = \infty^+$ c'est-à-dire x est dans $\{0, \infty\}$. \square

Théorème 7.8. *Soit $q \geq 5$. Supposons \mathfrak{p} de degré ≥ 5 tel que toute forme primitive de $H_{\mathfrak{p}}(\mathbb{C})$ est de rang analytique ≤ 1 . Alors la courbe $Y_0(\mathfrak{p})$ n'a pas de point K -rationnel (i.e., il n'existe pas de module de Drinfeld de rang 2 sur K avec une isogénie K -rationnelle cyclique d'ordre \mathfrak{p}).*

Cet énoncé partage la même condition sur le rang analytique des formes primitives que le théorème 7.5(ii). Des outils appropriés sur machine devraient permettre d'exhiber des couples (q, \mathfrak{p}) où le théorème 7.8 s'applique (nous n'avons pas eu l'occasion de le faire).

Démonstration. Supposons qu'il existe $x \in Y_0(\mathfrak{p})(K)$. Considérons le morphisme $f : X \rightarrow J$ qui envoie P sur la classe d'équivalence linéaire de $(P) - (w_{\mathfrak{p}}(P))$. L'image de f , qui est anti-invariante par $w_{\mathfrak{p}}$, est donc contenue dans la plus grande sous-variété abélienne de J annihilée par $(1 + w_{\mathfrak{p}})$. Cette variété abélienne est notée J_- . Elle est naturellement isogène à $J^- = J/(1 + w_{\mathfrak{p}})J$ sur K , dont le groupe de Mordell–Weil est fini d'après l'hypothèse sur \mathfrak{p} et la proposition 4.5. Donc $f(x)$ appartient à $J_-(K) \hookrightarrow J(K)_{\text{tors}}$. Par un théorème de Pál [2005, théorème 1.4] ce sous-groupe de torsion est égal au sous-groupe cuspidal. Ce dernier étant annihilé par η_l , on a alors $\eta_l(f(x)) = 0$ dans $J(K)$ pour un premier $l \neq \mathfrak{p}$. Le diviseur $T_l(x) + (q+1)(w_{\mathfrak{p}}(x)) - T_l(w_{\mathfrak{p}}(x)) - (q+1)(x)$ est non nul, d'après le lemme 7.7, et principal sur K . Il définit donc une fonction K -rationnelle non constante $X \rightarrow \mathbb{P}^1$ de degré $\leq 2(q+1)$. Donc la gonalgité de X sur K est $\leq 2(q+1)$. Comme $q \geq 5$ et $\deg \mathfrak{p} \geq 5$, on obtient une contradiction avec la proposition 7.2. \square

7E. Points rationnels : étude du cas général.

7E1. *L'argument de Mazur.* On reprend les notations introduites en 7C. Par propriété universelle, $\varphi^{(d)}$ et $u^{(d)}$ se prolongent de façon unique en des homomorphismes de $A[1/\mathfrak{p}]$ -schémas $\varphi^{(d)} : \mathcal{X}^{(d)} \rightarrow \mathcal{F}$ et $u^{(d)} : \mathcal{X}^{(d)} \rightarrow \mathcal{F}'$.

L'argument de Mazur utilise une propriété des immersions formelles. Soient $f : Y \rightarrow Z$ un morphisme de schémas noethériens, y un point de Y et $z = f(y)$. On dit que f est une *immersion formelle en y* si le morphisme d'anneaux $\widehat{\mathcal{O}}_{Z,z} \rightarrow \widehat{\mathcal{O}}_{Y,y}$ déduit de f par passage aux complétés est surjectif. D'après le lemme de Nakayama, cela revient à demander à ce que f induise une bijection entre les corps

résiduels en z et y et l'application déduite de f par passage aux espaces cotangents en z et y soit surjective. Si de plus Y est séparé de type fini, une immersion formelle f vérifie la propriété suivante : soient T un schéma intègre noethérien et t un point de T ; deux morphismes $T \rightarrow Y$ envoyant t sur y et qui coïncident après composition par f sont alors égaux.

On pourra comparer l'énoncé suivant à [Mazur 1978, corollaire 4.3] et [Kamieny 1992b, lemme 3.2, théorème 3.3].

Proposition 7.9. *Fixons un premier \mathfrak{l} . Soit \mathfrak{p} un premier de degré $> d$ deg \mathfrak{l} tel que les propriétés suivantes sont vérifiées :*

- (i) $J'(K)$ est fini.
- (ii) $u^{(d)} : \mathcal{X}^{(d)} \rightarrow \mathcal{F}'$ est une immersion formelle en $\infty_{\mathfrak{l}}^{(d)}$ (la restriction de $\infty^{(d)}$ à la fibre spéciale en \mathfrak{l}).

Alors pour toute extension L/K de degré d , la courbe $Y_1(\mathfrak{p})$ n'a pas de point L -rationnel.

Démonstration. S'il existe, un point y de $Y_1(\mathfrak{p})(L)$ définit $P \in X(L)$ et $x \in X^{(d)}(K)$ comme expliqué au paragraphe 7C. Par le lemme 7.4, on trouve que $u^{(d)}(w_{\mathfrak{p}}(x))$ est nul dans $J'(K)$. En particulier, on a $u^{(d)}(w_{\mathfrak{p}}(x)) = u^{(d)}(w_{\mathfrak{p}}(0))$ dans $\mathcal{F}'(A[1/\mathfrak{p}])$. De plus, $w_{\mathfrak{p}}(x)$ et $\infty^{(d)}$ ont même spécialisation en \mathfrak{l} (voir la preuve du lemme 7.4). La propriété rappelée pour l'immersion formelle $u^{(d)}$ en $\infty_{\mathfrak{l}}^{(d)}$ assure que les sections $w_{\mathfrak{p}}(x)$ et $\infty^{(d)}$ coïncident. Donc P est la pointe 0. Cela contredit l'interprétation modulaire de P . □

7E2. Espaces cotangents et immersion formelle. Implicitement, les espaces cotangents aux variétés abéliennes seront pris en la section nulle, ceux à $\mathcal{X}^{(d)}$ en la section $\infty^{(d)}$.

L'algèbre \mathbb{T} opère naturellement sur l'espace cotangent $\text{Cot } \mathcal{F}$ comme suit. Tout élément u de \mathbb{T} , vu comme endomorphisme de J sur K , s'étend de façon unique au modèle de Néron \mathcal{F} . Par passage aux espaces cotangents, il induit un endomorphisme de $\text{Cot } \mathcal{F}$ qu'on note $\text{cot}(u)$.

Jusqu'à la fin de 7E2, on suppose l'hypothèse 4.9 satisfaite par un idéal I de \mathbb{T} . Soit $J'_e(\mathfrak{p})$ le quotient raffiné relatif à I et $\mathcal{F}'_e(\mathfrak{p})$ son modèle de Néron. Commençons par donner un critère pour l'immersion formelle. Pour un idéal \mathcal{I} de \mathbb{T} et un espace V sur lequel \mathbb{T} opère, on note $V[\mathcal{I}]$ le sous-espace annulé par \mathcal{I} .

