HAL open science

Torsion rationnelle des modules de Drinfeld

Cécile Armana

▶ To cite this version:

Cécile Armana. Torsion rationnelle des modules de Drinfeld. Mathématiques [math]. Université Paris-Diderot - Paris VII, 2008. Français. NNT : . tel-00338117v2

HAL Id: tel-00338117

https://theses.hal.science/tel-00338117v2

Submitted on 28 Dec 2008

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Université Paris Diderot – Paris 7
École Doctorale de Sciences Mathématiques de Paris Centre

Thèse de doctorat
Discipline : Mathématiques

présentée par

Cécile Armana

Torsion rationnelle des modules de Drinfeld

Thèse dirigée par Loïc Merel

Soutenue le 5 novembre 2008 devant le jury composé de :

M. Sinnou David	(Université Pierre et Marie Curie – Paris 6)
M. Ernst-Ulrich Gekeler	(Universität des Saarlandes)
M. Laurent Lafforgue	(Institut des Hautes Études Scientifiques)
M. Loïc Merel	(Université Paris Diderot – Paris 7)
M. Jean-François Mestre	(Université Paris Diderot – Paris 7)
M. Marc Reversat	(Université Paul Sabatier – Toulouse 3)

Rapporteurs :

M. Bjorn Poonen	(Massachusetts Institute of Technology)
M. Marc Reversat	(Université Paul Sabatier – Toulouse 3)

Remerciements

Si la thèse s'apparente à une route longue et sinueuse, ce n'est pas sans un vertige certain que je me retourne aujourd'hui sur le chemin accompli, ses raccourcis et ses embûches. Voyageurs de passage ou compagnons de route, nombreux sont ceux à avoir partagé avec moi ce trajet.

Je remercie Loïc Merel d'avoir accepté d'être mon guide sur cette route. Il s'est acquitté de cette responsabilité avec une énergie, un optimisme à toute épreuve et une grande disponibilité en toutes circonstances. Je le remercie profondément de m'avoir fait partager sa passion des mathématiques et accordé sa confiance. Sa grande exigence, sa patience et son soutien ont été des éléments moteurs de mon travail. Comme ces mots ne sont probablement pas assez forts pour qualifier ce que je lui dois, je lui dis encore une fois simplement merci.

Je suis très honorée que Bjorn Poonen et Marc Reversat aient accepté de rapporter cette thèse. J'ai été touchée de l'intérêt qu'a porté Bjorn Poonen à mon travail, dès notre rencontre en 2004, et par ses encouragements répétés. Je remercie Marc Reversat de la diligence avec laquelle il a rapporté mon travail, de ses remarques et suggestions. C'est avec grand plaisir que j'ai appris qu'il se déplacerait pour faire partie de mon jury.

Je remercie très chaleureusement Sinnou David, Ernst-Ulrich Gekeler, Laurent Lafforgue et Jean-François Mestre de faire partie de mon jury et de l'intérêt qu'ils portent à ce travail. Tout au long de ces années, je n'ai cessé de lire et relire les travaux de Ernst-Ulrich Gekeler et j'ai bénéficié de ses encouragements : sa présence à ma soutenance me fait particulièrement plaisir.

David Goss, Joseph Oesterlé et Jeremy Teitelbaum ont pris le temps de répondre à mes questions : je les remercie pour leur aide. L'enthousiasme de David Goss et ses encouragements m'ont été précieux.

En 2005, j'ai eu la chance d'effectuer un mémorable séjour au National Center for Theoretical Sciences de Taïwan. Je suis très reconnaissante à Jing Yu de m'avoir accueillie dans d'excellentes conditions et avec une extrême gentillesse. Merci à Chieh-Yu Chang et Yih-Jeng Yu d'avoir facilité mon intégration linguistique durant ce séjour.

Je remercie Yacine Ait-Amrane, Chieh-Yu Chang et Benoît Jacob pour nos discussions mathématiques autour des modules de Drinfeld et leurs sages conseils.

François Brunault et Marusia Rebolledo m'ont fait partager leurs connaissances mathématiques et leur expérience bien au-delà des mathématiques. Je leur en suis très reconnaissante, ainsi que des conseils bienveillants et des encouragements qu'ils m'ont prodigués.

En parallèle avec le monde de la recherche, j'ai pris beaucoup de plaisir à enseigner

dans les UFR de mathématiques des universités Paris 7 et Paris 6. Merci notamment à Thomas Duquesne, Annie Hersant, Marc Hindry, François Liret et Stéphane Vassout.

L'Institut de Mathématiques de Jussieu m'a fourni d'excellentes conditions de travail pendant ces années de thèse. Cela est dû à un grand nombre de personnes, que je ne puis toutes remercier ici, et je les prie de m'en excuser. Je remercie très chaleureusement Gilles Godefroy pour ses encouragements et son soutien. J'ai beaucoup appris de Joël Marchand, de son recul et de la sagesse inestimable de ses points de vue. Rosita Monchanin, Marcelline Prosper-Cojande et Michèle Wasse m'ont fait bénéficier de leur expertise administrative et de leur disponibilité en toutes circonstances, et je leur en suis très reconnaissante. Merci à Pierre Charollois, Elisha Falbel, Vincent Maillot, ainsi qu'à Mladen Dimitrov pour son soutien et l'intérêt qu'il a porté à mon travail.

J'ai cotoyé un grand nombre de thésards, anciens et actuels, sur le plateau 7C : que tous soient remerciés pour la bonne ambiance qui y règne. Merci notamment, par ordre chronologico-alphabétique, à Christophe, Gwendal, Kenji, Samy K., Julien M., Nicolas R., Daniel, Hakim, Pierre W., Sébastien, Vincent, Benoît H., Ismaël, Juliette, Maria, Nabil, Nicolas B., Banafsheh, Clémence, Luc, Mirjam,... à ceux que j'ai omis de citer (et qui, je l'espère, me le pardonneront) ainsi qu'aux membres du Bureau Des Doctorants.

Les occupants du bureau 7C4 ont su créer des conditions propices au travail, agrémentées de pauses-thé, de carrés de chocolat et de bonne humeur. Merci aux anciens : Aïni, Aurélien, Charlotte, François, Joël, Lionel, Marco, Miguel, Mostafa et à nos nouveaux arrivants : Benjamin W., Bora, Wen, pour ces bons moments. À Benjamin C., Fabien, Jérôme, Julien C., Julien G., Manuel, Olivier, je dois des relectures de ma thèse, des soirées-jeux, de l'esprit *geek*, de l'assistance LaTeX, de l'improvisation, des discussions mathématiques, de la complicité, des encouragements dans les moments difficiles (en vrac, chacun ayant contribué à plusieurs de ces activités) et beaucoup, beaucoup plus encore !

Fabien « de Toulon » est passé maître dans l'art d'allier belles mathématiques, bonne chère, bonne humeur et passion des poulpes. Il est mon sage tout en haut de la montagne.

Mes parents m'ont encouragée depuis longtemps à suivre ma voie et m'ont donné les conditions affectives et matérielles indispensables au bon déroulement de mes études. Dès que je me suis engagée sur cette route longue et sinueuse, leur soutien discret, efficace et infaillible a été essentiel. C'est avec beaucoup d'émotion que je les remercie. Merci aussi à mes proches, à ceux qui sont venus de loin pour ma soutenance. Malgré l'éloignement, Nicolas et Sophie ont toujours été présents à mes côtés et leurs encouragements m'ont portée bien plus loin qu'ils ne l'imaginent.

Enfin, je remercie Nicolas de ce qui ne saurait franchir la barrière des mots.

Table des matières

Introduction **3**

Cadre général et notations **9**

1 Modules de Drinfeld **11**
1.1 Modules de Drinfeld (rappels) 11
1.2 Torsion des modules de Drinfeld (rappels) 16
1.3 Arguments locaux pour l'étude de la torsion 19
1.4 Courbes modulaires de Drinfeld (rappels) 21

2 Symboles modulaires de Teitelbaum **25**
2.1 Formes automorphes et arbre de Bruhat-Tits (rappels) 25
2.2 La présentation de Manin-Teitelbaum (rappels) 37
2.3 L'action de Hecke sur les symboles de Manin-Teitelbaum 42
2.4 Un critère d'indépendance linéaire dans les symboles de Manin-Teitelbaum 47
2.5 Une base explicite de symboles de Manin-Teitelbaum 48
2.6 L'élément d'enroulement $\mathbf{e}$ 52
2.7 Indépendance linéaire dans le module de Hecke engendré par $\mathbf{e}$ 55
2.8 L'analogue de l'homomorphisme d'enroulement de Mazur 58

3 Quotient d'enroulement de $J_0(\mathfrak{n})$ **63**
3.1 Variétés abéliennes sur les corps de fonctions (rappels) 63
3.2 La jacobienne $J_0(\mathfrak{n})$ de $X_0(\mathfrak{n})_K$ (rappels) 64
3.3 Le quotient d'enroulement $J_{\mathbf{e}}(\mathfrak{n})$ 69
3.4 Une minoration de la dimension de $J_{\mathbf{e}}(\mathfrak{n})$ 72
3.5 Étude du quotient d'enroulement lorsque $\deg \mathfrak{n}$ est petit 73
3.6 Une version raffinée de $J_{\mathbf{e}}(\mathfrak{n})$ 76

4 Formes modulaires pour $\mathbf{F}_q[T]$ **81**
4.1 Le module de Tate-Drinfeld (rappels) 81
4.2 Théorie algébrique des formes modulaires pour $\mathbf{F}_q[T]$ 83
4.3 L'action de Hecke sur le t-développement des formes modulaires 88
4.4 Sur les points de Weierstrass de $X_0(\mathfrak{n})_K$ 101
4.5 Sur la structure de Hecke des formes modulaires 103

5 Application aux points rationnels de courbes modulaires de Drinfeld 107
5.1 Torsion p-primaire des quotients optimaux de $J_0(\mathfrak{n})$ 107
5.2 Immersions formelles (rappels) 109
5.3 L'argument de Mazur 109
5.4 Application au cas où $\mathfrak{n}$ est de degré 3 ou 4 111
5.5 Étude du cas général 117

Bibliographie 125

Index des notations 131

Introduction

L'arithmétique des corps de fonctions a connu une avancée remarquable dans les années soixante-dix avec l'introduction par Drinfeld des *modules elliptiques*, appelés désormais *modules de Drinfeld*. Par leur similarité avec les courbes elliptiques, ils reflètent l'analogie profonde entre corps de nombres et corps de fonctions.

Soient p un nombre premier et q une puissance de p. Posons $A = \mathbf{F}_q[T]$ et $K = \mathbf{F}_q(T)$. Soit L une extension finie de K. Soit V le sous-L-espace vectoriel de $L[X]$ engendré par $(X^{q^i})_{i\geq 0}$. La composition des polynômes fait de lui un anneau non commutatif. Un module de Drinfeld ϕ sur L de rang r est la donnée d'un polynôme

$$\phi_T(X) = TX + a_1X^q + \ldots + a_rX^{q^r} \in V$$

avec $a_r \in L^\times$. Si $N = \sum_{i=0}^m n_iT^i \in A$, on pose

$$\phi_N(X) = \sum_{i=0}^m n_i(\phi_T(X))^i \in V.$$

L'ensemble des racines du polynôme $\phi_N(X)$ dans une clôture algébrique de L est un $\mathbf{F}_q$-espace vectoriel isomorphe à $(A/(N))^r$. Un point L-rationnel *de torsion* de ϕ est une racine dans L d'un polynôme $\phi_N(X)$ pour $N \in A, N \neq 0$. L'*ordre* d'un point de torsion x est l'idéal non nul $I = \{a \in A \mid \phi_a(x) = 0\}$ de A, de *degré* $\log_q(\#A/I)$. Les points de torsion L-rationnels forment un sous-A-module fini de L, noté $({}^\phi L)_{\mathrm{tors}}$. Poonen a formulé la conjecture suivante.

Conjecture 1 ([Poo97])**.** *Soit r un entier ≥ 1. Pour tout entier $d \geq 1$, il existe une constante $C_{r,d} > 0$ telle que, pour toute extension L de K de degré au plus d et pour tout module de Drinfeld ϕ sur L de rang r, on ait $\#({}^\phi L)_{\mathrm{tors}} \leq C_{r,d}$.*

Lorsque $r = 1$, c'est un théorème de Poonen [Poo97]. Dans cette thèse, nous nous intéressons au cas $r = 2$, qui a été abordé par Poonen, Schweizer, Rosen [Ros03] et Pál. Rappelons quelques uns de leurs résultats. D'après Poonen et Schweizer [Poo97, Sch03], il suffit d'établir la conjecture *a priori* plus faible suivante.

Conjecture 2. *Soit d un entier ≥ 1. Il existe une constante $C_d > 0$ telle que, pour toute extension L de K de degré au plus d et pour tout module de Drinfeld sur L de rang 2 ayant un point L-rationnel d'ordre $\mathfrak{n}$ ($\mathfrak{n}$ idéal premier de A), on ait $\deg \mathfrak{n} \leq C_d$.*

En août 2007, Pál a diffusé un texte [Pál07b] contenant une démonstration de la conjecture 1 pour $r = 2$, $d = 1$ et $q = 2$. Enfin, David et Denis ont étudié des questions

similaires par des méthodes transcendantes analogues à celles que Masser et Wüstholz ont employées pour les variétés abéliennes [DD99].

Dans le langage des systèmes dynamiques algébriques, la conjecture 1 admet la reformulation suivante. Considérons un polynôme $f(X) = TX + a_1X^q + \ldots + a_rX^{q^r} \in L[X]$ avec $a_r \in L^\times$. L'itération de f définit un système dynamique sur $\mathbf{P}^1_L$. Un point $x \in \mathbf{P}^1_L$ est dit *prépériodique* pour f s'il existe un entier naturel n tel que $f^{\circ n}(x)$ est périodique pour f. La conjecture 1 affirme qu'il existe une borne sur le cardinal des points prépériodiques de ces polynômes, ne dépendant que de r et du degré de l'extension L/K [Poo98, Sch04].

L'approche pour les courbes elliptiques sur les corps de nombres

Lorsqu'on remplace K par $\mathbf{Q}$ et « module de Drinfeld de rang 2 » par « courbe elliptique », la conjecture 1 est un théorème de Merel.

Théorème 3 ([Mer96])**.** *Soit d un entier ≥ 1. Il existe une constante $C'_d > 0$ telle que pour toute courbe elliptique E sur un corps de nombres L de degré d sur $\mathbf{Q}$, tout point P d'ordre N de $E(L)$ vérifie $N < C'_d$.*

Le cas $d = 1$ a été établi par Mazur en 1977 [Maz77]. À cette époque, Mazur a suggéré que la théorie qu'il avait mise en place serait applicable dans le cadre des corps de fonctions, suite à l'introduction alors récente des modules de Drinfeld (*loc. cit.* p. 39). Un tel projet été entrepris par Tamagawa [Tam95] et Pál [Pál05, Pál07a, Pál07b].

Résumons succintement le principe de la démonstration du théorème 3, qui repose sur les contributions de Mazur, Kolyvagin, Logachëv, Kamienny et Merel [Maz77, Maz78, KL89, KM95, Kam92b, Mer96].

(i) On se ramène à démontrer le théorème lorsque N est premier.

(ii) L'existence de P est équivalente à l'existence d'un point de la courbe modulaire $Y_1(N)$ défini sur une extension de $\mathbf{Q}$ de degré d.

(iii) Pour montrer le théorème, il suffit de vérifier que si la puissance symétrique d-ème $X_0(N)^{(d)}$ de la courbe modulaire $X_0(N)$ a un point $\mathbf{Q}$-rationnel qui rencontre la puissance symétrique d-ème $\infty^{(d)}$ de la pointe ∞ dans la fibre en l de $X_0(N)^{(d)}$, pour un nombre premier $l \nmid 2N$, on a $N < C'_d$.

(iv) Pour cela, on considère le morphisme

$$\begin{array}{ccc} X_0(N)^{(d)} & \longrightarrow & J_0(N) \\ (P_1, \ldots, P_d) & \longmapsto & (P_1) + \ldots + (P_d) - d(\infty) \end{array}$$

et une variété abélienne quotient B de la jacobienne $J_0(N)$ de $X_0(N)$. On cherche pour B une variété abélienne n'ayant qu'un nombre fini de points $\mathbf{Q}$-rationnels et telle que l'extension à $\mathrm{Spec}(\mathbf{Z})$ du morphisme composé

$$X_0(N)^{(d)} \longrightarrow J_0(N) \longrightarrow B$$

soit une immersion formelle en $\infty^{(d)}$ dans la fibre en l.

(v) Pour que $B(\mathbf{Q})$ soit fini, il suffit de choisir B telle que $L(B,1) \neq 0$, d'après les résultats connus sur la conjecture de Birch et Swinnerton-Dyer.

(vi) On peut définir le plus grand quotient B de $J_0(N)$ tel que $L(B,1) \neq 0$ ainsi : l'algèbre de Hecke $\mathscr{T} \subset \mathrm{End}(J_0(N))$ opère sur les symboles modulaires. Considérons l'idéal $\mathscr{I}_{\mathbf{e}}$ de $\mathscr{T}$ défini comme l'annulateur d'un symbole modulaire particulier, appelé élément d'enroulement et noté $\mathbf{e}$. Posons $J_{\mathbf{e}} = B = J_0(N)/\mathscr{I}_{\mathbf{e}} J_0(N)$.

(vii) Appliquée à $J_{\mathbf{e}}$, la condition d'immersion formelle équivaut à la $\mathbf{F}_l$-indépendance linéaire de d opérateurs de Hecke dans $\mathscr{T}/(\mathscr{I}_{\mathbf{e}} + l\mathscr{T})$.

(viii) Cette dernière condition revient à établir l'indépendance linéaire de d symboles modulaires donnés explicitement, ce qui s'obtient grâce à la théorie des symboles modulaires.

Les analogues de tous les objets mentionnés dans cette esquisse existent lorsqu'on remplace $\mathbf{Q}$ par K et « courbe elliptique » par « module de Drinfeld de rang 2 » [Dri74, Tei92a]. Notre projet consiste à étudier dans quelle mesure cette approche est pertinente.

Sa mise en œuvre pour les modules de Drinfeld de rang 2

L'étape (i) correspond à l'équivalence entre les conjectures 1 et 2. L'étape (ii) est un résultat élémentaire concernant la courbe modulaire de Drinfeld $Y_1(\mathfrak{n})$. L'étape (iii) est traitée dans le chapitre 1 et l'étape (iv) dans le chapitre 5. L'étape (v), qui utilise une partie de la conjecture de Birch et Swinnerton-Dyer, est moins profonde dans le cas des corps de fonctions et démontrée dans [Sch82]. Les étapes (vi) et (viii) sont traitées dans les chapitres 2 et 3.

Nous rencontrons une obstruction dans l'étape (vii), que nous proposons maintenant de décrire. Fixons des notations. *Jusqu'à la fin de l'introduction,* $\mathfrak{n}$ *désigne un idéal maximal de* A. Soient d un entier ≥ 1 et $\mathfrak{l}$ un idéal maximal distinct de $\mathfrak{n}$. Le corps $A/\mathfrak{l}$ est noté $\mathbf{F}_{\mathfrak{l}}$. Soit ∞ la place de K donnée par $\pi = \frac{1}{T}$. Soient K_∞ le complété de K par rapport à ∞, O_∞ son anneau des entiers et $\mathbf{C}_\infty$ le complété d'une clôture algébrique de K_∞. Soit $\mathcal{I}$ le sous-groupe de $\mathrm{GL}(2, O_\infty)$ formé des matrices $\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \mathrm{GL}(2, O_\infty)$ vérifiant $\gamma \equiv 0 \mod \pi$. Soient $\mathbf{A}$ l'anneau des adèles de K et $\mathbf{O}_f$ la partie finie de l'anneau des entiers de $\mathbf{A}$. Soit $\mathcal{K}_0(\mathfrak{n})_f$ le sous-groupe de $\mathrm{GL}(2, \mathbf{O}_f)$ formé des matrices $\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$ vérifiant $\gamma \in \mathfrak{n}$. Soit $\Gamma_0(\mathfrak{n})$ le sous-groupe de $\mathrm{GL}(2, A)$ formé des matrices $\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$ vérifiant $\gamma \in \mathfrak{n}$.

Contrairement à la situation classique, il existe deux théories quasi-dissociées de formes modulaires :

— le $\mathbf{C}$-espace vectoriel $\mathbf{H}(\mathbf{C})$ des formes automorphes paraboliques

$$\mathrm{GL}(2, K)\backslash \mathrm{GL}(2, \mathbf{A})/\mathcal{K}_0(\mathfrak{n})_f \times \mathrm{Z}(K_\infty)\mathcal{I} \longrightarrow \mathbf{C}$$

spéciales en ∞ [Dri74] ;

— le $A[1/\mathfrak{n}]$-module $\mathbf{S}$ des différentielles relatives globales de degré 1 de la courbe modulaire de Drinfeld $X_0(\mathfrak{n})$ sur $\mathrm{Spec}(A[1/\mathfrak{n}])$. Après extension des scalaires à $\mathbf{C}_\infty$, il coïncide avec l'espace des formes modulaires analytiques pour $\mathbf{F}_q[T]$ de poids 2, type 1 et doublement paraboliques pour $\Gamma_0(\mathfrak{n})$ [Gos80c, Gek88b].

Posons $\mathbf{S}(\mathbf{F}_\mathfrak{l}) = \mathbf{S} \otimes_{A[1/\mathfrak{n}]} \mathbf{F}_\mathfrak{l}$. Les formes modulaires $f \in \mathbf{S}(\mathbf{F}_\mathfrak{l})$ possèdent un t-développement dans $\mathbf{F}_\mathfrak{l}[[t]]$ de la forme $\sum_{i\geq 1} b_i(f)t^{1+i(q-1)}$. Le sous-anneau $\mathbf{T}$ de $\mathrm{End}(\mathbf{H}(\mathbf{C}))$ engendré par les opérateurs de Hecke agit sur $\mathbf{S}$. Contrairement à la situation classique, l'action de $\mathbf{T}$ sur $\mathbf{S}$ et $\mathbf{S}(\mathbf{F}_\mathfrak{l})$ est pour l'instant mal connue. Cela nous mène à considérer l'hypothèse suivante (cette question a déjà été évoquée par Goss, Gekeler et Pál [Gos80a, Gek88b, Pál07b]).

(H1) Il existe un idéal premier $\mathfrak{l}$ de degré 1 de A tel que l'homomorphisme de $\mathbf{F}_\mathfrak{l}$-espaces vectoriels

$$\begin{array}{rcl} \mathbf{T} \otimes_{\mathbf{Z}} \mathbf{F}_\mathfrak{l} & \longrightarrow & \mathrm{Hom}(\mathbf{S}(\mathbf{F}_\mathfrak{l}), \mathbf{F}_\mathfrak{l}) \\ s & \longmapsto & (f \mapsto b_1(sf)) \end{array}$$

est un isomorphisme.

Cet énoncé est à rapprocher d'une hypothèse de multiplicité un dans $\mathbf{S}(\mathbf{F}_\mathfrak{l})$ (prop. 4.48). L'hypothèse (H1) est vérifiée lorsque $\mathfrak{n}$ est de degré ≤ 3 (th. 4.51). De façon générale, nous manquons de méthodes numériques sur les formes modulaires pour $\mathbf{F}_q[T]$ permettant de vérifier cette hypothèse sur des exemples.

Soit $I_\mathbf{e}$ l'idéal de $\mathbf{T}$ maximal pour la propriété suivante : la variété abélienne $J_0(\mathfrak{n})/I_\mathbf{e}J_0(\mathfrak{n})$ sur K est de rang analytique nul (section 3.3). Pour éviter des problèmes liés au passage de suites exactes de variétés abéliennes aux espaces cotangents de leurs modèles de Néron, il est utile de considérer une variante du quotient d'enroulement de $J_0(\mathfrak{n})$ (sections 3.6 et 5.5.2). Pour cela, nous sommes conduits à l'hypothèse technique suivante, qu'on pourra comparer au corollaire 1.1 de [Maz78].

(H2) Il existe un idéal saturé I de $\mathbf{T}$ tel que $I_\mathbf{e} \subset I \subset I_\mathbf{e} + p\mathbf{T}$. Soit $\mathcal{J}_0(\mathfrak{n})$ (resp. $\mathcal{J}_I$) le modèle de Néron de la variété abélienne $J_0(\mathfrak{n})$ (resp. $J_0(\mathfrak{n})/IJ_0(\mathfrak{n})$) sur A. Le sous-espace de $\mathrm{Cot}_0\,\mathcal{J}_0(\mathfrak{n})$ annulé par I est contenu dans l'image de l'application canonique $\mathrm{Cot}_0\,\mathcal{J}_I \to \mathrm{Cot}_0\,\mathcal{J}_0(\mathfrak{n})$.

Nous donnons quelques cas simples où elle est vérifiée ($\mathfrak{n}$ est de degré ≤ 3, ou de degré 4 avec $p \neq 2$; prop. 3.29, section 5.5.2) ainsi qu'un critère (prop. 3.35). Cette hypothèse est vraisemblablement de nature moins profonde que (H1).

Le schéma de preuve présenté auparavant abouti alors à l'énoncé qui suit.

Théorème 4 (th. 5.30)**.** *Supposons les hypothèses (H1) et (H2) vérifiées. Alors :*

(i) la courbe $Y_1(\mathfrak{n})$ n'a pas de point défini sur une extension de K de degré $\leq q$, lorsque $\deg \mathfrak{n} \geq \max(q+1, 5)$; en particulier, la conjecture 2 est vraie pour $d \leq q$;

(ii) la courbe $Y_1(\mathfrak{n})$ n'a pas de point K-rationnel lorsque $\deg \mathfrak{n} \geq 3$.

La raison pour laquelle nous restreignons notre étude aux points de degré $\leq q$ est expliquée dans la section 4.3.

La torsion de degré 3 et 4 des modules de Drinfeld

Lorsque $\mathfrak{n}$ est de degré 1 ou 2, il existe une infinité de modules de Drinfeld possédant un point rationnel de torsion d'ordre $\mathfrak{n}$ (car la courbe modulaire $X_1(\mathfrak{n})$ est alors de genre nul).

Étudions en détail la situation lorsque $\mathfrak{n}$ est de degré 3 ou 4. Nous montrons que les hypothèses (H1) et (H2) sont satisfaites si $\deg \mathfrak{n} = 3$ (th. 4.51 et prop. 3.29). Nous obtenons même un résultat plus précis que la conclusion du théorème 4.

Théorème 5 (th. 5.11 et 5.15). *(i) Si $\mathfrak{n}$ est de degré 3, la courbe $Y_1(\mathfrak{n})$ n'a pas de point défini sur une extension de K de degré ≤ 2.*

(ii) Si $\mathfrak{n}$ est de degré 4 et L est une extension de K de degré $\leq d$, où

$$d = \begin{cases} 1 & si\ q = 2, 3 \\ 2 & si\ q = 4, 5 \\ 3 & si\ q \geq 7, \end{cases}$$

la courbe $Y_1(\mathfrak{n})$ n'a pas de point L-rationnel.

Cela confirme partiellement la conjecture suivante de Schweizer, qui précise la conjecture 1 lorsque $d = 1$ et $r = 2$.

Conjecture 6 ([Sch03]). *Soit ϕ un module de Drinfeld de rang 2 sur K. Alors on a un isomorphisme de A-modules*

$$({}^{\phi}K)_{\text{tors}} \simeq A/\mathfrak{m}_1 \oplus A/\mathfrak{m}_2$$

avec $\mathfrak{m}_1, \mathfrak{m}_2$ idéaux de A, $\mathfrak{m}_2 \subset \mathfrak{m}_1$ et $\deg \mathfrak{m}_1 + \deg \mathfrak{m}_2 \leq 2$.

Signalons que la démonstration du théorème 5 repose sur des variantes de notre schéma de preuve général, ne faisant intervenir ni symboles modulaires ni propriété d'immersion formelle. La situation est simplifiée lorsque $\mathfrak{n}$ est de degré 3 du fait du résultat suivant.

Proposition 7 (th. 3.19, cor. 3.23). *Si $\mathfrak{n}$ est de degré 3, la jacobienne $J_0(\mathfrak{n})$ est de rang nul sur K. Sa fonction L est constante égale à 1 et son groupe de Tate-Shafarevich est trivial.*

Le deuxième énoncé du théorème 5 est démontré plus généralement pour les idéaux $\mathfrak{n}$ tels que toute forme propre de $\mathbf{H}(\mathbf{C})$ est de rang au plus 1 (th. 5.15). Nous n'avons pas eu l'occasion de vérifier s'il s'applique à des courbes $Y_1(\mathfrak{n})$ pour $\deg \mathfrak{n} \geq 5$.

Enfin, des méthodes similaires permettent d'obtenir des informations partielles sur les points K-rationnels de la courbe $Y_0(\mathfrak{n})$.

Proposition 8 (prop. 5.12, 5.17 et th. 5.18). *(i) Si $\mathfrak{n}$ est de degré 3 ou 4, tout module de Drinfeld sur K de rang 2, possédant une $\mathfrak{n}$-isogénie cyclique K-rationnelle, a bonne réduction potentielle en tout idéal premier distinct de $\mathfrak{n}$.*

(ii) Soit $\mathfrak{n}$ un idéal de degré ≥ 5. Si $\deg \mathfrak{n} = 5$ (resp. $\deg \mathfrak{n} = 6$), on suppose $q \geq 4$ (resp. $q \geq 3$). Supposons que $\mathfrak{n}$ vérifie la propriété : toute forme propre de $\mathbf{H}(\mathbf{C})$ est de rang ≤ 1. Alors la courbe $Y_0(\mathfrak{n})$ n'a pas de point K-rationnel.

Les symboles modulaires pour $\mathbf{F}_q[T]$

Nous concentrons une partie importante de nos efforts à étudier les symboles modulaires pour $\mathbf{F}_q[T]$ introduits par Teitelbaum [Tei92a]. Le groupe $\mathbf{M}$ des symboles modulaires relatifs au sous-groupe de congruence $\Gamma_0(\mathfrak{n})$ de $\mathrm{GL}(2, A)$ admet une présentation par générateurs et relations. Les générateurs sont notés $\xi(u : v)$, pour $(u : v) \in \mathbf{P}^1(A/\mathfrak{n})$. Le groupe $\mathbf{M}$ est muni d'une action des opérateurs de Hecke. Nous montrons que l'action de ces opérateurs est donnée par la formule suivante.

Théorème 9 (th. 2.28)**.** *Pour tout idéal $\mathfrak{m}$ de A et $(u : v) \in \mathbf{P}^1(A/\mathfrak{n})$, on a*

$$T_{\mathfrak{m}}\, \xi(u : v) = \sum_{\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \mathscr{S}_{\mathfrak{m}}} \xi(\alpha u + \gamma v : \beta u + \delta v)$$

où $\mathscr{S}_{\mathfrak{m}} = \left\{ \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in M_2(A), \deg \alpha > \deg \beta, \deg \delta > \deg \gamma, (\alpha\delta - \beta\gamma) = \mathfrak{m}, \alpha \text{ et } \delta \text{ unitaires} \right\}$ *et la somme est restreinte aux matrices telles que $(\alpha u + \gamma v : \beta u + \delta v)$ soit défini dans $\mathbf{P}^1(A/\mathfrak{n})$.*

Elle peut être utilisée dans le cadre d'une étude algorithmique des formes automorphes. Comme autre application, on mentionne ce théorème de non-annulation.

Théorème 10 (th. 3.16)**.** *Soit $\mathscr{F}$ l'ensemble des formes automorphes de $\mathbf{H}(\mathbf{C})$ normalisées et propres pour $\mathbf{T}$. Si $\mathfrak{n}$ est de degré ≥ 3, il existe une constante $C > 0$ ne dépendant que de q telle que*

$$\#\{f \in \mathscr{F} \mid L(f, 1) \neq 0\} \geq C(\#\mathscr{F})^{1/2}.$$

Signalons que cette estimation est meilleure que celle obtenue par la même méthode pour les formes modulaires classiques dans [Par99].

Il est peut-être remarquable qu'une base explicite puisse être extraite du système de générateurs de $\mathbf{M}$ (il n'y a pas de phénomène analogue pour les symboles modulaires classiques).

Proposition 11 (th. 2.40)**.** *Si $\mathfrak{n}$ est de degré impair $d \geq 3$, les symboles modulaires $\xi(1 : 0)$ et $\xi(P : Q)$ où P et Q parcourent les polynômes unitaires de A premiers entre eux vérifiant $\deg Q < \deg P < d/2$, forment une base sur $\mathbf{Z}$ de $\mathbf{M}$.*

Cela pourrait être utile en vue d'investigations numériques sur les formes automorphes. Dans la section 2.8, on donne une application de ce résultat à la description de la structure du $\mathbf{T}$-module des symboles modulaires paraboliques lorsque $\mathfrak{n}$ est de degré 3.

Les implications logiques des chapitres sont représentées par le diagramme suivant.

$$\begin{tikzcd}
\text{chapitre 1} \arrow[dr, Rightarrow] & \text{chapitre 2} \arrow[d, Rightarrow] & \\
& \text{chapitre 3} \arrow[d, Rightarrow] & \text{chapitre 4} \arrow[dl, Rightarrow] \\
& \text{chapitre 5} &
\end{tikzcd}$$

Cadre général et notations

Le cadre dans lequel se situe le texte est le suivant :

— p est un nombre premier, q une puissance de p et $\mathbf{F}_q$ un corps fini à q éléments ;
— A est l'anneau de polynômes en une indéterminée $\mathbf{F}_q[T]$; il est muni de la fonction degré $\deg : A \to \mathbf{N} \cup \{-\infty\}$, en adoptant la convention $\deg 0 = -\infty$;
— K est le corps des fractions rationnelles $\mathbf{F}_q(T)$, c'est-à-dire le corps des fractions de A ; c'est une corps de fonctions algébriques sur $\mathbf{F}_q$, de degré de transcendance 1 ;
— ∞ est la place de K définie par $\pi = \frac{1}{T}$; les places de K sont ∞ et les idéaux maximaux de A, ces derniers correspondant aux idéaux premiers non nuls de A ;
— $K_\infty = \mathbf{F}_q((\pi))$ est le corps des séries de Laurent en π ; c'est le complété de K en la place ∞ ;
— la valeur absolue $|\cdot| = |\cdot|_\infty$ est normalisée sur K_∞ ($|\pi| = \frac{1}{q}$) ;
— $O_\infty = \mathbf{F}_q[[\pi]]$ est l'anneau de séries formelles en π ; c'est l'anneau d'entiers de K_∞ ;
— $\mathbf{C}_\infty$ est le complété d'une clôture algébrique de K_∞ ; c'est un corps algébriquement clos ;
— $\mathcal{H} = \mathbf{P}^1(\mathbf{C}_\infty) - \mathbf{P}^1(K_\infty) = \mathbf{C}_\infty - K_\infty$ est appelé le *demi-plan de Drinfeld* ;
— $\mathfrak{n}$ est un idéal non nul de A.

La notation ∞ désignera aussi bien la place ∞ que le bout ∞ de l'arbre de Bruhat-Tits ou la pointe ∞ d'une courbe modulaire : nous espérons que, d'après le contexte, il n'y aura pas de confusion possible.

Le groupe $\mathrm{GL}(2, A)$ agit sur $\mathcal{H}$ par transformations linéaires : $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) z = \frac{az+b}{cz+d}$. Pour un idéal $\mathfrak{n}$ de A, on pose : $\Gamma(\mathfrak{n}) = \{g \in \mathrm{GL}(2, A) \mid g \equiv \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \mod \mathfrak{n}\}$. Un sous-groupe de $\mathrm{GL}(2, A)$ est dit *de congruence* s'il contient $\Gamma(\mathfrak{n})$ pour un idéal $\mathfrak{n}$. Les groupes :

$$\Gamma_0(\mathfrak{n}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}(2, A) \mid c \in \mathfrak{n} \right\},$$
$$\Gamma_1(\mathfrak{n}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}(2, A) \mid a - 1, c \in \mathfrak{n} \right\}$$

en sont des exemples.

Si $\mathfrak{p}$ est un idéal maximal de A, le corps fini $A/\mathfrak{p}$ est noté $\mathbf{F}_\mathfrak{p}$. Si F est un corps quelconque, F^{alg} (resp. F^{sep}) désigne une clôture algébrique (resp. séparable) de F. Si R est un anneau, $\mathrm{Z}(R)$ est le centre de $\mathrm{GL}(2, R)$. L'exposant $^\times$ désigne le sous-groupe des éléments inversibles. Le cardinal d'un ensemble fini E est noté $\#E$.

Soient Y un schéma, X un schéma sur Y et $Y' \to Y$ un morphisme de schémas. Le changement de base de X à Y' est noté $X_{Y'}$. Muni de la projection $X_{Y'} \to Y'$, c'est un schéma sur Y'. Si Y' est le spectre d'un anneau R, on pose $X_{Y'} = X_R$.

Si G est un schéma en groupes lisse sur un schéma T, $\operatorname{Cot} G$ désignera l'espace cotangent de $G_{/T}$ le long de la section nulle.

En fin de texte, on trouvera un index non exhaustif de notations employées dans plusieurs chapitres.

Chapitre 1

Modules de Drinfeld

1.1 Modules de Drinfeld (rappels)

Ces objets ont été introduits par Drinfeld [Dri74] sous le nom de *modules elliptiques*. La théorie des modules de Drinfeld est valable dans un contexte plus général que celui dans lequel se situe ce texte : considérons une courbe projective lisse irréductible $\mathcal{C}$ sur $\mathbf{F}_q$, munie d'un point fermé ∞ de degré δ ; on peut remplacer A par l'anneau des fonctions régulières de $\mathcal{C} - \{\infty\}$, K par le corps des fractions de A, π par une uniformisante fixée en la place ∞ de K, K_∞ par le complété de K en ∞ (avec la valeur absolue normalisée par $|\pi| = q^{-\delta}$), O_∞ par son anneau d'entiers et $\mathbf{C}_\infty$ par le complété d'une clôture algébrique de K_∞. La majeure partie des énoncés de cette section, ainsi que la conjecture 1.12, sont valables dans ce contexte.

Notre référence pour la présentation suivante est [Gos96]. Les actes de conférence [GvdPRVG97] contiennent des présentations détaillées de la plupart des objets figurant dans cette thèse (à l'exception des symboles modulaires de Teitelbaum).

1.1.1 Définition

Un *A-corps* L est un corps équipé d'un morphisme $\gamma : A \to L$. Si le noyau de γ est non nul, on l'appelle la *A-caractéristique de L*, sinon on dit que L est de *A-caractéristique générique*. Les extensions finies de K sont de caractéristique générique.

Dans la suite de cette section, L désignera un A-corps. Les endomorphismes du schéma en groupes additif sont donnés par des polynômes additifs. On s'intéresse à ceux définis sur L et $\mathbf{F}_q$-linéaires :

$$\mathrm{End}_{L,\mathbf{F}_q}(\mathbf{G}_a) = \left\{ \sum_{\text{finie}} a_i X^{q^i} \mid a_i \in L \right\}.$$

Muni de la composition, c'est un anneau non commutatif. Soit $\tau : X \mapsto X^q$ l'endomorphisme de Frobenius relatif. Considérons l'anneau $L\{\tau\}$ des polynômes tordus de la forme $\sum_{\text{finie}} a_i \tau^i$ ($a_i \in L$) avec la multiplication définie par $\tau a = a^q \tau$ ($a \in L$). *Via* $X^{q^i} \mapsto \tau^i$, on a l'identification d'anneaux

$$\mathrm{End}_{L,\mathbf{F}_q}(\mathbf{G}_a) = L\{\tau\}.$$

Définition 1.1. Un *A-module de Drinfeld sur L* est un homomorphisme de $\mathbf{F}_q$-algèbres

$$\begin{array}{rccc} \phi : & A & \longrightarrow & L\{\tau\} \\ & a & \longmapsto & \phi_a \end{array}$$

vérifiant les conditions :

(i) pour tout a dans A, le terme constant de ϕ_a est $\gamma(a)$;

(ii) il existe $a \in A - \{0\}$ tel que ϕ_a n'est pas constant.

Par la suite, on abrègera « A-module de Drinfeld » en « module de Drinfeld ». Les coefficients des polynômes ϕ_a seront appelés les *coefficients de ϕ*.

On démontre qu'il existe un entier $r \geq 1$ tel que $\deg \phi_a = r \deg a$ pour tout a dans $A - \{0\}$. On appelle r le *rang* du module de Drinfeld. Un module de Drinfeld ϕ sur L de rang r est déterminé par la donnée du polynôme $\phi_T(X) = \gamma(T)X + l_1 X^q + \ldots + l_r X^{q^r}$, avec $l_1, \ldots, l_r \in L$ et $l_r \neq 0$. Par exemple, le *module de Carlitz* sur K (ou $\mathbf{C}_\infty$) est défini par $\rho_T(X) = TX + X^q$ et il est de rang 1. Le rang d'un module de Drinfeld en est un invariant fondamental. Le cas $r = 1$ présente de nombreuses similarités avec la théorie cyclotomique et le cas $r = 2$ avec les courbes elliptiques.

Soient ϕ et ψ deux modules de Drinfeld sur L. Un *morphisme* de ϕ dans ψ sur L est la donnée d'un polynôme $P \in L\{\tau\}$ tel que pour tout $a \in A$ on ait $P\phi_a = \psi_a P$ dans $L\{\tau\}$. Un morphisme non nul est appelé une *isogénie* et ne peut exister qu'entre modules de Drinfeld de même rang. Un isomorphisme de ϕ dans ψ sur L est la donnée d'un polynôme constant $u \in L^\times$ tel que, pour tout $a \in A$, on ait $u\phi_a = \psi_a u$ dans $L\{\tau\}$.

1.1.2 Théorie analytique

Les modules de Drinfeld sur $\mathbf{C}_\infty$ possèdent une description par des réseaux. Un *réseau de* $\mathbf{C}_\infty$ est un sous A-module de $\mathbf{C}_\infty$ discret et de type fini. Son *rang* est la dimension du K_∞-espace vectoriel qu'il engendre. Contrairement à la situation classique sur $\mathbf{C}$ où les réseaux similaires sont de rang 1 ou 2, il existe ici des réseaux de rang arbitrairement grand. À un tel réseau Λ on associe une fonction *exponentielle*, qui joue le rôle de la fonction $\wp$ de Weierstrass. Elle est définie par

$$e_\Lambda(z) = z \prod_{\lambda \in \Lambda, \lambda \neq 0} \left(1 - \frac{z}{\lambda}\right) \qquad (z \in \mathbf{C}_\infty).$$

C'est une fonction entière sur $\mathbf{C}_\infty$, au sens de l'analyse non-archimédienne. Ses zéros sont simples et ce sont les éléments de Λ. De plus, cette fonction est $\mathbf{F}_q$-linéaire, surjective sur $\mathbf{C}_\infty$ et donne un isomorphisme de groupes $e_\Lambda : \mathbf{C}_\infty/\Lambda \xrightarrow{\sim} \mathbf{C}_\infty$. Le diagramme commutatif suivant

$$\begin{tikzcd} 0 \arrow[r] & \Lambda \arrow[r] \arrow[d, "a"] & \mathbf{C}_\infty \arrow[r, "e_\Lambda"] \arrow[d, "a"] & \mathbf{C}_\infty \arrow[r] \arrow[d, "\phi_a^\Lambda"] & 0 \\ 0 \arrow[r] & \Lambda \arrow[r] & \mathbf{C}_\infty \arrow[r, "e_\Lambda"] & \mathbf{C}_\infty \arrow[r] & 0 \end{tikzcd}$$

définit de façon unique un module de Drinfeld $\phi^\Lambda : a \mapsto \phi_a^\Lambda$ sur $\mathbf{C}_\infty$ de rang r, vérifiant

$$e_\Lambda(az) = \phi_a^\Lambda(e_\Lambda(z)) \qquad (a \in A, z \in \mathbf{C}_\infty).$$

L'application $\Lambda \mapsto \phi^\Lambda$ est une équivalence de catégorie entre les réseaux de $\mathbf{C}_\infty$ de rang r (munis de leurs morphismes) et les modules de Drinfeld sur $\mathbf{C}_\infty$ de rang r (munis de leurs morphismes).

1.1.3 Le A-module des points rationnels

Soient ϕ un module de Drinfeld sur L et M une extension de L. On munit le groupe additif M d'une structure de A-module, différente de la structure canonique, donnée par l'action de ϕ suivante :

$$a \cdot x = \phi_a(x) \quad (a \in A, x \in M).$$

On appelle *module des points M-rationnels de ϕ* et on note ${}^\phi M$ ce A-module.

Pour $a \in A - \{0\}$, un *point de a-torsion M-rationnel* est une racine dans M du polynôme $\phi_a(x)$. Ces points forment un sous-A-module de ${}^\phi M$ noté $\phi[a](M)$. Les points de torsion M-rationnels forment un sous-module de ${}^\phi M$ noté $({}^\phi M)_{\text{tors}}$. L'*ordre* d'un point de torsion x est défini comme l'idéal non nul $\{a \in A \mid \phi_a(x) = 0\}$ de A. Le A-module $\phi[a](L^{\text{alg}})$ est contenu dans ${}^\phi L^{\text{sep}}$ et isomorphe à $(A/aA)^r$. On dispose du théorème de structure globale suivant.

Théorème 1.2 ([Poo95], th. 1)**.** *Soit ϕ un module de Drinfeld sur une extension finie L de K. Le A-module ${}^\phi L$ est la somme directe de $({}^\phi L)_{\text{tors}}$ et d'un A-module libre de rang infini dénombrable.*

La situation diffère donc de celle des courbes elliptiques sur les corps de nombres, pour lesquelles le groupe de Mordell-Weil est de type fini.

Définition 1.3. Soient $\mathfrak{n}$ un idéal de A et ϕ un module de Drinfeld sur L. Une *$\mathfrak{n}$-isogénie cyclique L-rationnelle* de ϕ est un polynôme $P(X) = \sum_i a_i X^{q^i} \in L[X]$ de degré $\#(A/\mathfrak{n})$ tel que $\text{Ker}(P) = \{x \in L^{\text{alg}} \mid P(x) = 0\}$ est un sous-module de $({}^\phi L^{\text{alg}})_{\text{tors}} \subset {}^\phi L^{\text{sep}}$ isomorphe à $A/\mathfrak{n}$.

Un tel polynôme P définit une isogénie entre ϕ et le module de Drinfeld ψ défini par $\psi_a(P(X)) = P(\phi_a(X))$ $(a \in A)$. Réciproquement, tout sous-module M de $({}^\phi L^{\text{alg}})_{\text{tors}}$, stable par $\text{Gal}(L^{\text{sep}}/L)$ et tel que $M \simeq A/\mathfrak{n}$ comme A-modules, définit une $\mathfrak{n}$-isogénie cyclique L-rationnelle par la formule suivante : $P(X) = \prod_{m \in M}(X - m)$. On a donc une bijection entre l'ensemble des $\mathfrak{n}$-isogénies cycliques L-rationnelles de ϕ et les sous-modules de $({}^\phi L)_{\text{tors}}$ stables par $\text{Gal}(L^{\text{sep}}/L)$ et isomorphes à $A/\mathfrak{n}$ comme A-modules.

1.1.4 Théorie de la réduction

Soient L un A-corps local, v sa valuation discrète, $\mathcal{O}$ son anneau de valuation, $\mathcal{M}$ son idéal maximal et k son corps résiduel. Soit ϕ un module de Drinfeld sur L de rang r. On adopte la définition suivante.

Définition 1.4. On appelle *modèle stable de ϕ sur L* la donnée d'un module de Drinfeld ψ sur L de rang r vérifiant les conditions :

(i) ϕ et ψ sont isomorphes sur L ;

(ii) ψ est à coefficients dans $\mathcal{O}$;

(iii) la réduction de ψ est un module de Drinfeld sur k.

Définition 1.5. Le module de Drinfeld ϕ a *réduction stable* s'il possède un modèle stable ψ sur L. Si r' désigne le rang de la réduction de ψ sur k, on dit alors que ϕ a *réduction stable de rang* r'.

Le module de Drinfeld ϕ a *réduction potentiellement stable (de rang* r'*)* s'il a réduction stable (de rang r') sur une extension finie (F, w) de (L, v). Le module de Drinfeld ϕ a *bonne réduction* (resp. *bonne réduction potentielle*) s'il a réduction stable de rang r (resp. réduction potentiellement stable de rang r).

Proposition 1.6. *Tout module de Drinfeld sur L a réduction potentiellement stable.*

Un module de Drinfeld sur L de rang 2 a donc soit bonne réduction potentielle, soit réduction potentiellement stable de rang 1. Sur une extension finie M de $K = \mathbf{F}_q(T)$, un module de Drinfeld a bonne réduction en toutes les places de M sauf un nombre fini d'entre elles.

Soit ϕ un module de Drinfeld sur L. D'après la proposition 1.6, ϕ possède un modèle stable ψ sur une extension finie (F, w) de (L, v). L'image d'un élément $x \in {}^{\phi}L$ par l'isomorphisme est un élément y de ${}^{\psi}F$.

Lemme 1.7. *Si y est entier, il en est de même de l'image de x dans tout autre modèle stable de ϕ sur une extension finie de (L, v).*

Démonstration. Supposons qu'il existe des extensions finies (F_1, w_1) et (F_2, w_2) de (L, v), un modèle stable ψ_1 de ϕ sur F_1 et un modèle stable ψ_2 de ϕ sur F_2. Notons r' le rang commun de la réduction de ψ_1 et ψ_2. Alors il existe $u_1 \in F_1^\times$ et $u_2 \in F_2^\times$ tels que $\psi_1 = u_1 \phi u_1^{-1}$ et $\psi_2 = u_2 \phi u_2^{-1}$. Soit F le compositum de F_1 et F_2 et w l'unique prolongement de w_1 et w_2 à F. Posons $u = u_1^{-1} u_2 \in F^\times$. Alors on a $\psi_2 = u \psi_1 u^{-1}$. Notons a_1 (resp. a_2) le coefficient en $\tau^{r'}$ de $(\psi_1)_T$ (resp. $(\psi_2)_T$). Comme les modèles sont à coefficients entiers, on a $w_1(a_1) = 0$ et $w_2(a_2) = 0$. Or $a_2 = u^{q^{r'}-1} a_1$ donc $w(u_1 u_2^{-1}) = 0$ c'est-à-dire $w_1(u_1) = w_2(u_2)$. L'image du point x dans le modèle ψ_1 (resp. ψ_2) est $u_1^{-1} x$ (resp. $u_2^{-1} x$). Si l'un est entier, l'autre l'est donc aussi. □

L'uniformisation de Tate-Drinfeld

Nous rappelons cette uniformisation dans le cas des modules de Drinfeld de rang 2. Supposons que $\mathcal{O}$ est un anneau de valuation discrète complet. Si ρ est un module de Drinfeld sur L, un *ρ-réseau de rang* 1 est un sous-A-module de ${}^{\rho}L^{\mathrm{sep}}$ projectif, de rang 1, discret et invariant par $\mathrm{Gal}(L^{\mathrm{sep}}/L)$.

Proposition 1.8 (Drinfeld [Dri74] §7)**.** *Il existe une bijection entre :*

(i) l'ensemble des classes d'isomorphisme sur L de modules de Drinfeld de rang 2 *sur L, à réduction potentiellement stable de rang* 1 *;*

(ii) l'ensemble des classes d'isomorphisme sur L de couples (Γ, ρ) où ρ est un module de Drinfeld de rang 1 *sur L et Γ est un ρ-réseau de rang* 1.

Rappelons quelques éléments de cette construction. Prenons un module de Drinfeld ρ de rang 1 sur L et un ρ-réseau Γ de rang 1. La fonction exponentielle associée à Γ :

$$e_\Gamma(z) = z \prod_{\alpha \in \Gamma - \{0\}} \left(1 - \frac{z}{\alpha}\right)$$

est une fonction entière sur L^{sep}, qui vérifie $e_\Gamma(z) \equiv z \mod \mathcal{M}$. Le module de Drinfeld ϕ associé au couple (Γ, ρ) est déterminé de façon unique par le diagramme commutatif suivant, pour tout $a \in A$:

$$\begin{tikzcd}
0 \arrow[r] & \Gamma \arrow[r] \arrow[d, "\rho_a"] & L^{\mathrm{sep}} \arrow[r, "e_\Gamma"] \arrow[d, "\rho_a"] & L^{\mathrm{sep}} \arrow[d, "\phi_a"] \\
0 \arrow[r] & \Gamma \arrow[r] & L^{\mathrm{sep}} \arrow[r, "e_\Gamma"] & L^{\mathrm{sep}}.
\end{tikzcd}$$

Rappelons la construction réciproque dans le cas où ϕ est un module de Drinfeld sur L de rang 2 défini par

$$\phi_T = T + g\tau + \Delta\tau^2 \in L\{\tau\},$$

avec $g \in \mathcal{O}^\times$ et $\Delta \in \mathcal{M}$. Il existe une série $e = 1 + \sum_{n=1}^{+\infty} u_n \tau^n$ dans l'anneau des séries formelles tordues $\mathcal{O}\{\{\tau\}\}$, et un module de Drinfeld ρ sur L de rang 1, à coefficients dans $\mathcal{O}$, tels que

$$\phi_a e = e\rho_a \quad (a \in A).$$

De plus, les réductions de ϕ et ρ modulo $\mathcal{M}$ coïncident et le module de Drinfeld ρ a bonne réduction. On notera encore e la fonction entière $x \mapsto 1 + \sum_{n=1}^{+\infty} u_n x^{q^n}$, qui définit un homomorphisme $L^{\mathrm{alg}} \to L^{\mathrm{alg}}$. Son noyau Γ est un ρ-réseau de dimension 1. Il est de la forme $\Gamma = \rho_A(\gamma)$ pour un élément $\gamma \in \Gamma$ vérifiant $w(\gamma) < 0$ (où w désigne l'unique prolongement de v à L^{alg}). Pour tout a non nul dans A, on a l'isomorphisme de A-modules

$$e : \rho_a^{-1}(\Gamma)/\Gamma \xrightarrow{\sim} \phi[a](L^{\mathrm{alg}}). \tag{1.1}$$

Comme ϕ est à coefficients dans $\mathcal{O}$, le groupe additif $\mathcal{O}$ muni de la loi $a \cdot x = \phi_a(x)$, est un sous A-module de ${}^\phi L$ noté ${}^\phi\mathcal{O}$. Le sous-A-module des racines dans $\mathcal{O}$ de l'équation $\phi_a(x) = 0$ est noté $\phi[a](\mathcal{O})$.