Proposition 7.10. *Soit \mathfrak{l} un premier distinct de \mathfrak{p} . Si l'application naturelle*

$$(\text{Cot } \mathcal{F}_{\mathbb{F}_{\mathfrak{l}}})[\tilde{I}_e] \longrightarrow \text{Cot } \mathcal{X}_{\mathbb{F}_{\mathfrak{l}}}^{(d)}$$

déduite de $\varphi^{(d)}$ est surjective, le morphisme $u^{(d)} : \mathcal{X}^{(d)} \rightarrow \mathcal{F}'_e(\mathfrak{p})$ est une immersion formelle en $\infty_{\mathfrak{l}}^{(d)}$.

Démonstration. Soit $\pi : J \rightarrow J'_e(\mathfrak{p})$ le morphisme canonique, qui s'étend aux modèles de Néron, et $\pi^* : \text{Cot } \mathcal{F}'_e(\mathfrak{p}) \rightarrow \text{Cot } \mathcal{F}$ le morphisme obtenu par passage aux espaces cotangents. On commence par montrer que l'image de π^* contient $(\text{Cot } \mathcal{F})[\tilde{I}_e]$.

Par (J3) de l'hypothèse 4.9, il existe des éléments \hat{t} dans \hat{I} et \tilde{t} dans \tilde{I}_e avec $1 = \hat{t} + \tilde{t}$ dans \mathbb{T} . Regardons \hat{t} comme un endomorphisme de J . Comme \hat{t} annule I , le morphisme $\hat{t} : J \rightarrow J$ se factorise par π . Le diagramme se prolonge aux modèles de Néron, par propriété universelle. En passant aux espaces cotangents, on en déduit le diagramme commutatif :

$$\begin{array}{ccc} \text{Cot } \mathcal{F} & \longrightarrow & \text{Cot } \mathcal{F}'_e(\mathfrak{p}) \\ & \searrow \text{cot}(\hat{t}) & \downarrow \pi^* \\ & & \text{Cot } \mathcal{F}. \end{array}$$

En particulier, l'image du morphisme π^* contient $\text{cot}(\hat{t})(\text{Cot } \mathcal{F})[\tilde{I}_e]$. Comme la relation $1 = \hat{t} + \tilde{t}$ est encore valable sur \mathcal{F} , on a

$$\text{cot}(\hat{t})(\text{Cot } \mathcal{F})[\tilde{I}_e] = \text{cot}(1 - \tilde{t})(\text{Cot } \mathcal{F})[\tilde{I}_e] = (\text{Cot } \mathcal{F})[\tilde{I}_e].$$

Donc l'image de π^* contient $(\text{Cot } \mathcal{F})[\tilde{I}_e]$. En passant aux fibres en \mathfrak{l} et en utilisant l'hypothèse de l'énoncé, on voit que l'homomorphisme $\text{Cot } \mathcal{F}'_e(\mathfrak{p})_{\mathbb{F}_\mathfrak{l}} \rightarrow \text{Cot } \mathcal{X}_{\mathbb{F}_\mathfrak{l}}^{(d)}$ déduit de $u^{(d)}$ est alors surjectif. Donc $u^{(d)}$ est une immersion formelle en $\infty_{\mathfrak{l}}^{(d)}$. □

Afin de reformuler la surjectivité de $(\text{Cot } \mathcal{F}_{\mathbb{F}_\mathfrak{l}})[\tilde{I}_e] \rightarrow \text{Cot } \mathcal{X}_{\mathbb{F}_\mathfrak{l}}^{(d)}$, on rend explicite ce morphisme. Notons $S_{\mathfrak{p}} = S(A[1/\mathfrak{p}])$ comme dans l'introduction. Rappelons que, d'après le lemme 6.8, on a un isomorphisme canonique

$$\text{Cot } \mathcal{F} \xrightarrow{\sim} S_{\mathfrak{p}}.$$

Par la proposition 5.4, le complété formel de \mathcal{X} le long de la section ∞ est isomorphe, *via* le module de Tate–Drinfeld, au spectre formel de $A[1/\mathfrak{p}][[t^{q-1}]]$. En d'autres termes, \mathcal{X} admet la coordonnée formelle locale $s = t^{q-1}$ en ∞ . L'espace cotangent à \mathcal{X} en la section ∞ est alors isomorphe, comme $A[1/\mathfrak{p}]$ -module, à sR/s^2R où $R = A[1/\mathfrak{p}][[s]]$. Il est de libre de rang 1 de base ds (on utilise d pour la notation différentielle). Notons s_1, \dots, s_d les coordonnées formelles locales du schéma-produit $\mathcal{X}^{(d)}$. Par construction du produit symétrique, les fonctions symétriques élémentaires $\sigma_1 = s_1 + \dots + s_d, \dots, \sigma_d = s_1 \cdots s_d$ sont des coordonnées formelles locales de $\mathcal{X}^{(d)}$ en $\infty^{(d)}$. Donc le $A[1/\mathfrak{p}]$ -module $\text{Cot}_{\infty^{(d)}} \mathcal{X}^{(d)}$ est libre de rang d de base $d\sigma_1, \dots, d\sigma_d$. Notons $\varphi^{(d)*} : \text{Cot } \mathcal{F} \rightarrow \text{Cot } \mathcal{X}^{(d)}$ le morphisme déduit de $\varphi^{(d)}$. On pourra comparer l'énoncé suivant avec les preuves de [Kamienny 1992a, proposition 3.2] et [Kamienny 1992b, proposition 3.1].

Proposition 7.11. *Avec les identifications précédentes, $\varphi^{(d)*}$ correspond à l'homomorphisme de $A[1/\mathfrak{p}]$ -modules*

$$S_{\mathfrak{p}} \rightarrow (A[1/\mathfrak{p}])^d, \quad f \mapsto (-b_1(f), b_2(f), \dots, (-1)^d b_d(f)),$$

où $\sum_{i \geq 1} b_i(f)t^{1+i(q-1)}$ est le t -développement de f .