Lemme 1.9 (voir aussi [Ros03] 5.3 et 5.4)**.** *Soit $a \in A$, $a \neq 0$. On a*

$$e(\rho[a](\mathcal{O})) = \phi[a](\mathcal{O}).$$

Démonstration. L'inclusion $e(\rho[a](\mathcal{O})) \subset \phi[a](\mathcal{O})$ est immédiate, car ρ et e sont à coefficients dans $\mathcal{O}$. Étudions l'autre inclusion. Les affirmations suivantes s'obtiennent en généralisant les arguments de la preuve du lemme 5.3 de [Ros03] (voir aussi la preuve du théorème 5.4 de *loc. cit.*). Soit λ_a un élément de ${}^\rho L^{\mathrm{alg}}$ d'ordre (a), c'est-à-dire une racine primitive de l'équation $\rho_a(x) = 0$. Soit $\gamma_a \in L^{\mathrm{alg}}$ une racine de l'équation $\rho_a(x) = \gamma$. L'ensemble

$$\{\rho_c(\lambda_a) + \rho_d(\gamma_a) \mid (c, d) \in A \times A, \deg c < \deg a, \deg d < \deg a\} \subset \rho_a^{-1}(\Gamma)$$

est un système de représentants de $\rho_a^{-1}(\Gamma)/\Gamma$. En effet, il possède $q^{2\deg a}$ éléments et deux éléments distincts de cet ensemble ne sont pas congrus modulo Γ. De plus, si $\deg c < \deg a$, $\deg d < \deg a$, $d \neq 0$, on a les inégalités suivantes :

$$\begin{aligned} w(\rho_c(\lambda_a)) &\geq 0 \\ w(\rho_d(\gamma_a)) &< 0 \\ w(e(\rho_c(\lambda_a))) &\geq 0 \\ w(e(\rho_d(\gamma_a)) &< 0. \end{aligned}$$

En utilisant la linéarité de l'exponentielle et (1.1), on en déduit

$$\phi[a](\mathcal{O}) \subset e(\rho[a](L^{\mathrm{alg}})).$$

Soit $z \in \phi[a](\mathcal{O})$. Il existe $y \in \rho[a](L^{\mathrm{alg}})$ tel que $z = e(y)$. L'élément de torsion y est séparable sur L. Soit $\sigma \in \mathrm{Gal}(L^{\mathrm{sep}}/L)$. Comme $z \in L$, on a $\sigma(z) = z$ donc $e(\sigma(y)) = \sigma(e(y)) = e(y)$. Par linéarité de l'exponentielle, on a $e(\sigma(y) - y) = 0$, donc $\sigma(y) - y \in \Gamma$. Par ailleurs, $\sigma(y) - y$ est un élément de a-torsion de Γ, qui est sans torsion. On obtient $\sigma(y) = y$, d'où $y \in L$. Ceci montre que

$$\phi[a](\mathcal{O}) \subset e(\rho[a](L)).$$

Enfin, tout élément de $\rho[a](L)$ est dans $\mathcal{O}$, car il est une racine du polynôme $\rho_a(X) \in \mathcal{O}[X]$ dont le coefficient dominant est inversible dans $\mathcal{O}$. On obtient

$$\phi[a](\mathcal{O}) \subset e(\rho[a](\mathcal{O})).$$

□

1.1.5 Modules de Drinfeld de rang 2 et invariant modulaire

Si ϕ est un module de Drinfeld de rang 2 sur un corps L donné par

$$\phi_T = T + g\tau + \Delta\tau^2 \qquad (g \in L, \Delta \in L^\times)$$

son *invariant modulaire* est $j(\phi) = \frac{g^{q+1}}{\Delta}$. Deux modules de Drinfeld de rang 2 sur L ont le même invariant modulaire si et seulement s'ils sont isomorphes sur L^{alg}. De plus, si L est un corps local, ϕ a bonne réduction potentielle si et seulement si $j(\phi)$ appartient à l'anneau de valuation de L ([Ros03] lemme 5.2).

1.2 Torsion des modules de Drinfeld (rappels)

Lemme 1.10 (voir aussi [Poo97], prop. 1)**.** *Soient L un A-corps et $P \in A$ non constant. Alors $({}^{\phi}L)_{\mathrm{tors}}$ est l'ensemble des éléments de L dont l'orbite sous l'itération de ϕ_P est finie.*

Démonstration. Soit $x \in L$ et I_x le noyau de l'homomorphisme d'anneaux

$$\begin{array}{ccc} A & \longrightarrow & L \\ a & \longmapsto & \phi_a(x). \end{array}$$

L'élément x est de torsion si et seulement si l'idéal I_x est non nul, ce qui revient à dire que A/I_x est fini. Par ailleurs, l'application précédente induit une bijection entre A/I_x et l'orbite de x sous ϕ. Si x est de torsion, cette orbite est finie et en particulier, l'orbite de x sous l'itération de ϕ_P est finie.

Réciproquement, si l'orbite sous l'itération de ϕ_P est finie, il existe un entier $n \geq 1$ tel que $\phi_P(x) = \phi_{P^n}(x)$, donc $\phi_{P^n - P}(x) = 0$. Comme P est non constant, le polynôme $P^n - P$ est non nul dans A, donc x est de torsion. □

Le lemme 1.10 fournit une description du sous-module de torsion en termes de systèmes dynamiques algébriques. Considérons le polynôme $\phi_T(X) = TX + a_1 X^q + \ldots + a_r X^{q^r} \in L[X]$ avec $a_r \in L^\times$. L'itération de $\phi_T(X)$ définit un système dynamique sur $\mathbf{P}^1_L$. Un point $x \in \mathbf{P}^1_L$ est dit *prépériodique* pour ϕ_T s'il existe un entier naturel n tel que $f^{\circ n}(x)$ est périodique pour f. Le A-module de torsion $({}^\phi L)_{\text{tors}}$ est alors l'ensemble des points de $\mathbf{P}^1_L$ prépériodiques pour ϕ_T (voir [Poo98, Sch04] pour de telles formulations).

Lemme 1.11. *Soit L une extension finie de K. Si ϕ est un module de Drinfeld sur L, le A-module $({}^\phi L)_{\text{tors}}$ est fini.*

Pour une démonstration élémentaire utilisant la théorie de la réduction, on peut consulter [Ros03] prop. 4.1. Le lemme se déduit aussi de la proposition 1 de [Poo97], qui affirme que, sur une extension finie de $K_\mathfrak{p}$ (le complété de K en une place $\mathfrak{p} \neq \infty$), la torsion d'un module de Drinfeld est finie. Enfin, ce lemme est aussi conséquence des propriétés de la hauteur canonique globale associée à un module de Drinfeld par Denis [Den92] : les points de torsion sont ceux de hauteur nulle et comme il n'existe qu'un nombre fini de points de hauteur bornée, ils sont en nombre fini.

Rappelons la conjecture suivante de Poonen, inspirée par une question analogue pour les courbes elliptiques et les variétés abéliennes sur les corps de nombres. Le rang du module de Drinfeld joue le rôle de paramètre.

Conjecture 1.12 (Poonen [Poo97])**.** Soient $r \geq 1$ et $d \geq 1$ des entiers. Il existe une constante $C_{r,d} > 0$ telle que, pour toute extension L de K de degré d et pour tout module de Drinfeld ϕ sur L de rang r, on ait $\#({}^\phi L)_{\text{tors}} \leq C_{r,d}$.

Denis avait formulé auparavant cette même question, sans toutefois faire apparaître la dépendance de la constante en le rang ([Den95], problème 3). Poonen a expliqué dans quelle mesure sa formulation est optimale et démontré la conjecture pour $r = 1$ avec une borne explicite optimale ([Poo97], th. 8). Par la suite, Schweizer a proposé une version raffinée de la borne.

Conjecture 1.13 ([Sch03] 3.1)**.** Soient $r \geq 1$ et $d \geq 1$ des entiers. Il existe une constante $b_{r,d}$, indépendante de q, telle que pour toute extension L de K de degré d et pour tout module de Drinfeld ϕ sur L de rang r, on ait $\#({}^\phi L)_{\text{tors}} \leq q^{b_{r,d}}$.

De plus, si $d = 1$, Schweizer formule une conjecture précise sur la structure du module de torsion.

Conjecture 1.14 ([Sch03] conj. 1)**.** Soit ϕ un module de Drinfeld de rang 2 sur K. Alors on a un isomorphisme de A-modules

$$({}^\phi K)_{\text{tors}} \simeq A/\mathfrak{m}_1 \oplus A/\mathfrak{m}_2$$

avec $\mathfrak{m}_1, \mathfrak{m}_2$ idéaux de A, $\mathfrak{m}_2 \subset \mathfrak{m}_1$ et $\deg \mathfrak{m}_1 + \deg \mathfrak{m}_2 \leq 2$.

Enfin, signalons que l'article [NY01] de NguyenKhac et Yamada prétend démontrer la conjecture pour $r = 2$, mais la démonstration ne semble pas être complète (voir [Sch03] §1 pour les détails).

Comme l'anneau A est principal, le module de torsion admet une décomposition

$$({}^{\phi}L)_{\text{tors}} = \bigoplus_{\mathfrak{p}} M_{\mathfrak{p}}$$

où

$$M_{\mathfrak{p}} = \{x \in ({}^{\phi}L)_{\text{tors}} \mid \exists n \geq 1,\ \phi_{P^n}(x) = 0\}$$

est la composante $\mathfrak{p}$-primaire de $({}^{\phi}L)_{\text{tors}}$ (P désigne un générateur de $\mathfrak{p}$) et la somme porte sur un nombre fini d'idéaux premiers $\mathfrak{p}$ de A.

Un des principaux résultats connus sur la conjecture pour les modules de Drinfeld de rang 2 est le suivant.

Théorème 1.15 (Schweizer [Sch03] th. 2.4, [Poo97] th. 6)**.** *Soient $\mathfrak{p}$ un idéal premier de A et $d \geq 1$ un entier. Il existe une constante $B_{d,\mathfrak{p}} > 0$ telle que, pour toute extension L de K de degré d et pour tout module de Drinfeld ϕ sur L de rang 2, la composante $\mathfrak{p}$-primaire de $({}^{\phi}L)_{\text{tors}}$ est de cardinal au plus $B_{d,\mathfrak{p}}$.*

Ce théorème est un analogue fort (c'est-à-dire uniforme en le corps) du théorème de Manin [Man69] sur la p-torsion des courbes elliptiques sur $\mathbf{Q}$. Plus précisément, c'est l'analogue d'un théorème de Kamienny et Mazur [KM95], dont la démonstration s'appuie sur un théorème de Frey, lui-même conséquence du théorème de Faltings (conjecture de Lang pour les points rationnels de sous-variétés des variétés abéliennes). La démonstration du théorème 1.15 repose sur des résultats similaires, en particulier la conjecture de Mordell-Lang pour les variétés abéliennes sur les corps de fonctions, prouvée par Hrushovski [Hru96].

Cet énoncé permet de ramener le problème de la torsion à celui *a priori* plus faible de la torsion première.

Conjecture 1.16. Pour tout entier $d \geq 1$, il n'y a qu'un nombre fini d'idéaux premiers $\mathfrak{p}$ de A pour lesquels il existe une extension L de K de degré d, un module de Drinfeld ϕ sur L de rang 2 et un élément de ${}^{\phi}L_{\text{tors}}$ d'ordre $\mathfrak{p}$.

Corollaire 1.17 ([Sch03])**.** *La conjecture 1.12 est vraie pour $r = 2$ si et seulement si la conjecture 1.16 est vérifiée.*

En effet, borner uniformément $\#({}^{\phi}L)_{\text{tors}}$ revient d'une part à borner uniformément le nombre d'idéaux premiers $\mathfrak{p}$ apparaissant dans la décomposition primaire $({}^{\phi}L)_{\text{tors}}$, d'autre part à borner uniformément le cardinal de chacune des composantes $\mathfrak{p}$-primaires. Le premier point revient à montrer la conjecture 1.16. Quant au deuxième, il découle du théorème 1.15. Dans cette thèse, nous nous intéressons à la conjecture 1.16.

***Remarque* 1.18.** La démonstration du théorème 1.15 ne fournit pas de borne explicite pour le cardinal de la composante $\mathfrak{p}$-primaire. Ainsi, même si on connaît explicitement les idéaux premiers $\mathfrak{p}$ intervenant dans la conjecture 1.16, cela ne suffit pas pour obtenir

une borne explicite dans la conjecture de Poonen. Dans le cas elliptique, le théorème de Merel n'est pas effectif pour la même raison. Cependant, Parent [Par99] a obtenu une borne effective en travaillant sur des courbes modulaires de niveau puissance d'un nombre premier. Une telle approche est envisageable pour la torsion des modules de Drinfeld de rang 2.

1.3 Arguments locaux pour l'étude de la torsion

Soit d un entier ≥ 1. Soient $\mathfrak{l}$ un idéal maximal de A et $K_{\mathfrak{l}}$ la complétion de K en $\mathfrak{l}$. Rappelons un résultat de Poonen sur la torsion des modules de Drinfeld à bonne réduction potentielle.

Théorème 1.19 ([Poo97], th. 5 et 7)**.** *Soit r un entier ≥ 1. Il existe une constante $C > 0$ telle que, si L est une extension finie de $K_{\mathfrak{l}}$ de degré au plus d et ϕ un A-module de Drinfeld de rang r sur L avec bonne réduction potentielle, on a $\#({}^{\phi}L)_{\mathrm{tors}} \leq C$.*

Un examen de la démonstration de Poonen montre que la borne explicite suivante convient :

$$C = q^{2d \deg \mathfrak{l}(q^{r \deg \mathfrak{l}}-1)}.$$

Précisons comment elle est obtenue. Soit P un générateur unitaire de $\mathfrak{l}$. La première étape de la démonstration, qui consiste à se ramener à $A = \mathbf{F}_q[P]$ et à $K = \mathrm{Frac}(\mathbf{F}_q[P])$, change le rang r en $r \deg \mathfrak{l}$ et le degré d en $d \deg \mathfrak{l}$. La deuxième étape permet de se ramener au cas où ϕ a bonne réduction sur une extension L' de L : l'extension L'/K construite est de degré au plus $d' = d(q^r - 1)$. Enfin, une fois ces simplifications faites, la dernière étape majore le cardinal de la torsion par $q^{2d'}$.

Dans le cas où $r = 2$ et $d = 1$, la borne obtenue est donc $q^{2(q^{2 \deg \mathfrak{l}}-1) \deg \mathfrak{l}}$. Ainsi, si le module de Drinfeld possède un point L-rationnel d'ordre $\mathfrak{n}$, on a $\deg \mathfrak{n} \leq 2(q^{2 \deg \mathfrak{l}} - 1) \deg \mathfrak{l}$. Lorsque $(\mathfrak{l}, \mathfrak{n}) = 1$, la proposition suivante montre que cette borne peut être améliorée. Cette estimation sera exploitée dans l'analogue de la méthode de Mazur (section 5.3).

Proposition 1.20. *Soient L une extension de $K_{\mathfrak{l}}$ de degré $\leq d$ et ϕ un module de Drinfeld sur L de rang 2 ayant un point de torsion L-rationnel x d'ordre $\mathfrak{n} \subsetneq A$ avec $(\mathfrak{l}, \mathfrak{n}) = 1$. Supposons vérifiée l'une des deux conditions suivantes :*

(i) ϕ a bonne réduction potentielle ;

(ii) $\mathfrak{n}$ est premier, ϕ a réduction potentiellement stable de rang 1 et x définit un point entier d'un modèle stable de ϕ sur une extension finie de L.

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

Démonstration. Posons $r = 2$ dans le cas (i) et $r = 1$ dans le cas (ii). Le module de Drinfeld ϕ est défini par $\phi_T = T + g\tau + \Delta\tau^2 \in L\{\tau\}$ avec $g \in L$ et $\Delta \in L^{\times}$. Soient 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 le corps obtenu en adjoignant α à L. C'est une extension séparable et totalement ramifiée de L de degré $q^r - 1$. Notons w l'unique valuation de F qui prolonge v et O l'anneau de valuation de F. Démontrons l'assertion suivante :

Il existe un module de Drinfeld ρ sur F de rang r, à coefficients dans O et bonne réduction, muni d'un point O-rationnel y d'ordre $\mathfrak{n}$.

Supposons la condition (i) vérifiée. Posons $u = \alpha^{-v(\Delta)} \in F^\times$. Alors on a $w(u) = -\frac{v(\Delta)}{q^2-1}$. De plus, comme le module de Drinfeld ϕ a bonne réduction potentielle, son invariant modulaire $\frac{g^{q+1}}{\Delta}$ est dans O, ce qui donne $v(\Delta) \leq (q+1)v(g)$ donc $w(u) \geq -\frac{v(g)}{q-1}$. Soit ρ le module de Drinfeld de rang 2 sur F défini par

$$\rho_T = T + u^{q-1}g\tau + u^{q^2-1}\Delta\tau^2.$$

Il est isomorphe à ϕ sur F et on a $w(u^{q-1}g) \geq 0$ et $w(u^{q^2-1}\Delta) = 0$. *Via* cet isomorphisme, ρ est muni d'un point de torsion F-rationnel d'ordre $\mathfrak{n}$, noté y. Soit $N \in A$ un générateur de $\mathfrak{n}$. On a

$$\rho_N(y) = Ny + \sum_{i=1}^{2\deg N} l_i y^{q^i} = 0, \tag{1.2}$$

où $l_1, \ldots, l_{2\deg N} \in O$ et $l_{2\deg N} \in O^\times$ (car ρ est de rang 2 et a bonne réduction). Comme $x \neq 0$, on a $y \neq 0$. D'après (1.2), on a alors $y \in O$.

Supposons la condition (ii) vérifiée. Posons $u = \alpha^{-v(g)} \in F^\times$. Alors on a $w(u) = -\frac{v(g)}{q-1}$. De plus, comme le module de Drinfeld ϕ n'a pas bonne réduction potentielle, son invariant modulaire $\frac{g^{q+1}}{\Delta}$ n'est pas entier donc $(q+1)w(g) < w(\Delta)$ et on a $w(u^{q^2-1}\Delta) > 0$. Soit ψ le module de Drinfeld sur F de rang 2 défini par

$$\psi_T = T + u^{q-1}g\tau + u^{q^2-1}\Delta\tau^2.$$

Il est isomorphe à ϕ sur F, à coefficients dans O et sa réduction modulo l'idéal maximal de O définit un module de Drinfeld de rang 1. Autrement dit, c'est un modèle stable de ϕ sur F. D'après le lemme 1.7, l'élément $x \in ({}^\phi L)_{\text{tors}}$ d'ordre $\mathfrak{n}$ définit un élément d'ordre $\mathfrak{n}$ de $({}^\psi O)_{\text{tors}}$, noté z. Soit (ρ, Γ) une uniformisation de Tate-Drinfeld de ψ sur F. Le module de Drinfeld ρ est de rang 1, à coefficients dans O et a bonne réduction. Appliquons le lemme 1.9. Il existe $y \in \rho[N](O)$ tel que $z = e(y)$. Il existe $b \in A, \deg b < \deg \mathfrak{n}$ et λ_N une racine primitive de ρ_N tels que $y = \rho_b(\lambda_N)$. Comme $\mathfrak{n}$ est premier et λ_N est d'ordre $\mathfrak{n}$, on voit que y est d'ordre $\mathfrak{n}$.

L'assertion est donc démontrée. Soit B le sous-A-module de $({}^\rho F)_{\text{tors}}$ engendré par y. Comme ρ est à coefficients dans O et $y \in O$, B est contenu dans O. La réduction modulo l'idéal maximal de O fournit un homomorphisme de groupes additifs de B dans le corps résiduel de F. Cet homomorphisme est injectif. En effet, soit z un élément de B ; il est annulé par N et vérifie donc

$$\rho_N(z) = Nz + l_1 z^q + \ldots + l_{r\deg N} z^{q^{r\deg N}} = 0,$$

avec $l_1, \ldots, l_{r\deg N} \in O$ et $l_{r\deg N} \in O^\times$ (car ρ a bonne réduction). Supposons que z est non nul et vérifie $w(z) > 0$. On aurait

$$N + l_1 z^{q-1} + \ldots + l_{r\deg N} z^{q^{r\deg N}-1} = 0,$$

donc $w(N) > 0$, ce qui est exclu car $(\mathfrak{l}, \mathfrak{n}) = 1$. Donc B s'injecte dans le corps résiduel de F, qui est celui de L car l'extension F/L est totalement ramifiée. Le corps résiduel de L

est une extension de degré au plus d de $A/\mathfrak{l}$, donc $\#B \leq (\#A/\mathfrak{l})^d \leq q^{d \deg \mathfrak{l}}$. Par ailleurs, comme y est d'ordre $\mathfrak{n}$, B est isomorphe à $A/\mathfrak{n}$ comme A-module, donc $\#B = q^{\deg \mathfrak{n}}$. Ainsi on a $\deg \mathfrak{n} \leq d \deg \mathfrak{l}$. □

On en déduit immédiatement l'énoncé global suivant.

Corollaire 1.21. *Soient $\mathfrak{l}$ un idéal maximal de A et L une extension de K de degré $\leq d$. Soit ϕ un module de Drinfeld sur L de rang 2 ayant un point de torsion L-rationnel x d'ordre $\mathfrak{n} \subsetneq A$ avec $(\mathfrak{l}, \mathfrak{n}) = 1$. Supposons vérifiée l'une des deux conditions suivantes :*

(i) ϕ a bonne réduction potentielle en un idéal premier au-dessus de $\mathfrak{l}$;

(ii) $\mathfrak{n}$ est premier, ϕ a réduction potentiellement stable de rang 1 en un idéal premier au-dessus de $\mathfrak{l}$ et x définit un point entier d'un modèle stable de ϕ sur une extension finie de L.

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

1.4 Courbes modulaires de Drinfeld (rappels)

Les variétés de modules des modules de Drinfeld de rang r ont été introduites dans [Dri74]. Leur étude, en particulier dans le cas des courbes ($r = 2$) a été approfondie notamment par Gekeler dans [Gek86a, Gek86b] (on pourra consulter aussi [GR96, Gek01] pour un panorama).

1.4.1 Modules de Drinfeld sur un schéma

Soient S un A-schéma et $\gamma : A \to \mathcal{O}_S$ l'homomorphisme associé. Soit r un entier ≥ 1. Un *A-module de Drinfeld sur S de rang r* est un couple $(\mathcal{L}, \phi)$ où $\mathcal{L}$ est un $\mathbf{F}_q$-fibré en droites sur S et

$$\begin{array}{rcl} \phi : A & \longrightarrow & \mathrm{End}_{\mathbf{F}_q,S}(\mathcal{L}) \\ a & \longmapsto & \phi_a \end{array}$$

est un homomorphisme d'anneaux $\mathbf{F}_q$-linéaire à valeurs dans l'anneau des endomorphismes $\mathbf{F}_q$-linéaires de $\mathcal{L}$ sur S vérifiant :

(i) pour tout corps F et tout homomorphisme de A-schémas $\mathrm{Spec}(F) \to S$, l'application induite $A \to \mathrm{End}_{\mathbf{F}_q,S}(\mathcal{L}_F)$ est un module de Drinfeld sur F de rang r (où $\mathcal{L}_F$ désigne le tiré-en-arrière de $\mathcal{L}$ par $\mathrm{Spec}(F) \to S$) ;

(ii) pour tout $a \in A$, la dérivée de ϕ_a dans l'espace tangent de $\mathcal{L}$ en la section nulle est la multiplication par $\gamma(a)$.

Si S est le spectre d'un corps, on retrouve la définition classique. Un *morphisme de modules de Drinfeld* de $(\mathcal{L}, \phi)$ dans $(\mathcal{L}', \phi')$ est un homomorphisme $\mathcal{L} \to \mathcal{L}'$ compatible aux actions de A données par ϕ et ϕ'. Si $\mathfrak{n}$ est un idéal de A, le *schéma de $\mathfrak{n}$-torsion* $\phi[\mathfrak{n}]$ est l'intersection schématique des noyaux de $\phi_a : \mathcal{L} \to \mathcal{L}$ pour tout $a \in \mathfrak{n}$. C'est un S-schéma en groupes plat, fini sur S de rang $\#(A/\mathfrak{n})^r$ et étale en dehors du support de $\mathfrak{n}$.

1.4.2 Courbes modulaires de Drinfeld $X_0(\mathfrak{n})$ et $X_1(\mathfrak{n})$

Pour la construction des schémas de modules classifiant les modules de Drinfeld de rang r sur un schéma munis d'une structure de niveau $\mathfrak{n}$, on consultera les références citées précédemment. Dans la suite de ce texte, nous nous intéresserons aux courbes modulaires $X_0(\mathfrak{n})$ et $X_1(\mathfrak{n})$, dont nous rappelons maintenant les propriétés.

Si $E = (\mathcal{L}, \phi)$ est un module de Drinfeld sur S, suivant Drinfeld et [KM85], un *sous-groupe cyclique de E d'ordre* $\mathfrak{n}$ est un sous-schéma en groupes C de $\phi[\mathfrak{n}]$ tel qu'il existe un changement de base, fini et fidèlement plat $T \to S$, et un point $P \in (\mathcal{L} \times_S T)(T)$ tel que sur $\mathcal{L} \times_S T$, on ait l'égalité de diviseurs de Cartier : $C_T = \sum_{a \in A/\mathfrak{n}} [aP]$.

Considérons le foncteur, de la catégorie des A-schémas dans celle des ensembles, qui à un A-schéma S associe l'ensemble des classes d'isomorphisme de couples (E, C), où E est un module de Drinfeld sur S de rang 2 et C un sous-schéma en groupes fini et plat de $\phi[\mathfrak{n}]$, de rang constant égal à $\#A/\mathfrak{n}$ sur S et cyclique (on appellera C une *structure de niveau* $\Gamma_0(\mathfrak{n})$ *sur* E). Ce foncteur possède un schéma de modules grossier $Y_0(\mathfrak{n})$ sur A, qui est affine et de type fini sur A, de dimension relative pure 1.

En particulier, si L est un corps de A-caractéristique disjointe de $\mathfrak{n}$, $Y_0(\mathfrak{n})(L)$ est en bijection avec l'ensemble des classes de L^{alg}-isomorphisme de couples (ϕ, u) où ϕ est un A-module de Drinfeld sur L de rang 2 et u est une $\mathfrak{n}$-isogénie cyclique L-rationnelle de ϕ.

Si $E = (\mathcal{L}, \phi)$ est un module de Drinfeld sur S, un *point d'ordre exactement* $\mathfrak{n}$ *de* E est un homomorphisme de A-modules $P : A/\mathfrak{n} \to \mathcal{L}(S)$ tel que le diviseur de Cartier effectif $\sum_{a \in A/\mathfrak{n}} [P(a)]$ est un sous-schéma en groupes de $\phi[\mathfrak{n}]$.

Considérons le foncteur, qui à un A-schéma S associe l'ensemble des classes d'isomorphisme de couples (E, P), où E est un module de Drinfeld sur S de rang 2 et P un point d'ordre exactement $\mathfrak{n}$ de E. Ce foncteur possède un schéma de modules grossier $Y_1(\mathfrak{n})$ sur A, qui est affine et de type fini sur A, de dimension relative pure 1.

En particulier, si L est un corps de A-caractéristique disjointe de $\mathfrak{n}$, $Y_1(\mathfrak{n})(L)$ est en bijection avec l'ensemble des classes de L^{alg}-isomorphisme de (ϕ, P) où ϕ est un A-module de Drinfeld sur L de rang 2 et $P \in {}^{\phi}L$ est un point de torsion L-rationnel d'ordre $\mathfrak{n}$.

On dispose d'une construction de $Y_0(\mathfrak{n})$ et $Y_1(\mathfrak{n})$ comme variétés analytiques rigides sur $\mathbf{C}_\infty$. Le demi-plan de Drinfeld $\mathcal{H}$ a une structure naturelle d'espace analytique rigide, connexe et lisse. L'action par transformations linéaires d'un sous-groupe de congruence Γ de $\mathrm{GL}(2, A)$ sur $\mathcal{H}$ donne un espace quotient $\Gamma \backslash \mathcal{H}$, qui est un espace analytique rigide sur $\mathbf{C}_\infty$ de dimension 1, connexe et lisse. On a un isomorphisme d'espaces analytiques rigides $\Gamma_i(\mathfrak{n}) \backslash \mathcal{H} \simeq Y_i(\mathfrak{n})^{\mathrm{an}}_{\mathbf{C}_\infty}$, où $Y_i(\mathfrak{n})^{\mathrm{an}}_{\mathbf{C}_\infty}$ désigne l'analytifiée de $Y_i(\mathfrak{n})$ sur $\mathbf{C}_\infty$ et $i \in \{0, 1\}$.

Des résultats de Drinfeld [Dri74], on déduit des compactifications $\mathcal{M}_0(\mathfrak{n})$ et $\mathcal{M}_1(\mathfrak{n})$ de $Y_0(\mathfrak{n})$ et $Y_1(\mathfrak{n})$ ayant les propriétés suivantes.

Théorème 1.22 (Drinfeld)**.** *Soit $i \in \{0, 1\}$.*

(i) L'ensemble $\mathcal{M}_i(\mathfrak{n}) - Y_i(\mathfrak{n})$ est fini sur A. On l'appelle ensemble des pointes de $\mathcal{M}_i(\mathfrak{n})$.

(ii) Le schéma $\mathcal{M}_i(\mathfrak{n})$ est propre, normal, plat et irréductible, de dimension relative 1 *sur* $\mathrm{Spec}(A)$.

(iii) Notons $X_i(\mathfrak{n})$ le schéma $\mathcal{M}_i(\mathfrak{n})_{A[1/\mathfrak{n}]}$. Le morphisme structurel $X_i(\mathfrak{n}) \to \mathrm{Spec}(A[1/\mathfrak{n}])$ est lisse et propre.

(iv) Le schéma $X_i(\mathfrak{n})_K$ est une courbe géométriquement connexe, lisse et propre sur K.

On trouvera une démonstration détaillée de la lissité dans [Tae06] 5.5.2.

Lorsque $\mathfrak{n}$ est un idéal premier, l'ensemble $X_0(\mathfrak{n})_K - Y_0(\mathfrak{n})_K$ est formé de deux pointes, notées 0 et ∞.

La courbe $X_0(\mathfrak{n})_K$ étant lisse, ses genres arithmétique et géométrique coïncident, et sont invariants par extension de corps de K. Cette quantité est appelée le genre de $X_0(\mathfrak{n})$, sans référence au corps de base, et notée $g(X_0(\mathfrak{n}))$. Les formules suivantes ont été obtenues par Gekeler.

Proposition 1.23 ([Gek80] Satz 3.4.18, [Gek01] §8)**.** *Si $\mathfrak{n}$ est premier, on a*

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

Chapitre 2

Symboles modulaires de Teitelbaum

2.1 Formes automorphes et arbre de Bruhat-Tits (rappels)

2.1.1 L'arbre de Bruhat-Tits de $\mathrm{PGL}(2, K_\infty)$

Notre présentation suit [Ser77] et [GR96] § 1.5 et 1.6. Commençons par quelques définitions et notations relatives aux graphes combinatoires. L'ensemble des sommets d'un graphe $\mathscr{G}$ est noté $X(\mathscr{G})$ et celui de ses arêtes orientées $Y(\mathscr{G})$. Si e est une arête orientée d'un graphe, $\overline{e}$ désigne l'arête opposée, $o(e)$ l'origine de e et $t(e)$ son extrémité. Un *chemin* d'un graphe est une suite d'arêtes adjacentes. Un *aller-retour* dans un chemin est un couple d'arêtes adjacentes de la forme $(e, \overline{e})$. Enfin, une *géodésique* est un chemin sans aller-retour.

On note $\mathbf{Z}[X(\mathscr{G})]$ (resp. $\mathbf{Z}[Y(\mathscr{G})]$) le groupe libre engendré par les sommets (resp. les arêtes orientées) de $\mathscr{G}$. L'application $e \mapsto (t(e)) - (o(e))$ s'étend linéairement en un homomorphisme de bord $\partial : \mathbf{Z}[Y(\mathscr{G})] \to \mathbf{Z}[X(\mathscr{G})]$ qui passe au quotient en

$$\overline{\partial} : \mathbf{Z}[Y(\mathscr{G})]/\mathbf{Z}[(e) + (\overline{e}) \mid e \in Y(\mathscr{G})] \longrightarrow \mathbf{Z}[X(\mathscr{G})].$$

Le premier groupe d'homologie $H_1(\mathscr{G}, \mathbf{Z})$ du graphe est le noyau de $\overline{\partial}$. Ses éléments sont appelés les *cycles* de $\mathscr{G}$. Plus généralement, si $\mathscr{S}$ est un sous-graphe de $\mathscr{G}$, le premier groupe d'homologie relative $H_1(\mathscr{G}, \mathscr{S}, \mathbf{Z})$ est le noyau de l'application déduite de ∂

$$\mathbf{Z}[Y(\mathscr{G})]/\mathbf{Z}[Y(\mathscr{S}), (e) + (\overline{e}) \mid e \in Y(\mathscr{G})] \longrightarrow \mathbf{Z}[X(\mathscr{G})]/\mathbf{Z}[X(\mathscr{S})].$$

L'arbre de Bruhat-Tits. L'arbre de Bruhat-Tits de $\mathrm{PGL}(2, K_\infty)$ possède une description classique par des classes d'homothétie de certains réseaux de K_∞^2 ([Ser77] II.1). Pour nos besoins, nous rappelons la description en termes d'espaces quotients de matrices de $\mathrm{GL}(2, K_\infty)$ qui s'en déduit.

***Notation* 2.1.** Soit G le schéma en groupes GL(2). Soit $\mathcal{I}$ le *sous-groupe d'Iwahori* de $\mathrm{G}(K_\infty)$ défini par

$$\mathcal{I} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{G}(O_\infty) \mid c \equiv 0 \mod \pi \right\}.$$

On pose

$$\begin{aligned} X(\mathcal{T}) &= \mathrm{G}(K_\infty)/\mathrm{G}(O_\infty)\mathrm{Z}(K_\infty) \\ Y(\mathcal{T}) &= \mathrm{G}(K_\infty)/\mathcal{I}\mathrm{Z}(K_\infty). \end{aligned}$$

Définition 2.2. L'*arbre de Bruhat-Tits* $\mathcal{T}$ de $\mathrm{PGL}(2, K_\infty)$ est le graphe combinatoire défini de la façon suivante :

(i) l'ensemble de ses sommets est $X(\mathcal{T})$;

(ii) l'ensemble de ses arêtes orientées est $Y(\mathcal{T})$;

(iii) l'application $e \mapsto o(e)$ est l'application canonique $Y(\mathcal{T}) \to X(\mathcal{T})$;

(iv) l'application $e \mapsto \overline{e}$ est l'application $X(\mathcal{T}) \to X(\mathcal{T})$ définie par $g \mapsto g\left(\begin{smallmatrix} 0 & 1 \\ \pi & 0 \end{smallmatrix}\right)$.

C'est un arbre c'est-à-dire un graphe infini connexe sans circuit ([Ser77] II.1.1). En particulier, il existe une unique géodésique reliant deux sommets donnés. L'arbre $\mathcal{T}$ est $(q+1)$-régulier, c'est-à-dire que de chaque sommet partent $q+1$ arêtes. Il est muni d'une action transitive de $\mathrm{G}(K_\infty)$. C'est un cas particulier de la notion d'immeuble associé aux groupes algébriques semisimples sur un corps local par Bruhat et Tits. La théorie des modules de Drinfeld de rang $r \geq 2$ fait intervenir l'immeuble de $\mathrm{PGL}(2, K_\infty)$.

Les bouts de l'arbre $\mathcal{T}$. Une *demi-droite* de $\mathcal{T}$ est un sous-graphe de $\mathcal{T}$ isomorphe à $\bullet$ —— $\bullet$ —— $\bullet$ —— $\cdots$. Un *bout* de $\mathcal{T}$ est une classe d'équivalence de demi-droites de $\mathcal{T}$, où deux demi-droites sont dites équivalentes si elles diffèrent d'un graphe fini. L'ensemble des bouts de $\mathcal{T}$ est noté $\mathrm{Bouts}(\mathcal{T})$.

Soit s un bout de $\mathcal{T}$. On choisit une demi-droite le représentant ; elle est donnée par des sommets adjacents correspondant aux classes de matrices $\left(\left(\begin{smallmatrix} a_k & b_k \\ c_k & d_k \end{smallmatrix}\right)\right)_{k\geq 0}$ dans $\mathrm{G}(K_\infty)$. On a alors une bijection

$$\begin{array}{rcl} \mathrm{Bouts}(\mathcal{T}) & \xrightarrow{\sim} & \mathbf{P}^1(K_\infty) \\ s & \longmapsto & \left(\bigcap_{k\geq 0}(d_k - c_k)O_\infty \oplus (a_k - b_k)O_\infty\right) K_\infty \end{array}$$

qui est indépendante du choix des représentants, et compatible à l'action de $\mathrm{G}(K_\infty)$. Par cette bijection, l'image de $\infty = (1:0) \in \mathbf{P}^1(K_\infty)$ (resp. $0 \in \mathbf{P}^1(K_\infty)$) est le bout défini par la demi-droite $\left(\left(\begin{smallmatrix} \pi^k & 0 \\ 0 & 1 \end{smallmatrix}\right)\right)_{k\geq 0}$ (resp. $\left(\left(\begin{smallmatrix} \pi^k & 0 \\ 0 & 1 \end{smallmatrix}\right)\right)_{k\leq 0}$). On appelle *bout rationnel* de $\mathcal{T}$ un bout dont l'image par la bijection est un élément de $\mathbf{P}^1(K)$.

Des systèmes de représentants de $X(\mathcal{T})$ et $Y(\mathcal{T})$. On dit qu'une arête orientée e *pointe* vers un bout de $\mathcal{T}$ s'il existe une demi-droite passant par e et représentant ce bout. Le bout ∞ définit une orientation de l'arbre, c'est-à-dire une décomposition $Y(\mathcal{T}) = Y^+ \sqcup Y^-$ avec $\overline{Y^+} = Y^-$. Une arête orientée e est dans Y^+ (*positive*) si elle pointe vers ∞ ; sinon elle est dans Y^- (*négative*). On a alors une bijection

$$\begin{array}{rcl} X(\mathcal{T}) & \xrightarrow{\sim} & Y^+ \\ v & \longmapsto & \text{l'unique arête positive d'origine } v. \end{array}$$

L'énoncé suivant est un résultat classique.

Lemme 2.3. *(i) Les matrices* $\left(\begin{smallmatrix}\pi^k & u\\ 0 & 1\end{smallmatrix}\right) \in \mathrm{G}(K_\infty)$*, pour* $k \in \mathbf{Z}$ *et* $u \in K_\infty$*,* $u \bmod \pi^k O_\infty$*, forment un système de représentants de* $X(\mathcal{T})$ *et de* Y^+*.*

(ii) Les matrices $\left(\begin{smallmatrix}\pi^k & u\\ 0 & 1\end{smallmatrix}\right)\left(\begin{smallmatrix}0 & 1\\ \pi & 0\end{smallmatrix}\right) \in \mathrm{G}(K_\infty)$*, pour* $k \in \mathbf{Z}$ *et* $u \in K_\infty$*,* $u \bmod \pi^k O_\infty$*, forment un système de représentants de* Y^-*.*

Le graphe $\Gamma\backslash\mathcal{T}$. Soit Γ un sous-groupe de congruence de $\mathrm{G}(A) = \mathrm{GL}(2, A)$. L'action de Γ sur l'arbre $\mathcal{T}$ est sans inversion ([Ser77] II.1.2 et II.1.3). De ce fait, on peut considérer le graphe quotient $\Gamma\backslash\mathcal{T}$, dont les sommets sont les classes d'équivalence $X(\Gamma\backslash\mathcal{T}) = \Gamma\backslash X(\mathcal{T})$ et les arêtes orientées les classes $Y(\Gamma\backslash\mathcal{T}) = \Gamma\backslash Y(\mathcal{T})$.

Si $\Gamma = \mathrm{G}(A)$, le graphe obtenu est de la forme $\bullet$ —— $\bullet$ —— $\bullet$ —— $\cdots$ et ses sommets et arêtes positives sont représentés par les matrices $\left(\begin{smallmatrix}\pi^{-k} & 0\\ 0 & 1\end{smallmatrix}\right)$, pour $k \geq 0$. Pour $k \geq 0$, un sommet (resp. une arête) de $\mathcal{T}$ est dite *de type* k si son image dans $\mathrm{GL}(2, A)\backslash\mathcal{T}$ est le sommet (resp. l'arête) représenté par la matrice $\left(\begin{smallmatrix}\pi^{-k} & 0\\ 0 & 1\end{smallmatrix}\right)$.

Revenons au cas où Γ est un sous-groupe de congruence de $\mathrm{G}(A)$. La structure du graphe quotient est la suivante

$$\Gamma\backslash\mathcal{T} = (\Gamma\backslash\mathcal{T})^0 \cup \bigcup_i h_i$$

où $(\Gamma\backslash\mathcal{T})^0$ est un graphe fini et les h_i sont des demi-droites disjointes, en nombre fini ([Ser77] II.2.3 th. 9 et II.2.8 p. 172). De plus, la réunion est disjointe sur les arêtes et $(\Gamma\backslash\mathcal{T})^0$ n'a qu'un sommet en commun avec chaque demi-droite. Ces demi-droites h_i sont en bijection avec les classes de bouts rationnels modulo Γ, c'est-à-dire $\Gamma\backslash\mathbf{P}^1(K)$. On les appelle les *pointes de* $\Gamma\backslash\mathcal{T}$ et on note leur ensemble ptes. La détermination explicite de tels « domaines fondamentaux » $\Gamma\backslash\mathcal{T}$ a été étudiée dans [Gek85, GN95].

Correspondances sur $Y(\Gamma_0(\mathfrak{n})\backslash\mathcal{T})$. Soit $\mathfrak{m}$ un idéal non nul de A, de générateur unitaire m. La double classe $\Gamma_0(\mathfrak{n})\left(\begin{smallmatrix}m & 0\\ 0 & 1\end{smallmatrix}\right)\Gamma_0(\mathfrak{n})$ est une réunion disjointe d'un nombre fini de classes à gauche pour $\Gamma_0(\mathfrak{n})$. Soit $R_{\mathfrak{n},\mathfrak{m}}$ un ensemble de représentants de ces classes à gauche. On définit la correspondance $\tau_\mathfrak{m}$ comme la somme formelle d'arêtes de $\Gamma_0(\mathfrak{n})\backslash\mathcal{T}$

$$\tau_\mathfrak{m}(\tilde{e}) = \sum_{g \in R_{\mathfrak{n},\mathfrak{m}}} \widetilde{ge},$$

où $e \in Y(\mathcal{T})$ est d'image $\tilde{e}$ dans $\Gamma_0(\mathfrak{n})\backslash\mathcal{T}$. Un système de représentants $R_{\mathfrak{n},\mathfrak{m}}$ est par exemple l'ensemble de matrices

$$\left\{\begin{pmatrix}a & b\\ 0 & d\end{pmatrix} \in \mathrm{GL}_2(K) \mid a, b, d \in A, (ad) = \mathfrak{m}, (a) + \mathfrak{n} = A, \deg b < \deg d, a \text{ et } d \text{ unitaires}\right\}.$$

Les correspondances $\tau_\mathfrak{m}$ satisfont aux propriétés usuelles suivantes :

(i) elles commutent deux à deux ;

(ii) pour $(\mathfrak{m}, \mathfrak{m}') = 1$, on a $\tau_\mathfrak{m}\tau_{\mathfrak{m}'} = \tau_{\mathfrak{m}\mathfrak{m}'}$;

(iii) pour $\mathfrak{p}$ premier et $i \geq 0$, on a

$$\begin{array}{ll} \text{si } (\mathfrak{p}, \mathfrak{n}) = 1 & \tau_{\mathfrak{p}^i}\tau_\mathfrak{p} = \tau_{\mathfrak{p}^{i+1}} + q^{\deg \mathfrak{p}}\tau_{\mathfrak{p}^{i-1}} \\ \text{si } (\mathfrak{p}, \mathfrak{n}) \neq 1 & \tau_{\mathfrak{p}^i} = (\tau_\mathfrak{p})^i \end{array}$$

2.1.2 Cochaînes harmoniques sur l'arbre $\mathcal{T}$

Définition 2.4. Soient R un groupe abélien et Γ un sous-groupe de $\mathrm{G}(A)$. Une *cochaîne harmonique parabolique pour* Γ sur $\mathcal{T}$ à valeurs dans R est une fonction $F : Y(\mathcal{T}) \to R$ vérifiant les conditions suivantes :

(i) F est *alternée* : $F(e) + F(\overline{e}) = 0$ pour tout $e \in Y(\mathcal{T})$;

(ii) F est *harmonique* : $\displaystyle\sum_{\substack{e \in Y(\mathcal{T}) \\ o(e)=v}} F(e) = 0$ pour tout $v \in X(\mathcal{T})$;

(iii) F est invariante par Γ : $F(\gamma e) = F(e)$ pour tout $\gamma \in \Gamma$, $e \in Y(\mathcal{T})$;

(iv) F est à support fini dans le graphe quotient $\Gamma\backslash\mathcal{T}$.

On notera $\underline{H}_!(\mathcal{T}, R)^\Gamma$ le groupe abélien formé des cochaînes harmoniques paraboliques pour Γ à valeurs dans R. La formation de $\underline{H}_!(\mathcal{T}, R)^\Gamma$ commute aux extensions d'anneaux plates. En particulier, les homomorphismes canoniques

$$\begin{array}{ccc} \underline{H}_!(\mathcal{T}, \mathbf{Z})^\Gamma \otimes_{\mathbf{Z}} \mathbf{Q} & \xrightarrow{\sim} & \underline{H}_!(\mathcal{T}, \mathbf{Q})^\Gamma \\ \underline{H}_!(\mathcal{T}, \mathbf{Z})^\Gamma \otimes_{\mathbf{Z}} \mathbf{C} & \xrightarrow{\sim} & \underline{H}_!(\mathcal{T}, \mathbf{C})^\Gamma \end{array}$$

sont des isomorphismes.

***Notation* 2.5.** On pose $\mathbf{H} = \underline{H}_!(\mathcal{T}, \mathbf{Z})^{\Gamma_0(\mathfrak{n})}$ et $\mathbf{H}(R) = \underline{H}_!(\mathcal{T}, R)^{\Gamma_0(\mathfrak{n})}$.

Cochaînes paraboliques pour Γ et cycles de $\Gamma\backslash\mathcal{T}$ ([GR96] §3)

Si v (resp. e) est un sommet (resp. une arête) de $\mathcal{T}$, on note Γ_v (resp. Γ_e) le stabilisateur de v (resp. e) dans Γ. Ce sont des groupes finis. Soit v un sommet de $\mathcal{T}$, d'image $\tilde{v}$ dans $\Gamma\backslash\mathcal{T}$. Le groupe Γ_v agit sur l'ensemble des arêtes de $\mathcal{T}$ d'origine v et les orbites correspondent aux arêtes de $\Gamma\backslash\mathcal{T}$ d'origine $\tilde{v}$. Si e est une arête d'origine v, le cardinal de l'orbite correspondante sous Γ_v est $m(e) = [\Gamma_v : \Gamma_e]$.

Une cochaîne F pour Γ peut être vue comme une fonction sur $Y(\Gamma\backslash\mathcal{T})$. Elle est alternée, et la condition d'harmonicité devient

$$\sum_{\substack{\tilde{e} \in Y(\Gamma\backslash\mathcal{T}) \\ o(\tilde{e})=\tilde{v}}} m(\tilde{e}) F(\tilde{e}) = 0 \qquad (\tilde{v} \in X(\Gamma\backslash\mathcal{T})). \tag{2.1}$$

De plus, si R est sans torsion, F s'annule sur les pointes de $\Gamma\backslash\mathcal{T}$ ([GR96] prop. 3.1.4).

Considérons l'application qui à un cycle $c \in H_1(\Gamma\backslash\mathcal{T}, \mathbf{Z})$ associe la fonction

$$\begin{array}{rcl} Y(\Gamma\backslash\mathcal{T}) & \longrightarrow & \mathbf{Z} \\ e & \longmapsto & \mathrm{mult}_c(e) - \mathrm{mult}_c(\overline{e}). \end{array}$$

Soit $\underline{H}_!(\Gamma\backslash\mathcal{T}, \mathbf{Z})$ le groupe des fonctions $Y(\Gamma\backslash\mathcal{T}) \to \mathbf{Z}$ à support compact vérifiant les conditions d'alternance et d'harmonicité dans $\Gamma\backslash\mathcal{T}$. L'application précédente donne par linéarité un isomorphisme de groupes

$$H_1(\Gamma\backslash\mathcal{T}, \mathbf{Z}) \xrightarrow{\sim} \underline{H}_!(\Gamma\backslash\mathcal{T}, \mathbf{Z}). \tag{2.2}$$

Par ailleurs, l'homomorphisme de groupes

$$\begin{array}{rcl} \underline{H}_!(\Gamma\backslash\mathcal{T},\mathbf{Z}) & \longrightarrow & \underline{H}_!(\mathcal{T},\mathbf{Z})^\Gamma \\ \varphi & \longmapsto & (e\mapsto n(e)\varphi(\tilde{e})), \end{array} \tag{2.3}$$

où $n(e)=[\Gamma_e:\Gamma\cap \mathrm{Z}(K)]$, est injectif de conoyau fini. C'est même un isomorphisme lorsque le sous-groupe de congruence est $\Gamma(\mathfrak{n})$ ([GR96] 3.4.5), $\Gamma_0(\mathfrak{n})$ ou $\Gamma_1(\mathfrak{n})$ ([GN95] 3.3. et 5.4).

En particulier, le groupe $\underline{H}_!(\mathcal{T},\mathbf{Z})^{\Gamma_0(\mathfrak{n})}$ est abélien et libre de rang g, où g est le genre de $\Gamma_0(\mathfrak{n})\backslash\mathcal{T}$, qui est égal à $\dim_{\mathbf{Q}}(\Gamma_0(\mathfrak{n})^{\mathrm{ab}}\otimes_{\mathbf{Z}}\mathbf{Q})$. Par ailleurs, d'après le théorème 2 de [Dri74], ce rang coïncide avec $g(X_0(\mathfrak{n}))$.

Les cochaînes harmoniques comme formes automorphes ([GR96], §4)

Notons $\mathbf{A}$ l'anneau des adèles de K et $\mathbf{O}$ son anneau des entiers. Soient $\mathcal{K}$ un sous-groupe ouvert de $\mathrm{G}(\mathbf{O})$ et F un corps de caractéristique zéro. Une fonction

$$\varphi:\mathrm{G}(K)\backslash\mathrm{G}(\mathbf{A})/\mathcal{K}\longrightarrow F$$

est appelée *forme automorphe parabolique pour $\mathcal{K}$ à valeurs dans F* si pour presque tout $\underline{g}\in\mathrm{G}(\mathbf{A})$, on a $\displaystyle\int_{K\backslash\mathbf{A}}\varphi\left(\begin{pmatrix}1&\underline{x}\\0&1\end{pmatrix}\underline{g}\right)d\underline{x}=0$, où $d\underline{x}$ est une mesure de Haar sur $K\backslash\mathbf{A}$.

La place non-archimédienne ∞ étant fixée, on a des décompositions en parties « finies » et « infinies »

$$\mathbf{A}=\mathbf{A}_f\times K_\infty\quad \mathbf{O}=\mathbf{O}_f\times O_\infty\quad \mathbf{A}^\times=\mathbf{A}_f^\times\times K_\infty^\times.$$

Nous nous intéressons aux formes automorphes paraboliques invariantes sous $\mathrm{Z}(K_\infty)$. On peut les voir comme des fonctions sur

$$Y(\mathcal{K}):=\mathrm{G}(K)\backslash\mathrm{G}(\mathbf{A})/\mathcal{K}\mathrm{Z}(K_\infty).$$

Supposons que $\mathcal{K}$ admette une décomposition en produit de sous-groupes $\mathcal{K}_f\times\mathcal{K}_\infty$ avec $\mathcal{K}_f\subset\mathrm{G}(\mathbf{O}_f)$ et $\mathcal{K}_\infty\subset\mathrm{G}(O_\infty)$. D'après le théorème d'approximation forte pour $\mathrm{SL}(2)$, le déterminant induit une bijection

$$\mathrm{G}(K)\backslash\mathrm{G}(\mathbf{A}_f)/\mathcal{K}_f\xrightarrow{\sim}K^\times\backslash\mathbf{A}_f^\times/\det\mathcal{K}_f.$$

Soit S un système de représentants de l'ensemble fini $\mathrm{G}(K)\backslash\mathrm{G}(\mathbf{A}_f)/\mathcal{K}_f$. Tout élément $\underline{g}$ de $\mathrm{G}(\mathbf{A})$ s'écrit $\underline{g}=\gamma\underline{x}\underline{k}g_\infty$ avec $\gamma\in\mathrm{G}(K)$, $\underline{x}\in S$, $\underline{k}\in\mathcal{K}_f$ et $g_\infty\in\mathrm{G}(K_\infty)$. Posons $\Gamma_{\underline{x}}=\mathrm{G}(K)\cap\underline{x}\mathcal{K}_f\underline{x}^{-1}\subset\mathrm{G}(\mathbf{A}_f)$. La projection sur la composante à l'infini induit une application

$$\begin{array}{rcl} Y(\mathcal{K}) & \longrightarrow & \Gamma_{\underline{x}}\backslash\mathrm{G}(K_\infty)/\mathcal{K}_\infty\mathrm{Z}(K_\infty) \\ \underline{g} & \longmapsto & g_\infty \end{array}$$

qui est bien définie et donne une bijection

$$Y(\mathcal{K})\simeq\bigsqcup_{\underline{x}\in S}\Gamma_{\underline{x}}\backslash\mathrm{G}(K_\infty)/\mathcal{K}_\infty\mathrm{Z}(K_\infty).$$

Posons désormais $\mathcal{K} = \mathcal{K}_f \times \mathcal{I}$ où $\mathcal{I}$ est le sous-groupe d'Iwahori. On a alors une identification

$$Y(\mathcal{K}_f \times I) \simeq \bigsqcup_{\underline{x} \in S} Y(\Gamma_{\underline{x}} \backslash \mathcal{T}). \tag{2.4}$$

En particulier, si Γ est le sous-groupe $\Gamma_0(\mathfrak{n})$ et si

$$\mathcal{K}_f = \mathcal{K}_0(\mathfrak{n})_f = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G(\mathbf{O}_f) \mid c \in \mathfrak{n} \right\},$$

on identifie $Y(\mathcal{K}_0(\mathfrak{n})_f \times \mathcal{I})$ aux arêtes $Y(\Gamma_0(\mathfrak{n}) \backslash \mathcal{T})$. En effet, dans ce cas, $\det(\mathcal{K}_0(\mathfrak{n})_f) = \mathbf{O}_f^\times$ et $K^\times \backslash \mathbf{A}_f^\times / \mathbf{O}_f^\times$ est canoniquement isomorphe au groupe des classes de $A = \mathbf{F}_q[T]$, qui est trivial. Les cochaînes harmoniques paraboliques pour $\Gamma_0(\mathfrak{n})$ à valeurs dans F sont alors des formes automorphes paraboliques $\mathrm{G}(K) \backslash \mathrm{G}(\mathbf{A}) / \mathcal{K}_0(\mathfrak{n})_f \times \mathrm{Z}(K_\infty)\mathcal{I} \to F$. Pour cette raison, on appellera dans ce texte *formes automorphes* les cochaînes harmoniques paraboliques pour $\Gamma_0(\mathfrak{n})$.

Parmi ces formes automorphes, il est naturel de se demander lesquelles correspondent aux cochaînes harmoniques. Soit $V_{\mathrm{sp},F}$ l'espace de fonctions

$$\{f : \mathbf{P}^1(K_\infty) \to F \mid f \text{ localement constante}\} \text{ modulo } F.$$

La *représentation spéciale* $\rho_{\mathrm{sp},F} : \mathrm{G}(K_\infty) \to \mathrm{GL}(V_{\mathrm{sp},F})$ de $\mathrm{G}(K_\infty)$ est celle donnée par l'action par translation à droite. Elle est irréductible. Soit $W_{\mathrm{sp}}(\mathcal{K}, F)$ l'espace des formes automorphes paraboliques

$$\varphi : \mathrm{G}(K) \backslash \mathrm{G}(\mathbf{A}) / \mathcal{K}_f \times \mathrm{Z}(K_\infty)\mathcal{I} \longrightarrow F$$

telles que la représentation de $\mathrm{G}(K_\infty)$ associée à φ soit isomorphe à une somme finie de copies de $\rho_{\mathrm{sp},F}$. Sous la bijection (2.4), l'espace de cochaînes harmoniques paraboliques $\oplus_{\underline{x} \in S} \underline{H}_!(\mathcal{T}, F)^{\Gamma_{\underline{x}}}$ s'identifie à $W_{\mathrm{sp}}(\mathcal{K}, F)$ ([Dri74], prop. 10.3). En particulier, $\mathbf{H}(F)$ s'identifie à $W_{\mathrm{sp}}(\mathcal{K}_0(\mathfrak{n})_f \times \mathcal{I}, F)$.

Le développement de Fourier des formes automorphes

Nous rappelons le développement d'une forme automorphe à valeurs dans $\mathbf{C}$, en suivant Weil et Gekeler [Wei71, Gek80, Gek95b]. Soient B le sous-groupe de Borel des matrices triangulaires supérieures dans G et $\Gamma_\infty = \mathrm{B}(A)$. Ce dernier est le stabilisateur du bout ∞ dans $\mathrm{G}(K_\infty)$ et il agit sur l'arbre de Bruhat-Tits sans inversion et en conservant l'orientation donnée par ce bout. On a donc un graphe quotient $\Gamma_\infty \backslash \mathcal{T}$, d'arêtes $Y(\Gamma_\infty \backslash \mathcal{T}) \simeq \Gamma_\infty \backslash \mathrm{G}(K_\infty) / \mathcal{I}\mathrm{Z}(K_\infty)$.

Nous nous plaçons dans un cadre un peu plus général, en étudiant le développement d'une fonction

$$F : Y^+(\Gamma_\infty \backslash \mathcal{T}) \longrightarrow \mathbf{C}.$$

Une forme automorphe pour $\Gamma_0(\mathfrak{n})$ rentre dans ce cadre, puisque $\Gamma_\infty \subset \Gamma_0(\mathfrak{n})$ et qu'une telle application est déterminée par sa restriction aux arêtes positives. Le théorème d'approximation forte donne l'isomorphisme

$$Y^+(\Gamma_\infty \backslash \mathcal{T}) \simeq \mathrm{B}(K) \backslash \mathrm{B}(\mathbf{A}) / \mathrm{B}(\mathbf{O})\mathrm{Z}(\mathbf{A}).$$

La fonction F est alors déterminée par sa restriction aux matrices $\left(\begin{smallmatrix} x & y \\ 0 & 1 \end{smallmatrix}\right)$ de $\mathrm{B}(\mathbf{A})$. On pose $F(\underline{x}, \underline{y}) = F(\left(\begin{smallmatrix} \underline{x} & \underline{y} \\ 0 & 1 \end{smallmatrix}\right))$. Soit ψ un caractère additif non trivial fixé de $\mathbf{A}/K$. Il lui est associé un idèle différentiel δ par la formule $\delta_v = \pi_v^{\mathrm{ord}_v(\psi)}$, pour toute place v de K. Les coefficients de Fourier de F sont définis par :

$$c_0(\underline{x}) = \int_{\mathbf{A}/K} F(\underline{x}, \underline{y}) d\underline{y} \quad \text{et} \quad c(\underline{x}) = \int_{\mathbf{A}/K} F(d^{-1}\underline{x}, \underline{y}) \psi(-\underline{y}) d\underline{y}$$

où $d\underline{y}$ est une mesure de Haar sur $\mathbf{A}/K$ normalisée de telle sorte que $\mathrm{vol}_{d\underline{y}}(\mathbf{A}/K) = 1$. La fonction F admet alors un développement en série de Fourier :

$$F(\underline{x}, \underline{y}) = c_0(\underline{x}) + \sum_{\xi \in K^\times} c(\xi\delta\underline{x})\psi(\xi\underline{y}).$$

Cette série ne porte en fait que sur les $\xi \in K^\times$ tels que le diviseur associé à $\xi d\underline{x}$ est effectif. C'est donc une somme finie.

Exprimons maintenant ces données sur la composante à l'infini, c'est-à-dire en fonction des valeurs de F sur le système de représentants des arêtes de $\mathcal{T}$ donné par le lemme 2.3. Soit η_0 un caractère additif fixé non trivial de $\mathbf{F}_p$ et $\eta : \mathbf{A}/K \to \mathbf{C}^\times$ le caractère obtenu en composant

$$\mathbf{A}/K = \mathbf{O} + K/K \xrightarrow{\sim} \mathbf{O}/\mathbf{F}_q \xrightarrow{\mathrm{proj}} O_\infty/((\pi^2) + \mathbf{F}_q) \xrightarrow{\mathrm{res}} \mathbf{F}_q \xrightarrow{\mathrm{tr}} \mathbf{F}_p \xrightarrow{\eta_0} \mathbf{C}^\times,$$

où proj est la projection sur la composante ∞, res l'application qui à $\sum a_i\pi^i$ associe a_1 et tr la trace. L'idèle différentiel associé à η est $\delta = (1, \ldots, 1, \pi^{-2})$.

En utilisant des propriétés d'invariance des fonctions c_0 et c, les intégrales adéliques qui les définissent s'expriment alors comme sommes finies :

$$c_0(\pi^k) = \begin{cases} F(\left(\begin{smallmatrix} \pi^k & 0 \\ 0 & 1 \end{smallmatrix}\right)) & \text{si } k \leq 1 \\ q^{1-k} \sum_{y \in (\pi)/(\pi^k)} F\left(\left(\begin{smallmatrix} \pi^k & y \\ 0 & 1 \end{smallmatrix}\right)\right) & \text{si } k \geq 1. \end{cases}$$

Soit M un diviseur effectif de K (on adoptera une notation multiplicative pour de tels diviseurs). Écrivons $M = \mathrm{div}(m)\infty^{\deg M}$ où $\mathrm{div}(m)$ est le diviseur principal associé à $m \in A$ et $\deg M$ le degré de M. Par abus de notation, η désignera la restriction de η à K_∞, c'est-à-dire le caractère

$$\begin{array}{rccc} \eta : & K_\infty & \longrightarrow & \mathbf{C}^\times \\ & \sum a_i\pi^i & \longmapsto & \eta_0(\mathrm{tr}(a_1)). \end{array}$$

L'intégrale adélique pour le coefficient de Fourier devient

$$c(M) = q^{-1-\deg M} \sum_{y \in (\pi)/(\pi^{2+\deg M})} F\left(\begin{pmatrix} \pi^{2+\deg M} & y \\ 0 & 1 \end{pmatrix}\right) \eta(-my)$$

et le développement de Fourier est la somme finie suivante

$$F\left(\begin{pmatrix} \pi^k & y \\ 0 & 1 \end{pmatrix}\right) = c_0(\pi^k) + \sum_{\substack{m \in A, m \neq 0 \\ \deg m \leq k-2}} c(\mathrm{div}(m)\infty^{k-2})\eta(my).$$

Soit $\nu : K_\infty \to \mathbf{Z}$ l'application qui à $\sum a_i \pi^i$ associe -1 si $a_1 \neq 0$, et $q-1$ sinon. Les coefficients et développement de Fourier peuvent encore s'exprimer ainsi :

$$c(M) = q^{-1-\deg M}\left(F\left(\begin{pmatrix} \pi^{2+\deg M} & 0 \\ 0 & 1 \end{pmatrix}\right) + \sum_{\substack{y \in \mathbf{F}_q^\times \backslash (\pi)/(\pi^{2+\deg M}) \\ y \neq 0}} F\left(\begin{pmatrix} \pi^{2+\deg M} & y \\ 0 & 1 \end{pmatrix}\right) \nu(my) \right)$$

$$F\left(\begin{pmatrix} \pi^k & y \\ 0 & 1 \end{pmatrix}\right) = c_0(\pi^k) + \sum_{\substack{m \in A, m \text{ unitaire} \\ \deg m \leq k-2}} c(\mathrm{div}(m)\infty^{k-2})\nu(my). \tag{2.5}$$

En particulier, si F est à valeurs dans $\mathbf{Z}$, ses coefficients de Fourier sont dans $\mathbf{Z}[1/p]$. Réciproquement, si F a tous ses coefficients de Fourier dans $\mathbf{Z}[1/p]$, alors elle est à valeurs dans $\mathbf{Z}[1/p]$.

Maintenant, voyons comment se traduit l'harmonicité de F sur $\mathcal{T}$ en termes de ses coefficients.

Lemme 2.6 ([Gek95b] lemme 2.13)**.** *Soit F une fonction sur les arêtes de $\mathcal{T}$, à valeurs dans $\mathbf{C}$, alternée et invariante pour Γ_∞. Alors F est harmonique si et seulement si ses coefficients de Fourier vérifient les deux conditions suivantes :*

(i) pour tout $k \in \mathbf{Z}$, $c_0(\pi^k) = q^{-k} c_0(1)$;

(ii) pour tout diviseur effectif de la forme $M = M_f \infty^k$, $c(M) = c(M_f) q^{-k}$.

Corollaire 2.7. *Soit $F \in \mathbf{H}(\mathbf{C})$. Le coefficient de Fourier c_0 de F est identiquement nul.*

Démonstration. D'après ce qui précède, il suffit de montrer que $c_0(1) = F(\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)) = 0$. Regardons F comme une fonction sur les arêtes de $\Gamma_\infty \backslash \mathcal{T}$. Un système de représentants des arêtes positives de $\Gamma_\infty \backslash \mathcal{T}$ est donné par $\left(\begin{smallmatrix} \pi^k & u \\ 0 & 1 \end{smallmatrix}\right)$, pour $k \in \mathbf{Z}$ et $u \in ((\pi)/(\pi^k))/\mathbf{F}_q^\times$ ([Gek95b], 3.1). En particulier, le graphe $\Gamma_\infty \backslash \mathcal{T}$ est la réunion (disjointe sur les arêtes) d'un graphe infini et de la demi-droite $(\left(\begin{smallmatrix} \pi^i & 0 \\ 0 & 1 \end{smallmatrix}\right))_{i \leq 1}$. L'arête représentée par $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ est située sur cette demi-droite. En utilisant l'harmonicité de F et le fait que $\mathbf{C}$ est sans torsion, on voit que F s'annule sur cette arête. □

Le produit de Petersson

Il correspond au produit de Petersson usuel sur les formes automorphes. Soit Γ un sous-groupe de congruence de $\mathrm{GL}(2, A)$. Soit la mesure μ sur les arêtes de $\Gamma \backslash \mathcal{T}$ définie par

$$vol_\mu(\tilde{e}) = \frac{1}{n(e)} = \frac{1}{[\Gamma_e : \Gamma \cap \mathrm{Z}(K)]}$$

($\tilde{e}$ est l'image dans $Y(\Gamma \backslash \mathcal{T})$ de $e \in Y(\mathcal{T})$). Le *produit hermitien de Petersson* est alors

$$\begin{array}{ccc} \underline{H}_!(\mathcal{T}, \mathbf{C})^\Gamma \times \underline{H}_!(\mathcal{T}, \mathbf{C})^\Gamma & \longrightarrow & \mathbf{C} \\ (F, G) & \longmapsto & (F, G)_\mu = \frac{1}{2} \sum_{\tilde{e} \in \Gamma \backslash \mathcal{T}} F(\tilde{e}) \overline{G(\tilde{e})} vol_\mu(\tilde{e}). \end{array}$$

Il s'agit d'une somme finie. Sa restriction fournit une application bilinéaire sur $\underline{H}_!(\mathcal{T}, \mathbf{Q})^\Gamma$.

Les opérateurs de Hecke

Soit R un groupe abélien. Soit $\mathfrak{m}$ un idéal non nul de A. La correspondance $\tau_{\mathfrak{m}}$ sur $Y(\Gamma_0(\mathfrak{n})\backslash\mathcal{T})$ donne lieu à l'opérateur $T_{\mathfrak{m}} \in \mathrm{End}(\mathbf{H}(R))$ défini par

$$(T_{\mathfrak{m}}F)(e) = \sum_{\substack{a,b,d\in A \\ (ad)=\mathfrak{m},\ (a)+\mathfrak{n}=A \\ \deg b<\deg d,\ a \text{ et } d \text{ unitaires}}} F\left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} e\right) \qquad (e \in Y(\mathcal{T})).$$

Les opérateurs $T_{\mathfrak{m}}$ héritent des propriétés des $\tau_{\mathfrak{m}}$ (page 27). De plus, si $R = \mathbf{C}$ et $(\mathfrak{m}, \mathfrak{n}) = 1$, $T_{\mathfrak{m}}$ est hermitien pour le produit de Petersson sur $\mathbf{H}(\mathbf{C})$.

***Notation* 2.8.** La sous-algèbre commutative de $\mathrm{End}(\mathbf{H}(\mathbf{C}))$ engendrée sur $\mathbf{Z}$ par les endomorphismes $T_{\mathfrak{m}}$, pour $\mathfrak{m}$ idéal de A, est notée $\mathbf{T}$, et appelée *algèbre de Hecke*.

Elle est de rang fini et sans torsion sur $\mathbf{Z}$. Si R est un sous-anneau de $\mathbf{C}$, $\mathbf{T}$ stabilise $\mathbf{H}(R)$. Une forme automorphe de $\mathbf{H}(\mathbf{C})$ est dite *propre* si elle est propre pour tous les éléments de $\mathbf{T}$. Elle est *normalisée* si son coefficient de Fourier $c((1))$ associé au diviseur trivial vaut 1. L'inégalité de Ramanujan-Petersson, démontrée par Drinfeld [Dri74], affirme que les valeurs propres de $T_{\mathfrak{m}}$ sont des entiers algébriques de valeur absolue $\leq 2q^{\frac{\deg \mathfrak{m}}{2}}$, pour tout $\mathfrak{m}$ premier.

L'*involution* $w_{\mathfrak{n}}$ est l'endomorphisme de $\mathbf{H}(\mathbf{C})$ défini par $(w_{\mathfrak{n}}F)(e) = F\left(\left(\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right)e\right)$ $(e \in Y(\mathcal{T}))$, où N est le générateur unitaire de $\mathfrak{n}$. Elle commute à $T_{\mathfrak{p}}$, pour tout $\mathfrak{p}$ premier ne divisant pas $\mathfrak{n}$. Lorsque $\mathfrak{n}$ est premier, $w_{\mathfrak{n}}$ coïncide avec $-T_{\mathfrak{n}}$; l'algèbre de Hecke $\mathbf{T}$ coïncide alors avec celle engendrée par $T_{\mathfrak{p}}$ (pour $\mathfrak{p}$ idéal premier distinct de $\mathfrak{n}$) et $w_{\mathfrak{n}}$.

Ajoutons une remarque sur l'opérateur pour la place ∞, défini par

$$(T_\infty F)(e) = \sum_{c\in\mathbf{F}_q} F\left(e\begin{pmatrix} \pi & c \\ 0 & 1 \end{pmatrix}\right) \qquad (e \in Y(\mathcal{T})).$$

Une fonction alternée sur $\mathcal{T}$ est harmonique si et seulement si elle est vecteur propre de T_∞ de valeur propre 1. Nous ne ferons donc pas intervenir l'opérateur T_∞ dans l'algèbre de Hecke.

Rappelons maintenant l'action des opérateurs de Hecke sur les coefficients de Fourier d'une forme automorphe $F \in \mathbf{H}(\mathbf{C})$. Soit $\mathfrak{m}$ un idéal premier non nul de A, de générateur unitaire m. Soit $c_F(M)$ le coefficient de Fourier de F correspondant au diviseur effectif M de K. On a

$$\begin{array}{ll} \text{si } m \nmid N & c_{T_{\mathfrak{m}}F}(M) = q^{\deg m} c_F(M\mathrm{div}(m)) + c_F(M\mathrm{div}(m)^{-1}) \ ; \\ \text{si } m \mid N & c_{T_{\mathfrak{m}}F}(M) = q^{\deg m} c_F(M\mathrm{div}(m)). \end{array}$$

En particulier,

$$c_{T_{\mathfrak{m}}F}((1)) = q^{\deg m} c(\mathrm{div}(m)). \tag{2.6}$$

Proposition 2.9 ([Gek95a] th. 3.17)**.** *On a l'accouplement non dégénéré de groupes abéliens*

$$\begin{array}{rcl} \mathbf{T}\times\mathbf{H} & \longrightarrow & \mathbf{Z} \\ (t, F) & \longmapsto & c_{tF}((1)) \end{array}$$

qui devient parfait après extension des scalaires à $\mathbf{Z}[1/p]$.

La fonction L

Nous suivons les présentations de [Wei71, TR92, Tan93, Gek95b]. Soit $F \in \mathbf{H}(\mathbf{C})$.

Définition 2.10. La *fonction L* de F est définie par la série de Dirichlet

$$L(F,s) = \sum_{M \text{ diviseur effectif de K}} c(M) q^{-(s-1)\deg M},$$

absolument convergente sur le demi-plan $\{s \in \mathbf{C} \mid \mathrm{Re}(s) > 1\}$ (cela vient du fait que F, qui est parabolique, est bornée ; voir [Wei71], corollaire de la proposition 1 et chapitre V).

Rappelons l'expression de cette fonction comme transformée de Mellin, qui permet d'obtenir une équation fonctionnelle et de la prolonger analytiquement à $\mathbf{C}$.

Définition 2.11. La *transformée de Mellin* de F est, pour $s \in \mathbf{C}$, la fonction holomorphe $\mathcal{M}(F,\cdot) : \mathbf{C} \to \mathbf{C}$ définie par

$$\mathcal{M}(F,s) = \sum_{k \in \mathbf{Z}} F\left(\begin{pmatrix} \pi^k & 0 \\ 0 & 1 \end{pmatrix}\right) q^{-ks}.$$

C'est une somme finie. En effet, la projection du chemin $(\left(\begin{smallmatrix} \pi^k & 0 \\ 0 & 1 \end{smallmatrix}\right))_{k \in \mathbf{Z}}$ dans $\Gamma_0(\mathfrak{n})\backslash\mathcal{T}$ relie la pointe 0 à ∞, et F y est nulle sauf pour un nombre fini d'arêtes car elle est parabolique pour $\Gamma_0(\mathfrak{n})$. On a l'énoncé plus précis suivant.

Proposition 2.12. *$\mathcal{M}(F,s)$ est un polynôme en q^{-s} de degré $\leq \deg(\mathfrak{n}) - 1$ et de valuation ≥ 2.*

Démonstration. Pour $k \in \mathbf{Z}$, l'arête représentée par la matrice $\left(\begin{smallmatrix} \pi^k & 0 \\ 0 & 1 \end{smallmatrix}\right)$ est de type k. Par ailleurs, comme F est parabolique, son support est contenu dans les arêtes de $\mathcal{T}$ de type $\leq \deg(\mathfrak{n}) - 1$: cela résulte de la proposition 2 de [TR92] (appliquée à $\mathfrak{n}\infty$, pour cause de différentes conventions de notations). Il reste alors $\mathcal{M}(F,s) = \sum_{k=0}^{\deg(\mathfrak{n})-1} F(\left(\begin{smallmatrix} \pi^k & 0 \\ 0 & 1 \end{smallmatrix}\right)) q^{-ks}$. Les arêtes représentées par $(\left(\begin{smallmatrix} \pi^k & 0 \\ 0 & 1 \end{smallmatrix}\right))_{k \leq 1}$ sont situées sur la demi-droite de $\Gamma_\infty\backslash\mathcal{T}$. Par un argument analogue à celui du corollaire 2.7, F s'annule sur ces arêtes. Donc $\mathcal{M}(F,s)$, vu comme polynôme en q^{-s}, est de valuation ≥ 2. □

Proposition 2.13 (voir aussi [Wei71] VII th. 2, [Tan93] (3.4))**.** *La transformée de Mellin vérifie l'équation fonctionnelle*

$$\mathcal{M}(F,s) = -q^{(\deg(\mathfrak{n})+1)s} \mathcal{M}(w_{\mathfrak{n}} F, -s) \qquad (s \in \mathbf{C}).$$

Démonstration. Posons $d = \deg \mathfrak{n}$. On a $\mathcal{M}(w_{\mathfrak{n}} F, -s) = \sum_{k \in \mathbf{Z}} F\left(\left(\begin{smallmatrix} 0 & -1 \\ N\pi^k & 0 \end{smallmatrix}\right)\right) q^{sk}$. La fonction F étant alternée, on a

$$F\left(\begin{pmatrix} 0 & -1 \\ N\pi^k & 0 \end{pmatrix}\right) = -F\left(\begin{pmatrix} 0 & -1 \\ N\pi^k & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ \pi & 0 \end{pmatrix}\right) = -F\left(\begin{pmatrix} -\pi & 0 \\ 0 & N\pi^k \end{pmatrix}\right).$$

En utilisant l'invariance à droite par $\mathcal{I}\mathrm{Z}(K_\infty)$, on obtient

$$F\left(\begin{pmatrix} -\pi & 0 \\ 0 & N\pi^k \end{pmatrix}\right) = F\left(\begin{pmatrix} \frac{1}{N\pi^{k-1}} & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} N\pi^k & 0 \\ 0 & N\pi^k \end{pmatrix}\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}\right) = F\left(\begin{pmatrix} \frac{1}{N\pi^{k-1}} & 0 \\ 0 & 1 \end{pmatrix}\right).$$

Écrivons $\frac{1}{N\pi^{k-1}} = \pi^{d-(k-1)}a$, avec $a \in O_\infty^\times$. Comme la matrice $\left(\begin{smallmatrix} a & 0 \\ 0 & 1 \end{smallmatrix}\right)$ appartient à $\mathcal{I}$, on a

$$F\left(\begin{pmatrix} \frac{1}{N\pi^{k-1}} & 0 \\ 0 & 1 \end{pmatrix}\right) = F\left(\begin{pmatrix} \pi^{d-(k-1)} & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}\right) = F\left(\begin{pmatrix} \pi^{d-(k-1)} & 0 \\ 0 & 1 \end{pmatrix}\right).$$

Cela donne, en rassemblant les résultats précédents,

$$\mathcal{M}(w_{\mathfrak{n}}F, -s) = -\sum_{k\in\mathbf{Z}} F\left(\begin{pmatrix} \pi^{d-(k-1)} & 0 \\ 0 & 1 \end{pmatrix}\right) q^{sk} = -q^{(d+1)s}\mathcal{M}(F, s).$$

□

Le résultat suivant se trouve dans [Gek95b] § 3.5. Nous en donnons une autre démonstration. Pour une généralisation de cet énoncé aux fonctions L tordues par un caractère, on consultera [Tan93] prop. 2 et [TR92] prop. 1.

Proposition 2.14. *Pour tout $s \in \mathbf{C}$ tel que $\mathrm{Re}(s) > 1$, on a*

$$L(F, s) = \frac{q^{2(s-1)}}{q-1}\mathcal{M}(F, s-1). \tag{2.7}$$

En particulier, $L(F, s)$ est un polynôme en q^{-s} de degré $\leq \deg(\mathfrak{n}) - 3$.

Démonstration. Soit $s \in \mathbf{C}$ de partie réelle > 1. En utilisant le développement de Fourier de F, on obtient

$$\frac{1}{q-1}\mathcal{M}(F, s-1) = \sum_{k\in\mathbf{Z}} \left(\sum_{\substack{m\in A, m\neq 0 \\ \deg m \leq k-2}} c(\mathrm{div}(m)\infty^{k-2})\right) q^{-k(s-1)},$$

où les deux sommes sont finies. Tout diviseur effectif de K de degré $k-2$ s'écrit $\mathrm{div}(m)\infty^{k-2}$ avec $m \in A$, $m \neq 0$ et $\deg m \leq k-2$. Réciproquement deux éléments m et m' donnent le même diviseur effectif de K si et seulement si $\frac{m'}{m} \in \mathbf{F}_q^\times$. Comme la fonction L converge absolument, on peut réorganiser la somme de la façon suivante (en sommant par paquets de diviseurs de degré fixé)

$$\frac{1}{q-1}\mathcal{M}(F, s-1) = \sum_{M \text{ diviseur effectif de } K} c(M)q^{-(s-1)(\deg M+2)} = q^{-2(s-1)}L(F, s).$$

□

Corollaire 2.15. *La formule* (2.7) *définit un unique prolongement holomorphe de la fonction L à $\mathbf{C}$, noté $L(F, s)$. En particulier, on a*

$$L(F, 1) = \frac{1}{q-1}\sum_{k\in\mathbf{Z}} F\left(\begin{pmatrix} \pi^k & 0 \\ 0 & 1 \end{pmatrix}\right) = \frac{1}{q-1}\sum_{k=2}^{\deg(\mathfrak{n})-1} F\left(\begin{pmatrix} \pi^k & 0 \\ 0 & 1 \end{pmatrix}\right)$$

et l'équation fonctionnelle

$$L(F, s) = -q^{(\deg(\mathfrak{n})-3)(1-s)}L(w_{\mathfrak{n}}F, 2-s) \qquad (s \in \mathbf{C}).$$

Proposition 2.16 (voir aussi [Tan93] cor. p. 305)**.** *Supposons* $\mathfrak{n}$ *premier. Soit* $F \in \mathbf{H}(\mathbf{C})$ *une forme propre normalisée pour* $\mathbf{T}$*. Alors* $L(F,s)$ *est un polynôme en* q^{-s} *de degré égal à* $\deg(\mathfrak{n}) - 3$*, et de terme constant égal à* 1*.*

Démonstration. Soit F une forme propre pour $\mathbf{T}$. On sait déjà que $L(F,s)$ est un polynôme en q^{-s} de degré $\leq \deg(\mathfrak{n}) - 3$. Comme $\mathfrak{n}$ est premier, F est propre pour $T_{\mathfrak{n}} = w_{\mathfrak{n}}$ et il existe $\varepsilon \in \{-1,+1\}$ tel que $w_{\mathfrak{n}}F = \varepsilon F$. D'après l'équation fonctionnelle, on a alors

$$L(F,s) = -\varepsilon q^{(\deg(\mathfrak{n})-3)(1-s)} L(F, 2-s) \quad (s \in \mathbf{C}).$$

En exprimant $L(F,2-s)$ à l'aide de la transformée de Mellin, un calcul montre que le coefficient du terme en $q^{-s(\deg(\mathfrak{n})-3)}$ du membre de droite est $-\varepsilon \frac{q^{\deg(\mathfrak{n})-1}}{q-1} F\left(\left(\begin{smallmatrix} \pi^2 & 0 \\ 0 & 1 \end{smallmatrix}\right)\right)$. De plu, d'après la formule (2.5) pour le développement de Fourier, on a

$$F\left(\begin{pmatrix} \pi^2 & 0 \\ 0 & 1 \end{pmatrix}\right) = (q-1)c((1)),$$

donc le coefficient du terme en $q^{-s(\deg(\mathfrak{n})-3)}$ dans $L(F,s)$ est donc $-\varepsilon q^{\deg(\mathfrak{n})-1} c((1))$. Comme F est propre, il est non nul d'après la formule (2.6). Un calcul similaire montre que le terme constant de $L(F,s)$, vu comme un polynôme en q^{-s}, est $c((1))$ c'est-à-dire 1 car F est normalisée. □

Corollaire 2.17. *Soit* $\mathfrak{n}$ *un idéal de* A *de degré* 3*. La fonction* $L(F,s)$ *est constante et égale au coefficient de Fourier de* F *associé au diviseur trivial. En particulier, si* F *est une forme propre, on a* $L(F,s) \neq 0$ *; de plus, si* F *est normalisée, on a* $L(F,s) = 1$*.*

Démonstration. Si on suppose $\mathfrak{n}$ premier, l'énoncé est un cas particulier de la proposition 2.16. Supposons $\mathfrak{n}$ quelconque de degré 3. D'après la proposition 2.14, $L(F,s)$ est constante. Le corollaire 2.15 donne $L(F,s) = L(F,1) = \frac{1}{q-1} F\left(\left(\begin{smallmatrix} \pi^2 & 0 \\ 0 & 1 \end{smallmatrix}\right)\right) = c((1))$. □

Rappelons que le *rang de* F désigne l'ordre d'annulation de la fonction $L(F,s)$ en $s = 1$. Mentionnons un corollaire immédiat de la proposition 2.16.

Corollaire 2.18. *Si* $\mathfrak{n}$ *est un idéal premier de* A *de degré* 4*, toute forme propre de* $\mathbf{H}(\mathbf{C})$ *est de rang au plus* 1*.*

La fonction L comme produit eulérien ([Wei71]). Soit $\mathfrak{m}$ un idéal premier de A et $q_{\mathfrak{m}} = q^{\deg \mathfrak{m}}$ le cardinal du corps résiduel. Supposons F propre pour $T_{\mathfrak{m}}$, de valeur propre $\lambda_{\mathfrak{m}} \in \mathbf{C}$. À $\lambda_{\mathfrak{m}}$ on associe une suite $(\gamma_{n,\mathfrak{m}})_{n \geq 0}$ de nombres complexes définie par l'égalité de séries formelles

$$\begin{array}{ll} \sum_{n=0}^{\infty} \gamma_{n,\mathfrak{m}} X^n = (1 - \frac{\lambda_{\mathfrak{m}}}{q_{\mathfrak{m}}} X + \frac{1}{q_{\mathfrak{m}}} X^2)^{-1} & \text{si } \mathfrak{n} \not\subseteq \mathfrak{m} \\ \sum_{n=0}^{\infty} \gamma_{n,\mathfrak{m}} X^n = (1 - \frac{\lambda_{\mathfrak{m}}}{q_{\mathfrak{m}}} X)^{-1} & \text{si } \mathfrak{n} \subset \mathfrak{m}. \end{array}$$

Si $(M,\mathfrak{m}) = 1$, les coefficients de Fourier de F vérifient $c(M\mathfrak{m}^n) = \gamma_{n,\mathfrak{m}} c(M)$. Si F est propre pour $\mathbf{T}$, le facteur L local en $\mathfrak{m}$ est défini par

$$L_{\mathfrak{m}}(F,s) = \begin{cases} (1 - \lambda_{\mathfrak{m}} q_{\mathfrak{m}}^{-s} + q_{\mathfrak{m}}^{1-2s})^{-1} & \text{si } \mathfrak{n} \not\subseteq \mathfrak{m} \\ (1 - \lambda_{\mathfrak{m}} q_{\mathfrak{m}}^{-s})^{-1} & \text{si } \mathfrak{n} \subset \mathfrak{m}. \end{cases}$$

Sa fonction L est alors

$$L(F,s) = \frac{1}{1-q^{-s}} \prod_{\mathfrak{m}} L_{\mathfrak{m}}(F,s) \qquad (s \in \mathbf{C}),$$

le produit portant sur les idéaux premiers non nuls de A.

2.2 La présentation de Manin-Teitelbaum (rappels)

Nous rappelons la théorie des symboles modulaires pour $\mathbf{F}_q[T]$ et l'analogue de la présentation de Manin, selon Teitelbaum [Tei92a].

2.2.1 Cas des sous-groupes de congruence quelconques

Les symboles modulaires

On rappelle qu'un diviseur à support dans $\mathbf{P}^1(K)$ est une somme finie formelle $\sum_i n_i(P_i)$ avec $n_i \in \mathbf{Z}$ et $P_i \in \mathbf{P}^1(K)$. Son degré est l'entier $\sum_i n_i$.

Soit M le groupe formé des diviseurs de degré nul à support dans $\mathbf{P}^1(K)$. Les éléments de M sont appelés *symboles modulaires* pour K. Pour $r, s \in \mathbf{P}^1(K)$, le symbole modulaire $(s)-(r)$ définit une géodésique de $\mathcal{T}$ allant du bout rationnel r au bout rationnel s, qui est unique du fait que $\mathcal{T}$ est un arbre.

Soit $\Gamma \subset \mathrm{GL}(2,A)$ un sous-groupe de congruence. Il agit par transformations linéaires sur $\mathbf{P}^1(K_\infty)$. Le groupe des *symboles modulaires pour* Γ est le groupe abélien

$$M_\Gamma = H_0(\Gamma, M) = M/\langle \gamma m - m \mid \gamma \in \Gamma, m \in M\rangle.$$

Plus généralement, si R est un $\mathbf{Z}$-module, le groupe des *symboles modulaires pour* Γ *à valeurs dans* R est

$$M_\Gamma(R) = H_0(\Gamma, M \otimes_{\mathbf{Z}} R).$$

Si r et s sont dans $\mathbf{P}^1(K)$, le symbole modulaire correspondant à la classe de $((s)-(r)) \otimes 1$ est noté $[r,s] \in M_\Gamma(R)$.

Soient B_Γ le groupe des diviseurs de degré nul à support dans $\Gamma\backslash\mathbf{P}^1(K)$ et $B_\Gamma(R) = B_\Gamma \otimes_{\mathbf{Z}} R$. L'application $[r,s] \mapsto (\Gamma s) - (\Gamma r)$ s'étend par linéarité en une application bord $M_\Gamma(R) \to B_\Gamma(R)$. Le groupe des *symboles modulaires paraboliques pour* Γ *à valeurs dans* R est le noyau de cette application. On le note $M^0_\Gamma(R)$ et on pose $M^0_\Gamma = M^0_\Gamma(\mathbf{Z})$.

Lorsque R est un $\mathbf{Z}$-module sans torsion, un argument de platitude montre que les homomorphismes canoniques

$$\begin{array}{rccc} & M_\Gamma \otimes_{\mathbf{Z}} R & \longrightarrow & M_\Gamma(R) \\ \text{et} & M^0_\Gamma \otimes_{\mathbf{Z}} R & \longrightarrow & M^0_\Gamma(R) \end{array}$$

sont des isomorphismes de R-modules.

Voici quelques propriétés vérifiées par les symboles modulaires. Pour tout $r, s, t \in \mathbf{P}^1(K)$ et $\gamma \in \Gamma$, on a :

(i) $[r,s] = -[s,r]$;

(ii) $[\gamma r, \gamma s] = [r, s]$;

(iii) $[r, s] + [s, t] = [r, t]$;

(iv) $[r, r] = 0$;

(v) $[r, \gamma r] = [s, \gamma s]$.

L'application

$$\begin{array}{ccc} \Gamma & \longrightarrow & M_\Gamma^0 \\ \gamma & \longmapsto & [r, \gamma r] \end{array}$$

est indépendante du choix de $r \in \mathbf{P}^1(K)$ et définit un homomorphisme de groupes surjectif (ceci résulte des propriétés précédentes).

La structure de M_Γ et M_Γ^0

L'application qui associe au symbole modulaire $[r, s]$ la projection dans $\Gamma\backslash\mathcal{T}$ de l'unique géodésique de $\mathcal{T}$ reliant le bout r au bout s s'étend par linéarité en un homomorphisme de groupes abéliens

$$M_\Gamma \longrightarrow H_1(\Gamma\backslash\mathcal{T}, \mathrm{ptes}, \mathbf{Z}).$$

Proposition 2.19 ([Tei92a] pp. 277-278)**.** *Soit Γ un sous-groupe de congruence contenu dans $\Gamma_0(\mathfrak{n})$ pour un idéal $\mathfrak{n} \subsetneq A$. On a les isomorphismes de groupes*

$$\begin{array}{rrcl} & M_\Gamma/(M_\Gamma)_{\mathrm{tors}} & \xrightarrow{\sim} & H_1(\Gamma\backslash\mathcal{T}, \mathrm{ptes}, \mathbf{Z}) \\ et & M_\Gamma^0/(M_\Gamma^0)_{\mathrm{tors}} & \xrightarrow{\sim} & H_1(\Gamma\backslash\mathcal{T}, \mathbf{Z}). \end{array}$$

En particulier, on a les égalités

$$\begin{array}{rrcl} & \dim M_\Gamma \otimes_{\mathbf{Z}} \mathbf{Q} & = & g + h - 1 \\ \text{et} & \dim M_\Gamma^0 \otimes_{\mathbf{Z}} \mathbf{Q} & = & g, \end{array}$$

où g est le genre du graphe $\Gamma\backslash\mathcal{T}$, c'est-à-dire le rang du $\mathbf{Z}$-module libre $H_1(\Gamma\backslash\mathcal{T}, \mathbf{Z})$, et h est le nombre de pointes de $\Gamma\backslash\mathcal{T}$. De plus, si $\Gamma = \Gamma_i(\mathfrak{n})$ ($i \in \{0, 1\}$), g (resp. h) coïncide avec le genre de la courbe modulaire $X_i(\mathfrak{n})$ (resp. son nombre de pointes).

***Remarque* 2.20.** Si Γ est l'un des sous-groupes $\Gamma_0(\mathfrak{n}), \Gamma_1(\mathfrak{n}), \Gamma(\mathfrak{n})$, la proposition précédente et les isomorphismes (2.2) et (2.3) p. 29 donnent un isomorphisme de groupes

$$M_\Gamma^0/(M_\Gamma^0)_{\mathrm{tors}} \xrightarrow{\sim} \underline{H}_!(\mathcal{T}, \mathbf{Z})^\Gamma.$$

Il est donc possible de choisir $\underline{H}_!(\mathcal{T}, \mathbf{Z})^\Gamma$ comme groupe des symboles modulaires paraboliques à torsion près. Ce point de vue semble avoir été adopté dans [Gek97b]. Signalons que la présentation finie de l'espace des symboles modulaires donnée par Teitelbaum, dont nous ferons un usage essentiel, ne semble pas avoir été établie par cette approche.

L'accouplement avec les cochaînes harmoniques

***Notation* 2.21.** Soient $[r,s] \in M_\Gamma(R)$ un symbole modulaire et $F \in \underline{H}_!(\mathcal{T},R)^\Gamma$ une cochaîne parabolique à valeurs dans un groupe abélien R. Soit c l'unique géodésique de $\mathcal{T}$ reliant le bout r au bout s. Alors l'intégrale $\int_{[r,s]} F$ est définie comme $\sum_{e\in c} F(e)$.

Cette notation ne dépend pas du choix d'un représentant de $[r,s]$. De plus, c'est une somme finie : en effet, le graphe $\Gamma\backslash\mathcal{T}$ est réunion d'un graphe fini et d'un nombre fini de pointes ; F étant Γ-invariante, la somme peut être calculée sur la projection de c dans $\Gamma\backslash\mathcal{T}$ et F est à support fini dans $\Gamma\backslash\mathcal{T}$. L'intégration s'étend en une application R-bilinéaire

$$\langle\ ,\ \rangle : M_\Gamma(R) \times \underline{H}_!(\mathcal{T},R)^\Gamma \longrightarrow R.$$

On peut alors reformuler le corollaire 2.15 dans ce langage (voir aussi [Tan93] prop. 2, [Tei92a] th. 23 et [Gek95b] 3.7).

Proposition 2.22. *Pour toute forme automorphe $F \in \mathbf{H}(\mathbf{C})$, on a*

$$L(F,1) = \frac{1}{q-1}\int_{[0,\infty]} F = \frac{1}{q-1}\langle [0,\infty], F\rangle.$$

***Remarque* 2.23.** Par l'isomorphisme $M_\Gamma^0/(M_\Gamma^0)_{\mathrm{tors}} \simeq \underline{H}_!(\mathcal{T},\mathbf{Z})^\Gamma$ de la remarque 2.20, on peut montrer que l'accouplement d'intégration $M_\Gamma^0 \times \underline{H}_!(\mathcal{T},\mathbf{Z})^\Gamma \to \mathbf{Z}$ correspond au produit de Petersson sur $\underline{H}_!(\mathcal{T},\mathbf{Z})^\Gamma$.

Théorème 2.24. *Soit $\Gamma = \Gamma_0(\mathfrak{n})$ (resp. $\Gamma_1(\mathfrak{n})$). On a une suite exacte de groupes abéliens*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & (M_\Gamma^0)_{\mathrm{tors}} & \longrightarrow & M_\Gamma^0 & \longrightarrow & \mathrm{Hom}(\underline{H}_!(\mathcal{T},\mathbf{Z})^\Gamma,\mathbf{Z}) & \longrightarrow & \Phi_\infty & \longrightarrow & 0, \\ & & & & m & \longmapsto & (F \mapsto \langle m,F\rangle) & & & & \end{array}$$

où Φ_∞ désigne[1] *le groupe des composantes connexes de la fibre spéciale du modèle de Néron de la jacobienne de la courbe modulaire $X_0(\mathfrak{n})$ (resp. $X_1(\mathfrak{n})$) en ∞. En particulier, on a une dualité parfaite de $\mathbf{Q}$-espaces vectoriels*

$$\langle\ ,\ \rangle : (M_\Gamma^0 \otimes_{\mathbf{Z}} \mathbf{Q}) \times \underline{H}_!(\mathcal{T},\mathbf{Q})^\Gamma \longrightarrow \mathbf{Q}.$$

Démonstration. La suite exacte est un cas particulier du théorème 14 de [Tei92a]. Signalons qu'en utilisant les remarques 2.20 et 2.23, on voit que cette suite exacte est contenue dans les travaux de Gekeler (corollaire 2.11 de [Gek95a], théorème 4.6 de [Gek97b]). En étendant les scalaires à $\mathbf{Q}$, on obtient l'isomorphisme

$$M_\Gamma^0 \otimes_{\mathbf{Z}} \mathbf{Q} \xrightarrow{\sim} \mathrm{Hom}(\underline{H}_!(\mathcal{T},\mathbf{Z})^\Gamma,\mathbf{Z}) \otimes_{\mathbf{Z}} \mathbf{Q}.$$

Enfin, comme $\underline{H}_!(\mathcal{T},\mathbf{Z})^\Gamma$ est libre de rang fini sur $\mathbf{Z}$, l'homomorphisme canonique de $\mathbf{Q}$-espaces vectoriels $\mathrm{Hom}(\underline{H}_!(\mathcal{T},\mathbf{Z}),\mathbf{Z})^\Gamma \otimes_{\mathbf{Z}} \mathbf{Q} \to \mathrm{Hom}(\underline{H}_!(\mathcal{T},\mathbf{Q})^\Gamma,\mathbf{Q})$ est un isomorphisme. □

1. On pourra consulter aussi le paragraphe 3.2.3.

Les symboles de Manin-Teitelbaum

Le R-module $M_\Gamma(R)$ admet une présentation par générateurs et relations [Tei92a] similaire à celle de Manin [Man72]. Le groupe Γ agit à gauche sur $\mathrm{GL}(2, A)$ et il est d'indice fini. L'application suivante est bien définie [2] :

$$\begin{array}{rcl} \Gamma\backslash\mathrm{GL}(2,A) & \longrightarrow & M_\Gamma \\ \Gamma g = \Gamma\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) & \longmapsto & [g(0), g(\infty)] = [\frac{b}{d}, \frac{a}{c}] \end{array}$$

et se prolonge par $\mathbf{Z}$-linéarité en un homorphisme surjectif :

$$\Phi : \mathbf{Z}[\Gamma\backslash\mathrm{GL}(2,A)] \longrightarrow M_\Gamma$$

(la surjectivité provient d'un développement en fractions continuées, [Tei92a] lemme 16). La classe Γg sera notée (g). Un *symbole de Manin-Teitelbaum* est $\Phi(g)$, pour $(g) \in \Gamma\backslash\mathrm{GL}(2, A)$.

Pour décrire l'espace des symboles modulaires, il reste à déterminer les relations entre ces générateurs. Posons dans $\mathrm{GL}(2, \mathbf{F}_q)$:

$$\sigma = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \text{ et } \tau = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}.$$

Ces matrices sont d'ordre respectivement 4 (2 si $\mathbf{F}_q$ est de caractéristique 2) et 3. Soit I_0 l'idéal de $\mathbf{Z}[\mathrm{GL}(2, \mathbf{F}_q)]$ engendré par les éléments $1 - d$ (pour d matrice diagonale de $\mathrm{GL}(2, \mathbf{F}_q)$), $1 + \sigma$ et $1 + \tau + \tau^2$. On a une suite exacte ([Tei92a], 16 à 20)

$$\mathbf{Z}[\mathrm{GL}(2,A)]I_0 \longrightarrow \mathbf{Z}[\mathrm{GL}(2,A)] \longrightarrow M \longrightarrow 0,$$

qui donne lieu à la présentation suivante (théorème 21 de [Tei92a] dans le cas $R = \mathbf{Z}$).

Théorème 2.25 ([Tei92a])**.** *Le groupe $M_\Gamma(R)$ est isomorphe au quotient du R-module libre $R[\Gamma\backslash\mathrm{GL}(2, A)]$ par les relations :*

$$\begin{array}{rcl} (g) - (gd) & = & 0 \\ (g) + (g\sigma) & = & 0 \\ (g) + (g\tau) + (g\tau^2) & = & 0 \end{array}$$

pour tout $g \in \mathrm{GL}(2, A)$ et d matrice diagonale dans $\mathrm{GL}(2, \mathbf{F}_q)$.

2.2.2 Cas du sous-groupe de congruence $\Gamma_0(\mathfrak{n})$

***Notation* 2.26.** Si R est un groupe abélien, on pose désormais

$$\begin{aligned} \mathbf{M} &= M_{\Gamma_0(\mathfrak{n})} \\ \mathbf{M}^0 &= M^0_{\Gamma_0(\mathfrak{n})} \\ \mathbf{M}(R) &= M_{\Gamma_0(\mathfrak{n})}(R) \\ \mathbf{M}^0(R) &= M^0_{\Gamma_0(\mathfrak{n})}(R). \end{aligned}$$

2. Teitelbaum a adopté la convention inverse $[g(\infty), g(0)]$.

Les opérateurs de Hecke

Soit $\mathfrak{m}$ un idéal non nul de A, de générateur unitaire m. Soit R un groupe abélien. On définit un endomorphisme du groupe $\mathbf{M}(R)$ par la formule

$$T_{\mathfrak{m}}[r,s] = \sum_{\substack{a,b,d\in A \\ (ad)=\mathfrak{m},\ (a)+\mathfrak{n}=A \\ \deg b<\deg d,\ a \text{ et } d \text{ unitaires}}} \left[\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} r, \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} s\right] \qquad ([r,s]\in\mathbf{M}(R)).$$

L'accouplement d'intégration est compatible aux opérateurs de Hecke : pour tout idéal $\mathfrak{m}$ et $F\in\mathbf{H}(\mathbf{C})$ on a

$$\langle T_{\mathfrak{m}}[r,s], F\rangle = \langle [r,s], T_{\mathfrak{m}}F\rangle \qquad ([r,s]\in\mathbf{M}(\mathbf{C}))$$

([Tei92a] lemme 9). De plus, d'après le théorème 2.24, cet accouplement donne une dualité parfaite de $\mathbf{C}$-espaces vectoriels

$$\mathbf{M}^0(\mathbf{C})\times\mathbf{H}(\mathbf{C})\longrightarrow\mathbf{C},$$

qui identifie $\mathbf{T}$ à la sous-algèbre de $\mathrm{End}(\mathbf{M}^0(\mathbf{C}))$ engendrée sur $\mathbf{Z}$ par $T_{\mathfrak{m}}$ ($\mathfrak{m}\in A$). On notera encore $\mathbf{T}$ cette algèbre. Pour tout sous-anneau $R\subset\mathbf{C}$, $\mathbf{T}$ stabilise $\mathbf{M}^0(R)$.

L'involution $w_{\mathfrak{n}}$

L'involution $w_{\mathfrak{n}}$ est l'élément de $\mathrm{End}(\mathbf{M})$ défini par

$$w_{\mathfrak{n}}[r,s] = \left[\begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix} r, \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix} s\right] = \left[-\frac{1}{Nr}, -\frac{1}{Ns}\right],$$

où N est le générateur unitaire de $\mathfrak{n}$. L'accouplement d'intégration est compatible à l'action de $w_{\mathfrak{n}}$. Lorsque $\mathfrak{n}$ est premier, on a $w_{\mathfrak{n}}=T_{\mathfrak{n}}$.

La présentation de Manin-Teitelbaum pour $\Gamma_0(\mathfrak{n})$

Dans toute classe de $\Gamma_0(\mathfrak{n})\backslash\mathrm{GL}(2,A)$, il est possible de choisir un représentant $\left(\begin{smallmatrix} u & v \\ a & b \end{smallmatrix}\right)$ de sorte que $ub-va\in\mathbf{F}_q^\times$. L'application

$$\begin{array}{rcl} \Gamma_0(\mathfrak{n})\backslash\mathrm{GL}(2,A) & \longrightarrow & \mathbf{P}^1(A/\mathfrak{n}) \\ \Gamma_0(\mathfrak{n})\left(\begin{smallmatrix} u & v \\ a & b \end{smallmatrix}\right) & \longmapsto & (a:b) \end{array}$$

est bijective. On note $\xi(a:b)$ le symbole de Manin-Teitelbaum $\Phi(\left(\begin{smallmatrix} u & v \\ a & b \end{smallmatrix}\right)) = [\frac{v}{b},\frac{u}{a}]$. Le groupe $\mathbf{M}(R)$ admet alors la présentation suivante.

Théorème 2.27. *Le groupe $\mathbf{M}(R)$ est isomorphe au quotient du R-module libre $R[\mathbf{P}^1(A/\mathfrak{n})]$ par les relations :*

$$\begin{array}{rcl} (a:b)-(da:d'b) & = & 0 \quad (d,d'\in\mathbf{F}_q^\times) \\ (a:b)+(-b:a) & = & 0 \\ (a:b)+(b:-a-b)+(-a-b:a) & = & 0. \end{array}$$

2.3 L'action de Hecke sur les symboles de Manin-Teitelbaum

Soit $M_2(A)$ l'ensemble des matrices 2×2 à coefficients dans A. L'action des opérateurs de Hecke sur les symboles de Manin-Teitelbaum s'exprime grâce aux formules suivantes.

Théorème 2.28. *Pour tout idéal $\mathfrak{m}$ de A et $(u:v) \in \mathbf{P}^1(A/\mathfrak{n})$, on a*

$$T_{\mathfrak{m}}\, \xi(u:v) = \sum_{M \in \mathscr{S}_{\mathfrak{m}}} \xi((u:v)M) = \sum_{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathscr{S}_{\mathfrak{m}}} \xi(au+cv : bu+dv)$$

où $\mathscr{S}_{\mathfrak{m}} = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_2(A), \deg a > \deg b,\ \deg d > \deg c, (ad-bc) = \mathfrak{m}, a$ et d unitaires$\}$ et la somme est restreinte aux matrices M telles que $(u:v)M$ soit défini dans $\mathbf{P}^1(A/\mathfrak{n})$.

Appliquons cette formule au symbole modulaire $[0,\infty] = \xi(0:1)$:

$$T_{\mathfrak{m}}[0,\infty] = \sum_{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathscr{S}_{\mathfrak{m}}} \xi(c:d) = \sum_{\substack{\deg d > \deg c \\ \deg a > \deg b \\ (ad-bc)=\mathfrak{m} \\ a \text{ et } d \text{ unitaires} \\ (c)+(d)+\mathfrak{n}=A}} \xi(c:d).$$

***Remarque* 2.29.** (i) Lorsque $\mathfrak{m}$ et $\mathfrak{n}$ sont premiers entre eux, il est inutile de restreindre la somme.

(ii) L'ensemble $\mathscr{S}_{\mathfrak{m}}$ ne dépend pas de $\mathfrak{n}$.

(iii) Un tel résultat pourrait être étendu à l'involution $w_{\mathfrak{n}}$ (voir [Mer94]).

(iv) Il existe d'autres formules valides du même type. Par exemple, l'action de σ à droite sur $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ permet de remplacer le terme $\xi(au+cv : bu+dv)$ par $-\xi(-bu-dv : au+cv)$.

Quelques exemples d'ensembles $\mathscr{S}_{\mathfrak{m}}$ seront donnés dans la section 2.3.2.

2.3.1 Démonstration du théorème 2.28

Elle repose sur des idées de [Mer94] (voir aussi la démonstration du lemme 2 de [Mer96]). Soit $\mathfrak{m}$ un idéal non nul de A, de générateur unitaire P.

Lemme 2.30. *L'ensemble de matrices $\mathscr{S}_{\mathfrak{m}}$ est fini.*

Démonstration. Soit $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ appartenant à $\mathscr{S}_{\mathfrak{m}}$. Comme $\deg a > \deg b$ et $\deg d > \deg c$, le degré de $ad-bc$ est égal à $\deg(ad) = \deg a + \deg d$. Or, $ad-bc = P$ donc $\deg a$ et $\deg d$ valent au plus $\deg P$, et il en est de même de $\deg b$ et $\deg c$. Les polynômes a, b, c et d étant à coefficients dans le corps fini $\mathbf{F}_q$, cela ne laisse qu'un nombre fini de possibilités pour ces polynômes. □

Le groupe $\mathrm{SL}_2(A)$ agit à droite sur l'ensemble $M_2(A)_P$ des matrices de déterminant P. L'ensemble des classes est noté $M_2(A)_P/\mathrm{SL}_2(A)$. Commençons par exhiber un système de représentants.

Proposition 2.31. *Les matrices $m(a,b) = \left(\begin{smallmatrix} a & b \\ 0 & \frac{P}{a} \end{smallmatrix}\right)$ avec $a \mid P$, a unitaire et $\deg a > \deg b$ forment un système de représentants de $M_2(A)_P/\mathrm{SL}_2(A)$. De plus, ces matrices sont les seuls éléments $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ de $\mathscr{S}_{\mathfrak{m}}$ avec $c = 0$.*

Démonstration. Soit $M \in M_2(A)_P$. Comme l'action de $\mathrm{SL}_2(A)$ sur $\mathbf{P}^1(K) = K \cup \{\infty\}$ est transitive, il existe $\gamma \in \mathrm{SL}_2(A)$ tel que $\gamma\infty = M^{-1}\infty$, c'est-à-dire $M\gamma\infty = \infty$. Posons $M' = M\gamma$; c'est un élément de $M_2(A)_P$. Comme $M'\infty = \infty$, M' est de la forme $\left(\begin{smallmatrix} a & b \\ 0 & \frac{P}{a} \end{smallmatrix}\right)$. Soit $\alpha \in \mathbf{F}_q^\times$ le coefficient dominant de a ; celui de $\frac{P}{a}$ est α^{-1}. Quitte à remplacer M' par $\left(\begin{smallmatrix} \alpha^{-1} & 0 \\ 0 & \alpha \end{smallmatrix}\right)M'$ (qui est dans la même classe que M'), on peut supposer que a est unitaire. Un calcul élémentaire montre que deux matrices $\left(\begin{smallmatrix} a & b \\ 0 & \frac{P}{a} \end{smallmatrix}\right)$ et $\left(\begin{smallmatrix} a' & b' \\ 0 & \frac{P}{a'} \end{smallmatrix}\right)$ sont congrues modulo $\mathrm{SL}_2(A)$ si et seulement si $a = a'$ et $b' \equiv b \bmod a$. On peut donc choisir b tel que $\deg a > \deg b$, et M' dans la classe de M de la forme $\left(\begin{smallmatrix} a & b \\ 0 & \frac{P}{a} \end{smallmatrix}\right)$ avec $\deg a > \deg b$. Enfin, la dernière assertion de l'énoncé vient de la définition de $\mathscr{S}_{\mathfrak{m}}$. $\square$

Proposition 2.32. *Soit $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathscr{S}_{\mathfrak{m}}$ avec $c \neq 0$ (c'est-à-dire $M\infty \neq \infty$). Alors il existe une unique matrice $M' \in \mathscr{S}_{\mathfrak{m}} \cap M\mathrm{SL}_2(A)$ telle que $M'0 = M\infty$.*

Soit $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathscr{S}_{\mathfrak{m}}$ avec $b \neq 0$ (c'est-à-dire $M0 \neq 0$). Alors il existe une unique matrice $M' \in \mathscr{S}_{\mathfrak{m}} \cap M\mathrm{SL}_2(A)$ telle que $M'\infty = M0$.

Démonstration. Nous démontrons le résultat dans le cas où $c \neq 0$, le cas $b \neq 0$ étant similaire. Commençons par l'existence. Considérons une matrice $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathscr{S}_{\mathfrak{m}}$ avec $c \neq 0$. Soit α l'inverse du coefficient dominant de c. En écrivant la division euclidienne de d par c, on obtient un unique polynôme unitaire Q de degré $\deg d - \deg c$ vérifiant $\deg(\alpha c) > \deg(cQ - \alpha^{-1}d)$. Posons

$$M' = M\begin{pmatrix} Q & \alpha \\ -\alpha^{-1} & 0 \end{pmatrix} = \begin{pmatrix} aQ - \alpha^{-1}b & \alpha a \\ cQ - \alpha^{-1}d & \alpha c \end{pmatrix}.$$

Cette matrice est de déterminant P. Comme $\deg Q \geq 1$ et $\deg a > \deg b$, on a $\deg(aQ - \alpha^{-1}b) = \deg(aQ) > \deg(\alpha A)$. Par construction de Q, on a $\deg(\alpha c) > \deg(cQ - \alpha^{-1}d)$. Enfin, αc est unitaire et il en est de même de $aQ - \alpha^{-1}b$ (son coefficient dominant est celui de aQ et a et Q sont unitaires). Donc la matrice M' appartient à l'ensemble $\mathscr{S}_{\mathfrak{m}}$. Elle vérifie $M'0 = \frac{a}{c} = M\infty$.