Démonstration. Posons $\Omega = \Omega_{\mathcal{X}/A[1/\mathfrak{p}]}$. On note temporairement δ l'exposant de la puissance symétrique afin d'éviter toute confusion avec la notation différentielle d . Par propriété de la puissance symétrique [Milne 1986, proposition 5.3], on a l'isomorphisme canonique β obtenu par composition :

$$S_{\mathfrak{p}} \xrightarrow{\sim} H^0(\mathcal{X}, \Omega) \xrightarrow{\sim} H^0(\mathcal{X}^{(\delta)}, \Omega).$$

Soit $r : H^0(\mathcal{X}^{(\delta)}, \Omega) \rightarrow \text{Cot } \mathcal{X}^{(\delta)}$ le morphisme naturel qui associe à une section sa restriction au fibré cotangent en $\infty^{(\delta)}$. On a le diagramme suivant :

$$\begin{array}{ccc}
 \text{Cot } \mathcal{F} & \xrightarrow{\varphi^{(\delta)*}} & \text{Cot } \mathcal{X}^{(\delta)} & \xrightarrow{\sim} & (A[1/\mathfrak{p}])^{\delta} \\
 \downarrow \sim & & \nearrow r & & \\
 S_{\mathfrak{p}} & & & & \\
 \downarrow \beta \sim & & & & \\
 H^0(\mathcal{X}^{(\delta)}, \Omega) & & & &
 \end{array}$$

Le triangle est commutatif par l'argument du lemme 2.1 de [Mazur 1978]. Explicitons $r \circ \beta$. Soit $f \in S_{\mathfrak{p}}$ de t -développement $\sum_{i \geq 1} b_i t^{1+i(q-1)}$. Pour $s = t^{q-1}$ le paramètre formel local de $X_0(\mathfrak{p})$ en ∞ , le développement de toute différentielle $f \in S(F)$ en ∞ est $-\sum_{i \geq 1} b_i s^{i-1} ds$ (équation (7)). Donc l'image de f dans $H^0(\mathcal{X}^{\delta}, \Omega)$ par l'application canonique est la différentielle régulière globale de développement formel

$$-\sum_{1 \leq i \leq \delta} \sum_{k \geq 1} b_k s_i^{k-1} ds_i.$$

Signalons qu'à partir de cette étape, les calculs menés dans [Kamienny 1992a, proposition 3.2] ne sont plus valables en caractéristique p . Posons $u_j = \sum_{1 \leq i \leq \delta} s_i^j ds_i$ pour $j \geq 0$. On a l'identité

$$-\sum_{1 \leq i \leq \delta} \sum_{k \geq 1} b_k s_i^{k-1} ds_i = -\sum_{k \geq 1} b_k u_{k-1}. \tag{17}$$

Pour obtenir l'image de f par $r \circ \beta$, il suffit de considérer l'image de (17) dans $H^0(\mathcal{X}^{(\delta)}, \Omega)$ puis prendre la partie linéaire de son développement.

En notant comme auparavant $\sigma_1 = s_1 + \dots + s_{\delta}, \dots, \sigma_{\delta} = s_1 \dots s_{\delta}$, on a les identités suivantes dans le module des différentielles de Kähler de $A[1/\mathfrak{p}, s_1, \dots, s_{\delta}]$

sur $A[1/\mathfrak{p}]$:

$$\sigma_m u_0 - \sigma_{m-1} u_1 + \cdots + (-1)^m u_m = d\sigma_{m+1} \quad (1 \leq m \leq \delta - 1), \quad (18)$$

$$(-1)^\delta \sigma_\delta u_{m-\delta} + \cdots - \sigma_1 u_{m-1} + u_m = 0 \quad (m \geq \delta). \quad (19)$$

La première est le lemme 5.4 de [Milne 1986]. Pour démontrer la deuxième, on considère les relations de Newton $s_i^\delta - \sigma_1 s_i^{\delta-1} + \cdots + (-1)^\delta \sigma_\delta = 0$ pour $1 \leq i \leq \delta$, qu'on multiplie par $s_i^{m-\delta} ds_i$ pour $m \geq \delta$, puis on somme ces relations sur $1 \leq i \leq \delta$. En évaluant en l'infini (18) et (19), on obtient les égalités dans $\text{Cot } \mathcal{X}^{(\delta)}$:

$$(-1)^m u_m = d\sigma_{m+1} \quad (1 \leq m \leq \delta - 1).$$

$$u_m = 0 \quad (m \geq \delta).$$

En substituant dans (17), on obtient pour la partie linéaire :

$$(r \circ \beta)(f) = - \sum_{1 \leq k \leq \delta} (-1)^{k+1} b_k d\sigma_k \in \text{Cot } \mathcal{X}^{(\delta)}. \quad \square$$

Corollaire 7.12. *Si \mathfrak{p} est premier de degré 3, le morphisme $u^{(q)} : \mathcal{X}^{(q)} \rightarrow \mathcal{Y}$ est une immersion formelle en $\infty_{\mathfrak{l}}^{(q)}$ pour tout \mathfrak{l} premier $\neq \mathfrak{p}$.*

Démonstration. Comme $\deg \mathfrak{p} = 3$, le quotient d'enroulement est égal à J par la proposition 4.4. Donc $u^{(q)} = \varphi^{(q)} : \mathcal{X}^{(q)} \rightarrow \mathcal{Y}$. Pour l'immersion formelle, il suffit alors de voir que

$$S(\mathbb{F}_{\mathfrak{l}}) \rightarrow (\mathbb{F}_{\mathfrak{l}})^q, \quad f \mapsto (b_1(f), \dots, b_q(f))$$

est surjective d'après la proposition 7.11. C'est précisément le résultat de la proposition 6.17 car X est ici de genre $g = q$ (proposition 3.2). \square

On obtient ainsi une nouvelle démonstration du théorème 7.5(i) : il s'agit de combiner le corollaire, la méthode de Mazur pour $J' = J$ (proposition 7.9) et la proposition 4.4.

Maintenant, donnons un critère pour l'immersion formelle en termes de formes modulaires de Drinfeld.

Théorème 7.13. *Supposons l'application linéaire*

$$S(\mathbb{F}_{\mathfrak{l}})[\tilde{I}_{\mathfrak{e}}] \rightarrow (\mathbb{F}_{\mathfrak{l}})^d, \quad f \mapsto (b_1(f), \dots, b_d(f))$$

surjective. Alors le morphisme $u^{(d)} : \mathcal{X}^{(d)} \rightarrow \mathcal{Y}'_{\mathfrak{e}}(\mathfrak{p})$ est une immersion formelle en $\infty_{\mathfrak{l}}^{(d)}$.

Démonstration. Par le lemme 6.8 et le changement de base (proposition 6.6), on a un isomorphisme canonique $\text{Cot}(\mathcal{Y}_{\mathbb{F}_{\mathfrak{l}}}) \simeq S(\mathbb{F}_{\mathfrak{l}})$ pour tout \mathfrak{l} premier distinct de \mathfrak{p} . On conclut alors avec les propositions 7.10 et 7.11. \square

7E3. Critère de Kamienny. On fixe un premier l distinct de p . Comme dans la section précédente, on suppose qu'il existe un idéal I vérifiant l'hypothèse 4.9 et son quotient raffiné est noté $J'_e(p)$. L'énoncé qui suit s'apparente à un critère de Kamienny [1992b, corollaire 3.4].