Passons à l'unicité. Soit une matrice M' vérifiant les propriétés demandées dans l'énoncé. Il suffit de montrer que $M^{-1}M'$ est déterminée de façon unique par M. Notons $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ et $M' = \left(\begin{smallmatrix} a' & b' \\ c' & d' \end{smallmatrix}\right)$ avec $M'0 = \frac{b'}{d'} = \frac{a}{c} = M\infty$. On a alors

$$M^{-1}M' = \begin{pmatrix} \frac{da'-bc'}{P} & \frac{db'-bd'}{P} \\ \frac{ac'-ca'}{P} & \frac{ad'-cb'}{P} \end{pmatrix}.$$

Comme $M^{-1}M'0 = \infty$, le terme diagonal $\frac{ad'-cb'}{P}$ est nul. De plus, $M^{-1}M'$ est de déterminant 1, donc de la forme $\left(\begin{smallmatrix} Q & \alpha \\ -\alpha^{-1} & 0 \end{smallmatrix}\right)$ pour un certain $\alpha \in \mathbf{F}_q^\times$. On a donc $M' = M\left(\begin{smallmatrix} Q & \alpha \\ -\alpha^{-1} & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} aQ-\alpha^{-1}b & \alpha a \\ cQ-\alpha^{-1}d & \alpha c \end{smallmatrix}\right)$. Comme M' est dans $\mathscr{S}_{\mathfrak{m}}$, αc est unitaire donc α est l'inverse du coefficient dominant de c. Il reste à montrer que le polynôme Q est déterminé de façon unique par la matrice M. Par identification, on a $\alpha a = b'$ donc $\deg b' = \deg a$. De même, on a $\alpha c = d'$ donc $\deg d' = \deg c$. La définition de $\mathscr{S}_{\mathfrak{m}}$ fournit les inégalités

$$\begin{aligned} \deg d > \deg c &= \deg d' > \deg c' \\ \text{et} \quad \deg a' > \deg b' &= \deg a > \deg b. \end{aligned}$$

Comme $Q = \frac{da'-bc'}{P}$, on a $\deg Q = \deg(da') - \deg P$. De plus, comme $\deg a' > \deg b' = \deg a$ et $\deg c = \deg d' > \deg c'$, on a $\deg(a'c - c'a) = \deg(a'c)$. Comme $-\alpha^{-1} = \frac{a'c-c'a}{P}$, on a $\deg P = \deg(a'c)$. On en déduit finalement $\deg Q = \deg(da') - \deg(a'c) = \deg d - \deg c$. Le polynôme Q vérifie $\deg c > \deg(cQ - \alpha^{-1}d)$. C'est donc le quotient de la division euclidienne de d par αc, et il est déterminé de façon unique par les polynômes c et d. $\square$

Démonstration du théorème 2.28. Soit $(u, v) \in A \times A$ vérifiant $\mathfrak{n} + (u) + (v) = A$. Soit $g = \left(\begin{smallmatrix} x & y \\ u & v \end{smallmatrix}\right) \in \mathrm{SL}(2, A)$. On a $\xi(u : v) = [g(0), g(\infty)] = [\frac{y}{v}, \frac{x}{u}]$. Pour δ et β polynômes vérifiant $\delta \mid P$, δ unitaire et $\deg \delta > \deg \beta$, on pose $m(\delta, \beta) = \left(\begin{smallmatrix} \delta & \beta \\ 0 & \frac{P}{\delta} \end{smallmatrix}\right)$ et $C(\delta, \beta) = m(\delta, \beta)\mathrm{SL}_2(A)$. Soit $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ telle que $(au + cv : bu + dv) \not\equiv (0, 0) \bmod \mathfrak{n}$. Alors la deuxième ligne de gM est non nulle modulo $\mathfrak{n}$. De plus, si M appartient à $g^{-1}C(\delta, \beta)$, on a $(\frac{P}{\delta}, \mathfrak{n}) = 1$ et

$$[m(\delta, \beta)^{-1}gM0, m(\delta, \beta)^{-1}gM\infty] = \xi\left(\frac{\delta}{P}(au + cv) : \frac{\delta}{P}(bu + dv)\right) = \xi(au+cv : bu+dv).$$

Les $m(\delta, \beta)$ formant un système de représentants de $M_2(A)_P/\mathrm{SL}_2(A)$ (proposition 2.31), on en déduit l'égalité des sommes, finies d'après le lemme 2.30,

$$\sum_{\substack{M \in \mathscr{S}_{\mathfrak{m}} \\ (u:v)M \text{ défini}}} \xi((u : v)M) = \sum_{\substack{\deg \beta < \deg \delta \\ \delta \mid P,\ \delta \text{ unitaire} \\ (\frac{P}{\delta}, \mathfrak{n}) = 1}} \sum_{M \in g^{-1}C(\delta,\beta) \cap \mathscr{S}_{\mathfrak{m}}} [m(\delta, \beta)^{-1}gM0, m(\delta, \beta)^{-1}gM\infty].$$

Comme le symbole modulaire $[r, s]$ ne dépend que de $(r) - (s)$ dans $\mathbf{Z}[\mathbf{P}^1(K)]$, la somme précédente ne dépend que de la somme suivante dans $\mathbf{Z}[\mathbf{P}^1(K)]$:

$$S = \sum_{\substack{\deg \beta < \deg \delta \\ \delta \mid P,\ \delta \text{ unitaire} \\ (\frac{P}{\delta}, \mathfrak{n}) = 1}} \sum_{M \in g^{-1}C(\delta,\beta) \cap \mathscr{S}_{\mathfrak{m}}} (m(\delta, \beta)^{-1}gM0) - (m(\delta, \beta)^{-1}gM\infty).$$

Soit M appartenant à $g^{-1}C(\delta, \beta) \cap \mathscr{S}_{\mathfrak{m}}$ avec $M0 \neq 0$. D'après la proposition 2.32, il existe une unique matrice $M' \in \mathscr{S}_{\mathfrak{m}} \cap M\mathrm{SL}_2(A)$ telle que $M'\infty = M0$. De plus, $M'\infty$ est distinct de ∞ (sinon on aurait $M'\infty = M0 = \infty = \frac{b}{d}$, donc $d = 0$ ce qui est exclu par $\deg d > \deg b$). On a donc l'égalité des sommes

$$\sum_{\substack{M \in g^{-1}C(\delta,\beta) \cap \mathscr{S}_{\mathfrak{m}} \\ M0 \neq 0}} (m(\delta, \beta)^{-1}gM0) = \sum_{\substack{M \in g^{-1}C(\delta,\beta) \cap \mathscr{S}_{\mathfrak{m}} \\ M'\infty \neq \infty}} (m(\delta, \beta)^{-1}gM'\infty).$$

En utilisant l'unicité dans la proposition 2.32, il ne reste que

$$\begin{aligned} S &= \sum_{\substack{\deg \beta < \deg \delta \\ \delta \mid P,\ \delta \text{ unitaire} \\ (\frac{P}{\delta}, \mathfrak{n}) = 1}} \left(\sum_{\substack{M \in g^{-1}C(\delta,\beta) \cap \mathscr{S}_{\mathfrak{m}} \\ M0 = 0}} (m(\delta, \beta)^{-1}gM0) - \sum_{\substack{M \in g^{-1}C(\delta,\beta) \cap \mathscr{S}_{\mathfrak{m}} \\ M'\infty = \infty}} (m(\delta, \beta)^{-1}gM'\infty) \right) \\ &= \sum_{\substack{\deg \beta < \deg \delta \\ \delta \mid P,\ \delta \text{ unitaire} \\ (\frac{P}{\delta}, \mathfrak{n}) = 1}} (m(\delta, \beta)^{-1}g0) - (m(\delta, \beta)^{-1}g\infty). \end{aligned}$$

En revenant aux symboles modulaires, on a

$$\sum_{\substack{M\in\mathscr{S}_{\mathfrak{m}}\\ (u:v)M \text{ défini}}} \xi((u:v)M) = \sum_{\substack{\deg\beta<\deg\delta\\ \delta|P,\ \delta \text{ unitaire}\\ (\frac{P}{\delta},\mathfrak{n})=1}} [m(\delta,\beta)^{-1}g0, m(\delta,\beta)^{-1}g\infty].$$

Enfin, comme $g0 = \frac{y}{v}$ et $g\infty = \frac{x}{u}$, on reconnaît $T_{\mathfrak{m}}[\frac{y}{v}, \frac{x}{u}] = T_{\mathfrak{m}}\ \xi(u:v)$ au membre de droite. □

2.3.2 Exemples d'ensembles $\mathscr{S}_{\mathfrak{m}}$

Soit P un générateur unitaire de l'idéal $\mathfrak{m}$. Si P est de degré 1, l'action de $T_{\mathfrak{m}}$ est donnée par la somme suivante de $2q$ symboles de Manin-Teitelbaum :

$$T_{\mathfrak{m}}\xi(u:v) = \sum_{\lambda\in\mathbf{F}_q} \xi(Pu:\lambda u+v) + \xi(u+\lambda v:Pv).$$

Si P est de degré 2, l'ensemble $\mathscr{S}_{\mathfrak{m}}$ est donné explicitement par l'énoncé suivant.

Proposition 2.33. *Soit $\mathfrak{m}$ l'idéal engendré par $P = T^2 + mT + n$ $(m, n \in \mathbf{F}_q)$. Posons*

$$M_1(Q) = \begin{pmatrix} P & Q \\ 0 & 1 \end{pmatrix} \qquad (Q \in A, \deg Q \leq 1)$$
$$M_2(Q) = \begin{pmatrix} 1 & 0 \\ Q & P \end{pmatrix} \qquad (Q \in A, \deg Q \leq 1)$$
$$N(a,c,d) = \begin{pmatrix} T+a & c \\ d & T+m-a \end{pmatrix} \qquad (a,c,d \in \mathbf{F}_q).$$

(i) Si P n'a pas de racine dans $\mathbf{F}_q$, alors $\mathscr{S}_{\mathfrak{m}}$ est formé des $3q^2 - q$ matrices

$$M_1(Q), M_2(Q) \qquad (Q \in A, \deg Q \leq 1)$$
$$N(a, c, \tfrac{-a^2+am-n}{c}) \qquad (a \in \mathbf{F}_q, c \in \mathbf{F}_q^\times).$$

(ii) Si P a une unique racine x dans $\mathbf{F}_q$, alors $\mathscr{S}_{\mathfrak{m}}$ est formé des $3q^2$ matrices

$$M_1(Q), M_2(Q) \qquad (Q \in A, \deg Q \leq 1)$$
$$N(-x, c, d) \qquad (c, d \in \mathbf{F}_q \text{ avec } c = 0 \text{ ou } d = 0)$$
$$N(a, c, \tfrac{-a^2+am-n}{c}) \qquad (a \in \mathbf{F}_q, a \neq -x, c \in \mathbf{F}_q^\times).$$

(iii) Si P a deux racines distinctes x_1, x_2 dans $\mathbf{F}_q$, alors $\mathscr{S}_{\mathfrak{m}}$ est formé des $3q^2 + q$ matrices

$$M_1(Q), M_2(Q) \qquad (Q \in A, \deg Q \leq 1)$$
$$N(-x_i, c, d) \qquad (i = 1 \text{ ou } 2, c, d \in \mathbf{F}_q \text{ avec } c = 0 \text{ ou } d = 0)$$
$$N(a, c, \tfrac{-a^2+am-n}{c}) \qquad (a \in \mathbf{F}_q, a \neq -x_1, a \neq -x_2, c \in \mathbf{F}_q^\times).$$

Démonstration. Soit $M = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \mathscr{S}_{\mathfrak{m}}$. Comme $\deg P = 2$, on a $\deg \alpha + \deg \delta = 2$. Si $\deg \alpha = 2$, alors δ est de degré 0 et unitaire, donc $\delta = 1$. Comme $\deg \gamma < \deg \delta$, γ est nul. En particulier, $P = \alpha\delta = \alpha$. La matrice est alors de la forme $M_1(\beta) = \left(\begin{smallmatrix} P & \beta \\ 0 & 1 \end{smallmatrix}\right)$ avec $\deg \beta \leq 2$. Le cas $\deg \delta = 2$ correspond aux matrices $M_2(\beta)$.

Il reste donc à traiter le cas où $\deg \alpha = \deg \delta = 1$. Écrivons $\alpha = T + a$ et $\delta = T + d$ ($a, d \in \mathbf{F}_q$), $\beta = b$ et $\gamma = c$. La condition $\det M = T^2 + mT + n$ est équivalente à :

$$\begin{cases} a + b &= m \\ ab - cd &= n. \end{cases}$$

En particulier, $cd = -a^2 + am - n$. Si x est une racine de P dans $\mathbf{F}_q$, alors $x^2 + mx + n = 0$ de sorte que $a = -x$, $b = m + x$ et $c = 0$ ou $d = 0$ conviennent. Si x n'est pas racine, les $a \in \mathbf{F}_q$ distincts des opposés des racines, $c \in \mathbf{F}_q^\times$ et $d = \frac{-a^2+am-n}{c}$ conviennent. $\square$

La méthode usuelle pour déterminer l'action d'un opérateur de Hecke sur un symbole de Manin-Teitelbaum est d'utiliser la définition de $T_{\mathfrak{m}}$ puis exprimer le résultat en termes de générateurs à l'aide de développement en fractions continuées ([Tei92a] p. 288). Le théorème 2.28 fournit une nouvelle méthode pour calculer les matrices d'opérateurs de Hecke dans une base de symboles de Manin-Teitelbaum. Pour l'opérateur $T_{\mathfrak{m}}$ sur $\mathbf{M}$, la méthode est la suivante.

(i) Établir la liste des éléments de $\mathbf{P}^1(A/\mathfrak{n})$.

(ii) Résoudre le système linéaire donné par les relations pour en extraire une base de générateurs.

(iii) Déterminer l'ensemble de matrices $\mathscr{S}_{\mathfrak{m}}$. Cela peut se faire en utilisant les conditions diophantiennes qui le définissent, ou l'algorithme présent dans la preuve du théorème 2.28.

(iv) Écrire la matrice de $T_{\mathfrak{m}}$ dans cette base à l'aide du théorème 2.28 et des relations entre les symboles modulaires.

Il serait intéressant d'avoir une estimation asymptotique de $\#\mathscr{S}_{\mathfrak{m}}$ afin de comparer la complexité de cette méthode à celle de la méthode usuelle.

Traitons l'exemple suivant : $q = 5$ et l'idéal premier $\mathfrak{n} = (T^3 + T + 1)$. L'espace des symboles modulaires est de dimension 6 et a pour base $\{\xi(1:0), \xi(T+a:1) \mid a \in \mathbf{F}_5\}$. Pour $\mathfrak{m} = (T^3 + 3T + 3)$, l'ensemble $\mathscr{S}_{\mathfrak{m}}$ est formé de 450 matrices. La matrice de l'opérateur $T_{\mathfrak{m}}$ dans cette base est :

$$\begin{pmatrix} 126 & 0 & 0 & 0 & 0 & 0 \\ 24 & -16 & -12 & -10 & -12 & -10 \\ 24 & -12 & -12 & -6 & -14 & -16 \\ 8 & 14 & 18 & 2 & 14 & 16 \\ 8 & 12 & 10 & 14 & 14 & 14 \\ 20 & -4 & -10 & -2 & -4 & -9 \end{pmatrix}$$

(nous avons traité cet exemple avec le logiciel de calcul Maple).

2.4 Un critère d'indépendance linéaire dans les symboles de Manin-Teitelbaum

Cette section est fondée sur une technique de Parent pour les symboles modulaires classiques ([Par99] § 5), elle-même suggérée par Merel.

***Notation* 2.34.** Soit $\mathcal{X}$ l'ensemble $\mathbf{P}^1(A/\mathfrak{n})/(\mathbf{F}_q^\times \times \mathbf{F}_q^\times)$. Soit $\mathcal{G}$ le graphe dont les sommets sont les éléments de $\mathcal{X}$ et dont les arêtes correspondent aux couples $(x, x\sigma), (x, x\tau)$ et $(x, x\tau^2)$ pour tout x dans $\mathcal{X}$.

Par abus de notation, l'image de $(u : v) \in \mathbf{P}^1(A/\mathfrak{n})$ dans $\mathcal{X}$ sera encore notée $(u : v)$. Contrairement à son analogue classique, le graphe $\mathcal{G}$ n'est pas forcément connexe. Par exemple si l'idéal $\mathfrak{n}$ est premier, les sommets $(1 : 1)$ et $(P : 1)$, où $P \in A$ est non constant et premier à $\mathfrak{n}$, ne sont pas dans la même composante connexe de $\mathcal{X}$.

Soit R un groupe abélien. Notons $R[\mathcal{X}]$ le R-module libre engendré par $\mathcal{X}$ et $R[\mathcal{X}]^\sigma$ (resp. $R[\mathcal{X}]^\tau$) le sous-module des éléments de $R[\mathcal{X}]$ stables par l'action de σ (resp. τ). La présentation de $\mathbf{M}(R)$ (théorème 2.27) donne la suite exacte

$$R[\mathcal{X}]^\sigma \times R[\mathcal{X}]^\tau \longrightarrow R[\mathcal{X}] \longrightarrow \mathbf{M}(R) \longrightarrow 0. \tag{2.8}$$

La première application est donnée par $(\sum_x \alpha_x[x], \sum_x \beta_x[x]) \mapsto \sum_x \alpha_x[x] + \sum_x \beta_x[x]$, la deuxième par $\sum_x \lambda_x[x] \mapsto \sum_x \lambda_x \xi(x)$.

Le résultat suivant est l'analogue de la proposition 5.4 de [Par99]. Sa démonstration, que nous rappelons ici, est de nature combinatoire et reste valable pour les symboles modulaires de Manin-Teitelbaum.

Proposition 2.35. *Soit S un sous-ensemble de $\mathcal{X}$ et x un élément de $\mathcal{X}$ n'appartenant pas à S. Supposons que $x\sigma$ et $x\tau$ (resp. $x\sigma$ et $x\tau^2$) sont dans la même composante connexe de $\mathcal{G} - (S \cup \{x\})$. Alors le symbole modulaire $\xi(x)$ n'appartient pas au sous-module de $\mathbf{M}(R)$ engendré par $\xi(S)$.*

Démonstration. Supposons qu'il existe une relation $\xi(x) = \sum_{y \in S} \lambda_y \xi(y)$, avec $\lambda_y \in R$ pour tout y. La différence des deux membres étant nulle dans $\mathbf{M}(R)$, on a par la suite exacte (2.8) l'égalité suivante dans $R[\mathcal{X}]$

$$x - \sum_{y \in S} \lambda_y y = \sum \alpha_z[z] - \sum \beta_z[z],$$

avec $\alpha_{z\sigma} = \alpha_z$ et $\beta_{z\tau} = \beta_z$ pour tout z. Pour z n'appartenant pas à $S \cup \{x\}$, le coefficient de z est nul donc $\alpha_z = \beta_z$. Soit $\mathcal{C}$ une composante connexe de $\mathcal{G} - (S \cup \{x\})$. Pour une arête de $\mathcal{C}$ de la forme $(z, z\sigma)$ (resp. $(z, z\tau)$, resp. $(z, z\tau^2)$), on a $\beta_z = \alpha_z = \alpha_{z\sigma} = \beta_{z\sigma}$ (resp. $\alpha_z = \beta_z = \beta_{z\tau} = \alpha_{z\tau}$, resp. $\alpha_z = \beta_z = \beta_{z\tau^2} = \alpha_{z\tau^2}$). En procédant de proche en proche, on voit que les suites $(\alpha_z)_{z \in S \cup \{x\}}$ et $(\beta_z)_{z \in S \cup \{x\}}$ sont constantes et égales dans $\mathcal{C}$.

Maintenant, soit $\mathcal{C}$ la composante connexe de $\mathcal{G} - (S \cup \{x\})$ contenant $x\sigma$ et $x\tau$ (resp. $x\sigma$ et $x\tau^2$). On obtient alors $\alpha_{x\sigma} = \beta_{x\tau}$ (resp. $\alpha_{x\sigma} = \beta_{x\tau^2}$). Cela contredit $1 = \alpha_x - \beta_x = \alpha_{x\sigma} - \beta_{x\tau}$ (resp. $\alpha_{x\sigma} - \beta_{x\tau^2}$). □

Par la suite nous ferons usage de l'ensemble suivant de sommets de $\mathcal{G}$.

Lemme 2.36. *Soit $x = (1 : P) \in \mathcal{X}$ avec $P \in A$. Supposons* $\deg \mathfrak{n} > 2 \deg P$.

(i) Les seuls couples $(c, d) \in A \times A$ vérifiant $\deg c < \deg d \leq \deg P$ *et $x = (c : d)$ sont les (λ, P) avec $\lambda \in \mathbf{F}_q^\times$.*

(ii) Considérons l'ensemble de sommets de $\mathcal{X}$:

$$\{x\sigma, x\sigma\tau^2, x\sigma\tau^2\sigma, x\tau\}$$

c'est-à-dire

$$\{(-P : 1) = (P : 1), (-P - 1 : P) = (P + 1 : P), (-P : P + 1) = (-P : -1 - P)\}.$$

Cet ensemble ne contient aucun sommet $(c : d)$ de $\mathcal{X}$ vérifiant $\deg c < \deg d \leq \deg P$. *En particulier, il ne contient pas x.*

Démonstration. (i) Soit $(c, d) \in A \times A$ avec $\deg c < \deg d \leq \deg P$ et $x = (c : d) \in \mathcal{X}$. Alors il existe $\alpha \in \mathbf{F}_q^\times$ tel que $\alpha c P - d \equiv 0 \mod \mathfrak{n}$.

Supposons $\alpha c P - d \neq 0$. Il est facile de voir que c est non nul. Le polynôme $\alpha c P - d$ est donc de degré $\leq 2\deg(P) - 1$ et engendre un idéal contenu dans $\mathfrak{n}$, ce qui contredit l'hypothèse.

On a donc $\alpha c P = d \in \mathbf{F}_q[T]$. Comme $\deg d > \deg c$, on en déduit que c est non nul. Un raisonnement sur le degré montre que $c \in \mathbf{F}_q^\times$. Comme P et d sont unitaires, on a $\alpha c = 1$, donc $d = P$ et $c = \alpha^{-1}$.

(ii) Soit $(c : d)$ tel que $\deg c < \deg d \leq \deg P$.

Si $x\sigma = (c : d)$, il existe $\alpha \in \mathbf{F}_q^\times$ tel que $dP - \alpha c \equiv 0 \mod \mathfrak{n}$. Le polynôme $dP - \alpha c$ est non nul : sinon, de l'égalité $dP = \alpha c$ et $d \neq 0$ on déduit $c \neq 0$, ce qui contredirait $\deg c < \deg d$. Par ailleurs, il est de degré $\deg d + \deg P \leq 2 \deg P$.

Si $x\tau = (c : d)$, il existe $\alpha_2 \in \mathbf{F}_q^\times$ tel que $dP + \alpha_2 c(P + 1) \equiv 0 \mod \mathfrak{n}$. Si $x\sigma\tau^2 = (c : d)$, il existe $\alpha_3 \in \mathbf{F}_q^\times$ tel que $d(P + 1) + \alpha_3 c P \equiv 0 \mod \mathfrak{n}$. Si $x\sigma\tau^2\sigma = (c : d)$, il existe $\alpha_4 \in \mathbf{F}_q^\times$ tel que $dP + \alpha_4 c(P + 1) \equiv 0 \mod \mathfrak{n}$. Comme précédemment, on montre que les polynômes de ces congruences sont non nuls et de degré $\leq 2 \deg P$. Dans tous les cas, $\mathfrak{n}$ est de degré $\leq 2 \deg P$, ce qui contredit l'hypothèse.

□

2.5 Une base explicite de symboles de Manin-Teitelbaum

Lorsque l'idéal $\mathfrak{n}$ est premier, nous exhibons une famille libre de symboles de Manin-Teitelbaum. Si $\mathfrak{n}$ est de degré impair, nous verrons que c'est une base de l'espace des symboles modulaires. Remarquons que dans la théorie classique des symboles modulaires [Man72], à notre connaissance, on ne sait pas en général exhiber de base de l'espace des symboles modulaires.

Proposition 2.37. *Soit $\mathfrak{n}$ un idéal premier de A de degré d. Supposons que R est $\mathbf{Z}$ ou un corps. Alors les symboles de Manin-Teitelbaum $\xi(1 : 0)$ et $\xi(P : Q)$, où P et Q parcourent les polynômes unitaires de A premiers entre eux et tels que* $\deg Q < \deg P < d/2$, *sont R-linéairement indépendants dans $\mathbf{M}(R)$.*

Démonstration. Notons $\mathcal{S}$ l'ensemble des couples $(1,0)$ et $(P,Q) \in A \times A$ avec P et Q unitaires premiers entre eux et vérifiant $\deg Q < \deg P < d/2$. Notons Σ l'image de $\mathcal{S}$ dans $\mathcal{X}$.

On commence par remarquer que les images des éléments de $\mathcal{S}$ dans Σ sont distinctes deux à deux. En effet, supposons qu'il existe (P_1, Q_1) et (P_2, Q_2) distincts dans $\mathcal{S}$ tels que $(P_1 : Q_1) = (P_2 : Q_2)$ dans $\mathcal{X}$. Alors il existerait $\alpha \in \mathbf{F}_q^\times$ tel que $\alpha P_1 Q_2 \equiv P_2 Q_1 \mod \mathfrak{n}$. Posons $R = \alpha P_1 Q_2 - P_2 Q_1 \in A$. Ce polynôme est non nul : en effet, si $R = 0$, en comparant les coefficients des termes de plus haut degré, on obtient $\alpha = 1$, donc $P_1 Q_2 = P_2 Q_1$. Ainsi, P_1, qui est premier à Q_1, divise P_2. De même, P_2 divise P_1 et, ces deux polynômes étant unitaires, ils sont égaux. On a alors $Q_1 = Q_2$ et on a montré que R est non nul. Finalement, comme R est divisible par $\mathfrak{n}$, on a $\deg \mathfrak{n} \leq \deg R < \frac{d}{2} + \frac{d}{2} = d$. Ceci est impossible, et l'affirmation est démontrée.

Ainsi, pour démontrer la proposition, il suffit de prouver que la famille de symboles modulaires $(\xi(x))_{x \in \Sigma}$ est libre sur R. Dans $\mathrm{SL}_2(\mathbf{F}_q)$, on a $\sigma\tau^2 = \left(\begin{smallmatrix} -1 & 0 \\ 1 & -1 \end{smallmatrix}\right)$ et, pour tout $k \in \mathbf{Z}$,

$$(\sigma\tau^2)^k = (-1)^k \begin{pmatrix} 1 & 0 \\ -k & 1 \end{pmatrix}, \quad \tau(\sigma\tau^2)^k = (-1)^k \begin{pmatrix} k & -1 \\ k+1 & -1 \end{pmatrix}.$$

En particulier, on a $\tau(\sigma\tau^2)^{p-1} = (-1)^p \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. Soit $x = (P : Q) \in \Sigma$. Considérons l'ensemble suivant de sommets de $\mathcal{G}$

$$\{x\tau, (x\tau)\tau, (x\tau)\tau\sigma, (x\tau)\tau(\sigma\tau^2), (x\tau)\tau(\sigma\tau^2)\sigma, \ldots, (x\tau)\tau(\sigma\tau^2)^{p-1}\}.$$

On a $x\tau = (Q : -P - Q)$ et $(x\tau)\tau(\sigma\tau^2)^{p-1} = ((-1)^p Q : (-1)^{p+1} P) = (Q : P) = x\sigma$ dans $\mathcal{X}$. Donc l'ensemble précédent est $\{(Q : -P - Q), (Q : P)\} \cup X \cup Y$ où X et Y sont définis comme suit :

$$X = \{x_k = (x\tau)\tau(\sigma\tau^2)^k = ((k+1)P + Q : P) \mid 0 \leq k \leq p-2\} \subset \mathcal{X},$$
$$Y = \{y_k = (x\tau)\tau(\sigma\tau^2)^k\sigma = (P : (k+1)P + Q) \mid 0 \leq k \leq p-2\} \subset \mathcal{X}.$$

Montrons que $X \cap \Sigma = \emptyset$. Supposons qu'il existe un entier k, $0 \leq k \leq p-2$, avec $x_k = (P_1 : Q_1)$ dans Σ. Alors il existerait $\lambda \in \mathbf{F}_q^\times$ vérifiant

$$Q_1((k+1)P + Q) + \lambda P_1 P \equiv 0 \mod \mathfrak{n}.$$

Soit D le polynôme du membre de gauche. Il est non nul : en effet, comme $k \leq p-2$, $k+1$ est non nul dans $\mathbf{F}_q$ donc $Q + (k+1)P$ est de degré $\deg P$. De plus, on a les inégalités

$$\begin{aligned} \deg Q_1 &< d/2 \\ \deg((k+1)P + Q) &< d/2 \\ \deg P_1 &< d/2 \\ \deg P &< d/2, \end{aligned}$$

de sorte que le degré de D est strictement inférieur à d. Cela contredit le fait que $D \equiv 0 \mod \mathfrak{n}$.

On démontre de la même façon que $Y \cap \Sigma = \emptyset$ et que $x\tau$ et $x\sigma$ ne sont pas dans Σ. Appliquons la proposition 2.35 : pour tout $(P : Q) \in \Sigma$, $\xi(P : Q)$ n'est pas combinaison R-linéaire des $\xi(P' : Q')$ pour $(P' : Q')$ dans Σ distinct de $(P : Q)$, ce qui traduit l'indépendance de la famille sur R. □

Le lemme suivant et son corollaire sont consacrés au dénombrement de cette famille.

Lemme 2.38. *Soient m et n des entiers tels que $m > n \geq 0$. Le cardinal $N_{n,m}$ de l'ensemble des couples $(P, Q) \in A \times A$ avec P, Q unitaires,* $\deg Q = n$, $\deg P = m$ *et P et Q non premiers entre eux est :*

$$N_{n,m} = \begin{cases} 0 & \textit{si } n = 0\,; \\ q^{m+n-1} & \textit{si } n > 0. \end{cases}$$

Démonstration. Fixons un entier $l > 0$. Nous allons montrer que pour tout $n \geq 0$,

$$N_{n,n+l} = \begin{cases} 0 & \text{si } n = 0\,; \\ q^{2n+l-1} & \text{si } n > 0 \end{cases}$$

par récurrence forte sur n. Si $n = 0$, il est facile de voir que $N_{0,l} = 0$. Supposons $n > 0$ et la propriété établie sur $N_{k,k+l}$ pour tout $k < n$. Soit un couple de polynômes (P, Q) unitaires non premiers entre eux avec $n = \deg Q < n + l = \deg P$. Le pgcd unitaire D de P et Q est de degré $1 \leq r \leq n$. On écrit alors de façon unique :

$$\begin{aligned} P &= D \cdot A_{n+l-r} \\ Q &= D \cdot B_{n-r}, \end{aligned}$$

avec A_{n+l-r} unitaire de degré $n+l-r$, B_{n-r} unitaire de degré $n-r$, premiers entre eux. Il y a q^r possibilités pour D. Pour les couples (A_{n+l-r}, B_{n-r}), il y a $q^{2(n-r)+l} - N_{n-r,n-r+l}$ possibilités. Ainsi, on a la relation de récurrence :

$$N_{n,n+l} = \sum_{r=1}^{n} q^r \left(q^{2(n-r)+l} - N_{n-r,n-r+l}\right).$$

Pour $r = n$, $N_{0,l} = 0$ et pour $r < n$, $N_{n-r,n-r+l}$ vaut $q^{2(n-r)+l-1}$ par hypothèse de récurrence. En remplaçant et en calculant les sommes des suites géométriques, on obtient :

$$N_{n,n+l} = \frac{q^{2n+l} - q^{n+l}}{q-1} - \frac{q^{2n+l-1} - q^{n+l}}{q-1} = q^{2n+l-1},$$

ce qu'il fallait démontrer. □

Corollaire 2.39. *Soit m un entier ≥ 1. Le cardinal de l'ensemble des couples $(P, Q) \in A \times A$ unitaires, premiers entre eux et vérifiant* $\deg Q < \deg P = m$, *est $N'_m = q^{2m-1}$.*

Démonstration. Notons r le degré de Q. Le cardinal de l'ensemble des couples $(P, Q) \in A \times A$ unitaires vérifiant $\deg Q < \deg P = m$ est :

$$q^m \sum_{r=0}^{m-1} q^r = \frac{q^m(q^m - 1)}{q-1}.$$

Parmi eux, ceux avec P et Q non premiers entre eux sont, d'après le lemme précédent, au nombre de :

$$\sum_{r=1}^{m-1} N_{r,m} = \sum_{r=1}^{m-1} q^{r+m-1} = \frac{q^{2m-1} - q^{2m}}{q-1}.$$

Le cardinal de l'ensemble cherché est la différence, qui vaut q^{2m-1}. □

Théorème 2.40. *Soit $\mathfrak{n}$ un idéal premier de A de degré impair $d \geq 3$. Les symboles de Manin-Teitelbaum $\xi(1:0)$ et $\xi(P:Q)$, où P et Q parcourent les polynômes unitaires de A premiers entre eux et tels que $\deg Q < \deg P < d/2$, forment une base sur $\mathbf{Z}$ de $\mathbf{M}$.*

***Remarque* 2.41.** (i) En particulier, si $\mathfrak{n}$ est premier de degré impair ≥ 3, le $\mathbf{Z}$-module $\mathbf{M}$ est libre, donc sans torsion (voir aussi la remarque de [Tei92a] p. 278).

(ii) Si $\mathfrak{n}$ est premier de degré pair, la torsion de $\mathbf{M}$ est non nulle, donc il sera impossible de trouver une base de $\mathbf{M}$ sur $\mathbf{Z}$. Par contre, on aimerait obtenir une présentation explicite minimale par générateurs et relations.

(iii) La démonstration ne fournit pas un algorithme ou une formule permettant d'exprimer n'importe quel symbole de Manin-Teitelbaum dans cette base, qu'il serait pourtant intéressant d'établir.

(iv) La formule donnant l'action des opérateurs de Hecke sur les symboles de Manin-Teitelbaum (théorème 2.28) ne stabilise pas les éléments de cette base. On se demande s'il serait possible de trouver une formule correspondant à un autre ensemble de matrices $\mathscr{S}_{\mathfrak{m}}$ et stabilisant une base explicite.

Démonstration. Posons $d = 2m+1$. D'après la proposition 2.37 appliquée à $R = \mathbf{Q}$, la famille de l'énoncé est libre sur $\mathbf{Q}$. En reprenant la notation du corollaire 2.39, elle possède

$$1 + \sum_{k=1}^{m} N'_k = 1 + \sum_{k=1}^{m} q^{2k-1}$$

éléments. Par ailleurs, le genre de $X_0(\mathfrak{n})$ est, d'après la proposition 1.23,

$$g(X_0(\mathfrak{n})) = \frac{q^{2m+1} - q}{q^2 - 1} = \frac{q(q^2-1)(1 + \ldots + q^{2(m-2)} + q^{2(m-1)})}{q^2-1} = \sum_{k=1}^{m} q^{2k-1}.$$

donc, d'après la proposition 2.19,

$$\dim_{\mathbf{Q}} \mathbf{M}(\mathbf{Q}) = 1 + \sum_{k=1}^{m} q^{2k-1}.$$

Ceci montre que la famille considérée est une base de $\mathbf{M}(\mathbf{Q})$. Montrons qu'elle engendre $\mathbf{M}$ sur $\mathbf{Z}$. Soit M le sous $\mathbf{Z}$-module de $\mathbf{M}$ qu'elle engendre. Montrons qu'il est d'indice 1 dans $\mathbf{M}$. Pour cela, supposons qu'il existe un nombre premier l divisant cet indice. Alors il existe un symbole modulaire $m \in \mathbf{M}$, $m \notin M$ avec $lm \in M$. Cela signifie qu'il existe $(\lambda_{P,Q})_{(P,Q)\in A\times A} \in \mathbf{Z}$ vérifiant

$$lm = \sum_{P,Q} \lambda_{P,Q}\, \xi(P:Q) \quad \in \mathbf{M}.$$

L'image de ce symbole modulaire dans $\mathbf{M}(\mathbf{F}_l)$ est nulle. D'après la proposition 2.37 appliquée à $R = \mathbf{F}_l$, $\lambda_{P,Q}$ est divisible par l pour tout (P,Q), ce qui contredit le fait que $m \notin M$. Donc la famille est génératrice sur $\mathbf{Z}$; comme elle est libre sur $\mathbf{Z}$, c'est une base de $\mathbf{M}$ sur $\mathbf{Z}$. □

Corollaire 2.42. *Soit $\mathfrak{n}$ un idéal premier de A de degré impair $d \geq 3$. Les symboles de Manin-Teitelbaum $\xi(P:Q)$, où P et Q parcourent les polynômes unitaires de A premiers entre eux et tels que $\deg Q < \deg P < d/2$, forment une base sur $\mathbf{Z}$ de $\mathbf{M}^0$.*

Démonstration. Comme $\mathfrak{n}$ est premier, le $\mathbf{Z}$-module $\mathbf{M}$ est la somme directe des sous-modules $\mathbf{M}^0$ et $\mathbf{Z}\xi(1:0)$. Il s'agit donc de montrer que le symbole modulaire $\xi(P:Q)$, où P, Q sont unitaires premiers entre eux et vérifient $\deg Q < \deg P < d/2$, est parabolique. Il existe $U, V \in A$ vérifiant $UP + VQ = 1$. La matrice $\left(\begin{smallmatrix} V & -U \\ P & Q \end{smallmatrix}\right)$ est dans $\mathrm{GL}(2, A)$ et on a

$$\xi(P:Q) = \left[-\frac{U}{Q} : \frac{V}{P}\right] = \left[-\frac{U}{Q} : 0\right] + \left[0 : \frac{V}{P}\right].$$

Prouvons que ces deux derniers symboles modulaires sont paraboliques. Soit N un générateur de $\mathfrak{n}$. On considère la fraction $\frac{U}{Q}$ comme réduite. Alors, comme N est premier, Q est premier à UN, et il existe $\alpha, \beta \in A$ tels que $\alpha Q + \beta UN = 1$. La matrice $\gamma = \left(\begin{smallmatrix} \alpha & -U \\ \beta N & Q \end{smallmatrix}\right) \in \Gamma_0(\mathfrak{n})$ vérifie $\gamma 0 = -\frac{U}{Q}$. On procède de la même manière pour $\frac{V}{P}$. Donc $\xi(P:Q)$ appartient à $\mathbf{M}^0$. □

***Remarque* 2.43.** Si $d = 3$, Gekeler a explicité une base du $\mathbf{Z}$-module $\mathbf{H}$ (voir [Gek85] et [Gek97b] 6.2.ii). D'après la remarque 2.20, ce résultat peut être rapproché du corollaire 2.42 lorsque $d = 3$.

2.6 L'élément d'enroulement e

Définition 2.44. On appelle *élément d'enroulement* l'unique symbole modulaire parabolique $\mathbf{e} \in \mathbf{M}^0(\mathbf{Q})$ qui correspond à la forme linéaire $F \mapsto \int_{[0,\infty]} F$ sur $\mathbf{H}(\mathbf{Q})$ d'après le théorème 2.24.

Notons que la propriété

$$\int_{[0,\infty]} F = \int_{\mathbf{e}} F \qquad (F \in \mathbf{H}(\mathbf{Q}))$$

s'étend par $\mathbf{C}$-linéarité aux formes automorphes $F \in \mathbf{H}(\mathbf{C})$.

Définition 2.45. La *partie d'Eisenstein* $\mathcal{E}$ est le noyau à gauche de l'accouplement d'intégration

$$\langle\ ,\ \rangle : \mathbf{M}(\mathbf{Q}) \times \mathbf{H}(\mathbf{Q}) \longrightarrow \mathbf{Q}.$$

C'est un sous $\mathbf{Q}$-espace vectoriel de $\mathbf{M}(\mathbf{Q})$.

On pourra comparer la définition précédente avec la définition 3.11.4 de [Gek97b], à la lumière de nos remarques 2.20 et 2.23.

Lemme 2.46. *L'application linéaire composée*

$$\mathbf{M}^0(\mathbf{Q}) \longrightarrow \mathbf{M}(\mathbf{Q}) \longrightarrow \mathbf{M}(\mathbf{Q})/\mathcal{E}$$

est un isomorphisme de $\mathbf{Q}$*-espaces vectoriels. Par cet isomorphisme, l'élément d'enroulement correspond à la classe de* $[0, \infty]$ *dans* $\mathbf{M}(\mathbf{Q})/\mathcal{E}$.

Démonstration. Notons $\varphi : \mathbf{M}^0(\mathbf{Q}) \to \mathbf{M}(\mathbf{Q})/\mathcal{E}$. Son noyau est $\mathbf{M}^0(\mathbf{Q}) \cap \mathcal{E}$, qui est nul d'après le théorème 2.24. Donc φ est injective et $\dim_{\mathbf{Q}} \mathbf{M}(\mathbf{Q})/\mathcal{E} \geq g(X_0(\mathfrak{n}))$. Par construction, $\mathcal{E}$ est le noyau de

$$\begin{array}{ccc} \mathbf{M}(\mathbf{Q}) & \longrightarrow & \mathrm{Hom}(\mathbf{H}(\mathbf{Q}), \mathbf{Q}) \\ m & \longmapsto & (F \mapsto \int_m F) \end{array}$$

donc $\mathbf{M}(\mathbf{Q})/\mathcal{E}$ s'injecte dans $\mathrm{Hom}(\mathbf{H}(\mathbf{Q}), \mathbf{Q})$ qui est de dimension $g(X_0(\mathfrak{n}))$. Nous avons démontré que φ est bijective. Pour la deuxième affirmation, il s'agit de montrer que $\mathbf{e} - [0, \infty]$ appartient à la partie d'Eisenstein. Cela vient précisément de la définition de $\mathbf{e}$. $\square$

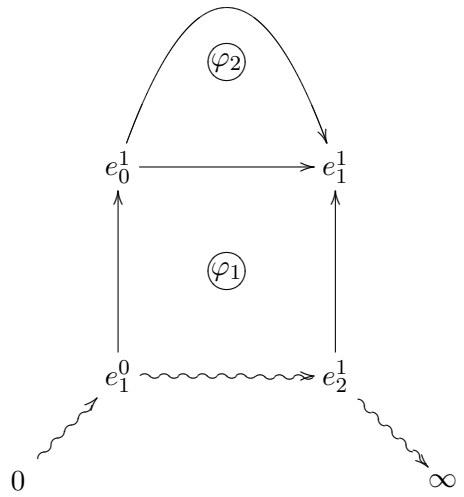
Un exemple de calcul de e. Pour un idéal $\mathfrak{n}$ donné, la détermination du graphe quotient $\Gamma_0(\mathfrak{n})\backslash\mathcal{T}$, comme dans [Gek85, GN95], permet d'exprimer $\mathbf{e}$ dans une base de cycles du graphe. L'accouplement

$$\begin{array}{rcl} H_1(\Gamma_0(\mathfrak{n})\backslash\mathcal{T}, \mathbf{Q}) \times H_1(\Gamma_0(\mathfrak{n})\backslash\mathcal{T}, \mathrm{ptes}, \mathbf{Q}) & \longrightarrow & \mathbf{Q} \\ (\varphi_1, \varphi_2) & \longmapsto & \langle \varphi_1, \varphi_2 \rangle = \displaystyle\sum_{\tilde{e} \in \Gamma_0(\mathfrak{n})\backslash\mathcal{T}} \frac{1}{n(\tilde{e})} \varphi_1(\tilde{e}) \varphi_2(\tilde{e}) \end{array}$$

correspond, d'après la remarque 2.23, à l'accouplement d'intégration entre formes automorphes et symboles modulaires. Pour simplifier, supposons $q = 2$ et $\mathfrak{n}$ de degré 3, auquel cas chaque arête du graphe fini $(\Gamma_0(\mathfrak{n})\backslash\mathcal{T})^0$ a une multiplicité, au sens de l'équation (2.1) page 28, égale à 1 (cela résulte du lemme 5.6 de [Gek85]). On a alors $n(\tilde{e}) = 1$ pour toute arête de $(\Gamma_0(\mathfrak{n})\backslash\mathcal{T})^0$.

Soit $\varphi_{(0,\infty)}$ la projection dans $H_1(\Gamma_0(\mathfrak{n})\backslash\mathcal{T}, \mathrm{ptes}, \mathbf{Q})$ de la géodésique de $\mathcal{T}$ reliant 0 à ∞. Soit $\mathbf{c}$ l'élément de $H_1(\Gamma_0(\mathfrak{n})\backslash\mathcal{T}, \mathbf{Q})$ correspondant à $\mathbf{e}$ via l'isomorphisme de la proposition 2.19. Le cycle $\mathbf{c}$ est alors l'unique élément de $H_1(\Gamma_0(\mathfrak{n})\backslash\mathcal{T}, \mathbf{Q})$ tel que l'on ait $\langle \varphi, \mathbf{c} \rangle = \langle \varphi, \varphi_{(0,\infty)} \rangle$ pour tout $\varphi \in H_1(\Gamma_0(\mathfrak{n})\backslash\mathcal{T}, \mathbf{Q})$.

Exemple 2.47 ($q = 2$, $\mathfrak{n} = (T^3 + T + 1)$ idéal premier)**.** Le graphe quotient $\Gamma_0(\mathfrak{n})\backslash\mathcal{T}$ est de genre 2 et possède 2 pointes. D'après [Gek85] (5.3), sa structure est la suivante :



(nous avons adopté les notations de [Gek85] pour les sommets du graphe – signalons qu'une coquille semble s'être glissée dans le tableau (5.3) de *loc. cit.* : avec ses notations, le représentant du sommet e_0^1 est u et non pas 0). Le cycle relatif aux pointes $\varphi_{(0,\infty)}$ est représenté en flèches ondulées.

Soient φ_1, φ_2 les deux cycles de longueur respectivement 4 et 2, orientés dans le sens trigonométrique, indiqués sur le diagramme. Ils forment une base de $H_1(\Gamma_0(\mathfrak{n})\backslash\mathcal{T}, \mathbf{Z})$.

Si $\varphi = a\varphi_1 + b\varphi_2$, avec $a, b \in \mathbf{Q}$, alors $\langle \varphi, \mathbf{c} \rangle = a$. En utilisant $\langle \varphi_1, \varphi_1 \rangle = 4$, $\langle \varphi_2, \varphi_2 \rangle = 2$ et $\langle \varphi_1, \varphi_2 \rangle = \langle \varphi_2, \varphi_1 \rangle = -1$, on obtient : $\mathbf{e} = \frac{1}{7}(2\varphi_1 + \varphi_2) \in H_1(\Gamma_0(\mathfrak{n})\backslash\mathcal{T}, \mathbf{Q})$.

Jusqu'à la fin de cette section, on suppose l'idéal $\mathfrak{n}$ *premier.*

***Notation* 2.48.** On pose, pour tout idéal $\mathfrak{m}$ de A,

$$\delta(\mathfrak{m}) = \sum_{\substack{\mathfrak{p} \text{ idéal} \\ \mathfrak{m} \subset \mathfrak{p}, (\mathfrak{p}, \mathfrak{n}) = 1}} q^{\deg \mathfrak{p}}$$

et $\eta_{\mathfrak{m}} = T_{\mathfrak{m}} - \delta(\mathfrak{m})$ dans $\mathrm{End}(\mathbf{M})$.

Lemme 2.49. *Pour tout idéal* $\mathfrak{m}$*, le symbole modulaire* $\eta_{\mathfrak{m}}[0, \infty]$ *appartient à* $\mathbf{M}^0$.

Démonstration. Soit N un générateur de $\mathfrak{n}$. Écrivons le générateur unitaire de $\mathfrak{m}$ sous la forme $P = N^j r$ avec $j \geq 0$, $r \in A$ et $(r, N) = 1$. Par définition, on a $T_{\mathfrak{m}}[0, \infty] = \sum [\frac{b}{d}, \infty]$, la somme portant sur les $b, d \in A$ tels que d est un diviseur unitaire de P, $(\frac{P}{d}, N) = 1$ et $\deg b < \deg d$. Elle vaut donc

$$T_{\mathfrak{m}}[0, \infty] = \sum \left[\frac{b}{N^j s}, \infty \right],$$

la somme portant sur les $s, b \in A$ avec s diviseur unitaire de r et $\deg b < \deg(N^j s)$. Si b n'est pas divisible par N^j, alors le symbole modulaire $\left[\frac{b}{N^j s}, \infty \right]$ est de bord nul car N divise $\frac{N^j s}{(b, N^j s)}$. Donc $T_{\mathfrak{m}}[0, \infty]$ a même bord que le symbole modulaire

$$\sum \left[\frac{b}{N^j s}, \infty \right],$$

où la somme porte sur les $s, b \in A$ avec s diviseur unitaire de r, $N^j \mid b$ et $\deg b < \deg(N^j s)$. Écrivons $[\frac{b}{N^j s}, \infty] = [\frac{b}{N^j s}, 0] + [0, \infty]$. Comme $N^j \mid b$, on a $(Nb, N^j s) = (b, N^j s)$ et le symbole modulaire correspondant $[\frac{b}{N^j s}, 0]$ est de bord nul. Donc $T_{\mathfrak{m}}[0, \infty]$ a même bord que le symbole modulaire $k\,[0, \infty]$, où k est le cardinal de l'ensemble des couples $(s, b) \in A \times A$ avec s diviseur unitaire de r, $\deg b < \deg(N^j s)$ et $N^j \mid b$. Or, k est aussi le cardinal de l'ensemble des couples $(s, \beta) \in A \times A$ avec s unitaire divisant r et $\deg \beta < \deg s$, c'est-à-dire

$$\sum_{s \text{ unitaire}, s \mid r} q^{\deg s} = \sum_{\substack{n \mid N^j r,\ (n, N) = 1 \\ n \text{ unitaire}}} q^{\deg n} = \delta(\mathfrak{m}).$$

□

Corollaire 2.50. *Pour tout idéal* $\mathfrak{m}$*, on a l'égalité*

$$\eta_{\mathfrak{m}}[0, \infty] = \eta_{\mathfrak{m}} \mathbf{e}$$

dans $\mathbf{M}^0$.

Démonstration. Les symboles modulaires $[0,\infty]$ et $\mathbf{e}$ définissent la même intégration des formes automorphes. Par compatibilité de l'accouplement aux opérateurs de Hecke, il en est de même de $\eta_{\mathfrak{m}}[0,\infty]$ et $\eta_{\mathfrak{m}}\mathbf{e}$. Comme ils sont tous deux dans $\mathbf{M}^0(\mathbf{Q})$ par le lemme précédent, ils sont égaux. □

Définition 2.51 (voir aussi [Pál05] 7.10)**.** On appelle *idéal d'Eisenstein* l'idéal de $\mathbf{T}$ engendré par les éléments $T_{\mathfrak{m}} - \delta(\mathfrak{m})$, où $\mathfrak{m}$ décrit les idéaux premiers de A distincts de $\mathfrak{n}$. On le note I_E.

D'après le corollaire 2.50, on a $I_E\mathbf{e} \subset \mathbf{M}^0$. Par un théorème de Pál ([Pál07a] th. 1.2), le groupe $\mathbf{T}/I_E$ est cyclique isomorphe à $\mathbf{Z}/n(\mathfrak{n})\mathbf{Z}$ où

$$n(\mathfrak{n}) = \begin{cases} \frac{q^{\deg \mathfrak{n}}-1}{q-1} & \text{si } \deg \mathfrak{n} \text{ est impair ;} \\ \frac{q^{\deg \mathfrak{n}}-1}{q^2-1} & \text{si } \deg \mathfrak{n} \text{ est pair.} \end{cases}$$

Proposition 2.52. *Il existe un plus petit entier $d_{\mathbf{e}} \in \mathbf{Z}$ tel que $d_{\mathbf{e}}\mathbf{e} \in \mathbf{M}^0$. On l'appelle dénominateur de $\mathbf{e}$. Il est premier à p.*

Démonstration. Soit $\overline{\mathbf{e}}$ la classe de $\mathbf{e}$ dans le $\mathbf{T}$-module $\mathbf{M}^0(\mathbf{Q})/\mathbf{M}^0$. Comme $I_E\mathbf{e} \subset \mathbf{M}^0$, on a $I_E\overline{\mathbf{e}} = 0$. L'homomorphisme canonique de $\mathbf{T}$-modules $\mathbf{T} \to \mathbf{T}\overline{\mathbf{e}}$ passe donc au quotient en un homomorphisme surjectif de $\mathbf{T}$-modules

$$\mathbf{T}/I_E \to \mathbf{T}\overline{\mathbf{e}}.$$

En particulier, $\mathbf{T}\overline{\mathbf{e}}$ est fini, donc $\overline{\mathbf{e}}$ est d'ordre fini dans le groupe abélien $\mathbf{M}^0(\mathbf{Q})/\mathbf{M}^0$. Son ordre est le dénominateur de $\mathbf{e}$. De plus, comme $n(\mathfrak{n})$ n'est pas divisible pas p, l'ordre de $\mathbf{T}\overline{\mathbf{e}}$ n'est pas divisible par p donc ce dénominateur est premier à p. □

***Notation* 2.53.** On note $\widetilde{\mathbf{e}}$ la classe de $d_{\mathbf{e}}\mathbf{e}$ dans $\mathbf{M}^0/p\mathbf{M}^0$.

2.7 Indépendance linéaire dans le module de Hecke engendré par e

On établit un énoncé d'indépendance linéaire d'opérateurs de Hecke en l'élément d'enroulement. Le symbole modulaire $[0,\infty]$ est plus explicite que l'élément d'enroulement $\mathbf{e}$: l'indépendance linéaire sera montrée sur $[0,\infty]$, puis relevée à $\mathbf{e}$, grâce à la proposition qui suit.

Dans cette section, $\mathfrak{n}$ est un idéal premier.

***Notation* 2.54.** Pour un entier $r \geq 0$, on note $\mathscr{P}_r$ (resp. $\mathscr{P}_{\leq r}$) l'ensemble des idéaux de A de degré r (resp. $\leq r$).

Proposition 2.55. *Supposons que les symboles modulaires $\{T_{\mathfrak{q}}[0,\infty] \mid \mathfrak{q} \in \mathscr{P}_{\leq r+1}\}$ sont $\mathbf{Z}$-linéairement indépendants dans $\mathbf{M}$. Alors, pour tout entier $0 \leq r' \leq r$, les symboles modulaires $\{T_{\mathfrak{q}}\mathbf{e} \mid \mathfrak{q} \in \mathscr{P}_{r'}\}$ sont $\mathbf{Z}$-linéairement indépendants dans $\mathbf{Te} \subset \mathbf{M}^0(\mathbf{Q})$.*

Démonstration. Fixons un idéal $\mathfrak{p}$ de A de degré 1. Supposons qu'il existe $\lambda_{\mathfrak{q}} \in \mathbf{Z}$ ($\mathfrak{q} \in \mathscr{P}_{r'}$) vérifiant

$$\sum_{\mathfrak{q} \in \mathscr{P}_{r'}} \lambda_{\mathfrak{q}} T_{\mathfrak{q}} \mathbf{e} = 0.$$

En appliquant l'élément $\eta_{\mathfrak{p}}$ de l'anneau commutatif $\mathbf{T}$, on obtient

$$\sum_{\mathfrak{q} \in \mathscr{P}_{r'}} \lambda_{\mathfrak{q}} T_{\mathfrak{q}} \eta_{\mathfrak{p}} \mathbf{e} = 0.$$

Puis, comme $\eta_{\mathfrak{p}} \mathbf{e} = \eta_{\mathfrak{p}}[0, \infty]$ d'après le corollaire 2.50,

$$\sum_{\mathfrak{q} \in \mathscr{P}_{r'}} \lambda_{\mathfrak{q}} T_{\mathfrak{q}} \eta_{\mathfrak{p}}[0, \infty] = \sum_{\mathfrak{q} \in \mathscr{P}_{r'}} \lambda_{\mathfrak{q}} T_{\mathfrak{q}} T_{\mathfrak{p}}[0, \infty] - \delta(\mathfrak{p}) \sum_{\mathfrak{q} \in \mathscr{P}_{r'}} \lambda_{\mathfrak{q}} T_{\mathfrak{q}}[0, \infty] = 0. \tag{2.9}$$

Or, d'après les propriétés des opérateurs de Hecke (page 27), $T_{\mathfrak{q}} T_{\mathfrak{p}}$ s'écrit comme la somme de $T_{\mathfrak{p}\mathfrak{q}}$ et d'une combinaison linéaire à coefficients dans $\mathbf{Z}$ d'opérateurs $T_{\mathfrak{r}}$, où $\deg \mathfrak{r} < \deg(\mathfrak{p}\mathfrak{q})$ c'est-à-dire $\mathfrak{r} \in \mathscr{P}_{\leq r'}$. Le coefficient de $T_{\mathfrak{p}\mathfrak{q}}[0, \infty]$ dans le membre du milieu de l'équation (2.9) est donc $\lambda_{\mathfrak{q}}$. D'après l'hypothèse, on a alors $\lambda_{\mathfrak{q}} = 0$ pour tout $\mathfrak{q} \in \mathscr{P}_{r'}$. □

Proposition 2.56. *Supposons que les symboles modulaires* $\{T_{\mathfrak{q}}[0, \infty] \mid \mathfrak{q} \in \mathscr{P}_{\leq r+1}\}$ *sont* $\mathbf{F}_p$*-linéairement indépendants dans* $\mathbf{M}(\mathbf{F}_p)$*. Alors, pour tout entier* $0 \leq r' \leq r$*, les symboles modulaires* $\{T_{\mathfrak{q}} \widetilde{\mathbf{e}} \mid \mathfrak{q} \in \mathscr{P}_{r'}\}$ *sont* $\mathbf{F}_p$*-linéairement indépendants dans* $\mathbf{M}^0/p\mathbf{M}^0$*.*

Démonstration. Fixons un idéal $\mathfrak{p}$ de A de degré 1. Supposons qu'il existe $\lambda_{\mathfrak{q}} \in \mathbf{F}_p$ ($\mathfrak{q} \in \mathscr{P}_{r'}$) vérifiant $\sum_{\mathfrak{q} \in \mathscr{P}_{r'}} \lambda_{\mathfrak{q}} T_{\mathfrak{q}} \widetilde{\mathbf{e}} = 0$. Soit $\mu_{\mathfrak{q}}$ un représentant de $\lambda_{\mathfrak{q}}$ dans $\mathbf{Z}$. On a alors

$$\sum_{\mathfrak{q} \in \mathscr{P}_{r'}} \mu_{\mathfrak{q}} d_{\mathbf{e}} T_{\mathfrak{q}} \mathbf{e} \in p\mathbf{M}^0.$$

En procédant comme dans la preuve de la proposition 2.55 on obtient

$$d_{\mathbf{e}} \sum_{\mathfrak{q} \in \mathscr{P}_{r'}} \mu_{\mathfrak{q}} T_{\mathfrak{q}} \eta_{\mathfrak{p}}[0, \infty] = d_{\mathbf{e}} \left(\sum_{\mathfrak{q} \in \mathscr{P}_{r'}} \mu_{\mathfrak{q}} T_{\mathfrak{q}} T_{\mathfrak{p}}[0, \infty] - \delta(\mathfrak{p}) \sum_{\mathfrak{q} \in \mathscr{P}_{r'}} \mu_{\mathfrak{q}} T_{\mathfrak{q}}[0, \infty] \right) \in p\mathbf{M}^0.$$

Comme $d_{\mathbf{e}}$ est premier à p (proposition 2.52), on obtient

$$\sum_{\mathfrak{q} \in \mathscr{P}_{r'}} \lambda_{\mathfrak{q}} T_{\mathfrak{q}} T_{\mathfrak{p}}[0, \infty] - \sum_{\mathfrak{q} \in \mathscr{P}_{r'}} \lambda_{\mathfrak{q}} T_{\mathfrak{q}}[0, \infty] = 0 \ \in \mathbf{M}/p\mathbf{M}.$$

Or, d'après les propriétés des opérateurs de Hecke, $T_{\mathfrak{q}} T_{\mathfrak{p}}$ s'écrit comme la somme de $T_{\mathfrak{p}\mathfrak{q}}$ et d'une combinaison linéaire à coefficients dans $\mathbf{F}_p$ d'opérateurs $T_{\mathfrak{r}}$, où $\deg \mathfrak{r} < \deg(\mathfrak{p}\mathfrak{q})$ c'est-à-dire $\mathfrak{r} \in \mathscr{P}_{\leq r'}$. D'après l'hypothèse, les $T_{\mathfrak{q}}[0, \infty]$, pour $\mathfrak{q}$ dans $\mathscr{P}_{\leq r+1}$, sont $\mathbf{F}_p$-linéairement indépendants dans $\mathbf{M}(\mathbf{F}_p)$ donc il en est de même dans $\mathbf{M}/p\mathbf{M}$. On a ainsi $\lambda_{\mathfrak{q}} = 0$ pour tout $\mathfrak{q} \in \mathscr{P}_{r'}$. □

Signalons que l'énoncé qui suit est valable si l'idéal $\mathfrak{n}$ n'est pas nécessairement premier.

Proposition 2.57. *Soient R un anneau dans lequel $q-1$ est inversible et $r \geq 0$ un entier. Si $\deg \mathfrak{n} \geq 2r+1$, les symboles modulaires $T_s[0,\infty]$, pour s dans $\mathscr{P}_{\leq r}$, sont R-linéairement indépendants dans $\mathbf{M}(R)$.*

Démonstration. Procédons par récurrence sur r. Si $\mathfrak{n} \neq A$, le bord de $[0,\infty]$ est non nul donc $[0,\infty]$ est libre sur R. Cela démontre l'affirmation pour $r=0$. Supposons l'énoncé vérifié pour $r-1$ et l'existence d'une relation

$$\sum_{s \in \mathscr{P}_{\leq r}} \lambda_s T_s[0,\infty] = 0, \tag{2.10}$$

avec $\lambda_s \in R$ ($s \in \mathscr{P}_{\leq r}$). Soit $\mathfrak{p} \in \mathscr{P}_{\leq r}$ de degré r et P le générateur unitaire de $\mathfrak{p}$. Démontrons que $\lambda_{\mathfrak{p}}$ est nul. L'hypothèse de récurrence permettra alors de conclure que tous les coefficients correspondant aux polynômes de degré $< r$ sont nuls. Appliquons la formule du théorème 2.28 :

$$T_{\mathfrak{p}}[0,\infty] = \sum_{\substack{\deg d > \deg c \\ \deg a > \deg b \\ (ad-bc)=\mathfrak{p} \\ a \text{ et } d \text{ unitaires} \\ (c,d) \not\equiv (0,0) \bmod \mathfrak{n}}} \xi(c:d).$$

On introduit les notations suivantes :

$$\begin{aligned} x =& (1:P) \in \mathcal{X}, \\ \Sigma_P =& \{(c,d) \in A \times A \mid \exists (a,b), \deg a > \deg b, a \text{ et } d \text{ unitaires}, ad-bc \in \mathscr{P}_{\leq r}, \\ & \deg c < \deg d, (c,d) \not\equiv (0,0) \bmod \mathfrak{n}\} \backslash \{(\lambda, P), \lambda \in \mathbf{F}_q^\times\} \end{aligned}$$

et Ω_P l'image de Σ_P dans $\mathcal{X}$. D'après l'équation (2.10), il existe des coefficients $\alpha_{c,d} \in R$ tels que

$$(q-1)\lambda_{\mathfrak{p}} \xi(1:P) = \sum_{(c,d) \in \Sigma_P} \alpha_{c,d} \xi(c:d). \tag{2.11}$$

Appliquons la proposition 2.35 à l'ensemble Ω_P et à l'élément x. D'après la première partie du lemme 2.36, x n'appartient pas à Ω_P. La deuxième partie du lemme 2.36 fournit un ensemble de sommets qui ne contient pas x et qui est disjoint de Ω_P. Toutes ces affirmations sont valables car $\deg \mathfrak{n} > 2 \deg P$.

Supposons maintenant $\lambda_{\mathfrak{p}} \neq 0$. Comme $q-1$ est inversible dans R, l'équation (2.11) montre que $\xi(1:P)$ est dans le sous-R-module de $\mathbf{M}(R)$ engendré par $\xi(\Omega_P)$: ceci est impossible d'après la proposition combinatoire 2.35.

□

Théorème 2.58. *Soit $r \geq 0$ un entier. Soit $\mathfrak{n}$ un idéal premier de A de degré $\geq 2r+3$. Pour tout entier $0 \leq r' \leq r$, les symboles modulaires $T_s\mathbf{e}$, pour s dans $\mathscr{P}_{r'}$, sont linéairement indépendants dans $\mathbf{M}^0(\mathbf{Q})$.*

Démonstration. Comme $\deg \mathfrak{n} \geq 2r+3$, d'après la proposition 2.57, les symboles modulaires $T_s[0,\infty]$, pour s dans $\mathscr{P}_{\leq r+1}$, sont linéairement indépendants dans $\mathbf{M}$. On remonte le résultat dans $\mathbf{M}^0(\mathbf{Q})$ à l'aide de la proposition 2.55. □

Corollaire 2.59. *Les affirmations suivantes sont équivalentes :*

(i) $\mathbf{e} \neq 0$ *dans* $\mathbf{M}^0(\mathbf{Q})$ *;*

(ii) $g(X_0(\mathfrak{n})) > 0$ *;*

(iii) $\deg \mathfrak{n} \geq 3$.

Démonstration. L'équivalence de (ii) et (iii) découle des formules exprimant le genre en fonction du degré de $\mathfrak{n}$ (proposition 1.23). Le théorème 2.58 appliqué à $r = 0$ donne l'implication (iii) $\Rightarrow$ (i). Enfin, l'implication (i) $\Rightarrow$ (ii) vient du fait que la dimension de $\mathbf{M}^0(\mathbf{Q})$ sur $\mathbf{Q}$ est égale à $g(X_0(\mathfrak{n}))$. □

Théorème 2.60. *Soit $r \geq 0$ un entier. Soit $\mathfrak{n}$ un idéal premier de A de degré $\geq 2r+3$. Pour tout entier $0 \leq r' \leq r$, les symboles modulaires $T_s\widetilde{\mathbf{e}}$, pour s dans $\mathscr{P}_{r'}$, sont $\mathbf{F}_p$-linéairement indépendants dans $\mathbf{M}^0/p\mathbf{M}^0$.*

Démonstration. D'après la proposition 2.57, comme $q-1$ est inversible dans $\mathbf{F}_p$, les symboles modulaires $T_s[0,\infty]$, pour s dans $\mathscr{P}_{\leq r+1}$, sont $\mathbf{F}_p$-linéairement indépendants dans $\mathbf{M}(\mathbf{F}_p)$. On remonte le résultat dans $\mathbf{M}^0/p\mathbf{M}^0$ à l'aide de la proposition 2.56. □

2.8 L'analogue de l'homomorphisme d'enroulement de Mazur

Dans cette section, $\mathfrak{n}$ est un idéal premier.

Lemme 2.61. *Si $\mathfrak{p}$ est un idéal premier distinct de $\mathfrak{n}$, on a*

$$\eta_{\mathfrak{p}}[0,\infty] \in (q-1)\mathbf{M}^0.$$

Démonstration. Soit P (resp. N) un générateur unitaire de $\mathfrak{p}$ (resp. $\mathfrak{n}$). Comme $\mathfrak{n}$ et $\mathfrak{p}$ sont premiers distincts, on a, par définition des opérateurs de Hecke,

$$\eta_{\mathfrak{p}}[0,\infty] = \sum_{\substack{b \in A, b \neq 0 \\ \deg b < \deg P}} \left[\frac{b}{P}, 0\right].$$

Comme P est premier à bN, il existe des polynômes A et C tels que la matrice $\gamma = \left(\begin{smallmatrix} A & b \\ CN & P \end{smallmatrix}\right)$ est dans $\Gamma_0(\mathfrak{n})$. On a $\gamma 0 = \frac{b}{P}$, donc le symbole modulaire $\left[\frac{b}{P}, 0\right]$ est parabolique. De plus, pour tout $\lambda \in \mathbf{F}_q^\times$, on a $[\frac{\lambda b}{P}, 0] = [\frac{b}{P}, 0]$, d'où

$$\eta_{\mathfrak{p}}[0,\infty] = (q-1) \sum_{\substack{b \in A, b \neq 0 \text{ unitaire} \\ \deg b < \deg P}} \left[\frac{b}{P}, 0\right] \quad \in (q-1)\mathbf{M}^0.$$

□

Définition 2.62 (voir aussi [Pál07a] 5.7)**.** Suivant Mazur, on appelle *homomorphisme d'enroulement* l'homomorphisme de $\mathbf{T}$-modules

$$\begin{array}{ccc} I_E & \longrightarrow & \mathbf{M}^0 \\ t & \longmapsto & \frac{t\mathbf{e}}{q-1}. \end{array}$$

Il est bien défini d'après le lemme précédent et le corollaire 2.50.

Lemme 2.63. *L'involution $w_{\mathfrak{n}}$ agit comme -1 sur l'image de l'homomorphisme d'enroulement.*

Démonstration. Soit $t \in I_E$. Comme $w_{\mathfrak{n}}$ commute à $\mathbf{T}$ et $w_{\mathfrak{n}}[0,\infty] = [\infty, 0]$, on a les égalités

$$w_{\mathfrak{n}}\left(\frac{t\mathbf{e}}{q-1}\right) = w_{\mathfrak{n}}\left(\frac{t[0,\infty]}{q-1}\right) = \frac{tw_{\mathfrak{n}}[0,\infty]}{q-1} = \frac{t[\infty,0]}{q-1} = -\frac{t\mathbf{e}}{q-1}.$$

□

L'énoncé qui suit donne la structure du $\mathbf{T}$-module $\mathbf{M}^0$ lorsque $\mathfrak{n}$ est de degré 3. Il peut être rapproché du théorème 18.10 de [Maz77] pour l'homomorphisme d'enroulement classique, localisé en un nombre premier d'Eisenstein.

Théorème 2.64. *Soit $\mathfrak{n}$ un idéal premier de A de degré 3. Alors les q symboles modulaires*

$$\frac{1}{q-1}\eta_{\mathfrak{p}}\mathbf{e} = \frac{1}{q-1}(T_{\mathfrak{p}} - (q+1))\mathbf{e},$$

où $\mathfrak{p}$ décrit les idéaux de degré 1, forment une base sur $\mathbf{Z}$ de $\mathbf{M}^0$. En particulier, l'homomorphisme d'enroulement

$$\begin{array}{ccc} I_E & \xrightarrow{\sim} & \mathbf{M}^0 \\ t & \longmapsto & \dfrac{t\mathbf{e}}{q-1} \end{array}$$

est un isomorphisme de $\mathbf{T}$-modules.

Démonstration. Soit P le générateur unitaire de $\mathfrak{p}$. Comme $\mathfrak{p}$ est de degré 1, on a d'après la démonstration du lemme 2.61

$$\eta_{\mathfrak{p}}\mathbf{e} = \eta_{\mathfrak{p}}[0,\infty] = (q-1)\left[\frac{1}{P}, 0\right] = -(q-1)\xi(P:1).$$

D'après le corollaire 2.42, les symboles $\xi(P:1)$ (pour P unitaire de degré 1) forment une base de $\mathbf{M}^0$, donc il en est de même de $(\frac{1}{q-1}\eta_{\mathfrak{p}}\mathbf{e})_{\deg \mathfrak{p}=1}$. □

Corollaire 2.65. *Soit $\mathfrak{n}$ un idéal premier de A de degré 3.*

(i) Les symboles modulaires $\frac{1}{q-1}\eta_{\mathfrak{p}}\mathbf{e}$, où $\mathfrak{p}$ décrit les idéaux de degré 1, forment une base sur $\mathbf{F}_p$ de $\mathbf{M}^0/p\mathbf{M}^0$.

(ii) Les éléments $\eta_{\mathfrak{p}}$ de l'algèbre de Hecke, où $\mathfrak{p}$ décrit les idéaux de degré 1, forment une base sur $\mathbf{F}_p$ de $\mathbf{T}/p\mathbf{T}$.

Démonstration. (i) D'après le théorème précédent, la famille de symboles modulaires $\frac{1}{q-1}\eta_{\mathfrak{p}}\mathbf{e}$, où $\mathfrak{p}$ décrit les idéaux de degré 1, est une base sur $\mathbf{Z}$ de $\mathbf{M}^0$. De plus, on a $\mathbf{M}^0/p\mathbf{M}^0 = \mathbf{M}^0 \otimes_{\mathbf{Z}} \mathbf{F}_p$. Donc par extension des scalaires, la famille est une base sur $\mathbf{F}_p$ de $\mathbf{M}^0/p\mathbf{M}^0$.

(ii) Le $\mathbf{Z}$-module $\mathbf{T}$ est libre de rang $g(X_0(\mathfrak{n})) = q$, donc $\mathbf{T}/p\mathbf{T} = \mathbf{T} \otimes_{\mathbf{Z}} \mathbf{F}_p$ est un $\mathbf{F}_p$-espace vectoriel de dimension q. Pour démontrer l'affirmation, il suffit de voir que les $\eta_{\mathfrak{p}}$, où $\mathfrak{p}$ décrit les idéaux de degré 1, sont $\mathbf{F}_p$-linéairement indépendants. Supposons qu'il existe $\lambda_{\mathfrak{p}} \in \mathbf{Z}$, avec $\deg \mathfrak{p} = 1$, vérifiant

$$\sum_{\deg \mathfrak{p}=1} \lambda_{\mathfrak{p}} \eta_{\mathfrak{p}} \in p\mathbf{T}.$$

Appliquons l'opérateur précédent à $d_{\mathbf{e}}\mathbf{e} \in \mathbf{M}^0$:

$$\sum_{\deg \mathfrak{p}=1} \lambda_{\mathfrak{p}} \eta_{\mathfrak{p}}(d_{\mathbf{e}}\mathbf{e}) = \sum_{\deg \mathfrak{p}=1} d_{\mathbf{e}} \lambda_{\mathfrak{p}}(q-1)\frac{\eta_{\mathfrak{p}}\mathbf{e}}{q-1} \in p\mathbf{M}^0.$$

La classe de ce symbole modulaire dans $\mathbf{M}^0/p\mathbf{M}^0$ est nulle. D'après (i), on a $d_{\mathbf{e}}\lambda_{\mathfrak{p}}(q-1) \equiv 0 \mod p$, pour tout $\mathfrak{p}$ de degré 1. De plus, $d_{\mathbf{e}}$ est premier à p par la proposition 2.52. Donc $\lambda_{\mathfrak{p}} \equiv 0 \mod p$, pour tout $\mathfrak{p}$ de degré 1. Cela montre que la famille $\eta_{\mathfrak{p}}$, où $\mathfrak{p}$ décrit les idéaux de degré 1, est libre sur $\mathbf{F}_p$.

□

Corollaire 2.66. *Soit $\mathfrak{n}$ un idéal premier de A de degré 3. Alors*

(i) $\mathbf{M}^0/p\mathbf{M}^0$ *est un* $\mathbf{T}/p\mathbf{T}$*-module libre de rang* 1 *;*

(ii) $\mathbf{H}/p\mathbf{H}$ *est un* $\mathbf{T}/p\mathbf{T}$*-module libre de rang* 1*. En particulier, l'action de* $\mathbf{T}/p\mathbf{T}$ *sur* $\mathbf{H}/p\mathbf{H}$ *est fidèle.*

Démonstration. (i) D'après [Pál07a], on a

$$p\mathbf{T} + I_E = \mathbf{T}. \tag{2.12}$$

En effet, supposons $p\mathbf{T} + I_E \subsetneq \mathbf{T}$. Il existe un idéal maximal $\mathcal{M}$ de $\mathbf{T}$ contenant I_E et $p\mathbf{T}$. Le corps $\mathbf{T}/\mathcal{M}$ est donc de caractéristique p et le morphisme canonique $\mathbf{T}/I_E \to \mathbf{T}/\mathcal{M}$ est surjectif. Ainsi l'ordre de $\mathbf{T}/I_E$ est divisible par p, ce qui contredit le théorème 1.2 de *loc. cit.*. Cela démontre (2.12).

Le morphisme canonique $I_E \to \mathbf{T}$ donne donc un isomorphisme de $\mathbf{T}$-modules

$$I_E/pI_E \xrightarrow{\sim} \mathbf{T}/p\mathbf{T}.$$

De l'isomorphisme $\mathbf{M}^0 \simeq I_E$ du théorème 2.64, on déduit l'isomorphisme de $\mathbf{T}/p\mathbf{T}$-modules $\mathbf{M}^0/p\mathbf{M}^0 \simeq \mathbf{T}/p\mathbf{T}$. Donc $\mathbf{M}^0/p\mathbf{M}^0$ est un $\mathbf{T}/p\mathbf{T}$-module libre de rang 1.

(ii) Le théorème 2.24 fournit la suite exacte de groupes abéliens

$$0 \longrightarrow (\mathbf{M}^0)_{\mathrm{tors}} \longrightarrow \mathbf{M}^0 \longrightarrow \mathrm{Hom}(\mathbf{H}, \mathbf{Z}) \longrightarrow \Phi_\infty \longrightarrow 0.$$

Le groupe $\mathbf{M}^0$ est sans torsion d'après le théorème 2.40. De plus, d'après Gekeler [Gek97b] 6.3 (ii), le groupe Φ_∞ est cyclique d'ordre $q^2 + q + 1$, donc premier à p. En localisant en l'idéal $p\mathbf{Z}$, on obtient l'isomorphisme de $\mathbf{Z}_{(p)}$-modules

$$\mathbf{M}^0_{(p)} \simeq \mathrm{Hom}(\mathbf{H}, \mathbf{Z})_{(p)},$$

d'où l'isomorphisme de groupes abéliens

$$\mathbf{M}^0/p\mathbf{M}^0 \simeq \mathrm{Hom}(\mathbf{H}/p\mathbf{H}, \mathbf{F}_p).$$

De plus, cette application est compatible à l'action de $\mathbf{T}/p\mathbf{T}$. Comme $\mathbf{M}^0/p\mathbf{M}^0$ est un $\mathbf{T}/p\mathbf{T}$-module libre de rang 1, il en est de même de $\mathbf{H}/p\mathbf{H}$.

□

***Remarque* 2.67.** Dans le chapitre 4, on donnera une autre démonstration du fait que $\mathbf{T}/p\mathbf{T}$ opère fidèlement sur $\mathbf{H}/p\mathbf{H}$ par la théorie des formes modulaires (remarque 4.52 (i)).

Lorsque $\mathfrak{n}$ est de degré 4, nous nous contentons de traiter un exemple.

Exemple 2.68 ($q = 2$, $\mathfrak{n} = (T^4+T+1)$ idéal premier)**.** Les relations entre les symboles de Manin-Teitelbaum sont

$$\begin{aligned}
\xi(1:1) &= 0\\
\xi(0:1) &= -\xi(1:0)\\
3\xi(T^2+T:1) &= 0\\
3\xi(T^2+T+1:1) &= 0\\
\xi(T^3+1:1) &= -\xi(T:1)\\
\xi(T^3+T^2+T:1) &= -\xi(T+1:1)\\
\xi(T^3+T^2+1:1) &= -\xi(T^2:1)\\
\xi(T^3+T+1:1) &= -\xi(T^2+1:1)\\
\xi(T^3:1) &= \xi(T+1:1)-\xi(T:1)\\
\xi(T^3+T^2+T+1:1) &= \xi(T:1)-\xi(T+1:1)\\
\xi(T^3+T:1) &= \xi(T^2:1)+\xi(T^2+1:1)\\
\xi(T^3+T^2:1) &= -\xi(T^2:1)-\xi(T^2+1:1)
\end{aligned}$$

et la famille de symboles modulaires

$$\{\xi(1:0), \xi(T:1), \xi(T+1:1), \xi(T^2:1), \xi(T^2+1:1)\}$$

est une base de $\mathbf{M}(\mathbf{Q})$ sur $\mathbf{Q}$. Par ailleurs, on a

$$\begin{aligned}
\eta_{(T)}\mathbf{e} &= T_{(T)}\xi(0:1) - 3\xi(0:1) = -\xi(T:1)\\
\eta_{(T+1)}\mathbf{e} &= T_{(T+1)}\xi(0:1) - 3\xi(0:1) = -\xi(T+1:1),
\end{aligned}$$

donc le sous-$\mathbf{Q}$-espace vectoriel de $\mathbf{M}^0(\mathbf{Q})$ engendré par l'image de l'homomorphisme d'enroulement est de dimension au moins 2. Un calcul montre que la matrice de l'involution $w_{\mathfrak{n}}$ dans cette base est

$$\begin{pmatrix} -1 & 0 & 0 & 0 & 0\\ 0 & -1 & 0 & 0 & -1\\ 0 & 0 & -1 & -1 & 0\\ 0 & 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Le sous-espace propre de $w_{\mathfrak{n}|\mathbf{M}^0(\mathbf{Q})}$ associé à la valeur propre -1 est engendré par $\xi(T:1)$ et $\xi(T+1:1)$. D'après le lemme 2.63, le sous-$\mathbf{Q}$-espace vectoriel de $\mathbf{M}^0(\mathbf{Q})$ engendré par l'image de l'homomorphisme d'enroulement est donc de dimension 2.

Poursuivons cette étude. La matrice de l'opérateur $T_{(T)}$ dans cette base est

$$\begin{pmatrix} 3 & 0 & 0 & 0 & 0 \\ 1 & -1 & -1 & 0 & 1 \\ 0 & 1 & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & -1 & -3 \end{pmatrix}.$$

Ses espaces propres sont décrits dans le tableau suivant.

valeur propre	base de l'espace propre associé
$\frac{1-\sqrt{5}}{2}$	$m_1 = \frac{-3-\sqrt{5}}{2}\xi(T:1) + \xi(T+1:1)$
$\frac{1+\sqrt{5}}{2}$	$m_2 = \frac{-3+\sqrt{5}}{2}\xi(T:1) + \xi(T+1:1)$
$\frac{-3+\sqrt{5}}{2}$	$m_3 = \frac{3-\sqrt{5}}{4}\xi(T:1) - \frac{1}{2}\xi(T+1:1) + \xi(T^2:1) + \frac{\sqrt{5}-3}{2}\xi(T^2+1:1)$
$\frac{-3-\sqrt{5}}{2}$	$m_4 = \frac{3+\sqrt{5}}{4}\xi(T:1) - \frac{1}{2}\xi(T+1:1) + \xi(T^2:1) + \frac{-\sqrt{5}-3}{2}\xi(T^2+1:1)$

Donc la famille $\{m_1, m_2, m_3, m_4\}$ est une base de $\mathbf{M}^0(\mathbf{C})$ formée de symboles modulaires propres pour $\mathbf{T}$ qui vérifient

$$\begin{array}{ll} w_{\mathfrak{n}} m_1 = -m_1 & w_{\mathfrak{n}} m_2 = -m_2 \\ w_{\mathfrak{n}} m_3 = m_3 & w_{\mathfrak{n}} m_4 = m_4. \end{array}$$

Chapitre 3

Quotient d'enroulement de $J_0(\mathfrak{n})$

3.1 Variétés abéliennes sur les corps de fonctions (rappels)

La fonction-L d'une variété abélienne. Dans ce paragraphe, F désigne un corps de fonctions en une indéterminée sur le corps fini $\mathbf{F}_q$. Fixons F^{sep} une clôture séparable de F. On considère une variété abélienne B sur F.

Soit l un nombre premier distinct de la caractéristique p de F. Le module de Tate l-adique est $T_l(B) = \varprojlim \overline{B}[l^n]$, où $\overline{B}[l^n]$ est le noyau de la multiplication par $l^n : B(F^{\mathrm{sep}}) \to B(F^{\mathrm{sep}})$. Le $\mathbf{Q}_l$-espace vectoriel $V_l(B) = T_l(B) \otimes_{\mathbf{Z}_l} \mathbf{Q}_l$ est de dimension $2\dim(B)$. L'action naturelle de $\mathrm{Gal}(F^{\mathrm{sep}}/F)$ sur $T_l(B)$ fournit une représentation l-adique $\rho_l : \mathrm{Gal}(F^{\mathrm{sep}}/F) \to \mathrm{Aut}(V_l(B))$. Elle a une représentation adjointe ρ_l^* sur le dual $V_l(B)^*$.

Soit v une place de F. En v, le corps résiduel $k(v)$ est fini, de cardinal $q_v = q^{n_v}$. Les sous-groupes de décomposition et d'inertie en v de $\mathrm{Gal}(F^{\mathrm{sep}}/F)$ sont notés respectivement $D(v)$ et I_v. Le Frobenius arithmétique, c'est-à-dire la puissance n_v-ème du Frobenius dans $\mathrm{Gal}(k(v)^{\mathrm{alg}}/k(v)) \simeq D(v)/I_v$, est noté ϕ_v. Considérons le polynôme suivant à coefficients entiers :

$$P_v(u) = \det(\mathrm{id} - u\rho_l^*(\phi_v^{-1}) \mid V_l(B)^{*I_v}).$$

En fait, $P_v(u)$ ne dépend pas de l ni du choix de ϕ_v. La *fonction* L de B est alors le produit infini sur toutes les places de F

$$L(B,s) = \prod_v L_v(B,s) = \prod_v P_v(q_v^{-s})^{-1}.$$

C'est une fonction rationnelle en q^{-s} à coefficients rationnels comme conséquence des travaux de Dwork ou de la cohomologie étale de Grothendieck ([Mil80] chap. VI). En particulier, $L(B,s)$ est une fonction méromorphe du plan complexe.

La conjecture de Birch et Swinnerton-Dyer pour les variétés abéliennes sur les corps de fonctions. Le théorème de Mordell-Weil affirme que le groupe abélien $B(F)$ est de type fini (voir par exemple [Lan83] pour une preuve sur les corps de fonctions). La conjecture relie notamment son rang r à l'ordre d'annulation de la fonction $L(B,s)$ en $s = 1$.

Conjecture 3.1 (Conjecture de Birch et Swinnerton-Dyer [Tat66]).

(i) $\mathrm{ord}_{s=1} L(B,s) = r$;

(ii) Le groupe de Tate-Shafarevich $Ш(B) = \mathrm{Ker}(H^1(K,B) \to \bigoplus_v H^1(K_v,B))$ est fini ;

(iii) $\lim_{s\to 1} \dfrac{L(B,s)}{(s-1)^r} = \dfrac{\#Ш(B)\cdot R\cdot \tau}{\#B(F)_{\mathrm{tors}}\cdot \#\hat{B}(F)_{\mathrm{tors}}}$

(R désigne un régulateur construit à partir de hauteurs d'un ensemble de générateurs de $B(F)$, τ un nombre de Tamagawa et $\hat{B}$ la variété abélienne duale de B). Nous terminons par un panorama de résultats connus sur cette conjecture. Pour le quotient d'enroulement, nous ferons usage de l'inégalité suivante.

Théorème 3.2 (Schneider [Sch82], Satz 11 (i)). *Pour toute variété abélienne B sur F, on a*

$$r \leq \mathrm{ord}_{s=1} L(B,s).$$

Milne a démontré la conjecture 3.1 pour les variétés abéliennes constantes [Mil68]. En toute généralité, on dispose du résultat suivant.

Théorème 3.3 (Kato-Trihan [KT03]). *L'affirmation (i) de la conjecture équivaut à l'existence d'un nombre premier l tel que la composante l-primaire du groupe de Tate-Shafarevich $Ш(B)$ est finie. Dans ce cas, les trois affirmations de la conjecture sont alors vérifiées pour B.*

Ce théorème fait suite aux travaux précédents de Tate [Tat66] (pour les courbes elliptiques et $l \neq p$, la finitude étant obtenue pour la partie première à p de $Ш(B)$), Milne [Mil75] (pour les courbes elliptiques sur F avec $p \neq 2$) et Schneider [Sch82] (pour les variétés abéliennes et $l \neq p$).

3.2 La jacobienne $J_0(\mathfrak{n})$ de $X_0(\mathfrak{n})_K$ (rappels)

3.2.1 La jacobienne $J_0(\mathfrak{n})$

La courbe $X_0(\mathfrak{n})_K$ est lisse et propre sur K. Sa jacobienne, notée $J_0(\mathfrak{n})$, est une variété abélienne sur K, de dimension égale à $g(X_0(\mathfrak{n}))$.

3.2.2 Les correspondances de Hecke sur $X_0(\mathfrak{n})$

Cette présentation suit celles de [Gek86b] 5.3, [GR96] 4.12, [Gek97a] §7. Soit $\mathfrak{m}$ un idéal de A. Si $(\mathfrak{m},\mathfrak{n}) \neq 1$, l'involution $w_{\mathfrak{m}}$ de $X_0(\mathfrak{n})$ est définie sur le problème de modules correspondant par

$$w_{\mathfrak{m}}(E,C) = (E/C, E[\mathfrak{n}]/C)$$

(E/C désigne l'unique module de Drinfeld de rang 2 tel qu'il existe une isogénie $E \to E/C$ de noyau C). On notera $w_{\mathfrak{n}}$ l'involution qu'elle induit sur $X_0(\mathfrak{n}\mathfrak{n}')$ (pour $\mathfrak{n}'$ idéal premier à $\mathfrak{n}$).

Si E est un module de Drinfeld de rang 2 sur un schéma, on note $\mathcal{E}_{E,\mathfrak{m}}$ l'ensemble des structures de niveau $\Gamma_0(\mathfrak{m})$ sur E. On définit une correspondance $T_\mathfrak{m}$ sur $X_0(\mathfrak{n})$ par la formule suivante :

$$T_\mathfrak{m}(E,C) = \sum_{\substack{D\in\mathcal{E}_{E,\mathfrak{m}}\\ D\cap C=\{0\}}} (E/D,(C+D)/D).$$

Si $\mathfrak{m}$ est premier à $\mathfrak{n}$, $T_\mathfrak{m}$ peut s'obtenir aussi par la construction qui suit. Le schéma $X_0(\mathfrak{n}\mathfrak{m})$ est un schéma de modules grossier pour le problème de modules (E,C,D), où E est un module de Drinfeld de rang 2, C une structure de niveau $\Gamma_0(\mathfrak{n})$ et D une structure de niveau $\Gamma_0(\mathfrak{m})$ sur E. Considérons le morphisme d'oubli $c : X_0(\mathfrak{n}\mathfrak{m}) \to X_0(\mathfrak{n})$ défini par $(E,C,D) \mapsto (E,C)$. L'opérateur $T_\mathfrak{m}$ est la correspondance sur $X_0(\mathfrak{n})$ définie par le diagramme suivant :

$$\begin{tikzcd} & X_0(\mathfrak{n}\mathfrak{m}) \arrow[dl, "c"'] \arrow[dr, "cw_\mathfrak{m}"] & \\ X_0(\mathfrak{n}) \arrow[rr, "T_\mathfrak{m}"] & & X_0(\mathfrak{n}). \end{tikzcd}$$

Les correspondances $w_\mathfrak{m}$ ($(\mathfrak{m},\mathfrak{n}) \neq 1$) et $T_\mathfrak{m}$ laissent invariant le groupe des diviseurs de $X_0(\mathfrak{n})$ à support dans les pointes. Si $\mathfrak{n}$ est premier, $w_\mathfrak{n}$ échange les pointes 0 et ∞ ; si $(\mathfrak{m},\mathfrak{n}) = 1$, $T_\mathfrak{m}$ agit sur une pointe comme multiplication par $(1+q^{\deg \mathfrak{m}})$. Ces correspondances induisent des endomorphismes de la jacobienne $J_0(\mathfrak{n})$, notés $w_\mathfrak{m}$ et $T_\mathfrak{m}$. Comme nous le verrons en 3.2.5, ces notations n'occasionneront pas de confusion avec les opérateurs $T_\mathfrak{m}$ et $w_\mathfrak{m}$ définis dans le chapitre 2.

3.2.3 La réduction de $J_0(\mathfrak{n})$

Notations : réduction des variétés abéliennes. Soit F un corps local, d'anneau des entiers R et de corps résiduel k. Soient B une variété abélienne sur F et $\mathcal{B}$ son modèle de Néron sur R. Sa fibre spéciale est notée $\mathcal{B}_k$ et la composante connexe de l'identité dans $\mathcal{B}_k$ est notée $\mathcal{B}_k^0$. On a une suite exacte de schémas en groupes sur k

$$0 \longrightarrow \mathcal{B}_k^0 \longrightarrow \mathcal{B}_k \longrightarrow \Phi_B \longrightarrow 0,$$

où Φ_B est un schéma en groupes étale et fini sur k appelé *groupe des composantes (connexes) de* $\mathcal{B}_k$. La variété abélienne B a *bonne réduction* si $\mathcal{B}_k$ est une variété abélienne sur k. Elle est dite à *réduction torique* (resp. *torique déployée*) si $\mathcal{B}_k^0$ est un tore algébrique (resp. un tore algébrique déployé) sur k.

Soit $\mathcal{J}_0(\mathfrak{n})_A$ le modèle de Néron de $J_0(\mathfrak{n})$ sur A. C'est un schéma lisse, séparé et de type fini sur A. De plus, comme $X_0(\mathfrak{n})$ est lisse, le changement de base de $\mathcal{J}_0(\mathfrak{n})_A$ à $A[1/\mathfrak{n}]$ est un schéma abélien, noté $\mathcal{J}_0(\mathfrak{n})$. La variété abélienne $J_0(\mathfrak{n})$ a donc bonne réduction en-dehors de $\mathfrak{n}$. Rappelons des résultats concernant les réductions de $X_0(\mathfrak{n})$ et $J_0(\mathfrak{n})$ en les places divisant $\mathfrak{n}$.

Soit $\mathfrak{p}$ un idéal premier de A. Soient L une extension finie de $\mathbf{F}_\mathfrak{p}$ de cardinal q^m et ϕ un A-module de Drinfeld sur L de rang r. Le module de Drinfeld ϕ est dit *supersingulier* si $\phi[\mathfrak{p}](L^{\mathrm{alg}}) = 0$. Comme pour les courbes elliptiques, on dispose de la caractérisation suivante.

Théorème 3.4 ([Gek91]). *Avec les notations précédentes, les affirmations suivantes sont équivalentes :*

(i) ϕ *est un module de Drinfeld supersingulier ;*

(ii) il existe une extension finie L' *de* L *telle que* $\mathrm{End}_{L'}(\phi) \otimes K$ *est de dimension* r^2 *sur* K.

Un point L-rationnel de $X_0(\mathfrak{n})$ est dit *supersingulier* si ce n'est pas une pointe et si le module de Drinfeld sous-jacent est supersingulier.

Proposition 3.5. *Supposons l'idéal* $\mathfrak{n}$ *premier.*

(i) La fibre spéciale $\mathcal{M}_0(\mathfrak{n})_{\mathbf{F}_\mathfrak{n}}$ *est réduite et réunion de deux copies de la courbe* $\mathcal{M}_0(1)_{\mathbf{F}_\mathfrak{n}}$ *qui se coupent transversalement aux* $n(\mathfrak{n})$ *points supersinguliers, avec*

$$n(\mathfrak{n}) = \begin{cases} \frac{q^{\deg \mathfrak{n}}-1}{q-1} & \textit{si } \deg \mathfrak{n} \textit{ est impair ;} \\ \frac{q^{\deg \mathfrak{n}}-1}{q^2-1} & \textit{si } \deg \mathfrak{n} \textit{ est pair.} \end{cases}$$

De plus, les deux copies de $\mathcal{M}_0(1)_{\mathbf{F}_\mathfrak{n}}$ *sont échangées par l'involution* $w_\mathfrak{n}$.

(ii) La jacobienne $J_0(\mathfrak{n})$ *a réduction torique en* $\mathfrak{n}$.

(iii) L'ordre du groupe des composantes du modèle de Néron de $J_0(\mathfrak{n})$ *en* $\mathfrak{n}$ *est* $n(\mathfrak{n})$.

Démonstration. La première affirmation vient de (5.3) et (5.9) de [Gek86b]. Les deux suivantes s'en déduisent par le théorème de Raynaud sur la spécialisation du foncteur de Picard ([Ray70], [Gek86b] (5.10)). □

3.2.4 La construction analytique de la jacobienne

Rappelons la description de la jacobienne, en tant que variété analytique rigide sur $\mathbf{C}_\infty$, comme le tore $(\mathbf{C}_\infty^\times)^{g(X_0(\mathfrak{n}))}$ modulo le réseau des périodes de certaines fonctions thêtas. Ce type de construction est valable pour les variétés abéliennes à réduction torique en une place. Pour les jacobiennes de courbes modulaires de Drinfeld, la construction explicite est due à Gekeler et Reversat ([GR96], notamment les paragraphes 5 à 9). Nous en rappelons les principaux résultats en nous plaçant dans le cas particulier $\Gamma = \Gamma_0(\mathfrak{n})$.

Soit Γ^{ab} l'abélianisé de Γ et $\overline{\Gamma} = \Gamma^{\mathrm{ab}}/(\Gamma^{\mathrm{ab}})_{\mathrm{tors}}$ le quotient abélien sans torsion maximal de Γ. Pour un élément γ de Γ, on notera $\overline{\gamma}$ son image dans $\overline{\Gamma}$. Une fonction méromorphe $\theta : \mathcal{H} \to \mathbf{C}_\infty$ est appelée *fonction thêta méromorphe pour* Γ s'il existe $c_\theta \in \mathrm{Hom}(\overline{\Gamma}, \mathbf{C}_\infty^\times)$ tel que

$$\theta(\gamma z) = c_\theta(\overline{\gamma})\theta(z) \qquad (z \in \mathcal{H}, \gamma \in \Gamma).$$

On définit une *fonction thêta holomorphe* de façon analogue. Leurs groupes multiplicatifs seront notés respectivement $\Theta_m(\Gamma)$ et $\Theta_h(\Gamma)$.

Si $D = (P_1) + \cdots + (P_r) - (Q_1) - \cdots - (Q_r)$ est un diviseur de degré zéro sur $\mathcal{H}$, le produit infini

$$\theta_D(z) = \prod_{\gamma \in \Gamma} \frac{(z-\gamma P_1)\cdots(z-\gamma P_r)}{(z-\gamma Q_1)\cdots(z-\gamma Q_r)}$$

converge dans $\mathcal{H}$ et définit une fonction thêta méromorphe pour Γ. La fonction c_{θ_D} qui lui est associée est notée c_D.

Pour $\alpha, \beta \in \Gamma$, la quantité $c_\alpha(\beta) = c_{(z)-(\alpha z)}(\beta)$ est indépendante du choix de $z \in \mathbf{C}_\infty$ et ne dépend que de $\overline{\alpha}$ et $\overline{\beta}$. Elle définit alors une application

$$\begin{array}{rcl} c : \overline{\Gamma} & \longrightarrow & \mathrm{Hom}(\overline{\Gamma}, \mathbf{C}_\infty^\times) \\ \alpha & \longmapsto & c_\alpha \end{array}$$

qui est injective et d'image discrète.

Si $\alpha \in \Gamma$ et $w \in \mathbf{C}_\infty$, la fonction $\theta_{\overline{\alpha}} = \theta_{(w)-(\alpha w)}$ est holomorphe, indépendante de w et ne dépend que du choix de $\overline{\alpha}$.

Soit $\underline{H}(\mathcal{T}, \mathbf{Z})$ le groupe abélien des fonctions harmoniques alternées sur $\mathcal{T}$ à valeurs dans $\mathbf{Z}$. La dérivée logarithmique de van der Put $r : Y(\mathcal{T}) \to \underline{H}(\mathcal{T}, \mathbf{Z})$ (voir [GR96] 1.7.3 pour sa définition) donne un homomorphisme de groupes $r : \Theta_h(\Gamma)/\mathbf{C}_\infty^\times \to \underline{H}(\mathcal{T}, \mathbf{Z})^\Gamma$. L'homomorphisme de groupes

$$\begin{array}{rcl} j : \overline{\Gamma} & \longrightarrow & \underline{H}_!(\mathcal{T}, \mathbf{Z})^\Gamma \\ \overline{\alpha} & \longmapsto & r(\theta_{\overline{\alpha}}) \end{array}$$

est un isomorphisme d'après [GN95]. L'application

$$\begin{array}{rcl} \Phi : \mathrm{Div}^0(\mathcal{H}) & \longrightarrow & \mathrm{Hom}(\overline{\Gamma}, \mathbf{C}_\infty^\times) \\ D & \longmapsto & c_D \end{array}$$

induit alors un morphisme $\Phi : \mathrm{Div}^0(Y_0(\mathfrak{n})(\mathbf{C}_\infty)) \to \mathrm{Hom}(\overline{\Gamma}, \mathbf{C}_\infty^\times)/c(\overline{\Gamma})$ puis un isomorphisme

$$J_0(\mathfrak{n})(\mathbf{C}_\infty) \simeq \mathrm{Hom}(\overline{\Gamma}, \mathbf{C}_\infty^\times)/c(\overline{\Gamma}).$$

Soit T_Γ le tore déployé $\mathrm{Hom}(\overline{\Gamma}, \mathbf{G}_m)$. On a alors les suites exactes

$$1 \longrightarrow \overline{\Gamma} \xrightarrow{c} T_\Gamma(\mathbf{C}_\infty) \xrightarrow{\Phi^{-1}} J_0(\mathfrak{n})(\mathbf{C}_\infty) \longrightarrow 0$$

$$1 \longrightarrow \overline{\Gamma} \xrightarrow{c} T_\Gamma(K_\infty) \xrightarrow{\Phi^{-1}} J_0(\mathfrak{n})(K_\infty) \longrightarrow 0 \tag{3.1}$$

([Gek97a], remarque 6.11).

3.2.5 La compatibilité de l'action des algèbres de Hecke

On suit l'approche de [Gek97a]. En utilisant la construction précédente, on peut réaliser $\mathrm{End}_K(J_0(\mathfrak{n}))$ comme sous-espace de $\mathrm{End}(\mathbf{H})$. En effet, par la suite exacte (3.1), tout endomorphisme de $J_0(\mathfrak{n})$ défini sur K peut être relevé en un endomorphisme de T_Γ. De plus, on a une équivalence de catégories contravariante entre les groupes abéliens libres de type fini et les tores déployés, donnée par $\overline{\Gamma} \mapsto T_\Gamma$. Enfin, on a l'isomorphisme $j : \overline{\Gamma} \simeq \mathbf{H}$. En rassemblant ces résultats, on obtient un morphisme injectif

$$\mathrm{End}_K(J_0(\mathfrak{n})) \hookrightarrow \mathrm{End}(\mathbf{H}) \hookrightarrow \mathrm{End}(\mathbf{H}(\mathbf{C})).$$

L'image de $T_\mathfrak{p} \in \mathrm{End}_K(J_0(\mathfrak{n}))$ est $T_\mathfrak{p} \in \mathrm{End}(\mathbf{H}(\mathbf{C}))$ (la compatibilité est vérifiée dans [GR96], § 9). Donc l'algèbre de Hecke $\mathbf{T}$ est isomorphe à la sous-algèbre de $\mathrm{End}_K(J_0(\mathfrak{n}))$ engendrée sur $\mathbf{Z}$ par $T_\mathfrak{p}$, pour $\mathfrak{p}$ idéal de A. Dorénavant, on identifie ces deux algèbres qu'on note $\mathbf{T}$. L'algèbre $\mathbf{T}$ opère fidèlement sur la jacobienne $J_0(\mathfrak{n})$, l'espace de symboles modulaires $\mathbf{M}^0$ et l'espace de formes automorphes $\mathbf{H}$.

3.2.6 L'action de l'involution $w_\mathfrak{n}$ sur $J_0(\mathfrak{n})$

Soit $X_0(\mathfrak{n})_K^+$ la courbe quotient $w_\mathfrak{n}\backslash X_0(\mathfrak{n})_K$ sur K. Sa jacobienne, notée $J_0(\mathfrak{n})^+$, s'identifie à la sous-variété abélienne $(1+w_\mathfrak{n})J_0(\mathfrak{n})$ de $J_0(\mathfrak{n})$ de la façon suivante. La projection $\pi : X_0(\mathfrak{n})_K \to X_0(\mathfrak{n})_K^+$ donne, par fonctorialité de Picard, un homomorphisme de variétés abéliennes $\pi^* : J_0(\mathfrak{n})^+ \to J_0(\mathfrak{n})$, qui est une immersion fermée car π est ramifié. Il identifie $J_0(\mathfrak{n})^+$ à une sous-variété abélienne de $J_0(\mathfrak{n})$. Par fonctorialité d'Albanese, le morphisme π donne un homomorphisme surjectif de variétés abéliennes $\pi_* : J_0(\mathfrak{n}) \to J_0(\mathfrak{n})^+$. L'application composée $\pi^* \circ \pi_* : J_0(\mathfrak{n}) \to J_0(\mathfrak{n})$ n'est autre que $1+w_\mathfrak{n}$. Donc $J_0(\mathfrak{n})^+$ s'identifie naturellement à $(1+w_\mathfrak{n})J_0(\mathfrak{n})$.

Soit $J_0(\mathfrak{n})^-$ la variété abélienne quotient $J_0(\mathfrak{n})/(1+w_\mathfrak{n})J_0(\mathfrak{n})$, définie sur K. On a alors la suite exacte de variétés abéliennes

$$0 \longrightarrow J_0(\mathfrak{n})^+ = (1+w_\mathfrak{n})J_0(\mathfrak{n}) \longrightarrow J_0(\mathfrak{n}) \longrightarrow J_0(\mathfrak{n})^- \longrightarrow 0. \tag{3.2}$$

Soit $J_0(\mathfrak{n})_-$ la plus grande sous-variété abélienne de $J_0(\mathfrak{n})$ annulée par $1+w_\mathfrak{n}$, définie sur K. La surjection canonique $J_0(\mathfrak{n}) \to J_0(\mathfrak{n})_-$ induit une isogénie entre $J_0(\mathfrak{n})_-$ et $J_0(\mathfrak{n})^-$.

3.2.7 La théorie d'Eichler-Shimura-Drinfeld

On suppose ici l'idéal $\mathfrak{n}$ premier. Il résulte de la théorie des formes automorphes que la $\mathbf{Q}$-algèbre $\mathbf{T}_\mathbf{Q}$ est commutative et semisimple de dimension $g = g(X_0(\mathfrak{n}))$. Soit $\mathscr{F}$ l'ensemble des formes propres pour $\mathbf{T}$ et normalisées. Elles forment une base du $\mathbf{C}$-espace vectoriel $\mathbf{H}(\mathbf{C})$. Le groupe $\mathrm{Gal}(\mathbf{Q}^{\mathrm{alg}}/\mathbf{Q})$ agit sur $\mathscr{F}$ *via* son action sur les coefficients de Fourier de F. Soit $\{F_1, \ldots, F_n\}$ un système de représentants des orbites de $\mathscr{F}$ sous $\mathrm{Gal}(\mathbf{Q}^{\mathrm{alg}}/\mathbf{Q})$. Soit K_i le corps de nombres totalement réel engendré par les coefficients de Fourier de F_i $(1 \leq i \leq n)$. On a alors un isomorphisme canonique de $\mathbf{Q}$-algèbres $\mathbf{T}_\mathbf{Q} \simeq K_1 \times \cdots \times K_n$.

Théorème 3.6. *(i) Soit $\mathfrak{p}_i$ le noyau du morphisme*

$$\begin{array}{ccc} \mathbf{T} & \longrightarrow & K_i \\ t & \longmapsto & \frac{tF_i}{F_i} \end{array}$$

et J_i la variété abélienne quotient $J_0(\mathfrak{n})/\mathfrak{p}_i J_0(\mathfrak{n})$ $(1 \leq i \leq n)$. Alors J_i est une variété abélienne simple sur K, de dimension $[K_i : \mathbf{Q}]$, et qui ne dépend que de l'orbite de F_i. Pour toute place v de K, on a l'égalité des fonctions L locales

$$L_v(J_i, s) = \prod_{\sigma : K_i \hookrightarrow \mathbf{C}} L_v(F_i^\sigma, s).$$

où σ parcourt les plongements de K_i dans $\mathbf{C}$. De plus, l'application canonique

$$J_0(\mathfrak{n}) \longrightarrow J_1 \times \cdots \times J_n$$

est une isogénie sur K.

(ii) Si I est un idéal de $\mathbf{T}$, on a une isogénie définie sur K

$$J_0(\mathfrak{n})/IJ_0(\mathfrak{n}) \sim \prod_{\substack{i \in \{1,\ldots,n\} \\ I \subset \mathfrak{p}_i}} J_i.$$

Une démonstration se trouve dans [Tam95] (proposition 4.2, remarque 4.3 et lemme 4.10). Ce théorème découle des résultats de Drinfeld [Dri74] et de la théorie des formes automorphes, notamment le théorème de multiplicité un. L'égalité des facteurs L locaux, en une place v ne divisant pas $\mathfrak{n}$, provient de la relation d'Eichler-Shimura et pour v quelconque, de résultats de Drinfeld et Deligne ([Dri87] th. A et rem. 2 et [Del73]).

3.2.8 La torsion K-rationnelle de la jacobienne

Si $\mathfrak{n}$ est premier, le sous-groupe cuspidal $\mathscr{C}$ de $J_0(\mathfrak{n})(K)$ est le sous-groupe engendré par la classe d'équivalence linéaire du diviseur $(0)-(\infty)$ dans $J_0(\mathfrak{n})(K)$.

Théorème 3.7 (Gekeler-Pál)**.** *Le groupe $\mathscr{C}$ coïncide avec le sous-groupe de torsion de $J_0(\mathfrak{n})(K)$. Il est cyclique d'ordre égal à*

$$n(\mathfrak{n}) = \begin{cases} \frac{q^{\deg \mathfrak{n}}-1}{q-1} & \textit{si } \deg \mathfrak{n} \textit{ est impair ;} \\ \frac{q^{\deg \mathfrak{n}}-1}{q^2-1} & \textit{si } \deg \mathfrak{n} \textit{ est pair.} \end{cases}$$

La cyclicité du groupe et le calcul de son cardinal sont dus à Gekeler ([Gek86b] cor. 5.11). L'identification avec $J_0(\mathfrak{n})(K)_{\mathrm{tors}}$ résulte des travaux de Pál sur l'idéal d'Eisenstein ([Pál05] th. 1.2 et 1.4).

3.3 Le quotient d'enroulement $J_{\mathbf{e}}(\mathfrak{n})$

Définition 3.8. Soit $I_{\mathbf{e}}$ l'annulateur dans $\mathbf{T}$ de l'élément d'enroulement $\mathbf{e} \in \mathbf{M}^0(\mathbf{Q})$. Soit $I_{\mathbf{e}}J_0(\mathfrak{n})$ la sous-variété abélienne de $J_0(\mathfrak{n})$ définie sur K engendrée par les tx, pour $t \in I_{\mathbf{e}}$ et $x \in J_0(\mathfrak{n})$. Le *quotient d'enroulement* $J_{\mathbf{e}}(\mathfrak{n})$ est la variété abélienne quotient $J_0(\mathfrak{n})/I_{\mathbf{e}}J_0(\mathfrak{n})$. Il est défini sur K.