Proposition 7.14. *Supposons les conditions suivantes vérifiées :*

(i) *L'application \mathbb{F}_l -linéaire*

$$\Phi_l : (\mathbb{T}/\tilde{I}_e) \otimes_{\mathbb{Z}} \mathbb{F}_l \longrightarrow \text{Hom}(S(\mathbb{F}_l)[\tilde{I}_e], \mathbb{F}_l),$$

qui envoie la classe de $u \in \mathbb{T}$ sur la forme linéaire $f \mapsto b_1(uf)$, est un isomorphisme.

(ii) *Il existe des éléments u_1, \dots, u_d de $\mathbb{T} \otimes_{\mathbb{Z}} \mathbb{F}_l$ vérifiant $b_i = b_1 \circ u_i$ ($1 \leq i \leq d$) et dont les images dans $(\mathbb{T}/\tilde{I}_e) \otimes_{\mathbb{Z}} \mathbb{F}_l$ sont libres sur \mathbb{F}_l .*

La condition (i) est vérifiée lorsque $\deg p = 3$. La condition (ii) est vérifiée pour $d = 1$, $\deg p \geq 3$ et pour $1 \leq d \leq q$, $\deg p \geq 5$. Alors le morphisme $u^{(d)} : \mathcal{X}^{(d)} \rightarrow \mathcal{Y}'_e(p)$ est une immersion formelle en $\infty_1^{(d)}$.

Démonstration. D'après le théorème 7.13, il suffit de voir les formes linéaires b_1, \dots, b_d sur $S(\mathbb{F}_l)[\tilde{I}_e]$ sont linéairement indépendantes. Par l'isomorphisme Φ_l , la forme linéaire b_i correspond à la classe de u_i dans $(\mathbb{T}/\tilde{I}_e) \otimes_{\mathbb{Z}} \mathbb{F}_l$. La condition (ii) dit que ces classes sont libres et le résultat se transpose à b_1, \dots, b_d par l'isomorphisme Φ_l . Donc $u^{(d)}$ est une immersion formelle.

Supposons p de degré 3. On commence par démontrer que l'idéal $(q-1)d_e\tilde{I}_e$ est contenu dans $p\mathbb{T}$. Soit $t \in \tilde{I}_e$ c'est-à-dire vérifiant $d_e t e \in pM^0$. Comme $\deg p = 3$, d'après la proposition 8.2 de [Armana 2011b] on a $M^0 = M^0$ et l'isomorphisme de \mathbb{T} -modules

$$I_E \rightarrow M^0, \quad u \mapsto ue/(q-1),$$

où I_E est l'idéal d'Eisenstein de \mathbb{T} , c'est-à-dire, celui engendré par les éléments $T_m - (q^{\deg m} + 1)$ pour tout m premier distinct de p . Donc il existe u dans I_E tel que l'élément $(q-1)d_e t - pu$ de l'algèbre de Hecke annule e . Il est nul par la proposition 4.4. Donc $(q-1)d_e t$ appartient à $p\mathbb{T}$. Cela démontre l'affirmation.

Un calcul mené en [Armana 2011b, 7.1.2] montre que le dénominateur d_e est ici $q^2 + q + 1$. Donc, comme \mathbb{F}_l est de caractéristique p et $(q^3 - 1)\tilde{I}_e \subset p\mathbb{T}$, on a $\tilde{I}_e \otimes \mathbb{F}_l = (q^3 - 1)\tilde{I}_e \otimes \mathbb{F}_l = 0$. De même, on a

$$S(\mathbb{F}_l) = S(\mathbb{F}_l)[p\mathbb{T}] \subset S(\mathbb{F}_l)[(q^3 - 1)\tilde{I}_e] = S(\mathbb{F}_l)[\tilde{I}_e]$$

donc l'inclusion est une égalité. Par ces considérations, la condition (i) revient à montrer que $\Phi_l : \mathbb{T} \otimes_{\mathbb{Z}} \mathbb{F}_l \rightarrow \text{Hom}(S(\mathbb{F}_l), \mathbb{F}_l)$ est bijectif. Les espaces considérés sont de dimension $g = q$ sur \mathbb{F}_l (car \mathbb{T} est libre de rang g sur \mathbb{Z} et, pour $S(\mathbb{F}_l)$, d'après la proposition 6.7). Montrons simplement la surjectivité de Φ_l . D'après le

théorème 6.15, les images de $\theta_1, \dots, \theta_q$ dans $\mathbb{T} \otimes_{\mathbb{F}_l} s$ envoient par Φ_l sur les formes linéaires b_1, \dots, b_q respectivement. Or, ces formes linéaires constituent une base du dual de $S(\mathbb{F}_l)$ par la proposition 6.17. Donc Φ_l est bijective.

Passons maintenant à la condition (ii). Supposons $d = 1$ et $\deg p \geq 3$. L'élément $u_1 = T_{(1)} = \text{id}$ de l'algèbre de Hecke vérifie naturellement $b_1 = b_1 \circ u_1$. Il s'agit ensuite de voir que $T_{(1)}$ est non nul dans $(\mathbb{T}/\tilde{I}_e) \otimes_{\mathbb{Z}} \mathbb{F}_l$. Il suffit de le vérifier dans \mathbb{T}/\tilde{I}_e , vu comme espace vectoriel sur \mathbb{F}_p . Or cela découle de la propriété : \tilde{e} est non nul dès que $\deg p \geq 3$ [Armana 2011b, théorème 7.10(ii)].

Supposons $\deg p \geq 5$ et vérifions la condition (ii) pour $d = q$. Les éléments $\theta_1, \dots, \theta_q$ de $\mathbb{T} \otimes_{\mathbb{Z}} A$ donnés par le théorème 6.15 vérifient $b_i = b_1 \circ \theta_i$ pour $1 \leq i \leq q$ dans le dual de $S(A[1/p])$, donc aussi dans le dual de $S(\mathbb{F}_l)$. Montrons que leurs images u_1, \dots, u_q dans $(\mathbb{T}/\tilde{I}_e) \otimes_{\mathbb{Z}} \mathbb{F}_l$ forment une famille libre. Pour cela, on commence par se ramener à d'autres éléments de l'algèbre de Hecke. Notons m_1, \dots, m_q les idéaux de A de degré 1 et M_1, \dots, M_q leurs générateurs unitaires respectifs. Par définition de θ_i , on a

$$\begin{pmatrix} \theta_1 \\ \vdots \\ \theta_q \end{pmatrix} = R \begin{pmatrix} T_{m_1} \\ \vdots \\ T_{m_q} \end{pmatrix} \text{ avec } R = (-1)^q \begin{pmatrix} \binom{q-1}{0}^{-1} & \dots & \binom{q-1}{0}^{-1} \\ \binom{q-1}{1}^{-1} M_1 & \dots & \binom{q-1}{1}^{-1} M_q \\ \vdots & & \vdots \\ \binom{q-1}{q-2}^{-1} M_1^{q-2} & \dots & \binom{q-1}{q-2}^{-1} M_q^{q-2} \\ 1 - M_1^{q-1} & \dots & 1 - M_q^{q-1} \end{pmatrix}.$$

Quitte à soustraire la première ligne de la dernière, on voit que le déterminant de R est de Vandermonde et vaut

$$(-1)^{q+1} \prod_{1 \leq i \leq q-2} \binom{q-1}{i}^{-1} \prod_{j < k} (M_j - M_k) \in \mathbb{F}_q^\times.$$

Donc R appartient à $GL_q(A)$. Ainsi, il suffit de démontrer l'indépendance linéaire des images de T_{m_1}, \dots, T_{m_q} dans $(\mathbb{T}/\tilde{I}_e) \otimes_{\mathbb{Z}} \mathbb{F}_l$. Là encore, il suffit de le vérifier dans le \mathbb{F}_p -espace vectoriel \mathbb{T}/\tilde{I}_e . Or, cela découle de [Armana 2011b, théorème 7.10(ii)] pour $\deg p \geq 5$. □

Remarque 7.15. Pour établir la condition (ii) pour $d > q$, il faudrait déjà disposer d'un élément u_{q+1} de $\mathbb{T} \otimes_{\mathbb{Z}} \mathbb{F}_l$ vérifiant $b_{q+1} = b_1 \circ u_{q+1}$. Pour cela, une idée naturelle est de généraliser le théorème 6.15 à des opérateurs de Hecke dont l'indice est de degré > 1 . C'est ce qui a été fait dans [Armana 2011a], mais un tel u_{q+1} n'a pas pu être exhibé. Lorsque $\deg p = 3$, on verra l'existence d'un tel u_{q+1} (proposition 7.17), sans en avoir une formule explicite.

Maintenant, nous sommes en mesure de prouver les résultats annoncés en introduction. En combinant les propositions 4.11, 7.9 et 7.14, on obtient le théorème 1.5 sur les points de $Y_1(\mathfrak{p})$. Un argument similaire, dans l'esprit de la proposition 7.6, démontre un résultat partiel sur les points de $Y_0(\mathfrak{p})$ (on laisse la preuve au lecteur).

Proposition 7.16. *Soit \mathfrak{p} de degré ≥ 3 . Supposons qu'il existe un premier \mathfrak{l} tel que $\Phi_{\mathfrak{l}}$ est un isomorphisme. Alors tout module de Drinfeld de rang 2 sur K possédant une isogénie K -rationnelle cyclique d'ordre \mathfrak{p} a bonne réduction potentielle en \mathfrak{l} .*

La borne uniforme de Schweizer sur la \mathfrak{p} -torsion [2003, théorème 2.4 et remarque 2.5] ramène la conjecture 1.1 pour q et d fixés à un problème, *a priori* plus faible, sur la torsion première : *montrer qu'il n'y a qu'un nombre fini de premiers \mathfrak{p} pour lesquels il existe une extension L/K de degré d , un module de Drinfeld ϕ de rang 2 sur L et un point de $({}^{\phi}L)_{\text{tors}}$ d'ordre \mathfrak{p}* . Cela revient à voir que le degré des premiers \mathfrak{p} comme ci-dessus est borné par une constante dépendant de q et d . Le théorème 1.5 établit ce fait si $1 \leq d \leq q$, à condition que ses hypothèses soient vérifiées. C'est ainsi qu'on obtient le corollaire 1.6 (on applique le théorème 1.5 aux \mathfrak{p} de degrés $\geq \max(q+1, 5, B_q)$).

Pour terminer, on revient sur la condition (i) de la proposition 7.14. Dans une version antérieure [Armana 2009] de ce travail, la condition (i) était remplacée par l'hypothèse plus forte : l'application $\Phi'_{\mathfrak{l}} : \mathbb{T} \otimes_{\mathbb{Z}} \mathbb{F}_{\mathfrak{l}} \rightarrow \text{Hom}(S(\mathbb{F}_{\mathfrak{l}}), \mathbb{F}_{\mathfrak{l}})$, qui envoie la classe de u sur $(f \mapsto b_1(uf))$, est un isomorphisme. Elle ne semble pas être systématiquement vérifiée. En effet, le théorème 6.15 permet de voir que $\sum_{\deg m \leq 1} T_m$ est dans le noyau de $\Phi'_{\mathfrak{l}}$. Mais des investigations numériques suggèrent que, pour $\deg \mathfrak{p} \geq 5$, cet élément est non nul dans $\mathbb{T} \otimes_{\mathbb{Z}} \mathbb{F}_{\mathfrak{l}}$, car non nul dans H/pH (voir [Armana 2011a, paragraphe 6.4 et conjecture 6.9]).

Lorsque $\deg \mathfrak{p} = 3$, on a vu dans la preuve de la proposition 7.14 que $\Phi'_{\mathfrak{l}}$ est un isomorphisme pour tout \mathfrak{l} . De cette dualité, on tire des informations sur la structure de Hecke des formes modulaires de Drinfeld.

Proposition 7.17. *Soit \mathfrak{p} premier de degré 3.*

- (i) *L'algèbre $\mathbb{T} \otimes_{\mathbb{Z}} \mathbb{F}_{\mathfrak{l}}$ opère fidèlement sur $S(\mathbb{F}_{\mathfrak{l}})$; l'algèbre $\mathbb{T}/p\mathbb{T}$ opère fidèlement sur H/pH .*
- (ii) *Pour tout $i \geq 1$, il existe $u_i \in \mathbb{T} \otimes_{\mathbb{Z}} \mathbb{F}_{\mathfrak{l}}$ avec $b_i = b_1 \circ u_i$.*
- (iii) *Toute forme modulaire de Drinfeld de $S(\mathbb{F}_{\mathfrak{l}})$ propre pour $(T_m)_{\deg m=1}$ est déterminée par ses valeurs propres, à un facteur multiplicatif près.*
- (iv) *Le \mathbb{F}_p -espace vectoriel $\mathbb{T}/p\mathbb{T}$ a pour base $(T_m)_{\deg m=1}$.*

Démonstration. (i) La première affirmation découle de l'isomorphisme $\Phi'_{\mathfrak{l}}$. Une preuve de la deuxième se trouve dans [Armana 2011b, corollaire 8.3]. On donne ici un autre argument, indépendant, utilisant $\Phi'_{\mathfrak{l}}$. Soit u un élément de $\mathbb{T}/p\mathbb{T}$, nul comme endomorphisme de H/pH . D'après Gekeler–Reversat, le $\mathbb{T}/p\mathbb{T}$ -module

H/pH s'identifie à une certaine \mathbb{F}_p -structure de l'espace $S(\mathbb{C}_\infty)$ de formes modulaires analytiques (proposition 6.9 et [Gekeler et Reversat 1996, diagramme 6.5]). Donc u , vu comme endomorphisme de $S(\mathbb{C}_\infty)$, est nul. Il en est de même sur $S(A[1/p])$. Par extension des scalaires (proposition 6.6), il en va de même sur $S(\mathbb{F}_l)$. Donc u est dans le noyau du morphisme composé

$$\mathbb{T}/p\mathbb{T} \longrightarrow \mathbb{T}/p\mathbb{T} \otimes_{\mathbb{F}_p} \mathbb{F}_l = \mathbb{T} \otimes_{\mathbb{Z}} \mathbb{F}_l \xrightarrow{\Phi'_l} \text{Hom}(S(\mathbb{F}_l), \mathbb{F}_l).$$

Le premier est naturellement injectif. Comme Φ'_l est un isomorphisme, u est nul.