L'involution $w_{\mathfrak{n}}$ échange les pointes 0 et ∞, donc $w_{\mathfrak{n}}[0,\infty] = [\infty, 0] = -[0,\infty]$ et, par conséquent, $w_{\mathfrak{n}}\mathbf{e} = -\mathbf{e}$. Donc l'idéal $I_{\mathbf{e}}$ contient $w_{\mathfrak{n}} + 1$. On a alors un morphisme surjectif $J_0(\mathfrak{n})^- \to J_{\mathbf{e}}(\mathfrak{n})$, qui fait de $J_{\mathbf{e}}(\mathfrak{n})$ un quotient de $J_0(\mathfrak{n})^-$.

Nous démontrons, grâce à la non-annulation de la fonction L de $J_{\mathbf{e}}(\mathfrak{n})$ en $s = 1$, que le groupe $J_{\mathbf{e}}(\mathfrak{n})(K)$ est fini.

Proposition 3.9. *Le $\mathbf{T} \otimes_{\mathbf{Z}} \mathbf{Q}$-module $\mathbf{M}^0(\mathbf{Q})$ est libre de rang 1.*

Démonstration. La proposition 2.9 fournit après, extension des scalaires à $\mathbf{Q}$, un accouplement parfait entre algèbre de Hecke et formes automorphes :

$$\begin{array}{rcl} \mathbf{T} \otimes_{\mathbf{Z}} \mathbf{Q} \times \mathbf{H}(\mathbf{Q}) & \longrightarrow & \mathbf{Q} \\ (t, F) & \longmapsto & c_{tF}((1)). \end{array}$$

Comme $\mathbf{T} \otimes_{\mathbf{Z}} \mathbf{Q}$ est commutative, cet accouplement est compatible à l'action de $\mathbf{T} \otimes_{\mathbf{Z}} \mathbf{Q}$. Par ailleurs, d'après le théorème 2.24, l'intégration le long des symboles modulaires donne un accouplement parfait et $(\mathbf{T} \otimes_{\mathbf{Z}} \mathbf{Q})$-équivariant entre $\mathbf{H}(\mathbf{Q})$ et $\mathbf{M}^0(\mathbf{Q})$, ce qui achève la démonstration. □

Proposition 3.10. *Si $F \in \mathbf{H}(\mathbf{C})$ est une forme propre, les deux propriétés suivantes sont équivalentes :*

(i) $I_{\mathbf{e}}F = 0$;

(ii) $L(F,1) \neq 0$.

Démonstration. Une démonstration similaire est présente dans [Oes] prop. 1. Soit $\mathcal{E}$ l'ensemble des orbites sous $\mathrm{Gal}(\mathbf{Q}^{\mathrm{alg}}/\mathbf{Q})$ des formes pour $\Gamma_0(\mathfrak{n})$ propres et normalisées. Si F est une telle forme, nous notons $[F]$ son orbite et $a_{[F]}$ l'annulateur de F dans $\mathbf{T}$ (il ne dépend que de $[F]$). L'application $[F] \mapsto a_{[F]}$ est une bijection entre $\mathcal{E}$ et l'ensemble des idéaux premiers minimaux de $\mathbf{T}$.

Le morphisme canonique $\varphi : \mathbf{T} \to \prod_{[F]\in\mathcal{E}} \mathbf{T}/a_{[F]}$ est injectif. Soit $b_{[F]}$ l'annulateur dans $\mathbf{T}$ de $a_{[F]}$. On a alors

$$b_{[F]} = \bigcap_{[F']\neq[F]} a_{[F']} \tag{3.3}$$

et la somme d'idéaux $\sum_{[F]} b_{[F]}$ est directe. Par ailleurs, l'image de φ est d'indice fini donc $\bigoplus_{[F]} b_{[F]}$ est d'indice fini dans $\mathbf{T}$. Comme $\mathbf{M}^0(\mathbf{Q})$ est un $\mathbf{T}\otimes_{\mathbf{Z}}\mathbf{Q}$-module libre de rang 1, on a la somme directe

$$\mathbf{M}^0(\mathbf{Q}) = \bigoplus_{[F]\in\mathcal{E}} b_{[F]}\mathbf{M}^0(\mathbf{Q}),$$

où les sous-modules $b_{[F]}\mathbf{M}^0(\mathbf{Q})$ sont simples et deux à deux non isomorphes. En particulier, il existe un sous-ensemble $\mathcal{E}_{\mathbf{e}}$ de $\mathcal{E}$ tel que

$$\mathbf{QTe} = \bigoplus_{[F]\in\mathcal{E}_{\mathbf{e}}} b_{[F]}\mathbf{M}^0(\mathbf{Q}). \tag{3.4}$$

L'intégration fournit un accouplement $\mathbf{H}(\mathbf{C})\times\mathbf{M}^0(\mathbf{Q}) \to \mathbf{C}$ non dégénéré. On en déduit que $a_{[F]}$ est l'annulateur dans $\mathbf{T}$ de $b_{[F]}\mathbf{M}^0(\mathbf{Q})$ et

$$I_{\mathbf{e}} = \bigcap_{[F]\in\mathcal{E}_{\mathbf{e}}} a_{[F]}. \tag{3.5}$$

Soit $F \in \mathbf{H}(\mathbf{C})$ une forme propre. Rappelons que $L(F,1) = \frac{1}{q-1}\langle \mathbf{e}, F\rangle$. D'après (3.3), pour tout $[F'] \neq [F]$, F est $\langle\ ,\ \rangle$-orthogonale à $b_{[F']}\mathbf{M}^0(\mathbf{Q})$. Comme F est propre, $\langle \mathbf{e}, F\rangle \neq 0$ revient à dire qu'il existe $c \in \mathbf{QTe}$ tel que $\langle c, F\rangle \neq 0$. D'après (3.4), cela revient à $[F] \in \mathcal{E}_{\mathbf{e}}$ c'est-à-dire, d'après (3.5), $I_{\mathbf{e}} \subset a_{[F]}$, soit encore $I_{\mathbf{e}}F = 0$. □

Jusqu'à la fin de cette section, on suppose l'idéal $\mathfrak{n}$ premier.

Théorème 3.11. *La fonction L du quotient d'enroulement est*

$$L(J_{\mathbf{e}}(\mathfrak{n}), s) = \prod_{\substack{F\in\mathbf{H}(\mathbf{C}),\ \textit{propre normalisée}\\ L(F,1)\neq 0}} L(F,s) \qquad (s \in \mathbf{C}).$$

Le quotient d'enroulement est le plus grand quotient de $J_0(\mathfrak{n})$ défini sur K dont la fonction L ne s'annule pas en $s = 1$. En particulier, $J_{\mathbf{e}}(\mathfrak{n})$ n'a qu'un nombre fini de points K-rationnels.

Démonstration. Avec les notations du théorème 3.6, d'après la construction d'Eichler-Shimura-Drinfeld, le quotient d'enroulement est isogène au produit suivant de variétés abéliennes

$$J_{\mathbf{e}}(\mathfrak{n}) \sim \prod_{\substack{i\in\{1,\dots,n\}\\ \mathfrak{p}_i\supset I_{\mathbf{e}}}} J_i$$

et

$$L(J_{\mathbf{e}}(\mathfrak{n}), s) = \prod_{\substack{i\in\{1,\dots,n\}\\ \mathfrak{p}_i\supset I_{\mathbf{e}}}} L(J_i, s).$$

De plus, on a $L(J_i, s) = \prod_{\sigma:K_i\hookrightarrow\mathbf{C}} L(F_i^\sigma, s)$ où σ parcourt les plongements de K_i dans $\mathbf{C}$. Donc

$$L(J_{\mathbf{e}}(\mathfrak{n}), s) = \prod_{\substack{F\in\mathbf{H}(\mathbf{C}),\ \text{propre normalisée}\\ I_{\mathbf{e}}F=0}} L(F, s) \qquad (s \in \mathbf{C}).$$

D'après la proposition 3.10, $L(J_{\mathbf{e}}(\mathfrak{n}), 1)$ est donc non nul. La finitude de $J_{\mathbf{e}}(\mathfrak{n})(K)$ s'en déduit par l'inégalité connue dans la conjecture de Birch et Swinnerton-Dyer (théorème 3.2 dû à Schneider). Le fait que $J_{\mathbf{e}}(\mathfrak{n})$ soit le plus grand quotient de $J_0(\mathfrak{n})$ vérifiant cette propriété découle de la proposition 3.10 et du théorème 3.6. □

***Remarque* 3.12.** D'après la conjecture de Birch et Swinnerton-Dyer, $J_{\mathbf{e}}(\mathfrak{n})$ serait le plus grand quotient de $J_0(\mathfrak{n})$ défini sur K n'ayant qu'un nombre fini de points rationnels sur K.

Corollaire 3.13. *La restriction de l'homomorphisme canonique $J_0(\mathfrak{n})(K) \to J_{\mathbf{e}}(\mathfrak{n})(K)$ au sous-groupe cuspidal $\mathscr{C}$ est injective.*

Démonstration. Considérons la variété abélienne $J = \tilde{J}^-$ de Tamagawa [Tam95]. C'est un quotient de $J_0(\mathfrak{n})$ défini sur K. D'après le théorème 5.7 de *loc. cit.*, le groupe $J(K)$ est fini et la composante l-primaire du groupe $Ш(J)$ est finie, pour tout nombre premier $l \neq p$. On en déduit que la fonction L de J ne s'annule pas en $s = 1$, d'après le théorème 11 (ii) de [Sch82]. Par le théorème 3.11, on a alors le diagramme commutatif

$$\begin{tikzcd} J_0(\mathfrak{n}) \arrow[r] \arrow[d] & J \\ J_{\mathbf{e}}(\mathfrak{n}) \arrow[ur] & \end{tikzcd},$$

qui donne un diagramme commutatif des groupes des points K-rationnels des variétés abéliennes. D'après la proposition 4.16 de [Tam95], la restriction du morphisme canonique $J_0(\mathfrak{n})(K) \to J$ à $\mathscr{C}$ est injective. Donc la restriction du morphisme canonique $J_0(\mathfrak{n})(K) \to J_{\mathbf{e}}(\mathfrak{n})(K)$ à $\mathscr{C}$ est injective. □

***Remarque* 3.14.** Pour la courbe modulaire classique $X_0(n)$, le morphisme canonique $J_0(n)(\mathbf{Q}) \to J_{\mathbf{e}}(n)(\mathbf{Q})$ donne, par restriction à $\mathscr{C}$, un isomorphisme de groupes finis $\mathscr{C} \simeq J_{\mathbf{e}}(n)(\mathbf{Q})$ (voir [Oes], remarque 3 p. 9). On peut s'attendre ici à un isomorphisme similaire.

3.4 Une minoration de la dimension de $J_{\mathbf{e}}(\mathfrak{n})$

Dans cette section, on suppose $\mathfrak{n}$ premier.

Comme $\mathrm{End}_K(J_0(\mathfrak{n}))$ est un $\mathbf{Z}$-module de type fini, il en est de même du $\mathbf{Z}$-module $\mathbf{T}$. On rappelle que $\mathbf{T} \otimes_{\mathbf{Z}} \mathbf{Q}$ est une $\mathbf{Q}$-algèbre de dimension $g(X_0(\mathfrak{n})) = \dim J_0(\mathfrak{n})$.

Proposition 3.15. *Le $\mathbf{Z}$-module $\mathbf{T}/I_{\mathbf{e}}$ est libre de rang égal à la dimension de $J_{\mathbf{e}}(\mathfrak{n})$.*

Démonstration. Le quotient $\mathbf{T}/I_{\mathbf{e}}$ est de type fini sur $\mathbf{Z}$. Par ailleurs, il est sans torsion : en effet, si $nt \in I_{\mathbf{e}}$ avec $n \in \mathbf{Z}$, $t \in \mathbf{T}$ alors $nt\mathbf{e} = 0 = t\mathbf{e}$ dans $\mathbf{M}^0(\mathbf{Q})$ donc $t \in I_{\mathbf{e}}$. Comme $\mathbf{Z}$ est principal, le quotient est donc un $\mathbf{Z}$-module libre. Il reste à montrer que $\dim_{\mathbf{Q}}(\mathbf{T}/I_{\mathbf{e}}) \otimes_{\mathbf{Z}} \mathbf{Q} = \dim J_{\mathbf{e}}(\mathfrak{n})$. Avec les notations du théorème 3.6, on a $\mathbf{T} \otimes_{\mathbf{Z}} \mathbf{Q} \simeq K_1 \times \cdots \times K_n$. Il existe un sous-ensemble Λ de $\{1, \ldots, n\}$ tel que $(\mathbf{T}/I_{\mathbf{e}}) \otimes_{\mathbf{Z}} \mathbf{Q} \simeq \prod_{i \in \Lambda} K_i$ et

$$\dim_{\mathbf{Q}}(\mathbf{T}/I_{\mathbf{e}}) \otimes_{\mathbf{Z}} \mathbf{Q} = \sum_{i \in \Lambda} [K_i : \mathbf{Q}].$$

Par ailleurs, $J_{\mathbf{e}}(\mathfrak{n})$ est isogène à $\displaystyle\prod_{\substack{i \in \{1,\ldots,n\} \\ \mathfrak{p}_i \supset I_{\mathbf{e}}}} J_i$, donc

$$\dim J_{\mathbf{e}}(\mathfrak{n}) = \sum_{\substack{i \in \{1,\ldots,n\} \\ \mathfrak{p}_i \supset I_{\mathbf{e}}}} \dim J_i = \sum_{\substack{i \in \{1,\ldots,n\} \\ \mathfrak{p}_i \supset I_{\mathbf{e}}}} [K_i : \mathbf{Q}].$$

Enfin, on voit facilement que $\Lambda = \{i \in \{1, \ldots, n\} \mid \mathfrak{p}_i \supset I_{\mathbf{e}}\}$. □

L'homomorphisme canonique $\mathbf{T} \to \mathbf{Te}$ se factorise en un isomorphisme de $\mathbf{T}$-modules $\mathbf{T}/I_{\mathbf{e}} \simeq \mathbf{Te}$. En particulier, la dimension de $J_{\mathbf{e}}(\mathfrak{n})$ est égale à $\mathrm{rg}_{\mathbf{Z}}\mathbf{Te} = \dim_{\mathbf{Q}}(\mathbf{T} \otimes_{\mathbf{Z}} \mathbf{Q})\mathbf{e}$. Minorer la dimension du quotient d'enroulement par un entier N revient alors à trouver une famille libre de symboles modulaires de la forme $t\mathbf{e}$ ($t \in \mathbf{T} \otimes_{\mathbf{Z}} \mathbf{Q}$), de cardinal au moins N. De telles familles ont précisément été exhibées dans la section 2.7.

Théorème 3.16. *Soit $\mathfrak{n}$ un idéal premier de degré $d \geq 3$.*

(i) On a la minoration $\dim J_{\mathbf{e}}(\mathfrak{n}) \geq q^{\left[\frac{d-3}{2}\right]}$.

(ii) Il existe une constante $C > 0$, ne dépendant que de q, telle que

$$\dim J_{\mathbf{e}}(\mathfrak{n}) \geq C(\dim J_0(\mathfrak{n}))^{1/2}.$$

(iii) Notons $\mathscr{F}$ l'ensemble des formes propres normalisées de $\mathbf{H}(\mathbf{C})$. Il existe une constante $C > 0$ ne dépendant que de q telle que

$$\#\{F \in \mathscr{F} \mid L(F, 1) \neq 0\} \geq C(\#\mathscr{F})^{1/2}.$$

Démonstration. (i) Soit $d \geq 3$. Posons $r = \left[\frac{d-3}{2}\right]$. On a alors $d \geq 2r + 3$. D'après le théorème 2.58, la dimension de $J_{\mathbf{e}}(\mathfrak{n})$ est au moins égale au cardinal de $\mathscr{P}_r$, qui est q^r.

(ii) La formule de la proposition 1.23 pour le genre donne l'estimation $g(X_0(\mathfrak{n})) = O(q^d)$ quand $d \to +\infty$. L'affirmation découle alors de (i).

(iii) La dimension de $J_0(\mathfrak{n})$ (resp. $J_{\mathbf{e}}(\mathfrak{n})$) est égale à $\#\mathscr{F}$ (resp. $\#\{F \in \mathscr{F} \mid L(F,1) \neq 0\}$), d'où la troisième assertion.

□

Corollaire 3.17. *Soit $\mathfrak{n}$ un idéal premier. Les affirmations suivantes sont équivalentes :*

(i) la variété abélienne $J_{\mathbf{e}}(\mathfrak{n})$ est non nulle ;

(ii) $\deg \mathfrak{n} \geq 3$ *;*

(iii) $g(X_0(\mathfrak{n})) > 0$.

Démonstration. L'équivalence de (ii) et (iii) vient du corollaire 2.59. Si le genre est nul, la variété abélienne $J_0(\mathfrak{n})$ est nulle ainsi que $J_{\mathbf{e}}(\mathfrak{n})$, ce qui montre (i)⇒(iii). Enfin, si $\deg \mathfrak{n} \geq 3$, la variété abélienne $J_{\mathbf{e}}(\mathfrak{n})$ est de dimension ≥ 1 d'après le théorème 3.16. Elle est donc non nulle, ce qui donne (ii)⇒(i). □

***Remarque* 3.18.** Notre estimation est meilleure que celle obtenue pour le quotient d'enroulement classique avec la même méthode : en effet, en niveau p^n, Parent obtient le minorant $C(\dim J_0(\mathfrak{n}))^{1/6}$ ([Par99] rem. p. 89). Des méthodes de théorie analytique des nombres permettent d'obtenir des estimations linéaires (comme $(\frac{1}{4} + o(1)) \dim J_0(\mathfrak{n})$ d'après Iwaniek et Sarnak [IS00] cor. 13).

3.5 Étude du quotient d'enroulement lorsque $\deg \mathfrak{n}$ est petit

3.5.1 Quotients d'enroulement triviaux

Théorème 3.19. *Soit $\mathfrak{n}$ un idéal premier. On a $J_0(\mathfrak{n}) = J_{\mathbf{e}}(\mathfrak{n})$ si et seulement si $\mathfrak{n}$ est de degré* 3.

Démonstration. Supposons $J_0(\mathfrak{n}) = J_{\mathbf{e}}(\mathfrak{n})$. Comme $J_{\mathbf{e}}(\mathfrak{n})$ est un quotient de $J_0(\mathfrak{n})^-$, on a alors

$$J_0(\mathfrak{n})^- = J_0(\mathfrak{n}).$$

D'après la suite exacte (3.2), on a donc $\dim J_0(\mathfrak{n})^+ = 0$. Cela signifie que la courbe $X_0(\mathfrak{n})$ est hyperelliptique. D'après Schweizer ([Sch97] th. 20), les seuls idéaux premiers $\mathfrak{n}$ pour lesquels $X_0(\mathfrak{n})$ est hyperelliptique sont ceux de degré 3.

Réciproquement, supposons $\mathfrak{n}$ premier de degré 3 et démontrons que $J_0(\mathfrak{n}) = J_{\mathbf{e}}(\mathfrak{n})$. Soit $F \in \mathscr{F}$. D'après le corollaire 2.17, $L(F,1)$ est non nul, donc $I_{\mathbf{e}}F = 0$ d'après la proposition 3.10. Soit $\mathfrak{p}$ l'idéal premier minimal de $\mathbf{T}$ associé à F. Alors $I_{\mathbf{e}}$ est contenu dans $\mathfrak{p}$. D'après l'équation (3.5) page 70, $I_{\mathbf{e}}$ est l'intersection des idéaux premiers minimaux de $\mathbf{T}$ contenant $I_{\mathbf{e}}$. Donc $I_{\mathbf{e}}$ est l'intersection des idéaux premiers minimaux de $\mathbf{T}$, c'est-à-dire l'idéal nul. La variété abélienne $I_{\mathbf{e}}J_0(\mathfrak{n})$ est nulle et $J_{\mathbf{e}}(\mathfrak{n}) = J_0(\mathfrak{n})$.

Signalons une démonstration alternative de ce résultat par les symboles modulaires. D'après le théorème 2.64, les symboles modulaires $\eta_{\mathfrak{p}}\mathbf{e}$, où $\mathfrak{p}$ décrit les idéaux de degré 1, forment une base de $\mathbf{M}^0(\mathbf{Q})$. Ceci montre que $\dim J_{\mathbf{e}}(\mathfrak{n}) \geq q$. Par ailleurs, $J_{\mathbf{e}}(\mathfrak{n})$ est un quotient de $J_0(\mathfrak{n})$, qui est de dimension q. On a donc l'égalité des dimensions et $J_{\mathbf{e}}(\mathfrak{n}) = J_0(\mathfrak{n})$. □

***Remarque* 3.20.** Le groupe fini $J_0(\mathfrak{n})(K)$ est cyclique d'ordre q^2+q+1, lorsque $\mathfrak{n}$ est premier de degré 3. C'est une conséquence du théorème 3.19 et de la description de $J_0(\mathfrak{n})(K)_{\mathrm{tors}}$ par le sous-groupe cuspidal (théorème 3.7).

Corollaire 3.21. *Toute courbe elliptique E sur K, à réduction multiplicative déployée en ∞ et de conducteur $\mathfrak{n}\cdot\infty$ où $\mathfrak{n}$ est un idéal premier de A de degré 3, est de rang nul.*

(Dans cet énoncé, ∞ désigne la place non-archimédienne $\frac{1}{T}$.)

Démonstration. L'assertion se déduit du théorème précédent grâce au théorème de modularité des courbes elliptiques sur les corps de fonctions, dû à Grothendieck, Jacquet-Langlands, Deligne et Drinfeld ([GR96], §8). □

Remarquons que ce corollaire est un cas particulier d'un résultat connu sur les courbes elliptiques sur les corps de fonctions : *toute courbe elliptique sur $\mathbf{F}_q(T)$ dont le conducteur est de degré 4 est de rang nul* (voir par exemple [Shi92], th. 4 et 7).

Exemple 3.22. D'après [Gek85] §9, les courbes elliptiques données dans le tableau ci-dessous sont de conducteur $\infty\cdot(T^3-f)$, où $f\in\mathbf{F}_q$ n'est pas une puissance cubique. Elles n'ont donc qu'un nombre fini de points sur K d'après ce qui précède.

p	équation affine	discriminant
$\neq 2,3$	$y^2=x^3-3T(T^3+8f)x+2(T^6-20fT^3-8f^2)$	$2^{12}3^3f(T^3-f)^3$
2	$y^2+Txy+(T^3+f)y=x^3$	$f(T^3+f)^3$

(on signale qu'une coquille s'est glissée dans le premier discriminant de *loc. cit.*).

Corollaire 3.23. *Soit $\mathfrak{n}$ un idéal premier de degré 3. La fonction L de la jacobienne $J_0(\mathfrak{n})$ est constante égale à 1 et le groupe de Tate-Shafarevich de $J_0(\mathfrak{n})$ est trivial.*

Démonstration. L'assertion sur la fonction L est une conséquence du corollaire 2.17 et du théorème 3.11. Le rang analytique de $J_0(\mathfrak{n})$ est alors nul et, d'après le théorème 3.2, il coïncide avec le rang de $J_0(\mathfrak{n})$ sur K. Par le théorème 3.3 de Kato-Trihan, la troisième affirmation de la conjecture de Birch et Swinnerton-Dyer est alors vérifiée et on a l'égalité

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

où $c_{\mathfrak{n}}$ (resp. c_∞) désigne l'ordre du groupe des composantes connexes de la fibre spéciale du modèle de Néron de $J_0(\mathfrak{n})$ en $\mathfrak{n}$ (resp. ∞). Évaluons ces quantités lorsque $\deg\mathfrak{n}=3$:

(i) l'ordre de $J_0(\mathfrak{n})(K)$ est q^2+q+1 (remarque 3.20) ;

(ii) $c_{\mathfrak{n}}=q^2+q+1$ d'après Gekeler (proposition 3.5) ;

(iii) $c_\infty=q^2+q+1$ d'après Gekeler [Gek97b] 6.3 (ii).

Il ne reste que $L(J_0(\mathfrak{n}),1)=1=\#Ш(J_0(\mathfrak{n}))$. □

3.5.2 Quelques quotients d'enroulement en degré supérieur

Reprenons l'exemple 2.68 ($q = 2$ et $\mathfrak{n} = (T^4 + T + 1)$ idéal premier). On a établi

$$\dim J_{\mathbf{e}}(\mathfrak{n}) = \dim_{\mathbf{Q}} \mathbf{QTe} \geq 2.$$

D'après l'équation fonctionnelle (corollaire 2.15), on a

$$\dim J_{\mathbf{e}}(\mathfrak{n}) = \#\{F \in \mathscr{F} \mid L(F,1) \neq 0\} \leq \#\{F \in \mathscr{F} \mid w_{\mathfrak{n}} F = -F\}.$$

Les calculs de l'exemple 2.68 ont montré qu'il existe exactement deux formes propres normalisées de valeur propre -1 pour $w_{\mathfrak{n}}$: ce sont celles correspondant aux symboles modulaires m_1 et m_2. Donc on obtient

$$\dim J_{\mathbf{e}}(\mathfrak{n}) = 2 < \dim J_0(\mathfrak{n}) = 4.$$

L'énoncé suivant généralise cet exemple.

Proposition 3.24. *Soit $\mathfrak{n}$ un idéal premier vérifiant la propriété : toute forme propre de $\mathbf{H}(\mathbf{C})$ est de rang ≤ 1 (c'est le cas par exemple si $\deg \mathfrak{n} = 4$ d'après le corollaire 2.18). Alors les variétés abéliennes $J_{\mathbf{e}}(\mathfrak{n})$ et $J_0(\mathfrak{n})^-$ sont égales.*

Soient N le générateur unitaire de $\mathfrak{n}$ dans A, $h(\sqrt{f})$ le nombre de classes de l'ordre $\mathbf{F}_q[T, \sqrt{f}]$. Il existe un unique couple $(S, R) \in A \times A$ tel que $N = S^2 + TR^2$. Posons $Q = \prod_P P^{\mathrm{ord}_P(R)}$, le produit fini portant sur les polynômes unitaires irréductibles de A, distincts de 1. Soit α un carré quelconque dans $\mathbf{F}_q^\times$. Alors la dimension de $J_{\mathbf{e}}(\mathfrak{n})$ est

(i) si q impair et $\deg \mathfrak{n}$ pair : $\frac{1}{2}h(\sqrt{\alpha N}) - 1$;

(ii) si q impair et $\deg \mathfrak{n}$ impair : $\frac{1}{2}(h(\sqrt{N}) + h(\sqrt{\alpha N})) - 1$;

(iii) si q pair et $\deg \mathfrak{n}$ pair : $\frac{1}{2}\left(\frac{q^{\deg \mathfrak{n}} - q^2}{q^2 - 1} + \sum_{f|Q} q^{\deg f} - 1\right)$;

(iv) si q pair et $\deg \mathfrak{n}$ impair : $\frac{1}{2}\left(\frac{q^{\deg \mathfrak{n}} - q}{q^2 - 1} + \sum_{f|Q} q^{\deg f} - 1\right)$.

Démonstration. Soit $F \in \mathbf{H}(\mathbf{C})$ une forme propre. Par hypothèse, on a : $w_{\mathfrak{n}} F = F$ si et seulement si $L(F, 1) = 0$. D'après (ii) du théorème 3.6 et la proposition 3.10, les variétés abéliennes $J_{\mathbf{e}}(\mathfrak{n})$ et $J_0(\mathfrak{n})^-$ sont donc isogènes sur K. Comme $w_{\mathfrak{n}} + 1 \in I_{\mathbf{e}}$, on en déduit par un argument de dimension que les sous-variétés abéliennes $I_{\mathbf{e}} J_0(\mathfrak{n})$ et $(w_{\mathfrak{n}} + 1) J_0(\mathfrak{n})$ sont égales, donc les quotients $J_{\mathbf{e}}(\mathfrak{n})$ et $J_0(\mathfrak{n})^-$ sont égaux.

En posant $g = \dim J_0(\mathfrak{n})$ et $g^+ = \dim J_0(\mathfrak{n})^+$, la suite exacte (3.2) donne

$$\dim J_0(\mathfrak{n})^- = g - g^+.$$

Par ailleurs, d'après la proposition 7 de Schweizer [Sch97], la formule de Hurwitz donne

$$g^+ = \begin{cases} \frac{1}{2}(2g + 2 - n) & \text{si } q \text{ impair} ; \\ \frac{1}{2}(g + 1 - n) & \text{si } q \text{ pair}, \end{cases}$$

où n est le nombre de points fixes de l'involution $w_{\mathfrak{n}}$ sur $X_0(\mathfrak{n})_K$. On en déduit

$$\dim J_0(\mathfrak{n})^- = \begin{cases} \frac{n}{2} - 1 & \text{si } q \text{ impair} ; \\ \frac{1}{2}(g - 1 + n) & \text{si } q \text{ pair}. \end{cases}$$

Comme $\mathfrak{n}$ est premier, $w_\mathfrak{n}$ échange les pointes, donc les points fixes éventuels de $w_\mathfrak{n}$ ne sont pas des pointes. Le nombre de tels points fixes est donné par la proposition 11 et le lemme 12 de *loc. cit.* :

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

□

3.6 Une version raffinée de $J_\mathbf{e}(\mathfrak{n})$

Dans cette section, on suppose $\mathfrak{n}$ premier.

3.6.1 Un raffinement

On rappelle que $\widetilde{\mathbf{e}}$ désigne la classe du symbole modulaire $d_\mathbf{e}\mathbf{e}$ dans $\mathbf{M}^0/p\mathbf{M}^0$ (notation 2.53).

***Notation* 3.25.** Soit $\widetilde{I_\mathbf{e}}$ l'annulateur de $\widetilde{\mathbf{e}}$ dans $\mathbf{T}$, c'est-à-dire l'ensemble des $t \in \mathbf{T}$ tels que $d_\mathbf{e} t\mathbf{e} \in p\mathbf{M}^0$.

L'idéal $\widetilde{I_\mathbf{e}}$ de $\mathbf{T}$ vérifie $I_\mathbf{e} + p\mathbf{T} \subset \widetilde{I_\mathbf{e}}$. Rappelons qu'un idéal I de $\mathbf{T}$ est dit *saturé* si le groupe abélien $\mathbf{T}/I$ est sans torsion.

Dans le chapitre 5, nous serons amenés à considérer une variante du quotient d'enroulement, pour éviter les problèmes posés par le passage de suite exactes de variétés abéliennes aux espaces cotangents de leurs modèles de Néron. *Jusqu'à la fin de cette sous-section, nous faisons l'hypothèse (H_I) suivante afin de construire cette variante.*

(H_I) On suppose qu'il existe un idéal saturé I de $\mathbf{T}$ vérifiant les propriétés :

(i) $I_\mathbf{e} \subset I$;

(ii) $I \subset \widetilde{I_\mathbf{e}}$;

(iii) $\widehat{I} + \widetilde{I_\mathbf{e}} = \mathbf{T}$, où $\widehat{I}$ désigne l'annulateur dans $\mathbf{T}$ de I.

Définition 3.26. Soit $IJ_0(\mathfrak{n})$ la sous-variété abélienne de $J_0(\mathfrak{n})$ engendrée par $\{tx \mid t \in I, x \in J_0(\mathfrak{n})\}$. Le *quotient raffiné* $J'_\mathbf{e}(\mathfrak{n})$ est la variété abélienne quotient $J_0(\mathfrak{n})/IJ_0(\mathfrak{n})$. Il est défini sur K.

Lemme 3.27. *Le $\mathbf{Z}$-module $\mathbf{T}/I$ est libre, de rang égal à la dimension de $J'_\mathbf{e}(\mathfrak{n})$.*

Démonstration. On procède comme dans la preuve de la proposition 3.15, étant donné que l'idéal I est saturé. □

Proposition 3.28. *(i) La variété abélienne $J'_\mathbf{e}(\mathfrak{n})$ n'a qu'un nombre fini de points K-rationnels.*

(ii) Soit $\mathfrak{n}$ un idéal premier de degré $d \geq 3$. On a $\dim J'_\mathbf{e}(\mathfrak{n}) \geq q^{\left[\frac{d-3}{2}\right]}$. En particulier, la variété abélienne $J'_\mathbf{e}(\mathfrak{n})$ est non nulle.

Démonstration. (i) Comme $I_{\mathbf{e}} \subset I$, on a le diagramme commutatif

$$\begin{tikzcd} J_0(\mathfrak{n}) \arrow[r, "\pi"] \arrow[d] & J'_{\mathbf{e}}(\mathfrak{n}) \\ J_{\mathbf{e}}(\mathfrak{n}) \arrow[ur] & \end{tikzcd} .$$

Donc $J'_{\mathbf{e}}(\mathfrak{n})$ est un quotient de $J_{\mathbf{e}}(\mathfrak{n})$, et n'a qu'un nombre fini de points K-rationnels, puisqu'il en est de même de ce dernier.

(ii) Soit $\mathfrak{n}$ un idéal premier de degré $d \geq 3$. Posons $r = [\frac{d-3}{2}]$. Comme $\deg \mathfrak{n} \geq 2r+3$, d'après le théorème 2.60, les images dans $\mathbf{T}/\widetilde{I}_{\mathbf{e}}$ de T_s, pour s dans $\mathscr{P}_r$, sont $\mathbf{F}_p$-linéairement indépendantes. Par ailleurs, on a $I \subset \widetilde{I}_{\mathbf{e}}$, donc l'homomorphisme canonique de $\mathbf{T}$-modules $\mathbf{T} \to \mathbf{T}/\widetilde{I}_{\mathbf{e}}$ se factorise en un homomorphisme surjectif $\mathbf{T}/I \to \mathbf{T}/\widetilde{I}_{\mathbf{e}}$. Ainsi, les images dans $\mathbf{T}/I$ de T_s, pour s dans $\mathscr{P}_r$, sont $\mathbf{Z}$-linéairement indépendantes. On en déduit, par le lemme 3.27, que la dimension de $J'_{\mathbf{e}}(\mathfrak{n})$ est au moins $\#\mathscr{P}_r = q^r$.

□

3.6.2 Quelques situations dans lesquelles l'hypothèse (H_I) est vérifiée

Il est raisonnable d'espérer que l'idéal $I_{\mathbf{e}}$ vérifie l'hypothèse (H_I), pour certains idéaux premiers $\mathfrak{n}$. En effet, l'idéal $I_{\mathbf{e}}$ est saturé et vérifie (i) et (ii). Il vérifie (iii) dès que $I_{\mathbf{e}} + \widehat{I}_{\mathbf{e}} + p\mathbf{T} = \mathbf{T}$.

Proposition 3.29. *Supposons l'une des deux conditions suivantes vérifiée :*

(i) $\mathfrak{n}$ *est un idéal premier de degré* 3 *;*

(ii) $p \neq 2$ *et l'idéal premier* $\mathfrak{n}$ *est tel que toute forme propre de* $\mathbf{H}(\mathbf{C})$ *est de rang* ≤ 1 *(c'est le cas par exemple si* $\deg \mathfrak{n} = 4$ *d'après le corollaire 2.18).*

Alors l'idéal $I_{\mathbf{e}}$ *vérifie l'hypothèse* (H_I).

Démonstration. Si $\mathfrak{n}$ est de degré 3, l'idéal $I_{\mathbf{e}}$ est nul d'après le théorème 3.19. Donc $\widehat{I}_{\mathbf{e}} = \mathbf{T}$ et $I_{\mathbf{e}}$ vérifie la propriété (iii) de l'hypothèse (H_I).

Supposons $p \neq 2$. Soit $\mathfrak{n}$ un idéal premier vérifiant la condition (ii) de la proposition. Si F est propre pour $\mathbf{T}$, on a alors

$$w_{\mathfrak{n}} F = F \quad \text{si et seulement si} \quad L(F,1) = 0. \tag{3.6}$$

Démontrons $I_{\mathbf{e}} + \widehat{I}_{\mathbf{e}} + p\mathbf{T} = \mathbf{T}$. Si I est un idéal de $\mathbf{T}$, on note I^{sat} sa saturation dans $\mathbf{T}$. Comme $(1+w_{\mathfrak{n}})\mathbf{T} \subset I_{\mathbf{e}}$ et $I_{\mathbf{e}}$ est saturé, on a $((1+w_{\mathfrak{n}})\mathbf{T})^{\mathrm{sat}} \subset I_{\mathbf{e}}$. Démontrons l'inclusion réciproque. Soit $t \in I_{\mathbf{e}}$. Soit F une forme propre pour $\mathbf{T}$. Si $L(F,1) \neq 0$, on a $I_{\mathbf{e}} F = 0$ donc $tF = 0$ (proposition 3.10). Si $L(F,1) = 0$, on a $(1-w_{\mathfrak{n}})F = 0$ d'après (3.6). Donc $(1-w_{\mathfrak{n}})t$ annule F. Comme $\mathbf{H}(\mathbf{C})$ possède une base de formes propres pour $\mathbf{T}$, on a $(1-w_{\mathfrak{n}})t = 0$ dans $\mathbf{T}$. On en déduit $2t = (1+w_{\mathfrak{n}})t$, donc $\frac{1}{2}(1+w_{\mathfrak{n}})t = t$ dans $\mathbf{T}$. Or, $\frac{1}{2}(1+w_{\mathfrak{n}})t$ appartient à $((1+w_{\mathfrak{n}})\mathbf{T})^{\mathrm{sat}} = ((1+w_{\mathfrak{n}})\mathbf{T} \otimes_{\mathbf{Z}} \mathbf{Q}) \cap \mathbf{T}$. On a donc $I_{\mathbf{e}} \subset ((1+w_{\mathfrak{n}})\mathbf{T})^{\mathrm{sat}}$ et

$$I_{\mathbf{e}} = ((1+w_{\mathfrak{n}})\mathbf{T})^{\mathrm{sat}}.$$

Démontrons
$$\widehat{I_{\mathbf{e}}} = ((1 - w_{\mathfrak{n}})\mathbf{T})^{\mathrm{sat}}.$$
Commençons par un résultat préliminaire.

Lemme 3.30. *Soit G un groupe abélien. Si I est un sous-groupe de G, on a $\widehat{I^{\mathrm{sat}}} = \widehat{I}^{\mathrm{sat}}$.*

Démonstration. Comme $I \subset I^{\mathrm{sat}}$, on a $\widehat{I^{\mathrm{sat}}} \subset \widehat{I}$. En passant aux saturations, cela donne $\widehat{I^{\mathrm{sat}}} \subset \widehat{I^{\mathrm{sat}}}^{\mathrm{sat}} \subset \widehat{I}^{\mathrm{sat}}$. Réciproquement, on a $I^{\mathrm{sat}} = (I \otimes_{\mathbf{Z}} \mathbf{Q}) \cap \mathbf{T}$ et $\widehat{I}^{\mathrm{sat}} = (\widehat{I} \otimes_{\mathbf{Z}} \mathbf{Q}) \cap \mathbf{T}$, d'où $\widehat{I}^{\mathrm{sat}} \subset \widehat{I^{\mathrm{sat}}}$. □

En appliquant le lemme au sous-groupe $I_{\mathbf{e}}$ de $\mathbf{T}$, on obtient
$$\widehat{I_{\mathbf{e}}} = \widehat{(I_{\mathbf{e}})^{\mathrm{sat}}} = ((\widehat{1 + w_{\mathfrak{n}}})\mathbf{T})^{\mathrm{sat}}.$$
Dans $\mathbf{T}$, on a $(1 + w_{\mathfrak{n}})(1 - w_{\mathfrak{n}}) = 0$. On en déduit $(1 - w_{\mathfrak{n}})\mathbf{T} \subset ((\widehat{1 + w_{\mathfrak{n}}})\mathbf{T})$, donc $((1 - w_{\mathfrak{n}})\mathbf{T})^{\mathrm{sat}} \subset ((\widehat{1 + w_{\mathfrak{n}}})\mathbf{T})^{\mathrm{sat}}$. Démontrons $((\widehat{1 + w_{\mathfrak{n}}})\mathbf{T})^{\mathrm{sat}} \subset ((1 - w_{\mathfrak{n}})\mathbf{T})^{\mathrm{sat}}$. Soit $t \in ((\widehat{1 + w_{\mathfrak{n}}})\mathbf{T})$. Écrivons $2t = (1 + w_{\mathfrak{n}})t + (1 - w_{\mathfrak{n}})t = (1 - w_{\mathfrak{n}})t$. On a donc $t \in ((1 - w_{\mathfrak{n}})\mathbf{T})^{\mathrm{sat}}$. Ceci montre $((\widehat{1 + w_{\mathfrak{n}}})\mathbf{T}) \subset ((1 - w_{\mathfrak{n}})\mathbf{T})^{\mathrm{sat}}$, d'où, en passant aux saturations,
$$((1 - w_{\mathfrak{n}})\mathbf{T})^{\mathrm{sat}} = ((\widehat{1 + w_{\mathfrak{n}}})\mathbf{T})^{\mathrm{sat}} = \widehat{I_{\mathbf{e}}}.$$
Comme $2 = (1 - w_{\mathfrak{n}}) + (1 + w_{\mathfrak{n}})$, on a
$$2\mathbf{T} \subset (1 - w_{\mathfrak{n}})\mathbf{T} + (1 + w_{\mathfrak{n}})\mathbf{T} \subset ((1 - w_{\mathfrak{n}})\mathbf{T})^{\mathrm{sat}} + ((1 + w_{\mathfrak{n}})\mathbf{T})^{\mathrm{sat}},$$
d'où
$$2\mathbf{T} + p\mathbf{T} \subset I_{\mathbf{e}} + \widehat{I_{\mathbf{e}}} + p\mathbf{T}.$$
Comme p est premier distinct de 2, $2\mathbf{T} + p\mathbf{T} = \mathbf{T}$ et la propriété $I_{\mathbf{e}} + \widehat{I_{\mathbf{e}}} + p\mathbf{T} = \mathbf{T}$ est démontrée. □

Nous suggérons maintenant un idéal $I'_{\mathbf{e}}$ qui pourrait vérifier l'hypothèse (H_I), pour certains idéaux $\mathfrak{n}$.

***Notation* 3.31.** Soit $\mathcal{S}$ l'ensemble des idéaux premiers minimaux de $\mathbf{T}$. Soit $\mathcal{S}'$ l'ensemble des $\mathfrak{p} \in \mathcal{S}$ tels qu'il existe un idéal maximal $\mathfrak{m}$ de $\mathbf{T}$ avec $\mathfrak{p} \subset \mathfrak{m}$ et $\widetilde{I_{\mathbf{e}}} \subset \mathfrak{m}$. On note $I'_{\mathbf{e}}$ l'idéal $\bigcap_{\mathfrak{p} \in \mathcal{S}'} \mathfrak{p}$ de $\mathbf{T}$ et $I''_{\mathbf{e}}$ l'annulateur dans $\mathbf{T}$ de $I'_{\mathbf{e}}$.

L'idéal $I'_{\mathbf{e}}$ est donc l'intersection des idéaux premiers minimaux $\mathfrak{p}$ de $\mathbf{T}$ tels que $\mathfrak{p} + \widetilde{I_{\mathbf{e}}} \subsetneq \mathbf{T}$.

Lemme 3.32. *On a $\prod_{\mathfrak{p} \notin \mathcal{S}'} \mathfrak{p} \subset I''_{\mathbf{e}}$.*

Démonstration. Soit $t \in I'_{\mathbf{e}}$ et $x_{\mathfrak{p}} \in \mathfrak{p}$ ($\mathfrak{p} \notin \mathcal{S}'$). Soit $\mathfrak{q}$ un idéal premier minimal de $\mathbf{T}$. Démontrons que $y = t \prod_{\mathfrak{p} \notin \mathcal{S}'} x_{\mathfrak{p}}$ appartient à $\mathfrak{q}$. Si $\mathfrak{q} \notin \mathcal{S}'$, alors $x_{\mathfrak{q}} \in \mathfrak{q}$ donc $y \in \mathfrak{q}$. Si $\mathfrak{q} \in \mathcal{S}'$, comme $I'_{\mathbf{e}} \subset \mathfrak{q}$, t appartient à $\mathfrak{q}$ donc $y \in \mathfrak{q}$. On a donc $t \in \bigcap_{\mathfrak{p} \in \mathcal{S}} \mathfrak{p}$. Rappelons que $\mathcal{S}$ est en bijection avec l'ensemble des classes de conjugaison de formes propres normalisées dans $\mathbf{H}(\mathbf{C})$. Alors t annule toutes les formes propres normalisées. Comme elles forment une base de $\mathbf{H}(\mathbf{C})$ et t est un endomorphisme de $\mathbf{H}(\mathbf{C})$, t est nul. On a montré que $I''_{\mathbf{e}}$ contient $\prod_{\mathfrak{p} \notin \mathcal{S}'} x_{\mathfrak{p}}$. Comme ces éléments engendrent $\prod_{\mathfrak{p} \notin \mathcal{S}'} \mathfrak{p}$, $I''_{\mathbf{e}}$ contient $\prod_{\mathfrak{p} \notin \mathcal{S}'} \mathfrak{p}$. □

Proposition 3.33. *(i) L'idéal $I'_{\mathbf{e}}$ est saturé.*

(ii) On a $I'_{\mathbf{e}} = \bigcap_{k\geq 1}(\widetilde{I}_{\mathbf{e}})^k$. En particulier, $I'_{\mathbf{e}} \subset \widetilde{I}_{\mathbf{e}}$.

(iii) On a $\widetilde{I}_{\mathbf{e}} + I''_{\mathbf{e}} = \mathbf{T}$.

Démonstration. (i) Il suffit de voir que le groupe abélien $\mathbf{T}/I'_{\mathbf{e}}$ est sans torsion. Supposons qu'il existe $t \in \mathbf{T}$ et $n \in \mathbf{Z}$ non nul vérifiant $nt \in I'_{\mathbf{e}}$. Alors, pour tout idéal premier minimal $\mathfrak{p} \in \mathcal{S}'$, on a $nt \in \mathfrak{p}$ donc $n \in \mathfrak{p}$ ou $t \in \mathfrak{p}$. Si $n \in \mathfrak{p}$, alors une forme propre F dans la classe de conjugaison associée à $\mathfrak{p}$ vérifierait $nF = 0$ dans $\mathbf{H}(\mathbf{C})$, d'où $n = 0$ ce qui est exclu. Ainsi t appartient à tout idéal premier minimal $\mathfrak{p}$ de $\mathcal{S}'$ c'est-à-dire à $I'_{\mathbf{e}}$.

(ii) Cela découle d'un résultat plus général d'algèbre commutative qu'on rappelle ici.

Lemme 3.34. *Soient R un anneau noetherien et I un idéal de R. Soit $\mathcal{S}$ l'ensemble des idéaux premiers minimaux de R. Alors on a*

$$\bigcap_{\substack{\mathfrak{p}\in\mathcal{S}\\ I+\mathfrak{p}\subsetneq R}} \mathfrak{p} = \bigcap_{k\geq 1} I^k.$$

Démonstration. Un argument similaire se trouve dans la proposition 4.11 de [Tam95]. Soit $\mathcal{L}$ un idéal maximal de R. Soit $R_{\mathcal{L}}$ le localisé de R par rapport à la partie multiplicative $R - \mathcal{L}$. On a le diagramme commutatif

$$\begin{tikzcd} R \arrow[r, hook] \arrow[d] & \prod_{\mathfrak{p}\in\mathcal{S}} R/\mathfrak{p} \arrow[d] \\ R_{\mathcal{L}} \arrow[r, hook] & \prod_{\mathfrak{p}\in\mathcal{S}} (R/\mathfrak{p})_{\mathcal{L}} \end{tikzcd}$$

où les flèches horizontales sont injectives, et

$$(R/\mathfrak{p})_{\mathcal{L}} = \begin{cases} 0 & \text{si } \mathfrak{p} \not\subseteq \mathcal{L}\ ; \\ \text{le localisé de } R/\mathfrak{p} \text{ par rapport à } R/\mathfrak{p} - \mathcal{L}/\mathfrak{p} & \text{si } \mathfrak{p} \subset \mathcal{L}. \end{cases}$$

Ce diagramme montre que le noyau du morphisme $R \to R_{\mathcal{L}}$ est $\bigcap_{\substack{\mathfrak{p}\in\mathcal{S}\\ \mathfrak{p}\subset\mathcal{L}}} \mathfrak{p}$.

Comme R est noetherien, on a alors, d'après le théorème de Krull (voir par exemple l'exercice 10/3 de [AM69]),

$$\begin{aligned} \bigcap_{k\geq 1} I^k &= \bigcap_{\substack{\mathcal{L} \text{ maximal}\\ I\subset\mathcal{L}}} \operatorname{Ker}(R \to R_{\mathcal{L}}) = \bigcap_{\substack{\mathcal{L} \text{ maximal}\\ I\subset\mathcal{L}}} \bigcap_{\substack{\mathfrak{p}\in\mathcal{S}\\ \mathfrak{p}\subset\mathcal{L}}} \mathfrak{p} \\ &= \bigcap_{\substack{\mathfrak{p}\in\mathcal{S}\\ \exists\mathcal{L} \text{ maximal avec } I+\mathfrak{p}\subset\mathcal{L}}} \mathfrak{p} = \bigcap_{\substack{\mathfrak{p}\in\mathcal{S}\\ I+\mathfrak{p}\subsetneq R}} \mathfrak{p}. \end{aligned}$$

□

(iii) Supposons que cela ne soit pas le cas. Alors il existe un idéal maximal $\mathfrak{m}$ de $\mathbf{T}$ tel que $\widetilde{I}_{\mathbf{e}} \subset \mathfrak{m}$ et $I''_{\mathbf{e}} \subset \mathfrak{m}$. Pour conclure, il suffit de montrer l'existence d'un

idéal premier minimal $\mathfrak{p} \notin \mathcal{S}'$ contenu dans $\mathfrak{m}$. En effet, comme $\widetilde{I}_{\mathbf{e}} \subset \mathfrak{m}$, alors $\mathfrak{p}$ appartiendra à $\mathcal{S}'$ par définition de cet ensemble, ce qui est impossible.

Supposons que tout idéal premier minimal $\mathfrak{p} \notin \mathcal{S}'$ n'est pas contenu dans $\mathfrak{m}$. Alors pour tout $\mathfrak{p} \notin \mathcal{S}'$, il existe un $x_{\mathfrak{p}} \in \mathfrak{p}$ qui n'est pas élément de $\mathfrak{m}$. Considérons le produit $\prod_{\mathfrak{p} \notin \mathcal{S}'} x_{\mathfrak{p}}$. Il n'appartient pas à $\mathfrak{m}$ car $\mathfrak{m}$ est premier. Par ailleurs, il appartient à $\prod_{\mathfrak{p} \notin \mathcal{S}'} \mathfrak{p} \subset I''_{\mathbf{e}}$. Cela contredit $I''_{\mathbf{e}} \subset \mathfrak{m}$.

□

L'énoncé suivant donne un critère pour que $I'_{\mathbf{e}}$ vérifie l'hypothèse (H_I).

Proposition 3.35. *Si $d_{\mathbf{e}}\mathbf{e}$ engendre le $\mathbf{T}$-module $\mathbf{M}^0/\widetilde{I}_{\mathbf{e}}\mathbf{M}^0$, on a $I_{\mathbf{e}} \subset I'_{\mathbf{e}}$.*

Démonstration. Comme $d_{\mathbf{e}}\mathbf{e}$ engendre $\mathbf{M}^0/\widetilde{I}_{\mathbf{e}}\mathbf{M}^0$, on a les décompositions suivantes de $\mathbf{M}^0$ en sous-$\mathbf{T}$-modules :

$$\begin{aligned}\mathbf{M}^0 &= \mathbf{T}d_{\mathbf{e}}\mathbf{e} + \widetilde{I}_{\mathbf{e}}\mathbf{M}^0 = \mathbf{T}d_{\mathbf{e}}\mathbf{e} + \widetilde{I}_{\mathbf{e}}(\mathbf{T}\mathbf{e} + \widetilde{I}_{\mathbf{e}}\mathbf{M}^0)\\ &= \mathbf{T}d_{\mathbf{e}}\mathbf{e} + \widetilde{I}_{\mathbf{e}}\mathbf{T}\mathbf{e} + (\widetilde{I}_{\mathbf{e}})^2\mathbf{M}^0 = \mathbf{T}d_{\mathbf{e}}\mathbf{e} + (\widetilde{I}_{\mathbf{e}})^2\mathbf{M}^0.\end{aligned}$$

En itérant ce procédé, on obtient $\mathbf{M}^0 = \mathbf{T}d_{\mathbf{e}}\mathbf{e} + (\widetilde{I}_{\mathbf{e}})^k\mathbf{M}^0$, pour tout $k \geq 1$. D'après la proposition 3.33 (ii), on a alors

$$\mathbf{M}^0 = \mathbf{T}d_{\mathbf{e}}\mathbf{e} + I'_{\mathbf{e}}\mathbf{M}^0. \tag{3.7}$$

Prouvons maintenant $I_{\mathbf{e}} \subset I'_{\mathbf{e}}$. L'idéal $I'_{\mathbf{e}}$ étant saturé, il est l'intersection des idéaux premiers minimaux de $\mathbf{T}$ le contenant. Soit $\mathfrak{p}$ un tel idéal, correspondant à la classe, sous $\mathrm{Gal}(\mathbf{Q}^{\mathrm{alg}}/\mathbf{Q})$, d'une forme propre $F \in \mathbf{H}(\mathbf{C})$. Il suffit alors de montrer que si $t \in I_{\mathbf{e}}$, on a $t \in \mathfrak{p}$, c'est-à-dire $tF = 0$. L'accouplement entre $\mathbf{M}^0(\mathbf{C})$ et $\mathbf{H}(\mathbf{C})$ étant parfait d'après le théorème 2.24, cela revient à montrer $\langle m, tF\rangle = 0$ $(m \in \mathbf{M}^0(\mathbf{C}))$. L'égalité (3.7) donne, après extension des scalaires,

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

Soit $m \in \mathbf{M}^0(\mathbf{C})$. Écrivons $m = t_1\mathbf{e} + t_2m_2$, avec $t_1 \in \mathbf{T} \otimes_{\mathbf{Z}} \mathbf{C}$, $t_2 \in I'_{\mathbf{e}}$ et $m_2 \in \mathbf{M}^0(\mathbf{C})$. Calculons l'accouplement :

$$\langle m, tF\rangle = \langle tm, F\rangle = \langle tt_1\mathbf{e} + tt_2m_2, F\rangle = \langle t_2tm_2, F\rangle = \langle tm_2, t_2F\rangle = 0$$

(on a utilisé $I'_{\mathbf{e}} \subset \mathfrak{p}$, c'est-à-dire $I'_{\mathbf{e}}F = 0$). On a donc $tF = 0$. □

Chapitre 4

Formes modulaires pour $\mathbf{F}_q[T]$

4.1 Le module de Tate-Drinfeld (rappels)

Nous rappelons la construction du « module de Tate-Drinfeld », analogue à la courbe de Tate classique, et son utilisation pour l'étude du voisinage des pointes de la courbe modulaire $X_0(\mathfrak{n})$. Une telle présentation a déjà été abordée, par exemple dans [Gos80c] 1.51, [Gek88b] 11.3 et [vdH06] §6. Par souci de complétude, nous rappelons les résultats adaptés à notre situation (module de Tate-Drinfeld sans niveau).

4.1.1 Construction

Considérons le module de Carlitz ρ de rang 1 sur $K((t))$ déterminé par

$$\rho_T = T + \tau \in K((t))\{\tau\}.$$

Soit $\Lambda = \rho_A(\frac{1}{t}) = \{\rho_a(\frac{1}{t}) \mid a \in A\} \subset A((t))$. C'est un ρ-réseau de rang 1. D'après l'uniformisation de Tate-Drinfeld (proposition 1.8), la donnée de (Λ, ρ) définit un module de Drinfeld TD sur $K((t))$ de rang 2 à réduction potentiellement stable de rang 1. De plus, les réductions de TD et ρ, modulo $tK[[t]]$, coïncident. On appelle TD le *module de Tate-Drinfeld*. Soit $e_\Lambda \in K((t))\{\{\tau\}\}$ l'exponentielle de Λ. On a alors

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

Proposition 4.1. *Le module de Tate-Drinfeld* TD *est un module de Drinfeld de rang* 2 *sur* $A((t))$*, à coefficients dans* $A[[t]]$*.*

Démonstration. Les paragraphes 6.4 et 6.5 de [vdH06] contiennent une démonstration de ce résultat pour le module de Tate-Drinfeld avec structure de niveau $\mathfrak{n} \neq A$. Toutefois, cette dernière hypothèse n'intervient pas dans la démonstration, qui est donc encore valable pour TD.