(ii) L'affirmation provient de la surjectivité de Φ'_l .

(iii) Soit f propre pour $(T_m)_{\deg m=1}$ de valeurs propres $(\lambda_m)_{\deg m=1}$. Par le théorème 6.15, on peut exprimer les coefficients $b_1(f), \dots, b_q(f)$ en fonction des valeurs propres $(\lambda_m)_{\deg m=1}$ et $b_1(f)$. Par ailleurs, comme le genre est $g = q$, la forme modulaire f est déterminée de façon unique par ses coefficients $b_1(f), \dots, b_q(f)$ (proposition 6.17) Donc f est déterminée, à un facteur multiplicatif près, par les valeurs propres $(\lambda_m)_{\deg m=1}$.

(iv) Dans la preuve de la proposition 7.14, on a vu que $\theta_1, \dots, \theta_q$ est une base de $\mathbb{T} \otimes_{\mathbb{Z}} \mathbb{F}_l$ sur \mathbb{F}_l pour $\deg p = 3$. Via la matrice $R \in \text{GL}_q(A)$ de la preuve, on en déduit que $(T_m)_{\deg m=1}$ est aussi une base. En prenant pour l une place de degré 1, on a $\mathbb{T} \otimes_{\mathbb{Z}} \mathbb{F}_l \simeq \mathbb{T} \otimes_{\mathbb{Z}} \mathbb{F}_p \simeq \mathbb{T}/p\mathbb{T}$, d'où le résultat. \square

Remerciements

Je tiens à remercier Loïc Merel pour ses conseils lors de l'élaboration de ce travail de doctorat ainsi que le rapporteur pour ses remarques et sa relecture attentive. Je suis reconnaissante au Max-Planck-Institut für Mathematik pour son accueil lors de la rédaction de l'article.

Bibliographie

- [Armana 2008] C. Armana, *Torsion rationnelle des modules de Drinfeld*, thèse, Université Paris Diderot, 2008, Disponible à <http://tel.archives-ouvertes.fr/docs/00/34/93/10/PDF/these-armana.pdf>.
- [Armana 2009] C. Armana, "Torsion des modules de Drinfeld de rang 2 et formes modulaires de Drinfeld", *C. R. Math. Acad. Sci. Paris* **347**:13-14 (2009), 705–708. MR 2010h:11079 Zbl 1207.11055
- [Armana 2011a] C. Armana, "Coefficients of Drinfeld modular forms and Hecke operators", *J. Number Theory* **131**:8 (2011), 1435–1460. MR 2012f:11096 Zbl 05899186
- [Armana 2011b] C. Armana, "Une base explicite de symboles modulaires sur les corps de fonctions", prépublication, 2011, Disponible à <http://tinyurl.com/armana-symbolesmodulaires-pre>.
- [Atiyah et Macdonald 1969] M. F. Atiyah et I. G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley, Reading, MA, 1969. MR 39 #4129 Zbl 0175.03601

- [Böckle 2002] G. Böckle, “An Eichler–Shimura isomorphism over function fields between Drinfeld modular forms and cohomology classes of crystals”, prépublication, 2002, Disponible à <http://tinyurl.com/boeckleES2002>.
- [Bosch et al. 1990] S. Bosch, W. Lütkebohmert et M. Raynaud, *Néron models*, *Ergeb. Math. Grenzgeb.* (3) **21**, Springer, Berlin, 1990. MR 91i:14034 Zbl 0705.14001
- [Deligne 1973] P. Deligne, “Les constantes des équations fonctionnelles des fonctions L ”, pp. 501–597 dans *Modular functions of one variable* (Antwerp, 1972), vol. 2, édité par P. Deligne et W. Kuyk, *Lecture Notes in Math.* **349**, Springer, Berlin, 1973. MR 50 #2128 Zbl 0271.14011
- [Deligne et Rapoport 1973] P. Deligne et M. Rapoport, “Les schémas de modules de courbes elliptiques”, pp. 143–316 dans *Modular functions of one variable* (Antwerp, 1972), vol. 2, *Lecture Notes in Math.* **349**, Springer, Berlin, 1973. MR 49 #2762 Zbl 0281.14010
- [Denis 1995] L. Denis, “Problèmes diophantiens sur les t -modules” (*Les dix-huitièmes journées arithmétiques*, Bordeaux, 1993), *J. Théor. Nombres Bordeaux* **7**:1 (1995), 97–110. MR 98f:11061 Zbl 0842.11026
- [Drinfeld 1974] V. G. Drinfeld, “Elliptic modules”, *Mat. Sb. (N.S.)* **94(136)** (1974), 594–627. En russe; traduction anglaise : *Math. USSR-Sb* **23**:4 (1974), 561–592. MR 52 #5580
- [Drinfeld 1984] V. G. Drinfeld, “Two-dimensional l -adic representations of the Galois group of a global field of characteristic p and automorphic forms on $GL(2)$: Automorphic functions and number theory, II”, *Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov.* **134** (1984), 138–156. En russe; traduction anglaise : *J. Soviet Math.* **36**(1), 93–105 (1987). MR 86i:11066
- [Drinfeld 1988] V. G. Drinfeld, “Proof of the Petersson conjecture for $GL(2)$ over a global field of characteristic p ”, *Funktsional. Anal. i Prilozhen.* **22**:1 (1988), 34–54. En russe; traduction anglaise : *Funct. Anal. Appl.* **22** (1988), 28–43. MR 90c:11038
- [Gekeler 1980] E.-U. Gekeler, *Drinfeld-Moduln und modulare Formen über rationalen Funktionenkörpern*, *Bonner Math. Schriften* **119**, Universität Bonn Mathematisches Institut, Bonn, 1980. MR 83a:10042 Zbl 0446.14018
- [Gekeler 1986] E.-U. Gekeler, “Über Drinfeldsche Modulcurven vom Hecke-Typ”, *Compositio Math.* **57**:2 (1986), 219–236. MR 87d:11041 Zbl 0599.14032
- [Gekeler 1988] E.-U. Gekeler, “On the coefficients of Drinfeld modular forms”, *Invent. Math.* **93**:3 (1988), 667–700. MR 89g:11043 Zbl 0653.14012
- [Gekeler 1995a] E.-U. Gekeler, “Analytical construction of Weil curves over function fields”, pp. 27–49 dans *Les dix-huitièmes journées arithmétiques* (Bordeaux, 1993), *J. Théor. Nombres Bordeaux* **7**, 1995. MR 97g:11060 Zbl 0846.11037
- [Gekeler 1995b] E.-U. Gekeler, “Improper Eisenstein series on Bruhat–Tits trees”, *Manuscripta Math.* **86**:3 (1995), 367–391. MR 95m:11043 Zbl 0884.11025
- [Gekeler 1997a] E.-U. Gekeler, “Jacquet–Langlands theory over K and relations with elliptic curves”, pp. 224–257 dans *Drinfeld modules, modular schemes and applications* (Alden–Biesen, 1996), édité par E.-U. Gekeler et al., World Sci. Publ., River Edge, NJ, 1997. MR 99e:11078 Zbl 0929.11051
- [Gekeler 1997b] E.-U. Gekeler, “On the cuspidal divisor class group of a Drinfeld modular curve”, *Doc. Math.* **2** (1997), 351–374. MR 98m:11057 Zbl 0895.11024
- [Gekeler et Nonnengardt 1995] E.-U. Gekeler et U. Nonnengardt, “Fundamental domains of some arithmetic groups over function fields”, *Internat. J. Math.* **6**:5 (1995), 689–708. MR 96i:11043 Zbl 0858.11025

- [Gekeler et Reversat 1996] E.-U. Gekeler et M. Reversat, “Jacobians of Drinfeld modular curves”, *J. Reine Angew. Math.* **476** (1996), 27–93. MR 97f:11043 Zbl 0848.11029
- [Goss 1980a] D. Goss, “Modular forms for $\mathbf{F}_r[T]$ ”, *J. Reine Angew. Math.* **317** (1980), 16–39. MR 82m:10049 Zbl 0422.10021
- [Goss 1980b] D. Goss, “ π -adic Eisenstein series for function fields”, *Compositio Math.* **41**:1 (1980), 3–38. MR 82e:10053 Zbl 0422.10020
- [Hartshorne 1977] R. Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics **52**, Springer, New York, 1977. MR 57 #3116 Zbl 0367.14001
- [van der Heiden 2006] G.-J. van der Heiden, “Drinfeld modular curve and Weil pairing”, *J. Algebra* **299**:1 (2006), 374–418. MR 2007b:11086 Zbl 1177.11049
- [Iwaniec et Sarnak 2000] H. Iwaniec et P. Sarnak, “The non-vanishing of central values of automorphic L -functions and Landau–Siegel zeros”, *Israel J. Math.* **120**:part A (2000), 155–177. MR 2002b:11115 Zbl 0992.11037
- [Kamienny 1992a] S. Kamienny, “Torsion points on elliptic curves and q -coefficients of modular forms”, *Invent. Math.* **109**:2 (1992), 221–229. MR 93h:11054 Zbl 0773.14016
- [Kamienny 1992b] S. Kamienny, “Torsion points on elliptic curves over fields of higher degree”, *Internat. Math. Res. Notices* **1992**:6 (1992), 129–133. MR 93e:11072 Zbl 0807.14022
- [Kamienny et Mazur 1995] S. Kamienny et B. Mazur, “Rational torsion of prime order in elliptic curves over number fields”, pp. 81–100 dans *Columbia University Number Theory Seminar* (New York, 1992), Astérisque **228**, Société Mathématique de France, Paris, 1995. MR 96c:11058 Zbl 0846.14012
- [Kato et Trihan 2003] K. Kato et F. Trihan, “On the conjectures of Birch and Swinnerton–Dyer in characteristic $p > 0$ ”, *Invent. Math.* **153**:3 (2003), 537–592. MR 2004h:11058 Zbl 1046.11047
- [Katz 1973] N. M. Katz, “ p -adic properties of modular schemes and modular forms”, pp. 69–190 dans *Modular functions of one variable, III* (Antwerp, 1972), édité par W. Kuyk et J.-P. Serre, Lecture Notes in Mathematics **350**, Springer, Berlin, 1973. MR 56 #5434 Zbl 0271.10033
- [Kowalski et Michel 1999] E. Kowalski et P. Michel, “The analytic rank of $J_0(q)$ and zeros of automorphic L -functions”, *Duke Math. J.* **100**:3 (1999), 503–542. MR 2001b:11060 Zbl 1161.11359
- [Liu 2002] Q. Liu, *Algebraic geometry and arithmetic curves*, Oxford Graduate Texts in Mathematics **6**, Oxford University Press, 2002. MR 2003g:14001 Zbl 0996.14005
- [Manin 1969] Y. Manin, “The p -torsion of elliptic curves is uniformly bounded”, *Izv. Akad. Nauk SSSR Ser. Mat.* **33** (1969), 459–465. En russe; traduction anglaise : *Math. USSR-Izv.* **3**:3 (1969), 433–438. MR 42 #7667
- [Mazur 1977] B. Mazur, “Modular curves and the Eisenstein ideal”, *Inst. Hautes Études Sci. Publ. Math.* **47** (1977), 33–186. MR 80c:14015 Zbl 0394.14008
- [Mazur 1978] B. Mazur, “Rational isogenies of prime degree”, *Invent. Math.* **44**:2 (1978), 129–162. MR 80h:14022 Zbl 0386.14009
- [Merel 1996] L. Merel, “Bornes pour la torsion des courbes elliptiques sur les corps de nombres”, *Invent. Math.* **124**:1-3 (1996), 437–449. MR 96i:11057 Zbl 0936.11037
- [Milne 1986] J. S. Milne, “Jacobian varieties”, pp. 167–212 dans *Arithmetic geometry* (Storrs, CT, 1984), édité par G. Cornell et J. H. Silverman, Springer, New York, 1986. MR 861976 Zbl 0604.14018