□

D'après ce qui précède, le polynôme TD_T s'écrit sous la forme

$$\mathrm{TD}_T = T + g^*(t)\tau + \Delta^*(t)\tau^2 \quad \text{avec } g^*(t) \in A[[t]]^\times \text{ et } \Delta^*(t) \in A((t))^\times \cap tA[[t]].$$

Il est possible d'adopter un point de vue analytique pour cette construction ([Gos80c] 1.78, [Gek88b] 11.3). Signalons comment relier ces deux définitions.

Par la théorie analytique (voir les rappels du paragraphe 1.1.2), le module de Carlitz ρ correspond à un réseau de $\mathbf{C}_\infty$ de rang 1 de la forme $\overline{\pi}A$, où $\overline{\pi} \in \mathbf{C}_\infty^\times$ est défini à multiplication par un élément de $\mathbf{F}_q^\times$ près. Par la suite, on fixe un tel choix de $\overline{\pi}$. Soit e_A l'exponentielle associée au réseau A. Suivant la convention de [Gek88b] 4.1, on pose

$$t(z) = \frac{1}{\overline{\pi} e_A(z)} \qquad (z \in \mathbf{C}_\infty - A).$$

En substituant $t(z)$ à t dans TD, on obtient un module de Drinfeld TD(z) de rang 2 sur $\mathbf{C}_\infty$, qui est le module de Drinfeld associé au réseau $\overline{\pi}(Az \oplus A)$. Ses coefficients sont reliés aux formes modulaires g et Δ pour $\mathbf{F}_q[T]$ (voir [Gos80c] ou [Gek88b] pour leur définition) par les formules qui suivent :

$$\begin{aligned} g^*(t(z)) &= \overline{\pi}^{1-q} g \\ \Delta^*(t(z)) &= \overline{\pi}^{1-q^2} \Delta. \end{aligned}$$

4.1.2 Torsion

***Notation* 4.2.** Pour $Q \in A$, on fixe :
— une racine primitive λ_Q de l'équation $\rho_Q(x) = 0$ dans K^{alg} ;
— une racine γ_Q de l'équation $\rho_Q(x) = \frac{1}{t}$ dans $K((t))^{\mathrm{alg}}$.

Soit N un générateur unitaire de $\mathfrak{n}$. D'après l'uniformisation de Tate (équation (1.1)), l'ensemble des points de $\mathfrak{n}$-torsion du module de Tate-Drinfeld est

$$\begin{aligned} \mathrm{TD}[\mathfrak{n}](K((t))^{\mathrm{alg}}) &= e_\Lambda(\rho_N^{-1}(\Lambda)/\Lambda) \\ &= \{e_\Lambda(\rho_a(\lambda_N) + \rho_b(\gamma_N)) \mid a, b \in A, \deg a < \deg N, \deg b < \deg N\}. \end{aligned}$$

Donc l'ensemble des sous-A-modules de $\mathrm{TD}[\mathfrak{n}](K((t))^{\mathrm{alg}})$ isomorphes à $A/\mathfrak{n}$ est

$$\{\mathrm{TD}_A e_\Lambda(\rho_a(\lambda_N) + \rho_b(\gamma_N)) \mid (a,b) \in A/\mathfrak{n} \times A/\mathfrak{n}, (a,b) \text{ d'ordre } \mathfrak{n}\} / (A/\mathfrak{n})^\times$$

et il est en bijection avec $\mathbf{P}^1(A/\mathfrak{n})$. Les structures de niveau $\Gamma_0(\mathfrak{n})$ sur TD sont

$$\begin{aligned} C_\mathfrak{n} &= \mathrm{TD}_A e_\Lambda(\lambda_N) = \mathrm{TD}[\mathfrak{n}](K^{\mathrm{alg}}[[t]]) \ ; \\ C_{d,b} &= \mathrm{TD}_A e_\Lambda(\rho_b(\lambda_d) + \rho_{\frac{N}{d}}(\gamma_d)) \quad (d \mid N, d \neq 1, \deg b < \deg d). \end{aligned}$$

Le module de Tate-Drinfeld TD(t) sur $A((t))$, muni de son sous-module $C_\mathfrak{n}$, définit par interprétation modulaire une section du morphisme structurel $Y_0(\mathfrak{n}) \to \mathrm{Spec}(A((t)))$. Soit $u \in \mathbf{F}_q^\times$. Le module de Drinfeld TD$(\frac{t}{u})$ est construit à partir du réseau $\rho_A(\frac{u}{t}) = u\rho_A(\frac{1}{t})$. Donc les modules de Drinfeld TD(t) et TD$(\frac{t}{u})$ sont isomorphes sur $\mathbf{F}_q$. De plus, le A-module $C_\mathfrak{n}(\frac{t}{u})$ de TD$(\frac{t}{u})$ n'est autre que $uC_\mathfrak{n}(t)$. Donc les couples $(\mathrm{TD}(t), C_\mathfrak{n}(t))$ et $(\mathrm{TD}(\frac{t}{u}), C_\mathfrak{n}(\frac{t}{u}))$ sont isomorphes sur $\mathbf{F}_q$. Par interprétation modulaire, les sections de $Y_0(\mathfrak{n})$ sur $A((t))$ qu'ils induisent coïncident. Notons-les $\mathfrak{u} : \mathrm{Spec}(A((t))) \to Y_0(\mathfrak{n})$. L'inclusion $A((t^{q-1})) \to A((t))$ donne un morphisme $\mathrm{Spec}(A((t))) \to \mathrm{Spec}(A((t^{q-1})))$. Le morphisme $\mathfrak{u}$ se factorise alors en $\mathfrak{t} : \mathrm{Spec}(A((t^{q-1}))) \to Y_0(\mathfrak{n})$.

Proposition 4.3. *Le morphisme* $\mathfrak{t}$ *se prolonge en un morphisme*

$$\mathfrak{t} : \mathrm{Spec}(A[1/\mathfrak{n}][[t^{q-1}]]) \to X_0(\mathfrak{n}).$$

De plus, on a $\mathfrak{t} \circ r = \infty$*, où* $r : \mathrm{Spec}(A[1/\mathfrak{n}]) \to \mathrm{Spec}(A[1/\mathfrak{n}][[t^{q-1}]])$ *est le morphisme induit par* $t^{q-1} \mapsto 0$*. Enfin,* $\mathfrak{t}$ *induit un isomorphisme entre le complété formel de* $X_0(\mathfrak{n})$ *le long de la section* ∞ *et le spectre formel de* $A[1/\mathfrak{n}][[t^{q-1}]]$*.*

Démonstration. Pour le prolongement naturel de $\mathfrak{t}$, on se réfère à la démonstration du lemme 9.3 de [vdH06]. Les autres assertions se déduisent de la proposition 9.1 et des théorèmes 9.2 et 10.3 de *loc. cit.*. □

Proposition 4.4. *Soient* L *un* A*-corps local complet et* $\mathcal{O}$ *son anneau de valuation. Notons* v *sa valuation discrète et* w *l'unique prolongement de* v *à* L^{alg}*. Soit* ϕ *un module de Drinfeld de rang* 2 *sur* L *à coefficients dans* $\mathcal{O}$ *et à réduction stable de rang* 1*. Alors il existe* $t_0 \in L^{\mathrm{alg}}$ *vérifiant* $w(t_0) > 0$ *et tel que le module de Drinfeld obtenu à partir de* TD *par le changement de base*

$$\begin{array}{rcl} A[[t]] & \longrightarrow & L^{\mathrm{alg}} \\ \sum_{i\geq 0} c_i t^i & \longmapsto & \sum_{i\geq 0} c_i t_0^i \end{array}$$

est un module de Drinfeld isomorphe à ϕ *sur* L^{alg}*.*

Démonstration. Le module de Drinfeld ϕ possède une uniformisation de Tate-Drinfeld (Γ, ψ) (proposition 1.8). Il existe $\gamma \in L^{\mathrm{alg}}$ vérifiant $w(\gamma) < 0$ et tel que $\Gamma = \psi_A(\gamma)$. Par ailleurs, le module de Drinfeld ψ de rang 1 est déterminé par $\psi_T = T + b\tau$, avec $b \in \mathcal{O}^\times$. Soit u une racine $(q-1)$-ème de b^{-1} dans L^{alg}. Alors $u\psi u^{-1}$ est le module de Carlitz ρ et $\Gamma = u^{-1}\rho_A(u\gamma)$. Posons $t_0 = \frac{1}{u\gamma} \in L^{\mathrm{alg}}$. Comme $w(u) < 0$ et $w(\gamma) < 0$, on a $w(t_0) > 0$. Le changement de base de TD par le morphisme d'anneaux $A[[t]] \to L^{\mathrm{alg}}$ défini par $t \mapsto t_0$ est un module de Drinfeld φ sur L^{alg} dont l'uniformisation de Tate-Drinfeld est donnée par le réseau $\rho_A(\frac{1}{t_0}) = \rho_A(u\gamma)$ et le module de Carlitz ρ de rang 1. D'après ce qui précède, φ est isomorphe sur L^{alg} à ϕ. □

Les propositions 4.3 et 4.4, conjointement au lemme 1.9, amènent au résultat suivant concernant l'interprétation modulaire de la pointe ∞.

Proposition 4.5. *Soit* L *une extension finie de* K*, d'anneau des entiers* $\mathcal{O}_L$*. Soit* ϕ *un module de Drinfeld de rang* 2 *sur* L *muni d'un point* $P \in {}^{\phi}L_{\mathrm{tors}}$*. La donnée de* (ϕ, P) *définit une section* $x : \mathrm{Spec}(\mathcal{O}_L) \to X_0(\mathfrak{n})$*. On suppose que* ϕ *a réduction stable de rang* 1 *en une place* $\mathfrak{L}$ *de* L*. Alors* P *définit un point entier d'un modèle stable de* ϕ *si et seulement si les spécialisations en* $\mathfrak{L}$ *des sections* x *et* ∞ *coïncident.*

4.2 Théorie algébrique des formes modulaires pour $\mathbf{F}_q[T]$

Les formes modulaires (analytiques) pour $\mathbf{F}_q[T]$, parfois appelées *formes modulaires de Drinfeld*, ont été introduites et étudiées par Goss [Gos80b, Gos80c] puis notamment Gekeler [Gek88b]. Dans cette section, nous mettons en place une approche algébrique des formes modulaires pour $\mathbf{F}_q[T]$ de poids 2 associées au sous-groupe de congruence $\Gamma_0(\mathfrak{n})$.

Pour les formes modulaires classiques, il existe plusieurs théories algébriques (Serre, Katz [Kat73], Deligne-Rapoport [DR73]). Ces constructions ont notamment été comparées dans [Maz77] II.4, dans le cas des formes de poids 2 pour $\Gamma_0(N)$. Pour les formes modulaires pour $\mathbf{F}_q[T]$, l'état d'avancement actuel de la théorie est le suivant. Gekeler a mis en place une théorie à la Serre des formes modulaires pour $\mathrm{GL}(2, A)$ modulo un idéal premier de A ([Gek88b] §12). Pour les formes modulaires de niveau $\mathfrak{n}$, Goss a mis en place une théorie algébrique à la Katz [Gos80c]. Nous introduisons ici une théorie *via* les sections du faisceau des différentielles relatives, qui sera suffisante pour nos besoins. Il resterait à faire le lien entre cette approche et celles de Gekeler et Goss.

La nature des liens entre la théorie des formes modulaires pour $\mathbf{F}_q[T]$ et celle des formes automorphes à valeurs dans $\mathbf{C}$ n'est pas claire. Citons toutefois le résultat important suivant : les formes modulaires analytiques pour $\mathbf{F}_q[T]$ peuvent s'interpréter comme la réduction modulo p d'une version un peu affaiblie de formes automorphes à valeurs dans un anneau de caractéristique nulle. Il est dû à Reversat [Rev00] en poids quelconque, après [Tei91] et un travail préliminaire en poids 2 dans [GR96] (voir aussi [Gek97a, Tei92b]). Reversat signale que cet énoncé pourrait apporter un éclairage nouveau aux obstructions rencontrées dans notre travail. Nous avions tenté cette approche sans succès, mais estimons que des investigations plus approfondies sont nécessaires et pourraient peut-être aboutir.

4.2.1 Définition et t-développement

Soit R une $A[1/\mathfrak{n}]$-algèbre. Le schéma $X_0(\mathfrak{n})_R$ sur R est muni de son faisceau $\Omega^1_{X_0(\mathfrak{n})_R/R}$ des différentielles relatives (de degré 1). On adopte la définition suivante.

Définition 4.6. On appelle *forme modulaire sur R (pour $\Gamma_0(\mathfrak{n})$)* une section globale de $\Omega^1_{X_0(\mathfrak{n})_R/R}$.

On note $\mathbf{S}(R)$ le R-module $H^0(X_0(\mathfrak{n})_R, \Omega^1_{X_0(\mathfrak{n})_R/R})$ des formes modulaires sur R. Le morphisme $\mathfrak{u}$ induit un morphisme

$$\mathfrak{u}_R : \mathrm{Spec}(R[[t]]) \longrightarrow X_0(\mathfrak{n})_R.$$

Définition 4.7. Soit $f \in \mathbf{S}(R)$. Il existe une unique série formelle $F(t) \in t^2R[[t]]$ telle que le tiré-en-arrière $\mathfrak{u}_R^*(f)$ soit $F(t)\frac{dt}{t^2}$. On appelle $F(t)$ le *t-développement de f* (en la pointe ∞).

Le choix du facteur de normalisation t^2 sera justifié en 4.2.4. D'après ce qui précède, on a $F(t)\frac{dt}{t^2} = F\left(\frac{t}{u}\right) u\frac{dt}{t^2}$ d'où $F(t) = uF(\frac{t}{u})$, pour tout $u \in \mathbf{F}_q^\times$. Le t-développement de f est donc de la forme

$$F(t) = \sum_{i\geq 1} a_{1+i(q-1)} t^{1+i(q-1)} \in t^2R[[t]].$$

Cela nous ramène à poser

$$b_i = a_{1+i(q-1)} \qquad (i \geq 1).$$

Lemme 4.8. *Posons $s = t^{q-1}$. On a $\mathfrak{t}_R^*(f) = -\sum_{i\geq 1} b_i s^{i-1} ds$.*

Démonstration. On a $\frac{ds}{s} = -\frac{dt}{t}$, donc

$$\mathfrak{u}_R^*(f) = F(t)\frac{dt}{t^2} = \sum_{i\geq 1} b_i t^{1+i(q-1)}\frac{dt}{t^2} = -\sum_{i\geq 1} b_i s^{i-1} ds.$$

Notons $i : R[[t^{q-1}]] \to R[[t]]$ l'inclusion canonique. Comme $\mathfrak{t}_R \circ \mathrm{Spec}(i) = \mathfrak{u}_R$, on a

$$\mathfrak{u}_R^*(f) = \mathrm{Spec}(i)^*(\mathfrak{t}_R^*(f)) = \mathfrak{t}_R^*(f)$$

d'où la conclusion. □

L'énoncé qui suit est un principe du t-développement.

Proposition 4.9. *L'homomorphisme de R-modules*

$$\begin{array}{ccc} \mathbf{S}(R) & \longrightarrow & t^2R[[t]] \\ f & \longmapsto & F(t) \end{array}$$

est injectif.

Démonstration. La démonstration du théorème 1.6.1 de [Kat73] est encore valable dans notre contexte, en utilisant le fait que le schéma $X_0(\mathfrak{n})_R$ est de Cohen-Macaulay, car lisse sur R. □

4.2.2 Changement de base

On pourra comparer l'énoncé suivant à la proposition II.3.3 de [Maz77].

Proposition 4.10. *Soit F un corps, qui est une extension de K ou le corps $\mathbf{F}_\mathfrak{l}$ (pour un idéal maximal $\mathfrak{l}$ de A avec $(\mathfrak{l}, \mathfrak{n}) = 1$). L'application F-linéaire canonique*

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

est un isomorphisme.

Démonstration. Pour alléger les notations, on pose $X = X_0(\mathfrak{n})$ et $\Omega = \Omega^1_{X_0(\mathfrak{n})/A[1/\mathfrak{n}]}$. Toute extension F de K, munie de sa structure canonique de $A[1/\mathfrak{n}]$-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 $\Omega^1_{X/A[1/\mathfrak{n}]}$ commute aux changements de base sur $\mathrm{Spec}(A[1/\mathfrak{n}])$ ([Har77] III.9.3 et II.8.10).

Soient $\mathfrak{l}$ un idéal maximal de A avec $(\mathfrak{l}, \mathfrak{n}) = 1$ et P un générateur de $\mathfrak{l}$. Le morphisme structurel $X \to \mathrm{Spec}(A[1/\mathfrak{n}])$ étant lisse, le faisceau Ω est inversible. En particulier, il est sans $A[1/\mathfrak{n}]$-torsion. Le morphisme de multiplication par P sur Ω est donc injectif. On a la suite exacte de faisceaux cohérents sur X

$$0 \longrightarrow \Omega \xrightarrow{P} \Omega \longrightarrow \Omega/P\Omega = \Omega \otimes_{A[1/\mathfrak{n}]} \mathbf{F}_\mathfrak{l} = \Omega^1_{X_{\mathbf{F}_\mathfrak{l}}/\mathbf{F}_\mathfrak{l}} \longrightarrow 0$$

car la formation de $\Omega^1_{X/A[1/\mathfrak{n}]}$ commute aux changements de base. On en déduit la suite exacte longue en cohomologie

$$0 \to H^0(X,\Omega) \xrightarrow{P} H^0(X,\Omega) \to H^0(X_{\mathbf{F}_\mathfrak{l}}, \Omega^1_{X_{\mathbf{F}_\mathfrak{l}}/\mathbf{F}_\mathfrak{l}}) \to H^1(X,\Omega) \xrightarrow{P} H^1(X,\Omega).$$

L'application canonique

$$H^0(X,\Omega)\otimes_{A[1/\mathfrak{n}]}\mathbf{F}_{\mathfrak{l}}\longrightarrow H^0(X_{\mathbf{F}_{\mathfrak{l}}},\Omega^1_{X_{\mathbf{F}_{\mathfrak{l}}}/\mathbf{F}_{\mathfrak{l}}}) \tag{4.1}$$

est donc injective. De plus, son conoyau est le noyau de la multiplication par P sur $H^1(X,\Omega)$. Le schéma X est régulier donc son faisceau dualisant est Ω. Par dualité de Grothendieck, $H^1(X,\Omega)$ est le $A[1/\mathfrak{n}]$-dual de $H^0(X,\mathcal{O}_X)\simeq A[1/\mathfrak{n}]$. La multiplication par P sur $A[1/\mathfrak{n}]$ étant injective, l'application (4.1) est un isomorphisme. □

Lemme 4.11. *Le* $A[1/\mathfrak{n}]$*-module* $\mathbf{S}(A[1/\mathfrak{n}])$ *est libre de rang* $g(X_0(\mathfrak{n}))$.

Démonstration. Reprenons les notations de la démonstration précédente. Le $A[1/\mathfrak{n}]$-module $H^0(X,\Omega)$ est sans torsion, donc libre. Par ailleurs, d'après la proposition 4.10, on a

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

Donc le rang du $A[1/\mathfrak{n}]$-module $\mathbf{S}(A[1/\mathfrak{n}])=H^0(X,\Omega)$ est égal à la dimension sur K de $H^0(X_K,\Omega^1_{X_K/K})$, c'est-à-dire au genre (géométrique) de $X_0(\mathfrak{n})_K$. □

Corollaire 4.12. *Soit* F *un corps, qui est une extension de* K *ou le corps* $\mathbf{F}_{\mathfrak{l}}$ *(pour un idéal maximal* $\mathfrak{l}$ *de* A *avec* $(\mathfrak{l},\mathfrak{n})=1$*). Le* F*-espace vectoriel* $\mathbf{S}(F)$ *est de dimension* $g(X_0(\mathfrak{n}))$.

Démonstration. C'est une conséquence directe du lemme 4.11 et de la proposition 4.10. □

4.2.3 Opérateurs de Hecke

Reprenons les notations de la section 3.2 : $\mathcal{J}_0(\mathfrak{n})$ désigne le modèle de Néron de $X_0(\mathfrak{n})_K$ sur $A[1/\mathfrak{n}]$.

Proposition 4.13 ([Maz78] 2e)**.** *On a un isomorphisme canonique*

$$\mathrm{Cot}(\mathcal{J}_0(\mathfrak{n}))\xrightarrow{\sim}\mathbf{S}(A[1/\mathfrak{n}]).$$

Démonstration. Pour alléger les notations, on pose $X=X_0(\mathfrak{n})$ et $S=\mathrm{Spec}(A[1/\mathfrak{n}])$. Comme X est propre sur S, le sous-foncteur $Pic^0_{X_0(\mathfrak{n})/S}$ du foncteur de Picard relatif est représentable par un S-schéma lisse et séparé, qu'on notera $\mathrm{Pic}^0_{X/S}$ ([BLR90] th. 9.4/2). D'après [BLR90] th. 9.5/4, le morphisme naturel $\mathrm{Pic}^0_{X/S}\to\mathcal{J}_0(\mathfrak{n})_{/S}$ identifie $\mathrm{Pic}^0_{X/S}$ avec la composante connexe de l'identité $\mathcal{J}_0(\mathfrak{n})^0$. En passant aux espaces tangents en la section 0 sur S, on obtient l'isomorphisme $H^1(X,\mathcal{O}_X)\simeq\mathrm{Tan}(\mathcal{J}_0(\mathfrak{n}))$ ([BLR90] th. 8.4/1). Le schéma X_S est régulier donc de Cohen-Macaulay. Son faisceau dualisant est le faisceau $\Omega^1_{X/S}$ des différentielles relatives de degré 1. La dualité de Grothendieck permet alors de voir $H^0(X_S,\Omega^1_{X/S})$ comme le $\mathcal{O}_S$-dual de $H^1(X_S,\mathcal{O}_X)$. Par ailleurs, $\mathrm{Cot}(\mathcal{J}_0(\mathfrak{n}))$ est naturellement le $\mathcal{O}_S$-dual de $\mathrm{Tan}(\mathcal{J}_0(\mathfrak{n}))$. L'isomorphisme précédent donne donc un isomorphisme $\mathrm{Cot}(\mathcal{J}_0(\mathfrak{n}))\simeq H^0(X,\Omega^1_{X/S})$. □

Soit $\mathfrak{m}$ un idéal de A. Les endomorphismes $T_\mathfrak{m}$ et $w_\mathfrak{n}$ de $J_0(\mathfrak{n})$ s'étendent en des endomorphismes du modèle de Néron $\mathcal{J}_0(\mathfrak{n})$ (par propriété universelle des modèles de Néron), de l'espace cotangent $\mathrm{Cot}(\mathcal{J}_0(\mathfrak{n}))$ et, par la proposition précédente, de $\mathbf{S}(A[1/\mathfrak{n}])$. Si F est un corps, qui est une extension de K ou le corps $\mathbf{F}_\mathfrak{l}$ (pour un idéal maximal $\mathfrak{l}$ de A ne divisant pas $\mathfrak{n}$), ces endomorphismes induisent par extension des scalaires (proposition 4.10) des endomorphismes de $\mathbf{S}(F)$, notés $T_\mathfrak{m}$ et $w_\mathfrak{n}$. L'espace de formes modulaires $\mathbf{S}(F)$ est donc muni d'une action de l'algèbre de Hecke $\mathbf{T}$, vue comme sous-algèbre de $\mathrm{End}_K(J_0(\mathfrak{n}))$. Comme F est de caractéristique p, $\mathbf{T}$ agit sur $\mathbf{S}(F)$ *via* son quotient $\mathbf{T}/p\mathbf{T}$. Nous ignorons si cette action est fidèle, et reviendrons sur cette question dans la section 4.5.

***Remarque* 4.14.** Si $(\mathfrak{m},\mathfrak{n}) = 1$ et $k \geq 0$, on a l'identité $T_{\mathfrak{m}^k}T_\mathfrak{m} = T_{\mathfrak{m}^{k+1}}$ dans $\mathrm{End}(\mathbf{S}(F))$ ([Gos80c] 3.3). Ainsi, $T_{\mathfrak{p}\mathfrak{q}} = T_\mathfrak{p}T_\mathfrak{q}$ pour *tous* $\mathfrak{p}$ et $\mathfrak{q}$ 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 $\mathbf{H}(\mathbf{C})$, qui est causée par la caractéristique p.

4.2.4 Digression sur la théorie transcendante

Les énoncés de cette section, qui ne seront pas utilisés de façon essentielle par la suite, resituent la théorie des formes modulaires (algébriques) sur $\mathbf{C}_\infty$ par rapport à la littérature existante sur les formes modulaires analytiques pour $\mathbf{F}_q[T]$.

Définition 4.15 ([GR96] 2.7)**.** Soient k un entier ≥ 1 et $m \in \mathbf{Z}/(q-1)\mathbf{Z}$. Une *forme modulaire (analytique) de poids k et type m pour* $\Gamma_0(\mathfrak{n})$ est une fonction $f : \mathcal{H} \to \mathbf{C}_\infty$ vérifiant :

(i) $f(\gamma z) = (\det\gamma)^{-m}(cz+d)^k f(z)$ pour tout $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(\mathfrak{n})$;

(ii) f est rigide holomorphe sur $\mathcal{H}$;

(iii) f est holomorphe aux pointes de $\Gamma_0(\mathfrak{n})$.

Précisons la signification de la dernière condition. Posons

$$t(z) = \frac{1}{\overline{\pi} e_A(z)} \quad (z \in \mathbf{C}_\infty - A).$$

La fonction $t : \mathcal{H} \to \mathbf{C}_\infty$ est invariante par translation par A. Soient $c \in \mathbf{R}^+$ et $\mathcal{H}_c = \{z \in \mathcal{H} \mid \inf_{x\in K_\infty}|z-x| \geq c\}$. Si c est suffisamment grand, la fonction t induit un isomorphisme d'espaces analytiques rigides entre $A\backslash\mathcal{H}$ et un disque de $\mathbf{C}_\infty$ centré en 0 et épointé. La forme modulaire f est invariante par translation par A, donc possède un développement au voisinage de ∞ en puissances de $t(z)$. Dire que f est *holomorphe en* ∞ signifie que les seules puissances qui interviennent sont positives ou nulles. Soient $s \in \mathbf{P}^1(K)$ représentant une pointe de $\Gamma_0(\mathfrak{n})\backslash\mathcal{H}$ et $v \in \mathrm{GL}(2,K)$ tel que $v\infty = s$. Posons $f_{[v]}(z) = (\det\gamma)^m(cz+d)^{-k}f(vz)$. La fonction f est dite *holomorphe en s* si $f_{[v]}$ est holomorphe en ∞.

On dit que f est *doublement parabolique* si son développement en toute pointe s'annule à l'ordre au moins 2.

Les formes modulaires de poids k et type m pour $\Gamma_0(\mathfrak{n})$ forment un $\mathbf{C}_\infty$-espace vectoriel noté $M_{k,m}(\Gamma_0(\mathfrak{n}))$. Le sous-espace des formes doublement paraboliques est noté $M^2_{k,m}(\Gamma_0(\mathfrak{n}))$.

On peut supposer $k \equiv 2m \bmod (q-1)$. Dans le cas contraire, $M_{k,m}(\Gamma_0(\mathfrak{n}))$ est nul, comme on le voit en faisant agir la matrice $\left(\begin{smallmatrix} u & 0 \\ 0 & u \end{smallmatrix}\right)$ sur une forme modulaire (pour $u \in \mathbf{F}_q^\times$).

Pour tout $u \in \mathbf{F}_q^\times$, on a la relation $t(uz) = \frac{1}{u}t(z)$. Ainsi, le développement de $f \in M^2_{k,m}(\Gamma_0(\mathfrak{n}))$ en la pointe ∞ est de la forme $\sum_{i\geq 2} a_i t(z)^i = \sum_{i\geq 1} a_{1+i(q-1)} t(z)^{1+i(q-1)}$.

Proposition 4.16. *On a un isomorphisme de* $\mathbf{C}_\infty$*-espaces vectoriels*

$$\begin{array}{ccccc} M^2_{2,1}(\Gamma_0(\mathfrak{n})) & \xrightarrow{\sim} & H^0(X_0(\mathfrak{n})^{\mathrm{an}}, \Omega^1_{\mathrm{an}}) & \simeq & \mathbf{S}(\mathbf{C}_\infty) \\ f & \longmapsto & -\frac{1}{\overline{\pi}} f(z)dz & & \end{array}$$

où $H^0(X_0(\mathfrak{n})^{\mathrm{an}}, \Omega^1_{\mathrm{an}})$ *désigne l'espace des formes différentielles holomorphes sur l'analytifiée* $X_0(\mathfrak{n})^{\mathrm{an}}$ *au sens de la géométrie rigide. De plus, si* $g \in \mathbf{S}(\mathbf{C}_\infty)$ *a pour* t*-développement* $\sum_{i\geq 2} a_i t^i$*, le développement de la forme analytique qui lui est associée est* $\sum_{i\geq 2} a_i t(z)^i$*.*

Démonstration. Pour le premier isomorphisme, on consultera [GR96] 2.10 (leur définition de $t(z)$ diffère de celle que nous avons adopté par une constante multiplicative). L'apparition des formes *doublement* paraboliques, contrairement aux formes paraboliques classiques est due à la relation $dz = -\overline{\pi}\frac{dt(z)}{t(z)^2}$, remarquée initialement par Goss [Gos80c]. Par un énoncé de type GAGA, on peut identifier les formes différentielles algébriques et analytiques sur la courbe projective $X_0(\mathfrak{n})_{\mathbf{C}_\infty}$. □

Soit $\mathfrak{p}$ un idéal de A, de générateur unitaire P. On définit un endomorphisme de $M_{k,m}(\Gamma_0(\mathfrak{n}))$ par la formule

$$T_{\mathfrak{p}}(f)(z) = \frac{1}{P} \sum_{\substack{a,b,d\in A \\ \deg b<\deg d \\ a,d \text{ unitaires} \\ (ad)=\mathfrak{p},(a)+\mathfrak{n}=A}} a^k f\left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} z\right) \qquad (f \in M_{k,m}(\Gamma_0(\mathfrak{n}))).$$

Elle diffère de celle de [Gos80c, Gos80b, Gek88b] par le facteur $\frac{1}{P}$. Cette normalisation est justifiée par le résultat suivant : par l'isomorphisme de la proposition 4.16, les endomorphismes $T_{\mathfrak{p}}$ de $M^2_{2,1}(\Gamma_0(\mathfrak{n}))$ et $\mathbf{S}(\mathbf{C}_\infty)$ coïncident.

4.3 L'action de Hecke sur le t-développement des formes modulaires

4.3.1 Polynômes de Goss

Rappelons les résultats concernant les polynômes de Goss [Gos80c, Gek88b] dans le cas d'un réseau fini, ce qui couvrera nos besoins. Soit Λ un $\mathbf{F}_q$-réseau de $\mathbf{C}_\infty$ c'est-à-dire un sous-$\mathbf{F}_q$-module de $\mathbf{C}_\infty$ discret. On suppose Λ fini. Soit m la dimension de Λ, c'est-à-dire $\log_q \#\Lambda$. L'exponentielle associée à Λ

$$e_\Lambda(X) = X \prod_{0\neq\lambda\in\Lambda} \left(1 - \frac{X}{\lambda}\right) \in \mathbf{C}_\infty[X]$$

est un polynôme en l'indéterminée X, qui est $\mathbf{F}_q$-linéaire et Λ-périodique. Il s'écrit

$$e_\Lambda(X) = \sum_{i=0}^{m} \alpha_i X^{q^i},$$

avec $\alpha_i \in \mathbf{C}_\infty$ $(i \geq 0)$ et $\alpha_0 = 1$.

***Notation* 4.17.** Pour $k \geq 0$, on pose

$$\begin{array}{l} S_0 = 0 \\ S_k(X) = S_{k,\Lambda}(X) = \sum_{\lambda\in\Lambda} \frac{1}{(X+\lambda)^k} \quad \in \mathbf{C}_\infty(X) \end{array}$$

et

$$t_\Lambda(X) = \frac{1}{e_\Lambda(X)} = \sum_{\lambda\in\Lambda} \frac{1}{X-\lambda} \quad \in \mathbf{C}_\infty(X).$$

La dernière égalité provient de la relation $\frac{de_\Lambda(X)}{dX} = 1$. Les fractions rationnelles $S_k(X)$ sont les sommes de Newton associées au polynôme réciproque de

$$e_\Lambda(Y-X) = e_\Lambda(Y) - e_\Lambda(X) \in \mathbf{C}_\infty[X][Y].$$

Proposition 4.18 ([Gek88b] 3.4–3.9)**.**

(i) Il existe un unique polynôme $G_k = G_{k,\Lambda}(Y) \in \mathbf{C}_\infty[Y]$, appelé k-ème polynôme de Goss, défini par les conditions suivantes :

(a) Si $k \leq q$, $G_k(Y) = Y^k$;

(b) $G_k(Y) = Y(G_{k-1}(Y) + \alpha_1 G_{k-q}(Y) + \alpha_2 G_{k-q^2}(Y) + \ldots)$ $\qquad (k - q^i \geq 0)$.

(ii) On a

$$G_{k,\Lambda}(Y) = \sum_{0\leq j\leq k-1} \sum_{\underline{i}} \binom{j}{\underline{i}} \alpha^{\underline{i}} Y^{j+1}, \tag{4.2}$$

où $\underline{i} = (i_0, \ldots, i_m)$ parcourt les $(m+1)$-uplets d'entiers naturels vérifiant les conditions

$$\begin{cases} i_0 + \ldots + i_m = j \\ i_0 + i_1 q + \ldots + i_m q^m = k-1. \end{cases}$$

On a posé $\alpha^{\underline{i}} = \alpha_0^{i_0} \cdots \alpha_m^{i_m}$ et $\binom{j}{\underline{i}}$ est le coefficient multinomial $\frac{j!}{i_0! \cdots i_m!}$.

(iii) Ce polynôme vérifie les propriétés :

(a) $S_k(X) = G_k(t_\Lambda(X))$;

(b) G_k est unitaire de degré k ;

(c) $G_k(0) = 0$;

(d) $G_{pk} = (G_k)^p$ où p est la caractéristique de $\mathbf{F}_q$;

(e) $Y^2 G_k'(Y) = kG_{k+1}(Y)$.

(iv) Le polynôme $G_k(Y)$ est divisible par Y^n où $n = \left[\frac{k}{q^m}\right] + 1$.

Pour $k = 0$, on pose $G_{0,\Lambda}(Y) = 0$ si $\Lambda \neq 0$ et $G_{0,\Lambda}(Y) = 1$ si $\Lambda = 0$.

4.3.2 Opérateurs de Hecke et t-développement

Soit ρ le module de Carlitz de rang 1 sur K. Pour tout $d \in A$, notons

$$\Lambda_d = \mathrm{Ker}(\rho_d) \subset K^{\mathrm{sep}}.$$

C'est un $\mathbf{F}_q$-réseau fini de $\mathbf{C}_\infty$ de dimension $\deg d$. Soit e_{Λ_d} l'exponentielle associée à Λ_d.

Lemme 4.19. *On a l'égalité de polynômes dans* $K^{\mathrm{sep}}[X]$ *:*

$$e_{\Lambda_d}(X) = \frac{\rho_d(X)}{d}.$$

Démonstration. L'ensemble des racines de ces polynômes est Λ_d. Le coefficient en X de $e_{\Lambda_d}(X)$ est 1 et celui de $\rho_d(X)$ est d, ce qui achève la démonstration. □

***Notation* 4.20.** On note $\alpha_0(d), \ldots, \alpha_{\deg d}(d)$ les coefficients de l'exponentielle associée au réseau Λ_d. On a donc $e_{\Lambda_d}(z) = \sum_{i=0}^{\deg d} \alpha_i(d) z^{q^i}$. Posons

$$l_i(P) = P\alpha_i(P) \qquad (0 \leq i \leq \deg d).$$

D'après le lemme 4.19, le module de Carlitz en P est alors donné par

$$\rho_P = \sum_{i=0}^{\deg d} l_i(P)\tau^i \quad \in K\{\tau\}.$$

On a donc $l_i(P) \in A$ $(i \geq 0)$ et la relation de récurrence

$$l_i(P) = \frac{l_{i-1}^q(P) - l_{i-1}(P)}{T^{q^i} - T} \qquad (i \geq 1),$$

avec $l_0(P) = P$ et $l_{\deg d}(P) = 1$. On note $G_{i,d}$ le i-ème polynôme de Goss associé au réseau Λ_d.

Lemme 4.21. *Soit* $d \in A$*. Le polynôme* $\frac{1}{d}G_{i,d}(dY)$ *appartient à* $A[Y]$*, pour tout* $i \geq 0$*.*

Démonstration. Démontrons-le par récurrence sur i. L'énoncé est évident pour $i = 0$. Si $1 \leq i \leq q$, d'après la proposition 4.18 (i), on a $G_{i,d}(dY) = d^i Y^i$ donc $\frac{1}{d}G_{i,d}(dY) \in A[Y]$. Supposons $i > q$. On a alors d'après la proposition 4.18 (i),

$$\frac{1}{d}G_{i,d}(dY) = Y(G_{i-1,d}(dY) + \alpha_1(d)G_{i-q,d}(dY) + \ldots). \tag{4.3}$$

De plus, $d\alpha_i$ appartient à A $(i \geq 1)$. Par hypothèse de récurrence, $G_{i-q^k,d}(dY) \in dA[Y]$. On a donc $\alpha_k(d)G_{i-q^k,d}(dY) \in A[Y]$ pour tout $k \geq 0$. D'après (4.3), on obtient donc $\frac{1}{d}G_{i,d}(dY) \in A[Y]$. □

***Notation* 4.22.** Pour $d \in A$, on pose $\varphi_d(t) = \frac{1}{\rho_d(\frac{1}{t})} \in A[[t]]$.

Proposition 4.23. *On a*

$$\sum_{b\in A,\ \deg b<\deg d} \frac{1}{\left(\rho_{\frac{P}{d}}(\gamma_d)+\rho_b(\lambda_d)\right)^i} = G_{i,d}(d\varphi_{\frac{P}{d}}(t)) \quad (i\geq 0).$$

Cette égalité a lieu dans $dA[[t]]$.

Démonstration. Remarquons que $\rho_b(\lambda_d)$, pour $\deg b < \deg d$, décrit le réseau $\mathrm{Ker}(\rho_d) = \Lambda_d$. La somme précédente s'écrit donc, en utilisant la proposition 4.18 (iii) et le lemme 4.19,

$$\begin{aligned}\sum_{\lambda\in\Lambda_d} \frac{1}{(\rho_{\frac{P}{d}}(\gamma_d)+\lambda)^i} &= S_{i,\Lambda_d}(\rho_{\frac{P}{d}}(\gamma_d))\\ &= G_{i,d}\left(\frac{1}{e_{\Lambda_d}(\rho_{\frac{P}{d}}(\gamma_d))}\right)\\ &= G_{i,d}\left(\frac{d}{\rho_d\rho_{\frac{P}{d}}(\gamma_d)}\right)\\ &= G_{i,d}\left(\frac{d}{\rho_P(\gamma_d)}\right).\end{aligned}$$

Comme $\rho_d(\gamma_d)=\frac{1}{t}$, on a $\rho_P(\gamma_d)=\rho_{\frac{P}{d}}\rho_d(\gamma_d)=\rho_{\frac{P}{d}}(\frac{1}{t})$. La somme est donc égale à

$$G_{i,d}\left(\frac{d}{\rho_{\frac{P}{d}}(1/t)}\right) = G_{i,d}(d\varphi_{\frac{P}{d}}(t)).$$

Enfin, le membre de droite est dans $dA[[t]]$ d'après le lemme 4.21. □

Jusqu'à la fin de la section 4.3, F désignera l'anneau $A[1/\mathfrak{n}]$ ou un corps, qui est une extension de K ou le corps $\mathbf{F}_\mathfrak{l}$ (pour un idéal maximal $\mathfrak{l}$ de A avec $(\mathfrak{l},\mathfrak{n})=1$).

Proposition 4.24. *Soit $f\in\mathbf{S}(F)$, de t-développement $\sum_{i\geq 2} a_it^i \in F[[t]]$. Alors le t-développement de la forme modulaire $T_\mathfrak{p}f$ est donné par*

$$\sum_{i\geq 2}\sum_{\substack{d|P,(\frac{P}{d},N)=1\\ d\ \text{unitaire}}} \frac{P}{d^2}a_iG_{i,d}(d\varphi_{\frac{P}{d}}(t)) \quad \in F[[t]]. \tag{4.4}$$

Démonstration. Tout d'abord, on constate que cette expression est bien dans $F[[t]]$ d'après la proposition 4.23. Nous démontrons (4.4) pour $f\in\mathbf{S}(A[1/\mathfrak{n}])$; les énoncés sur les corps considérés s'en déduisent par changement de base (proposition 4.10).

Considérons le module de Tate-Drinfeld $\mathrm{TD}=\mathrm{TD}(t)$ sur $L=K((t))^{\mathrm{sep}}$. Ses structures de niveau $\Gamma_0(\mathfrak{p})$ d'intersection nulle avec le A-module $C_\mathfrak{n}$ sont :

$$\begin{aligned}C_\mathfrak{p} &= \mathrm{TD}_A e_\Lambda(\lambda_P)\\ C_{d,b} &= \mathrm{TD}_A e_\Lambda(\rho_b(\lambda_P)+\rho_{\frac{P}{d}}(\gamma_d))\end{aligned}$$

où (b,d) parcourt les éléments de $A \times A$ vérifiant $d \mid P, d \neq 1, d$ unitaire, $\left(\frac{P}{d}, N\right) = 1$ et $\deg b < \deg d$. Soit $\mathcal{E}$ l'ensemble de ces structures. On a donc, par définition de $T_{\mathfrak{p}}$ comme correspondance sur $X_0(\mathfrak{n})$,

$$\begin{aligned} T_{\mathfrak{p}}(\mathrm{TD}(t), C_{\mathfrak{n}}) &= \sum_{D \in \mathcal{E}} (\mathrm{TD}(t)/D, (C_{\mathfrak{n}} + D)/D) \\ &= (\mathrm{TD}(t)/C_{\mathfrak{p}}, (C_{\mathfrak{n}} + C_{\mathfrak{p}})/C_{\mathfrak{p}}) + \sum_{\substack{d \in A \\ d \mid P, d \neq 1 \\ d \text{ unitaire} \\ (P/d, N)=1}} \sum_{\substack{b \in A \\ \deg b < \deg d}} (\mathrm{TD}(t)/C_{d,b}, (C_{\mathfrak{n}} + C_{d,b})/C_{d,b}). \end{aligned}$$

Posons $\chi_{d,b}(t) = \frac{1}{\rho_b(\lambda_P) + \rho_{\frac{P}{d}}(\gamma_P)}$. Le module de Drinfeld $\mathrm{TD}(t)/C_{\mathfrak{p}}$ (resp. $\mathrm{TD}(t)/C_{d,b}$) est $\mathrm{TD}(\varphi_P(t))$ (resp. $\mathrm{TD}(\chi_{d,b}(t))$). On a alors l'égalité de diviseurs sur $X_0(\mathfrak{n})$

$$T_{\mathfrak{p}}(\mathrm{TD}(t), C_{\mathfrak{n}}) = \mathrm{TD}(\varphi_P(t), C_{\mathfrak{n}}) + \sum_{\substack{d \mid P, d \neq 1 \\ d \text{ unitaire} \\ (P/d, N)=1}} \sum_{\deg b < \deg d} (\mathrm{TD}(\chi_{d,b}(t)), C_{\mathfrak{n}}).$$

Considérons les morphismes d'anneaux

$$\begin{array}{rcl} \varphi_P : A[1/\mathfrak{n}][[t]] & \longrightarrow & A[1/\mathfrak{n}][[t]] \\ \sum_{i \geq 0} c_i t^i & \longmapsto & \sum_{i \geq 0} c_i \varphi_P(t)^i \end{array}$$

et

$$\begin{array}{rcl} \chi_{d,b} : A[1/\mathfrak{n}][[t]] & \longrightarrow & K^{\mathrm{sep}}((\gamma_d)) \\ \sum_{i \geq 0} c_i t^i & \longmapsto & \sum_{i \geq 0} c_i \chi_{d,b}(t)^i. \end{array}$$

Ils induisent les morphismes de schémas

$$\begin{aligned} \mathfrak{u}_P &: \mathrm{Spec}(A[1/\mathfrak{n}][[t]]) \xrightarrow{\mathrm{Spec}(\varphi_P)} \mathrm{Spec}(A[1/\mathfrak{n}][[t]]) \xrightarrow{\mathfrak{u}} X_0(\mathfrak{n}) \\ \mathfrak{u}_{d,b} &: \mathrm{Spec}(K^{\mathrm{sep}}((\gamma_d))) \xrightarrow{\mathrm{Spec}(\chi_{d,b})} \mathrm{Spec}(A[1/\mathfrak{n}][[t]]) \xrightarrow{\mathfrak{u}} X_0(\mathfrak{n}). \end{aligned}$$

Soit $f \in \mathbf{S}(A[1/\mathfrak{n}])$. L'action de $T_{\mathfrak{p}}$ sur le t-développement de f est alors donnée par

$$\mathfrak{u}^*(T_{\mathfrak{p}} f) = \mathfrak{u}_P^*(f) + \sum_{\substack{d \mid P, d \neq 1 \\ d \text{ unitaire} \\ (P/d, N)=1}} \sum_{\deg b < \deg d} \mathfrak{u}_{d,b}^*(f).$$

Un calcul élémentaire montre que

$$\frac{d(\varphi_P(t))}{(\varphi_P(t))^2} = P \frac{dt}{t^2} \quad \text{et} \quad \frac{d(\chi_{d,b}(t))}{(\chi_{d,b}(t))^2} = \frac{P}{d^2} \frac{dt}{t^2}.$$

On en déduit

$$\begin{aligned}
\mathfrak{u}^*(T_{\mathfrak{p}}f) &= (\mathrm{Spec}(\varphi_P))^*\mathfrak{u}^*(f) + \sum_{\substack{d|P, d\neq 1\\ d \text{ unitaire}\\ (P/d,N)=1}} \sum_{\deg b<\deg d} (\mathrm{Spec}(\chi_{d,b}))^*\mathfrak{u}^*(f)\\
&= (\mathrm{Spec}(\varphi_P))^*\left(F(t)\frac{dt}{t^2}\right) + \sum_{\substack{d|P, d\neq 1\\ d \text{ unitaire}\\ (P/d,N)=1}} \sum_{\deg b<\deg d} (\mathrm{Spec}(\chi_{d,b}))^*\left(F(t)\frac{dt}{t^2}\right)\\
&= P\cdot F(\varphi_P(t))\frac{dt}{t^2} + \sum_{\substack{d|P, d\neq 1\\ d \text{ unitaire}\\ (P/d,N)=1}} \sum_{\deg b<\deg d} \frac{P}{d^2}F(\chi_{d,b}(t))\frac{dt}{t^2}.
\end{aligned}$$

Comme $F(t) = \sum_{i\geq 2} a_i t^i$, le t-développement de $T_{\mathfrak{p}}f$ est donc donné par la formule

$$\begin{aligned}
&\sum_{i\geq 2} a_i \left(P\varphi_P(t)^i + \sum_{\substack{d|P, d\neq 1\\ d \text{ unitaire}\\ (P/d,N)=1}} \frac{P}{d^2} \sum_{\deg b<\deg d} \frac{1}{(\rho_b(\lambda_P) + \rho_{\frac{P}{d}}(\gamma_P))^i} \right)\\
=&\sum_{i\geq 2} a_i \sum_{\substack{d|P, d \text{ unitaire}\\ (P/d,N)=1}} \frac{P}{d^2} \sum_{\deg b<\deg d} \frac{1}{\left(\rho_{\frac{P}{d}}(\gamma_d) + \rho_b(\lambda_d)\right)^i}.
\end{aligned}$$

On conclut alors à l'aide de la proposition 4.23. □

Proposition 4.25. *Soit $f \in \mathbf{S}(F)$ une forme modulaire, de t-développement $\sum_{i\geq 2} a_i(f)t^i$. Soit $\mathfrak{p}$ un idéal de A de degré d. Alors on a*

$$a_q(T_{\mathfrak{p}}f) = \sum_{\underline{m}} \binom{q-1}{\underline{m}} l(P)^{\underline{m}} a_{1+m_0+m_1q+\ldots+m_dq^d}(f), \tag{4.5}$$

la somme portant sur les $(d+1)$-uplets d'entiers naturels $(m_0,\ldots,m_d)$ vérifiant $m_0+m_1+\ldots+m_d = q-1$. La notation $l(P)^{\underline{m}}$ désigne $l_0(P)^{m_0}\cdots l_d(P)^{m_d}$.

***Remarque* 4.26.** (i) Quand $q = p$ premier, les coefficients binomiaux $\binom{q-1}{\underline{m}}$ sont non nuls modulo p. Ce n'est pas le cas en général comme le montre l'exemple $p = 3$, $q = 9$ et $\underline{m} = (2,2,4)$.

(ii) La formule (4.5) exprime $a_q(T_{\mathfrak{p}}f)$ comme combinaison linéaire de $a_q(f)$ et des $a_n(f)$, où n décrit les entiers naturels dont l'écriture en base q a au plus $d+1$ chiffres et la somme de ces chiffres est égale à q. En particulier, ces entiers n ne dépendent que du degré de $\mathfrak{p}$. Cette remarque sera exploitée par la suite.

Démonstration. Pour alléger les notations, posons $a_i = a_i(f)$. Rappelons que, d'après la proposition 4.24, le t-développement de $T_{\mathfrak{p}}(f)$ est donné par

$$P\sum_{i\geq 2} \sum_{\substack{\delta|P, (\frac{P}{\delta},N)=1\\ \delta \text{ unitaire}}} \frac{1}{\delta^2} a_i G_{i,\delta}(\delta\varphi_{\frac{P}{\delta}}(t)). \tag{4.6}$$

Déterminons le terme en t^q dans $G_{i,\delta}(\delta\varphi_{\frac{P}{\delta}}(t))$. Le t-développement de $\varphi_{\frac{P}{\delta}}(t)$ est divisible par $t^{q^{d-\deg\delta}}$. Comme $G_{i,\delta}(X)$ se factorise par X, le t-développement de $G_{i,\delta}(\delta\varphi_{\frac{P}{\delta}}(t))$ est divisible par $t^{q^{d-\deg\delta}}$. On peut donc supposer $d-\deg\delta \leq 1$.

D'après (4.2), le polynôme de Goss est

$$G_{i,\delta}(X) = \sum_{0\leq j\leq i-1} \delta^{-j} \sum_{\underline{m}} \binom{j}{\underline{m}} l(\delta)^{\underline{m}} X^{j+1}, \tag{4.7}$$

où $n = \deg\delta$, $\underline{m} = (m_0, \ldots, m_n)$ parcourt les $(n+1)$-uplets d'entiers naturels vérifiant $m_0 + \ldots + m_n = j$ et $m_0 + m_1 q + \ldots + m_n q^n = i-1$.

Supposons $d = \deg\delta$, c'est-à-dire $P = \delta$. On a alors $G_{i,\delta}(\delta\varphi_{\frac{P}{\delta}}(t)) = G_{i,P}(Pt)$. Sa contribution en t^q dans l'équation (4.6) est

$$\sum_{\underline{m}} \binom{q-1}{\underline{m}} l(\delta)^{\underline{m}} a_{1+m_0+m_1q+\ldots+m_dq^d},$$

la somme portant sur les $(n+1)$-uplets $(m_0, \ldots, m_n)$ vérifiant $m_0+m_1+\ldots+m_n = q-1$.

Supposons $d = \deg\delta + 1$. Comme $\varphi_{\frac{P}{\delta}}(t)$ est divisible par t^q, en comparant avec l'équation (4.7), on voit que le seul entier i pour lequel $G_{i,\delta}(d\varphi_{\frac{P}{\delta}}(t))$ possède un terme en t^q est $i = 1$. C'est impossible car $i \geq 2$. □

Digression sur les formes modulaires analytiques en poids supérieur. Les propositions 4.24 et 4.25 admettent des analogues pour les formes modulaires analytiques en poids supérieur. Plus précisément, en adaptant les démonstrations au cadre analytique, on obtient l'énoncé qui suit.

Proposition 4.27. *Soit* $\mathfrak{p}$ *un idéal de* A *de degré* d *et de générateur unitaire* P.

(i) Soit $f \in M_{k,m}(\Gamma_0(\mathfrak{n}))$ *de développement* $\sum_{i\geq 0} a_i(f)t^i$. *On a*

$$T_{\mathfrak{p}}(f) = P^{k-1} \sum_{i\geq 0} \sum_{\substack{d|P,\ (\frac{P}{d},N)=1 \\ d \text{ unitaire}}} \frac{1}{d^k} a_i(f) G_{i,d}(dt_{\frac{P}{d}}),$$

où $t_{\frac{P}{d}}$ *désigne la fonction* $\mathcal{H} \to \mathbf{C}_\infty$ *définie par* $z \mapsto \varphi_{\frac{P}{d}}(t(z))$.

(ii) Si $f \in M^2_{k,1}(\Gamma_0(\mathfrak{n}))$, *on a*

$$a_q(T_{\mathfrak{p}}f) = \sum_{\underline{m}} \binom{q-1}{\underline{m}} l(P)^{\underline{m}} a_{1+m_0+m_1q+\ldots+m_dq^d}(f)$$

la somme portant sur les $(d+1)$*-uplets d'entiers naturels* $(m_0, \ldots, m_d)$ *vérifiant* $m_0 + m_1 + \ldots + m_d = q-1$.

Le deuxième énoncé généralise [Gek88b] 7.4 (qui traitait le cas $d = 1$ et $\mathfrak{n} = A$).

Problématique. L'analogue de la formule (4.5) pour les formes modulaires classiques est la relation fondamentale suivante :

$$a_1(T_n f) = a_n(f) \qquad (n \in \mathbf{N}),$$

où T_n désigne le n-ème opérateur de Hecke. Pour les formes modulaires pour $\mathbf{F}_q[T]$, la situation présente *a priori* une différence fondamentale. En effet, la formule (4.5) ne fait apparaître, dans son second membre, que la famille de coefficients $(a_n(f))_n$ où n décrit les entiers dont la somme des chiffres de l'écriture en base q est égale à q. Ces entiers sont de densité naturelle nulle dans les entiers naturels. Cependant, rien n'exclut que les coefficients manquants puissent être obtenus par un autre procédé. Nous formulons donc la question qui, à l'heure actuelle, est ouverte.

Question 4.28. Considérons les coefficients du t-développement comme formes linéaires sur l'espace vectoriel $\mathbf{S}(F)$. Pour tout entier $j \geq 0$, existe-t-il un élément θ_j de l'algèbre $\mathbf{T} \otimes_{\mathbf{Z}} A$ vérifiant $b_j = b_1 \circ \theta_j$?

Dans la fin de cette section, nous exhibons des opérateurs $\theta_1, \ldots, \theta_q$, répondant partiellement cette question. Puis nous suggérons un opérateur candidat pour θ_j lorsque j vérifie la condition suivante : la somme des chiffres de l'écriture de j en base q est égale à q. Enfin, nous étudierons une variante de la question 4.28 et y apporterons une réponse positive lorsque $\mathfrak{n}$ est premier de degré 3.