- [Ogg 1978] A. P. Ogg, “On the Weierstrass points of $X_0(N)$ ”, *Illinois J. Math.* **22**:1 (1978), 31–35. MR 57 #3136 Zbl 0374.14005
- [Pál 2005] A. Pál, “On the torsion of the Mordell–Weil group of the Jacobian of Drinfeld modular curves”, *Doc. Math.* **10** (2005), 131–198. MR 2006c:11070 Zbl 1119.11031
- [Pál 2010] A. Pál, “On the torsion of Drinfeld modules of rank two”, *J. Reine Angew. Math.* **640** (2010), 1–45. MR 2011i:11087 Zbl 05697008
- [Parent 1999] P. Parent, “Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres”, *J. Reine Angew. Math.* **506** (1999), 85–116. MR 99k:11080 Zbl 0919.11040
- [Poonen 1997] B. Poonen, “Torsion in rank 1 Drinfeld modules and the uniform boundedness conjecture”, *Math. Ann.* **308**:4 (1997), 571–586. MR 98h:11073 Zbl 0891.11034
- [Rosen 2003] M. Rosen, “Formal Drinfeld modules”, *J. Number Theory* **103**:2 (2003), 234–256. MR 2004j:11056 Zbl 1049.11060
- [Schneider 1982] P. Schneider, “Zur Vermutung von Birch und Swinnerton–Dyer über globalen Funktionenkörpern”, *Math. Ann.* **260**:4 (1982), 495–510. MR 84i:14027 Zbl 0509.14022
- [Schweizer 1997] A. Schweizer, “Hyperelliptic Drinfeld modular curves”, pp. 330–343 dans *Drinfeld modules, modular schemes and applications* (Alden–Biesen, 1996), édité par E.-U. Gekeler et al., World Sci. Publ., River Edge, NJ, 1997. MR 99h:11061 Zbl 0930.11039
- [Schweizer 2003] A. Schweizer, “On the uniform boundedness conjecture for Drinfeld modules”, *Math. Z.* **244**:3 (2003), 601–614. MR 2004e:11062 Zbl 1037.11041
- [Schweizer 2011] A. Schweizer, “Strong Weil curves over $\mathbb{F}_q(T)$ with small conductor”, *J. Number Theory* **131**:2 (2011), 285–299. MR 2012f:11110 Zbl 1218.11059
- [Tamagawa 1995] A. Tamagawa, “The Eisenstein quotient of the Jacobian variety of a Drinfeld modular curve”, *Publ. Res. Inst. Math. Sci.* **31**:2 (1995), 203–246. MR 96b:11077 Zbl 1045.11510
- [Tan 1993] K.-S. Tan, “Modular elements over function fields”, *J. Number Theory* **45**:3 (1993), 295–311. MR 95d:11158 Zbl 0802.11026
- [Teitelbaum 1992] J. T. Teitelbaum, “Modular symbols for $\mathbf{F}_q(T)$ ”, *Duke Math. J.* **68**:2 (1992), 271–295. MR 93h:11055 Zbl 0777.11021
- [Ulmer 2002] D. Ulmer, “Elliptic curves with large rank over function fields”, *Ann. of Math.* (2) **155**:1 (2002), 295–315. MR 2003b:11059 Zbl 1109.11314
- [VanderKam 2000] J. VanderKam, “Linear independence of Hecke operators in the homology of $X_0(N)$ ”, *J. London Math. Soc.* (2) **61**:2 (2000), 349–358. MR 2001e:11045 Zbl 0963.11023
- [Weil 1971] A. Weil, *Dirichlet series and automorphic forms: Lezioni fermiane*, Lecture Notes in Mathematics **189**, Berlin, 1971. Zbl 0218.10046

Communicated by Bjorn Poonen

Received 2011-07-14

Revised 2011-11-08

Accepted 2011-12-10

armana@math.jussieu.fr

Max-Planck Institut für Mathematik, Vivatsgasse 7,
D-53111 Bonn, Germany

Algebra & Number Theory

msp.berkeley.edu/ant

EDITORS

MANAGING EDITOR

Bjorn Poonen
Massachusetts Institute of Technology
Cambridge, USA

EDITORIAL BOARD CHAIR

David Eisenbud
University of California
Berkeley, USA

BOARD OF EDITORS

Georgia Benkart	University of Wisconsin, Madison, USA	Susan Montgomery	University of Southern California, USA
Dave Benson	University of Aberdeen, Scotland	Shigefumi Mori	RIMS, Kyoto University, Japan
Richard E. Borcherds	University of California, Berkeley, USA	Raman Parimala	Emory University, USA
John H. Coates	University of Cambridge, UK	Jonathan Pila	University of Oxford, UK
J-L. Colliot-Thélène	CNRS, Université Paris-Sud, France	Victor Reiner	University of Minnesota, USA
Brian D. Conrad	University of Michigan, USA	Karl Rubin	University of California, Irvine, USA
Hélène Esnault	Universität Duisburg-Essen, Germany	Peter Sarnak	Princeton University, USA
Hubert Flenner	Ruhr-Universität, Germany	Joseph H. Silverman	Brown University, USA
Edward Frenkel	University of California, Berkeley, USA	Michael Singer	North Carolina State University, USA
Andrew Granville	Université de Montréal, Canada	Vasudevan Srinivas	Tata Inst. of Fund. Research, India
Joseph Gubeladze	San Francisco State University, USA	J. Toby Stafford	University of Michigan, USA
Ehud Hrushovski	Hebrew University, Israel	Bernd Sturmfels	University of California, Berkeley, USA
Craig Huneke	University of Virginia, USA	Richard Taylor	Harvard University, USA
Mikhail Kapranov	Yale University, USA	Ravi Vakil	Stanford University, USA
Yujiro Kawamata	University of Tokyo, Japan	Michel van den Bergh	Hasselt University, Belgium
János Kollár	Princeton University, USA	Marie-France Vignéras	Université Paris VII, France
Yuri Manin	Northwestern University, USA	Kei-Ichi Watanabe	Nihon University, Japan
Barry Mazur	Harvard University, USA	Andrei Zelevinsky	Northeastern University, USA
Philippe Michel	École Polytechnique Fédérale de Lausanne	Efim Zelmanov	University of California, San Diego, USA

PRODUCTION

contact@msp.org

Silvio Levy, Scientific Editor

See inside back cover or www.jant.org for submission instructions.

The subscription price for 2012 is US \$175/year for the electronic version, and \$275/year (+\$40 shipping outside the US) for print and electronic. Subscriptions, requests for back issues from the last three years and changes of subscribers address should be sent to Mathematical Sciences Publishers, Department of Mathematics, University of California, Berkeley, CA 94720-3840, USA.

Algebra & Number Theory (ISSN 1937-0652) at Mathematical Sciences Publishers, Department of Mathematics, University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

ANT peer review and production are managed by EditFLOW[®] from Mathematical Sciences Publishers.

PUBLISHED BY

 **mathematical sciences publishers**

<http://msp.org/>

A NON-PROFIT CORPORATION

Typeset in L^AT_EX

Copyright ©2012 by Mathematical Sciences Publishers

Algebra & Number Theory

Volume 6 No. 6 2012

The smallest prime that does not split completely in a number field XIANNAN LI	1061
On the geometric realization of the inner product and canonical basis for quantum affine \mathfrak{sl}_n KEVIN MCGERTY	1097
Combinatorics of the tropical Torelli map MELODY CHAN	1133
On fusion categories with few irreducible degrees SONIA NATALE and JULIA YAEL PLAVNIK	1171
Cusp form motives and admissible G -covers DAN PETERSEN	1199
Ideals of degree one contribute most of the height AARON LEVIN and DAVID MCKINNON	1223
Torsion des modules de Drinfeld de rang 2 et formes modulaires de Drinfeld CÉCILE ARMANA	1239



1937-0652(2012)6:6;1-9