4.3.3 L'action de T_P lorsque P est de degré 1

Si P désigne un générateur unitaire de $\mathfrak{p}$, l'opérateur $T_{\mathfrak{p}}$, vu comme endomorphisme de $\mathbf{S}(F)$, sera noté T_P.

Appliquons la proposition 4.25 dans le cas où P est de degré 1. On obtient la formule, pour tout $f \in \mathbf{S}(F)$:

$$a_q(T_P f) = \sum_{0 \leq v < q} \tbinom{q-1}{v} P^{q-v-1} a_{q+v(q-1)}(f) \quad (P \in A, \deg P = 1). \tag{4.8}$$

Si $P_1, \ldots, P_q$ désignent les q polynômes unitaires de A degré 1, l'équation (4.8) fournit le système linéaire

$$\begin{pmatrix} a_q(T_{P_1}) \\ \vdots \\ a_q(T_{P_q}) \end{pmatrix} = \begin{pmatrix} \binom{q-1}{0} P_1^{q-1} & \binom{q-1}{1} P_1^{q-2} & \cdots & \binom{q-1}{q-1} 1 \\ \vdots & \vdots & & \vdots \\ \binom{q-1}{0} P_q^{q-1} & \binom{q-1}{1} P_q^{q-2} & \cdots & \binom{q-1}{q-1} 1 \end{pmatrix} \begin{pmatrix} a_q \\ \vdots \\ a_{q+(q-1)^2} \end{pmatrix} \tag{4.9}$$

où a_i désigne la forme linéaire sur $\mathbf{S}(F)$ définie par $f \mapsto a_i(f)$.

Lemme 4.29. *Le déterminant du système* (4.9) *appartient à* $\mathbf{F}_q^\times$.

Démonstration. Ce déterminant est

$$\prod_{i=0}^{q-1} \binom{q-1}{i} \begin{vmatrix} P_1^{q-1} & P_1^{q-2} & \cdots & 1 \\ \vdots & \vdots & & \vdots \\ P_q^{q-1} & P_q^{q-2} & \cdots & 1 \end{vmatrix} = \prod_{i=0}^{q-1} \binom{q-1}{i} \prod_{j<i} (P_i - P_j)$$

Par un théorème de Lucas, le coefficient binomial $\binom{a+b}{b}$ est non nul modulo p si et seulement si la somme $a+b$ en base p s'effectue sans retenue à partir des écritures de a et b. Comme $q = p^n$, ce critère montre que $\binom{q-1}{i} \neq 0$ dans $\mathbf{F}_p$ pour tout $0 \leq i \leq q-1$. Par ailleurs, pour $i \neq j$, $P_i - P_j \in \mathbf{F}_q^\times$ car ces polynômes sont unitaires, de degré 1 et distincts. □

Nous résolvons ce système linéaire, en utilisant des sommes de puissances de polynômes de degré fixé, qui disposent, en caractéristique p, de propriétés d'annulations connues.

***Notation* 4.30.** Pour un entier naturel r, on note A_{r+} l'ensemble des polynômes unitaires de A de degré r et

$$S_r(m) = \sum_{P \in A_{r+}} P^m \qquad (m \in \mathbf{N}).$$

Lemme 4.31 (Carlitz, Lee [Lee43], Gekeler [Gek88a])**.** *Soient $m, r \in \mathbf{N}$ et $l(m)$ la somme des chiffres de l'écriture de m en base q.*

(i) Si $r > \frac{l(m)}{q-1}$ alors $S_r(m) = 0$.

(ii) Si $q = p$ alors $S_r(m) = 0$ si et seulement si $r > \frac{l(m)}{q-1}$.

Signalons que de telles sommes apparaissent dans les sommes partielles de la fonction zêta de K aux entiers négatifs au sens de Goss [Gos79]. Signalons que les propriétés de congruence de ces sommes donnent lieu à un critère de Kummer pour les extensions abéliennes de $\mathbf{F}_q(T)$ [Gos82].

Proposition 4.32. *Soit f une forme modulaire dans $\mathbf{S}(F)$, de t-développement $\sum_{i \geq 2} a_i(f) t^i$. On a*

$$a_{q+n(q-1)}(f) = \begin{cases} -\binom{q-1}{n}^{-1} a_q \left(\sum_{P \in A_{1+}} P^n T_P f \right) & \text{si } 0 \leq n \leq q-2\,; \\ -a_q \left(\sum_{P \in A_{1+}} P^{q-1} T_P f + f \right) & \text{si } n = q-1. \end{cases}$$

Démonstration. On pose $a_i = a_i(f)$. En sommant la formule (4.8) pour tout $P \in A_{1+}$, on obtient, pour tout $n \geq 0$,

$$\begin{aligned} a_q \left(\sum_{P \in A_{1+}} P^n T_P f \right) &= \sum_{0 \leq v \leq q-1} \left(\sum_{P \in A_{1+}} P^{n+q-v-1} \right) \binom{q-1}{v} a_{q+v(q-1)} \\ &= \sum_{0 \leq v \leq q-1} S_1(n+q-v-1) \binom{q-1}{v} a_{q+v(q-1)}. \end{aligned} \tag{4.10}$$

Pour tout $v \in [0, q-1]$, posons $m_v = n+q-v-1$.

Supposons $0 \leq n \leq q-2$. On a $0 \leq m_v \leq 2q-3$. La seule valeur de m_v pour laquelle $l(m_v) \geq q-1$ est $m_v = q-1$, qui correspond à $v = n$. D'après le lemme 4.31, le seul terme restant dans (4.10) est donc

$$a_q \left(\sum_{P \in A_{1+}} P^n T_P f \right) = S_1(q-1) \binom{q-1}{n} a_{q+n(q-1)}.$$

Par le corollaire 3.14 de [Gek88a], $S_1(q-1)$ vaut -1 d'où

$$a_q\left(\sum_{P\in A_{1+}} P^n T_P f\right) = -\tbinom{q-1}{n} a_{q+n(q-1)}.$$

Supposons maintenant $n = q-1$. On a $q-1 \leq m_v \leq 2q-2$. Les seules valeurs de m_v pour lesquelles $l(m_v) \geq q-1$ sont $m_v = q-1$ et $2q-2$, qui correspondent respectivement à $v = n$ et $v = 0$. D'après le lemme 4.31, les termes restants dans (4.10) sont

$$a_q\left(\sum_{P\in A_{1+}} P^{q-1} T_P f\right) = S_1(q-1)\tbinom{q-1}{q-1} a_{q+(q-1)^2} + S_1(2q-2)\tbinom{q-1}{0} a_q$$

Le corollaire 3.14 de [Gek88a] donne $S_1(q-1) = -1 = S_1(2q-2)$, donc

$$a_q\left(\sum_{P\in A_{1+}} P^{q-1} T_P f\right) = -a_{q+(q-1)^2} - a_q.$$

□

***Remarque* 4.33.** Les valeurs de $S_1(m)$ peuvent être évaluées facilement sans faire appel au lemme 4.31. Nous avons préféré donner une preuve faisant intervenir ces outils car une généralisation de la proposition 4.32 aux polynômes de degré supérieur pourrait faire intervenir des sommes $(S_r(m))_{r,m}$. Nous y reviendrons en 4.3.4.

On obtient alors le résultat suivant en direction de la question 4.28.

Théorème 4.34. *Les éléments de* $\mathbf{T} \otimes_{\mathbf{Z}} A$ *définis par*

$$\theta_j = -\tbinom{q-1}{j-1}^{-1} \sum_{P\in A_{1+}} P^{j-1} T_P \qquad (1 \leq j \leq q-1)$$
$$\theta_q = -\sum_{P\in A_{1+}} (P^{q-1}-1) T_P$$

vérifient l'identité de formes linéaires sur $\mathbf{S}(F)$ *:*

$$b_j = b_1 \circ \theta_j \qquad (1 \leq j \leq q).$$

En particulier, si $f \in \mathbf{S}(F)$ *est une forme modulaire de t-développement*

$$\sum_{i\geq 1} b_i(f) t^{1+i(q-1)}$$

et si, pour tout $P \in A$ *de degré* ≤ 1*, on a* $b_1(T_P f) = 0$*, alors* $b_i(f) = 0$ *pour tout* $1 \leq i \leq q$*.*

Démonstration. Posons $\theta'_q = -\left(\sum_{P\in A_{1+}} P^{q-1} T_P + T_1\right) \in \mathbf{T} \otimes_{\mathbf{Z}} A$. D'après la proposition 4.32, on a

$$b_j = b_1 \circ \theta_j \qquad (1 \leq j \leq q-1)$$

et $b_q = b_1 \circ \theta'_q$. Notons que T_1 et $\theta_1 = -\sum_{P\in A_{1+}} T_P$ vérifient $b_1 = b_1 \circ T_1$ et $b_1 = b_1 \circ \theta_1$. Comme $\theta_q = \theta'_q + T_1 - \theta_1$, on a donc l'identité $b_q = b_1 \circ \theta_q$ dans $\mathrm{End}(\mathbf{S}(F))$. □

Remarquons que les expressions de $\theta_1, \ldots, \theta_q$ sont indépendantes de l'idéal $\mathfrak{n}$. On donnera une application du théorème 4.34 à un théorème de multiplicité un pour les formes modulaires lorsque $\mathfrak{n}$ est premier de degré 3, dans la section 4.5. Auparavant, voici une autre conséquence.

Lemme 4.35. *Notons $P_1, \ldots, P_q$ les polynômes unitaires de A de degré 1. On a*

$$\begin{pmatrix} \theta_1 \\ \vdots \\ \theta_q \end{pmatrix} = M \begin{pmatrix} T_{P_1} \\ \vdots \\ T_{P_q} \end{pmatrix},$$

où M est la matrice

$$M = (-1)^q \prod_{i=1}^{q-2} \tbinom{q-1}{i}^{-1} \begin{pmatrix} 1 & \ldots & 1 \\ P_1 & \ldots & P_q \\ \vdots & & \vdots \\ P_1^{q-2} & \ldots & P_q^{q-2} \\ 1 - P_1^{q-1} & \ldots & 1 - P_q^{q-1} \end{pmatrix} \in \mathrm{GL}(q, A).$$

Démonstration. Quitte à soustraire la première ligne à la dernière, on voit que le déterminant de M est un déterminant de Vandermonde. Il vaut $-\prod_{i<j}(P_i - P_j)$. Si $i < j$, les polynômes P_i et P_j sont unitaires et distincts, donc leur différence appartient à $\mathbf{F}_q^\times$. On a donc $\det M \in \mathbf{F}_q^\times$, ce qui montre que $M \in \mathrm{GL}(q, A)$. □

Proposition 4.36. *Supposons $q = p$ et l'idéal $\mathfrak{n}$ premier de degré ≥ 5. Les éléments $\theta_1, \ldots, \theta_q$ de l'algèbre de Hecke sont A-linéairement indépendants dans $\mathbf{T} \otimes_{\mathbf{Z}} A$.*

Le cas $\deg \mathfrak{n} = 3$ sera traité dans la section 4.5.

Démonstration. D'après le lemme 4.35, la famille $\theta_1, \ldots, \theta_q$ est linéairement indépendante sur A dans $\mathbf{T} \otimes_{\mathbf{Z}} A$ si et seulement si $\{T_{P_1}, \ldots, T_{P_q}\}$ est A-linéairement indépendante dans $\mathbf{T} \otimes_{\mathbf{Z}} A$. Supposons qu'il existe $\lambda_1, \ldots, \lambda_q$ dans A non tous nuls vérifiant $\lambda_1 T_{P_1} + \ldots + \lambda_q T_{P_q} = 0$ dans $\mathbf{T} \otimes_{\mathbf{Z}} A$. Quitte à diviser par leur pgcd, on peut supposer que $\lambda_1, \ldots, \lambda_q$ sont premiers entre eux dans leur ensemble. Soit $\mathfrak{l}$ un idéal de A de degré 1. Notons $\overline{\lambda_i} \in \mathbf{F}_{\mathfrak{l}} \simeq \mathbf{F}_p$ la réduction modulo $\mathfrak{l}$ de λ_i. On a l'égalité

$$\overline{\lambda_1} T_{P_1} + \ldots + \overline{\lambda_q} T_{P_q} = 0$$

dans $(\mathbf{T} \otimes_{\mathbf{Z}} A)/\mathfrak{l}(\mathbf{T} \otimes_{\mathbf{Z}} A) = \mathbf{T} \otimes_{\mathbf{Z}} \mathbf{F}_{\mathfrak{l}} = \mathbf{T} \otimes_{\mathbf{Z}} \mathbf{F}_p$. L'algèbre de Hecke $\mathbf{T} \otimes_{\mathbf{Z}} \mathbf{F}_p = \mathbf{T}/p\mathbf{T}$ agit sur $\mathbf{M}^0/p\mathbf{M}^0$. On a donc

$$\overline{\lambda_1} T_{P_1} \widetilde{\mathbf{e}} + \ldots + \overline{\lambda_q} T_{P_q} \widetilde{\mathbf{e}} = 0 \quad \in \mathbf{M}^0/p\mathbf{M}^0.$$

Comme $\deg \mathfrak{n} \geq 5$, les symboles modulaires $T_{P_1}\widetilde{\mathbf{e}}, \ldots, T_{P_q}\widetilde{\mathbf{e}}$ sont $\mathbf{F}_p$-linéairement indépendants d'après le théorème 2.60, donc $\overline{\lambda_i} = 0$ $(1 \leq i \leq q)$. Ainsi $\lambda_1, \ldots, \lambda_q$ appartiennent à l'idéal $\mathfrak{l}$, ce qui contredit le fait qu'ils sont premiers entre eux. On a donc $\lambda_1 = \ldots = \lambda_q = 0$. □

4.3.4 L'action de T_P lorsque P est de degré > 1

À partir de la proposition 4.25, on ne sait pas obtenir une formule générale donnant *tout* coefficient $a_i(f)$ comme combinaison linéaire de $a_q(T_P f)$, pour $P \in A$ (voir remarque 4.26). On peut cependant espérer le faire lorsque i est un entier dont la somme des chiffres dans l'écriture en base q est égale à q. Nous discutons une généralisation du théorème 4.34 aux opérateurs de Hecke dont l'indice est de degré > 1. Pour cela, nous suivons l'idée selon laquelle des sommes de puissances de polynômes, dont la plupart s'annulent, permettent d'isoler les coefficients de f dans la formule (4.5). Notre discussion est motivée par des investigations numériques.

***Notation* 4.37.** Pour tous entiers naturels $i_0, \ldots, i_{d-1}$, on définit la somme de polynômes

$$S_d(i_0, \ldots, i_{d-1}) = \sum_{P \in A_{d+}} l_0(P)^{i_0} \cdots l_{d-1}(P)^{i_{d-1}} \quad \in A$$

et l'élément suivant de $\mathbf{T} \otimes_{\mathbf{Z}} A$

$$\Theta_d(i_0, \ldots, i_{d-1}) = \sum_{P \in A_{d+}} l_0(P)^{i_0} \cdots l_{d-1}(P)^{i_{d-1}} T_P.$$

On notera a_i le i-ème coefficient du t-développement de f. D'après la proposition 4.25, on a, pour $f \in \mathbf{S}(F)$,

$$a_q(\Theta_d(i_0, \ldots, i_{d-1})f) = \sum_{\substack{\underline{m}=(m_0,\ldots,m_d) \\ m_0+\ldots+m_d=q-1}} \binom{q-1}{\underline{m}} S_d(m_0+i_0, \ldots, m_{d-1}+i_{d-1}) a_{1+m_0+m_1q+\ldots+m_dq^d}.$$

Nous traitons des exemples lorsque P est de degré 2 et 3. Les sommes $S_d(i_0, \ldots, i_{d-1})$ ont été calculées à l'aide du logiciel Magma.

Soit $P = T^2 + aT + b \in A$ avec $a, b \in \mathbf{F}_q$. On a

$$\begin{aligned} l_0(P) &= P \\ l_1(P) &= T^q + T + a \\ l_2(P) &= 1. \end{aligned}$$

Exemple 4.38 ($q = 3$, opérateurs de degré 2)**.**

$$a_3(T_P f) = l_0(P)^2 a_3 + l_1(P)^2 a_7 + a_{19} + 2l_0(P)l_1(P)a_5 + 2l_0(P)a_{11} + 2l_1(P)a_{13}.$$

i_0	i_1	$a_3(\Theta_2(i_0, i_1)f)$
0	2	a_3
1	1	$2a_5$
2	0	a_7
1	2	$2a_{11}$
2	1	$2a_{13}$
2	2	$a_{19} + a_3 + a_7$

m_0	m_1	m_2	$a_{1+m_0+3m_1+9m_2}(f)$
2	0	0	a_3
1	1	0	a_5
0	2	0	a_7
1	0	1	a_{11}
0	1	1	a_{13}
0	0	2	a_{19}

Exemple 4.39 ($q = 5$, opérateurs de degré 2)**.**

$$\begin{aligned} a_5(T_P f) \;=\; & l_0(P)^4 a_5 + l_1(P)^4 a_{21} + a_{101} + 4l_0(P)^3 l_1(P) a_9 + 4l_0(P)^3 a_{29} + 4l_1(P)^3 a_{41} \\ & + 4l_0(P) l_1(P)^3 a_{17} + 4l_1(P) a_{81} + 4l_0(P) a_{77} + l_0(P)^2 l_1(P)^2 a_{13} + l_0(P)^2 a_{53} \\ & + l_1(P)^2 a_{61}. \end{aligned}$$

i_0	i_1	$a_5(\Theta_2(i_0,i_1)f)$
0	4	a_5
1	3	$4a_9$
2	2	a_{13}
3	1	$4a_{17}$
4	0	a_{21}
1	4	$4a_{29}$
4	1	$4a_{41}$
2	4	a_{53}
4	2	a_{61}
3	4	$4a_{77}$
4	3	$4a_{81}$
4	4	$a_{101} + a_5 + a_{21}$

m_0	m_1	m_2	$a_{1+m_0+5m_1+25m_2}(f)$
4	0	0	a_5
3	1	0	a_9
2	2	0	a_{13}
1	3	0	a_{17}
0	4	0	a_{21}
3	0	1	a_{29}
0	3	1	a_{41}
2	0	2	a_{53}
0	2	2	a_{61}
1	0	3	a_{77}
0	1	3	a_{81}
0	0	4	a_{101}

Soit $P = T^3 + aT^2 + bT + c \in A$ avec $a, b, c \in \mathbf{F}_q$. On a

$$\begin{aligned} l_0(P) &= P \\ l_1(P) &= (T + T^q)(a + T^q) + T^2 + b \\ l_2(P) &= T^{q^2} + T^q + T + a \\ l_3(P) &= 1. \end{aligned}$$

Exemple 4.40 ($q = 3$, opérateurs de degré 3)**.**

$$\begin{aligned} a_3(T_P f) = & l_0(P)^2 a_3 + l_1(P)^2 a_7 + l_2(P)^2 a_{19} + a_{55} + 2l_0(P) l_1(P) a_5 + 2l_0(P) l_2(P) a_{11} \\ & + 2l_0(P) a_{29} + 2l_1(P) l_2(P) a_{13} + 2l_1(P) a_{31} + 2l_2(P) a_{37}. \end{aligned}$$

i_0	i_1	i_2	$a_5(\Theta_3(i_0,i_1,i_2)f)$
0	2	2	$2a_3$
1	1	2	a_5
2	0	2	$2a_7$
1	2	1	a_{11}
2	1	1	a_{13}
2	2	0	$2a_{19}$
1	2	2	a_{29}
2	1	2	a_{31}
2	2	1	a_{37}
2	2	2	$2a_{55} + 2a_3 + 2a_7 + 2a_{19}$

m_0	m_1	m_2	m_3	$a_{1+m_0+3m_1+9m_2+27m_3}(f)$
2	0	0	0	a_3
1	1	0	0	a_5
0	2	0	0	a_7
1	0	1	0	a_{11}
0	1	1	0	a_{13}
0	0	2	0	a_{19}
1	0	0	1	a_{29}
0	1	0	1	a_{31}
0	0	1	1	a_{37}
0	0	0	2	a_{55}

Au vu de ces résultats, nous sommes naturellement amenés à formuler la question suivante.

Question 4.41. Soient q un nombre premier, $d \geq 1$ un entier et $\underline{m} = (m_0, \ldots, m_d)$ un $(d+1)$-uplet d'entiers naturels vérifiant $m_0 + \ldots + m_d = q - 1$. A-t-on les égalités suivantes :

(i) Si $(m_0, \ldots, m_{d-1}) \neq (0, \ldots, 0)$,

$$a_{1+m_0+m_1q+\ldots+m_dq^d}(f) = (-1)^d \binom{q-1}{\underline{m}}^{-1} a_q(\Theta_d(q-1-m_0, \ldots, q-1-m_{d-1})f).$$

(ii) Si $(m_0, \ldots, m_{d-1}) = (0, \ldots, 0)$ c'est-à-dire $m_d = q - 1$,

$$\begin{aligned} a_{1+(q-1)q^d}(f) = \; & a_q((-1)^d \Theta_d(q-1, \ldots, q-1)f) \\ & -a_q(\Theta_d(0, q-1, \ldots, q-1)f - \ldots - \Theta_d(q-1, \ldots, q-1, 0)f). \end{aligned}$$

pour tout $f \in \mathbf{S}(F)$?

D'après les résultats numériques précédents, ces égalités sont vérifiées pour $q = 3$ et $q = 5$ dans le cas $d = 2$, $q = 3$ dans le cas $d = 3$, et q quelconque dans le cas $d = 1$. Pour les démontrer, il semble naturel d'établir des résultats d'annulation sur les sommes $S_d(i_0, \ldots, i_{d-1})$ dans $\mathbf{F}_q[T]$.

4.4 Sur les points de Weierstrass de $X_0(\mathfrak{n})_K$

Soit $\mathcal{C}$ une courbe algébrique projective lisse de genre $g \geq 2$ sur un corps k. Un point x de $\mathcal{C}$ est dit *de Weierstrass* s'il existe une différentielle régulière non nulle dans $H^0(\mathcal{C}, \Omega^1_{\mathcal{C}/k})$ s'annulant à l'ordre $\geq g$ en x. Par le théorème de Riemann-Roch, cela équivaut à l'existence d'une fonction rationnelle non nulle de $k(\mathcal{C})$, régulière en-dehors de x et ayant un pôle d'ordre $\leq g$ en x. Comme $\mathcal{C}$ est lisse, le genre est invariant par extension de corps de k. Donc un point de $\mathcal{C}$ est de Weierstrass si et seulement si c'est un point de Weierstrass de la courbe $\mathcal{C}_{k'}$ sur k', pour toute extension k' de k.

Dans cette section, on suppose l'idéal $\mathfrak{n}$ premier.

4.4.1 L'argument de Ogg pour les points de Weierstrass de $X_0(\mathfrak{n})$

Proposition 4.42. *Soit $\mathfrak{n}$ un idéal premier de A de degré ≥ 3. Soit x un point K-rationnel de $X_0(\mathfrak{n})$. Il s'étend de façon unique en une section x de $\mathcal{M}_0(\mathfrak{n})$ sur A. On suppose que la réduction de x en $\mathfrak{n}$ n'est pas supersingulière. Alors x n'est pas un point de Weierstrass de $X_0(\mathfrak{n})$. En particulier, les pointes de $X_0(\mathfrak{n})_K$ ne sont pas des points de Weierstrass.*

Démonstration. Il s'agit de l'argument géométrique de [Ogg78] pour les courbes modulaires classiques. Soit x un tel point. Soit c un entier ≥ 1 qui n'est pas une lacune en x c'est-à-dire qu'il existe une fonction f du corps des fonctions de $X_0(\mathfrak{n})_K$ ayant un pôle en x d'ordre c et régulière ailleurs. D'après le théorème de Riemann-Roch, montrer que x n'est pas un point de Weierstrass revient à vérifier que $c \geq 1 + g(X_0(\mathfrak{n}))$.

Comme x est K-rationnel, on peut supposer f définie sur K. L'involution $w_\mathfrak{n}$ est définie sur K ; on pose $x' = w_\mathfrak{n}(x) \in X_0(\mathfrak{n})(K)$. On peut supposer $f(x') = 0$, quitte à ajouter à f une constante de K.

D'après Gekeler (voir la proposition 3.5), la réduction en $\mathfrak{n}$ de $\mathcal{M}_0(\mathfrak{n})$ est stable, formée de deux copies Z et Z' de $\mathcal{M}_0(1)$ sur le corps fini $\mathbf{F}_\mathfrak{n}$, qui se coupent transversalement aux $n(\mathfrak{n})$ points supersinguliers. De plus, Z et Z' sont échangées par $w_\mathfrak{n}$. On peut donc supposer que la réduction $\widetilde{x}$ de x est dans Z et celle $\widetilde{x'}$ de x' dans Z'. Quitte à multiplier f par une constante dans $K^\times$, on peut supposer que la réduction $\widetilde{f}$ de f en $\mathfrak{n}$ est une fonction réduite non constante.

Sur Z', la restriction $\widetilde{f}_{|Z'}$ a un zéro $\widetilde{x'}$ et aucun pôle, puisque le point $\widetilde{x} \in Z$ n'est pas supersingulier. Donc $\widetilde{f}_{|Z'} \equiv 0$. En particulier, $\widetilde{f}_{|Z'}$ s'annule en les points supersinguliers de $Z \cap Z'$. Sur Z, la restriction $\widetilde{f}_{|Z}$ a au moins $n(\mathfrak{n})$ zéros et au plus un pôle $\widetilde{x}$ d'ordre c. Comme $\deg(\mathrm{div}(\widetilde{f}_{|Z})) = 0$, on obtient $n(\mathfrak{n}) \leq c$. Enfin, le nombre de points supersinguliers vérifie $n(\mathfrak{n}) = 1 + g(X_0(\mathfrak{n}))$ ([Gek86b] cor. 5.4), d'où $c \geq 1 + g(X_0(\mathfrak{n}))$. Donc x n'est pas un point de Weierstrass de $X_0(\mathfrak{n})$. □

4.4.2 Hyperellipticité de $X_0(\mathfrak{n})_{\mathbf{F}_\mathfrak{l}}$ d'après Gekeler

Théorème 4.43. *Soit* $\mathfrak{n}$ *un idéal premier de* A *de degré* 3*. Pour tout idéal maximal* $\mathfrak{l}$ *distinct de* $\mathfrak{n}$*, la réduction en* $\mathfrak{l}$ *de la courbe modulaire de Drinfeld* $X_0(\mathfrak{n})$ *est une courbe hyperelliptique sur* $\mathbf{F}_\mathfrak{l}$*.*

Démonstration. D'après le corollaire 3.8 de [Gek86b], la courbe $X_0(\mathfrak{n})_K$ est hyperelliptique sur K. Comme $X_0(\mathfrak{n})$ a bonne réduction en $\mathfrak{l}$, un résultat de spécialisation dit que $X_0(\mathfrak{n})_{\mathbf{F}_\mathfrak{l}}$ est hyperelliptique sur $\mathbf{F}_\mathfrak{l}$ (Schweizer [Sch97] lem. 17, [LK79] th. 5.5, déf. 5.12 et prop. 5.14). □

Corollaire 4.44. *Soit* $\mathfrak{n}$ *un idéal premier de* A *de degré* 3*. Pour tout idéal premier* $\mathfrak{l}$ *distinct de* $\mathfrak{n}$*, les pointes* $0_{\mathbf{F}_\mathfrak{l}}$ *et* $\infty_{\mathbf{F}_\mathfrak{l}}$ *ne sont pas des points de Weierstrass de la réduction en* $\mathfrak{l}$ *de* $X_0(\mathfrak{n})$*.*

Démonstration. Rappelons que dans le cas d'une courbe hyperelliptique $\mathcal{C}$ sur k, les points de Weierstrass sont les points de ramification de son morphisme séparable de degré 2 de $\mathcal{C}$ vers $\mathbf{P}^1_k$, c'est-à-dire les points fixes de son involution hyperelliptique. D'après le corollaire 3.8 de [Gek86b], l'involution hyperelliptique de $X_0(\mathfrak{n})_K$ est l'involution $w_\mathfrak{n}$, donc l'involution hyperelliptique de $X_0(\mathfrak{n})_{\mathbf{F}_\mathfrak{l}}$ est $(w_\mathfrak{n})_{\mathbf{F}_\mathfrak{l}}$. Les pointes $0_{\mathbf{F}_\mathfrak{l}}$ et $\infty_{\mathbf{F}_\mathfrak{l}}$ étant échangées par $(w_\mathfrak{n})_{\mathbf{F}_\mathfrak{l}}$, ce ne sont pas des points fixes de $(w_\mathfrak{n})_{\mathbf{F}_\mathfrak{l}}$ donc ce ne sont pas des points de Weierstrass de $X_0(\mathfrak{n})_{\mathbf{F}_\mathfrak{l}}$. □

4.4.3 Application au développement des formes modulaires

Le lemme suivant est une propriété bien connue des points de Weierstrass.

Lemme 4.45. *Soit* $\mathcal{C}$ *une courbe sur un corps* k*. Soient* x *un point de* $\mathcal{C}$ *et* s *un paramètre formel de* $\mathcal{C}$ *en* x*. Le développement formel d'un élément de* $\omega \in H^0(\mathcal{C}, \Omega^1_{\mathcal{C}/k})$ *en* x *s'écrit* $\sum_{n\geq 0} c_n s^n ds$*. Le point* x *n'est pas de Weierstrass si et seulement si l'application* k*-linéaire*

$$\begin{array}{rcl} H^0(\mathcal{C}, \Omega^1_{\mathcal{C}/k}) & \longrightarrow & k^g \\ \omega & \longmapsto & (c_0, \ldots, c_{g-1}) \end{array}$$

est un isomorphisme.

Démonstration. Le point x n'est pas de Weierstrass si et seulement si toute différentielle régulière non nulle sur $\mathcal{C}/k$ s'annule à l'ordre $< g$ en x, ce qui revient à dire que l'application est injective. Enfin, $\dim_k(H^0(\mathcal{C}, \Omega^1_{C/k})) = g$, ce qui permet de conclure. $\square$

Soit $\mathfrak{n}$ un idéal premier de A. Soit F une extension de K ou le corps $\mathbf{F}_\mathfrak{l}$ (pour $\mathfrak{l}$ un idéal premier de A avec $(\mathfrak{l}, \mathfrak{n}) = 1$). Comme $s = t^{q-1}$ est un paramètre formel de $X_0(\mathfrak{n})$ en ∞ (proposition 4.3), le développement formel de $f \in \mathbf{S}(F)$ est $-\sum_{i\geq 1} b_i(f) s^{i-1} ds$ (lemme 4.8). Quelque soit F, le genre de la courbe $X_0(\mathfrak{n})_F$ est égal à $g(X_0(\mathfrak{n}))$, et noté g. Dans cette situation, le lemme 4.45 prend la forme ci-dessous.

Corollaire 4.46. *Supposons que ∞ n'est pas un point de Weierstrass de $X_0(\mathfrak{n})_F$. Alors l'application linéaire*

$$\begin{array}{rcl} \mathbf{S}(F) & \longrightarrow & F^g \\ f & \longmapsto & (b_1(f), \ldots, b_g(f)) \end{array}$$

est un isomorphisme.

Ce corollaire, conjointement à la proposition 4.42 et au corollaire 4.44, donne le résultat principal de cette section.

Proposition 4.47. *Supposons l'une des conditions suivantes vérifiées :*

(i) F est une extension de K et $\deg \mathfrak{n} \geq 3$;

(ii) $F = \mathbf{F}_\mathfrak{l}$, où $\mathfrak{l}$ est un idéal maximal de A avec $(\mathfrak{l}, \mathfrak{n}) = 1$, et $\deg \mathfrak{n} = 3$.

Alors l'application F-linéaire

$$\begin{array}{rcl} \mathbf{S}(F) & \longrightarrow & F^g \\ f & \longmapsto & (b_1(f), \ldots, b_g(f)) \end{array}$$

est un isomorphisme. En particulier, une forme modulaire dans $\mathbf{S}(F)$ est alors déterminée, de façon unique, par les g premiers coefficients de son t-développement.

On mentionne la conséquence suivante, dont nous ne connaissons pas d'autre démonstration : si l'une des conditions de la proposition est vérifiée, il existe une forme modulaire $f \in \mathbf{S}(F)$ avec $b_1(f) \neq 0$.

4.5 Sur la structure de Hecke des formes modulaires

Dans cette section, on suppose l'idéal $\mathfrak{n}$ premier. Soit $\mathfrak{l}$ un idéal maximal de A avec $(\mathfrak{l}, \mathfrak{n}) = 1$. Soit F un corps, qui est une extension de K ou le corps $\mathbf{F}_\mathfrak{l}$.

4.5.1 Quelques questions

Proposition 4.48. *Les affirmations suivantes sont équivalentes :*

(i) L'accouplement de F-espaces vectoriels

$$\begin{array}{rcl} \mathbf{S}(F) \times \mathbf{T} \otimes_\mathbf{Z} F & \longrightarrow & F \\ (f, t) & \longmapsto & b_1(tf) \end{array}$$

est parfait.

(ii) L'application linéaire

$$\begin{array}{rcl} \Psi : \mathbf{T} \otimes_{\mathbf{Z}} F & \longrightarrow & \mathrm{Hom}(\mathbf{S}(F), F) \\ t & \longmapsto & (f \mapsto b_1(tf)) \end{array}$$

est injective.

(iii) L'application Ψ *est surjective.*

(iv) Pour tout $j \geq 1$*, il existe* $t_j \in \mathbf{T} \otimes_{\mathbf{Z}} F$ *vérifiant* $b_j = b_1 \circ t_j$ *dans* $\mathrm{Hom}(\mathbf{S}(F), F)$*.*

On notera (H_F) *n'importe laquelle de ces affirmations.*

L'énoncé (iv) n'est qu'une variante de la question 4.28, obtenue en remplaçant $\mathbf{T} \otimes_{\mathbf{Z}} A$ par $\mathbf{T} \otimes_{\mathbf{Z}} F$.

Démonstration. On montre que les espaces vectoriels $\mathbf{T} \otimes_{\mathbf{Z}} F$ et $\mathbf{S}(F)$ ont même dimension. L'algèbre de Hecke $\mathbf{T}$ est un $\mathbf{Z}$-module libre, de type fini et de rang $g = g(X_0(\mathfrak{n}))$. Par extension des scalaires, $\mathbf{T} \otimes_{\mathbf{Z}} F$ est un F-espace vectoriel de dimension g. Par ailleurs, l'espace $\mathbf{S}(F)$ est de dimension g d'après le corollaire 4.12. On a l'équivalence des trois premières affirmations.

L'implication (iii) $\Rightarrow$ (iv) est immédiate. Supposons l'affirmation (iv). Les formes linéaires $(b_j)_{j\geq 1}$ sont alors dans l'image de Ψ. On démontre qu'elles engendrent $\mathrm{Hom}(\mathbf{S}(F), F)$. Supposons que le sous-espace vectoriel V qu'elles engendrent est distinct de $\mathrm{Hom}(\mathbf{S}(F), F)$. Alors il existe une forme modulaire non nulle $f \in \mathbf{S}(F)$ telle que $l(f) = 0$ $(l \in V)$. En particulier, $b_j(f) = 0$ pour tout $j \geq 1$. D'après le principe du t-développement (proposition 4.9), f est nulle, ce qui est impossible. On a donc montré que Ψ est surjective, c'est-à-dire (iii). □

L'hypothèse (H_F) semble être ouverte à l'heure actuelle. En 4.5.2, on examinera une situation dans laquelle elle est vérifiée. Étudions quelques conséquences de (H_F), à commencer par un énoncé de multiplicité un (voir aussi [Gek88b] 7.5 pour une problématique similaire).

Lemme 4.49. *Si l'hypothèse* (H_F) *est vérifiée, alors toute forme propre de* $\mathbf{S}(F)$ *est déterminée par ses valeurs propres, à un facteur multiplicatif près.*

Démonstration. Comme Ψ est surjective, il existe $(t_j)_{j\geq 1} \in \mathbf{T} \otimes_{\mathbf{Z}} F$ vérifiant $b_j = b_1 \circ t_j$ pour tout $j \geq 1$. Soit f une forme propre et λ_j sa valeur propre associée à t_j. Alors on a

$$b_j(f) = b_1(t_j f) = b_1(\lambda_j f) = \lambda_j b_1(f) \qquad (j \geq 1).$$

Donc les coefficients du t-développement de f sont déterminés, à un facteur multiplicatif près, par les valeurs propres. Par le principe du t-développement, f est déterminée, à un facteur multiplicatif près, par $(\lambda_j)_{j\geq 1}$. □

Lemme 4.50. *(i) Si l'hypothèse* (H_F) *est vérifiée,* $\mathbf{T} \otimes_{\mathbf{Z}} F$ *opère fidèlement sur* $\mathbf{S}(F)$*.*

(ii) Si l'hypothèse $(H_{\mathbf{F}_\ell})$ *est vérifiée,* $\mathbf{T}/p\mathbf{T}$ *opère fidèlement sur* $\mathbf{H}/p\mathbf{H}$*.*

Démonstration. La première affirmation est immédiate. Démontrons la deuxième. Soit t un élément de $\mathbf{T}/p\mathbf{T}$, nul comme endomorphisme de $\mathbf{H}/p\mathbf{H}$. D'après les travaux de Gekeler et Reversat, le $\mathbf{T}/p\mathbf{T}$-module $\mathbf{H}/p\mathbf{H}$ s'identifie à une certaine $\mathbf{F}_p$-structure de $\mathbf{S}(\mathbf{C}_\infty)$ ([GR96] §6, notamment le diagramme 6.5). Donc t, vu comme endomorphisme de $\mathbf{S}(\mathbf{C}_\infty)$, est nul. D'après la proposition 4.10, t est nul comme élément de $\mathrm{End}(\mathbf{S}(A[1/\mathfrak{n}]))$ puis, par extension des scalaires, dans

$$\mathrm{End}(\mathbf{S}(\mathbf{F}_\mathfrak{l})) = \mathrm{End}(\mathbf{S}(A[1/\mathfrak{n}]) \otimes_{A[1/\mathfrak{n}]} \mathbf{F}_\mathfrak{l}).$$

Donc t est dans le noyau du morphisme composé

$$\mathbf{T}/p\mathbf{T} \longrightarrow \mathbf{T}/p\mathbf{T} \otimes_{\mathbf{F}_p} \mathbf{F}_\mathfrak{l} = \mathbf{T} \otimes_\mathbf{Z} \mathbf{F}_\mathfrak{l} \xrightarrow{\Psi} \mathrm{Hom}(\mathbf{S}(\mathbf{F}_\mathfrak{l}), \mathbf{F}_\mathfrak{l}).$$

Le premier morphisme est injectif, et le deuxième l'est par l'hypothèse $(H_{\mathbf{F}_\mathfrak{l}})$. Donc t est nul dans $\mathbf{T}/p\mathbf{T}$. □

4.5.2 Cas où $\mathfrak{n}$ est de degré 3

Jusqu'à la fin du chapitre, on suppose $\mathfrak{n}$ de degré 3.

Théorème 4.51. *L'hypothèse (H_F) est vérifiée.*

Démonstration. Démontrons que l'application Ψ est surjective. Soit t_j l'image, dans $\mathbf{T} \otimes_\mathbf{Z} F = (\mathbf{T} \otimes_\mathbf{Z} A) \otimes_A F$, de l'élément θ_j du théorème 4.34 ($1 \leq j \leq q$). D'après ce théorème, on a $b_j = b_1 \circ t_j$. La famille $(b_1 \circ t_j)_{(1 \leq j \leq q)}$ est libre dans $\mathrm{Hom}(\mathbf{S}(F), F)$: c'est une conséquence de la proposition 4.47. L'espace vectoriel $\mathrm{Hom}(\mathbf{S}(F), F)$ étant de dimension q, cette famille en est une base. Elle est contenue dans l'image de Ψ, donc l'application Ψ est surjective. □

***Remarque* 4.52.** (i) D'après le lemme 4.50, $\mathbf{T}/p\mathbf{T}$ opère alors fidèlement sur $\mathbf{H}/p\mathbf{H}$. Cet énoncé avait déjà été démontré à l'aide des symboles modulaires (corollaire 2.66 (ii)).

(ii) Il resterait à donner des formules explicites pour $(t_j)_{j \geq q+1}$, ce que nous ne pensons pas pouvoir faire, en toute généralité, par les méthodes de la section 4.3.

Lemme 4.53. *Le F-espace vectoriel* $\mathrm{Hom}(\mathbf{S}(F), F)$ *a pour base* $(b_1 \circ T_\mathfrak{p})_{(\deg \mathfrak{p}=1)}$.

Démonstration. Dans la preuve du théorème 4.51, nous avons vu que la famille $(b_1 \circ t_j)_{(1 \leq j \leq q)}$ est une base de $\mathrm{Hom}(\mathbf{S}(F), F)$. La matrice exprimant $(t_j)_{1 \leq j \leq q}$ comme combinaisons linéaires de $(T_\mathfrak{p})_{(\deg \mathfrak{p}=1)}$ est de déterminant dans $\mathbf{F}_q^\times$, par le lemme 4.35. Donc la famille $(b_1 \circ T_\mathfrak{p})_{(\deg \mathfrak{p}=1)}$ est une base de $\mathrm{Hom}(\mathbf{S}(F), F)$. □

Remarquons que les opérateurs $(T_\mathfrak{p})_{(\deg \mathfrak{p}=1)}$ appartiennent à la $\mathbf{Z}$-algèbre $\mathbf{T}$, ce qui n'est pas le cas de $\theta_1, \ldots, \theta_q$. On pourra comparer l'énoncé suivant avec le corollaire 2.65.

Corollaire 4.54. *Le $\mathbf{F}_p$-espace vectoriel $\mathbf{T}/p\mathbf{T}$ a pour base* $(T_\mathfrak{p})_{(\deg \mathfrak{p}=1)}$.

Démonstration. L'hypothèse $(H_{\mathbf{F}_\mathfrak{l}})$ étant vérifiée, l'application Ψ est un isomorphisme. D'après le lemme 4.53, $(b_1 \circ T_\mathfrak{p})_{(\deg \mathfrak{p}=1)}$ est une base de $\mathrm{Hom}(\mathbf{S}(\mathbf{F}_\mathfrak{l}), \mathbf{F}_\mathfrak{l})$, donc $(T_\mathfrak{p})_{(\deg \mathfrak{p}=1)}$ est une base de $\mathbf{T} \otimes_\mathbf{Z} \mathbf{F}_\mathfrak{l}$. Soit $\mathfrak{l}$ une place de degré 1. Alors $\mathbf{T} \otimes_\mathbf{Z} \mathbf{F}_\mathfrak{l} \simeq \mathbf{T} \otimes_\mathbf{Z} \mathbf{F}_p \simeq \mathbf{T}/p\mathbf{T}$, d'où la conclusion. □

L'énoncé suivant complète la proposition 4.36.

Proposition 4.55. *Supposons* $q = p$ *et l'idéal* $\mathfrak{n}$ *premier de degré* 3*. Les éléments* $\theta_1, \ldots, \theta_q$ *sont* A*-linéairement indépendants dans* $\mathbf{T} \otimes_{\mathbf{Z}} A$*.*

Démonstration. Il s'agit de la démonstration de la proposition 4.36. On remplace le recours aux symboles modulaires par le corollaire 4.54, qui assure que la famille $T_{P_1}, \ldots, T_{P_q}$ est libre sur $\mathbf{F}_p$ dans $\mathbf{T}/p\mathbf{T}$. □

Mentionnons également le résultat suivant, qui est une version forte du lemme 4.49.

Théorème 4.56. *Soit* $f \in \mathbf{S}(F)$ *une forme propre pour les opérateurs* $T_{\mathfrak{p}}$ *(*$\mathfrak{p}$ *de degré* 1*). Alors* f *est déterminée, à un coefficient multiplicatif près, par son système de valeurs propres.*

Démonstration. Soit f une forme propre pour $(T_{\mathfrak{p}})_{(\deg \mathfrak{p}=1)}$, de valeurs propres $(\lambda_{\mathfrak{p}})_{(\deg \mathfrak{p}=1)}$. Par le théorème 4.34, on obtient l'expression suivante des q premiers coefficients du développement de f en fonction des valeurs propres :

$$b_j(f) = \begin{cases} -\binom{q-1}{j-1}^{-1}(\sum_{P \in A_{1+}} P^{j-1}\lambda_P)b_1(f) & \text{si } 1 \leq j \leq q-1 \\ -(\sum_{P \in A_{1+}} P^{q-1}\lambda_P + 1)b_1(f) & \text{si } j = q. \end{cases}$$

Comme le genre de $X_0(\mathfrak{n})$ est égal à q, f est déterminée de façon unique par ses coefficients $(b_i(f))_{(1 \leq i \leq q)}$ d'après la proposition 4.47. Donc f est déterminée, à un coefficient multiplicatif près, par son système de valeurs propres de degré 1. □

Chapitre 5

Application aux points rationnels de courbes modulaires de Drinfeld

5.1 Torsion p-primaire des quotients optimaux de $J_0(\mathfrak{n})$

Nous présenterons dans la section 5.3 une approche analogue à celle de Mazur pour l'étude des points rationnels de courbes modulaires de Drinfeld. La présente section est consacrée à une difficulté technique rencontrée lors de sa mise en œuvre en caractéristique p. Mazur utilisait un résultat de spécialisation pour les schémas en groupes sur un anneau de valuation discrète de caractéristique nulle : si l est un nombre premier ≥ 3 et G est un schéma en groupes sur $\mathbf{Z}_l$, un point d'ordre fini de $G(\mathbf{Z}_l)$ et sa spécialisation en l ont même ordre ([Maz78] 1c, [Ray74] 3.3.6, [BLR90] 7.5).

Ce résultat n'est plus valable si on remplace $\mathbf{Z}$ par un anneau de caractéristique p, comme A. Voici un contre-exemple. Considérons la courbe elliptique sur $\mathbf{F}_3((T))$ définie par l'équation affine $y^2 = x^3 + T^6x^2 + 2x$. Elle a bonne réduction supersingulière en (T) et un point $(\frac{1}{T^2}, T + \frac{1}{T^3})$ d'ordre 3 : en la place (T), ce point se spécialise donc en 0. Cependant, ce cas de figure ne se produit pas pour les courbes elliptiques quotients de $J_0(\mathfrak{n})$, lesquelles ont réduction multiplicative en $\mathfrak{n}$, et plus généralement pour les quotients optimaux de $J_0(\mathfrak{n})$: c'est ce que nous détaillons dans cette section. L'outil principal est la proposition 5.2 due à Papikian.

Nous gardons les notations sur les variétés abéliennes introduites dans la section 3.2. Si G est un groupe fini et l un nombre premier, $G[l^\infty]$ désigne la composante l-primaire de G.

5.1.1 Torsion p-primaire de variétés abéliennes à réduction torique en égale caractéristique

Lemme 5.1 (voir aussi [Pál05], lemme 7.13)**.** *Soient F un corps local de caractéristique p et k son corps résiduel. Soit A une variété abélienne définie sur F à réduction torique. Alors le sous-groupe de torsion p-primaire de $A(F)$ s'injecte dans le groupe des composantes $\Phi_A(k)$.*

Démonstration. Soient R l'anneau de valuation discrète de F et $\mathcal{A}$ le modèle de Néron de A sur R. Comme la formation des modèles de Néron commute aux changements de base étales, donc aux extensions non ramifiées, on peut remplacer F par une extension non ramifiée sur laquelle A a réduction torique déployée. On considère l'homomorphisme de groupe suivant, noté h,

$$A(F) \simeq \mathcal{A}(R) \xrightarrow{\text{red}} \mathcal{A}_k(k) \longrightarrow \Phi_A(k),$$

où l'isomorphisme est donné par la propriété universelle des modèles de Néron et red est l'application de réduction. La variété abélienne A ayant réduction torique déployée, le théorème de Mumford-Raynaud [Ray71] donne une uniformisation analytique rigide de l'analytifiée A^{an} de A et on a une suite exacte

$$0 \longrightarrow \Lambda \longrightarrow (F^\times)^d \longrightarrow A^{\text{an}}(F) \longrightarrow 0,$$

où Λ est un réseau de $(F^\times)^d$ (d entier naturel). De plus, *via* cette uniformisation, le noyau de h est isomorphe à $(R^\times)^d$. Comme $R^\times \subset F^\times$ et F est de caractéristique p, la p-torsion de $(R^\times)^d$ est nulle. Donc la composante p-primaire de $A(F)_{\text{tors}}$ s'injecte par h dans $\Phi_A(k)$. □

Le résultat suivant est une reformulation du lemme 2.3 de [Pap07].

Proposition 5.2 (Papikian)**.** *Soit F un corps local de caractéristique p et de corps résiduel k. Soient B une variété abélienne définie sur F à réduction torique, A une sous-variété abélienne de B et $C = B/A$ la variété abélienne quotient, définies sur F. Alors l'homomorphisme canonique*

$$\Phi_B(k)[p^\infty] \longrightarrow \Phi_C(k)[p^\infty]$$

est surjectif.

5.1.2 Application aux quotients optimaux de $J_0(\mathfrak{n})$

Définition 5.3. Soit $\mathfrak{n}$ un idéal premier de $A = \mathbf{F}_q[T]$. Un *quotient optimal de* $J_0(\mathfrak{n})$ est une variété abélienne quotient J de $J_0(\mathfrak{n})$ définie sur K telle que le noyau de $\pi : J_0(\mathfrak{n}) \to J$ est un sous-schéma en groupes connexe, c'est-à-dire une sous-variété abélienne de $J_0(\mathfrak{n})$.

Proposition 5.4. *Soit $\mathfrak{n}$ un idéal premier de A. Si J est un quotient optimal de $J_0(\mathfrak{n})$, la composante p-primaire de $J(K)_{\text{tors}}$ est nulle.*

Démonstration. La variété abélienne $J_0(\mathfrak{n})$ a réduction torique en $\mathfrak{n}$. Soient $K_\mathfrak{n}$ le complété de K en $\mathfrak{n}$ et $k_\mathfrak{n}$ son corps résiduel. Le groupe $J(K)_{\text{tors}}$ s'injecte canoniquement dans $J(K_\mathfrak{n})_{\text{tors}}$ et en utilisant le lemme 5.1, on a l'injection

$$J(K)_{\text{tors}}[p^\infty] \hookrightarrow \Phi_J(k_\mathfrak{n}).$$

D'après la proposition 5.2, le morphisme $\Phi_{J_0(\mathfrak{n})}(k_\mathfrak{n})[p^\infty] \to \Phi_J(k_\mathfrak{n})[p^\infty]$ est surjectif. Or, la composante p-primaire de $\Phi_{J_0(\mathfrak{n})}(k_\mathfrak{n})$ est triviale puisque, par la proposition 3.5, l'ordre de $\Phi_{J_0(\mathfrak{n})}(k_\mathfrak{n})$ divise $n(\mathfrak{n})$, qui est premier à p. Donc le groupe $\Phi_J(k_\mathfrak{n})$ a une composante p-primaire nulle, et il en est de même de $J(K)_{\text{tors}}$. □

***Remarque* 5.5.** (i) La proposition s'applique par exemple au quotient d'enroulement et au quotient raffiné, qui ont été définis au chapitre 3.

(ii) Il n'est pas clair que l'argument de la démonstration soit encore valable en remplaçant la place $\mathfrak{n}$ par ∞, en laquelle $J_0(\mathfrak{n})$ a également réduction torique (déployée) : en effet, l'ordre du groupe des composantes de $J_0(\mathfrak{n})$ en ∞ peut être divisible par p (voir l'exemple 5.3.3. de [Gek97b]).

(iii) Lorsque $J = J_0(\mathfrak{n})$, la proposition est conséquence du fait que le groupe fini $J_0(\mathfrak{n})(K)_{\text{tors}}$ est d'ordre premier à p (théorème 3.7 de Gekeler et Pál).

5.2 Immersions formelles (rappels)

Soient X et Y deux schémas noethériens. Soit $f : X \to Y$ un morphisme de schémas, x un point de X et $y = f(x)$. On note $\mathcal{O}_{X,x}$ et $\mathcal{O}_{Y,y}$ les anneaux locaux de X en x et Y en y, ainsi que $\widehat{\mathcal{O}}_{X,x}$ et $\widehat{\mathcal{O}}_{Y,y}$ leurs complétés. Le morphisme f est une *immersion formelle en x* si le morphisme d'anneaux $\widehat{f_x} : \widehat{\mathcal{O}}_{Y,y} \to \widehat{\mathcal{O}}_{X,x}$ est surjectif.

Proposition 5.6 ([Gro67] th. 17.4.1 et prop 17.4.4)**.** *Soient X et Y deux schémas noethériens. Soit $f : X \to Y$ un morphisme de schémas, x un point de X et $y = f(x)$. Notons $\mathfrak{m}_x$ (resp. $\mathfrak{m}_y$) l'idéal maximal de l'anneau local en x (resp. en y) et $k(x)$ (resp. $k(y)$) le corps résiduel en x (resp. y). Le morphisme f est une immersion formelle en x si et seulement si les deux conditions suivantes sont vérifiées :*

(i) le morphisme $k(y) \to k(x)$ déduit de f est un isomorphisme ;

(ii) l'application $\mathfrak{m}_y/\mathfrak{m}_y^2 \to \mathfrak{m}_x/\mathfrak{m}_x^2$ déduite de f par passage aux espaces cotangents est surjective.

La principale propriété des immersions formelles qui nous sera utile est la suivante.

Proposition 5.7. *Soit $f : X \to Y$ un morphisme de schémas noethériens avec X séparé de type fini tel que f soit une immersion formelle en $x \in X$. Soit T un schéma intègre noethérien, t un point de T et g_1, g_2 deux morphismes de T dans X tels que $g_1(t) = g_2(t) = x$ et $f \circ g_1 = f \circ g_2$. Alors on a $g_1 = g_2$.*

Démonstration. Nous rappelons la démonstration donnée dans [Oes]. Comme $f \circ g_1 = f \circ g_2$, les morphismes $\widehat{g_1}_t \circ \widehat{f_x}$ et $\widehat{g_2}_t \circ \widehat{f_x}$ entre les complétés $\widehat{\mathcal{O}}_{Y,y}$ et $\widehat{\mathcal{O}}_{T,t}$ sont égaux. Le morphisme $\widehat{f_x}$ étant surjectif, on a $\widehat{g_1}_t = \widehat{g_2}_t : \widehat{\mathcal{O}}_{X,x} \to \widehat{\mathcal{O}}_{T,t}$. Les schémas X et T sont noethériens, donc leurs anneaux locaux $\mathcal{O}_{X,x}$ et $\mathcal{O}_{T,t}$ le sont aussi et ils s'identifient à des sous-anneaux de $\widehat{\mathcal{O}}_{X,x}$ et $\widehat{\mathcal{O}}_{T,t}$ respectivement. Donc les morphismes $\mathcal{O}_{X,x} \to \mathcal{O}_{T,t}$ induits par g_1 et g_2 coïncident. Comme X est de type fini, g_1 et g_2 coïncident dans un voisinage ouvert de t donc au point générique de T ([Gro60] I.6.5.1). Enfin, X étant séparé et T intègre, les sections g_1 et g_2 sont égales ([Gro60] 5.4.7). □

5.3 L'argument de Mazur

Soit d un entier ≥ 1. Soient $\mathfrak{n}$ un idéal premier de A et $X_0(\mathfrak{n})_K^{(d)}$ la puissance symétrique d-ème de $X_0(\mathfrak{n})_K$ (on pourra consulter [Mil86] §3 à 5 pour des résultats généraux sur les puissances symétriques de courbes). C'est une variété lisse sur K dont

les points K-rationnels s'identifient aux diviseurs K-rationnels effectifs sur $X_0(\mathfrak{n})_{K^{\mathrm{sep}}}$ de degré d (on rappelle qu'un diviseur D de $X_0(\mathfrak{n})_{K^{\mathrm{sep}}}$ est dit K-rationnel si $D^\sigma = D$ pour tout $\sigma \in \mathrm{Gal}(K^{\mathrm{sep}}/K)$). Considérons le morphisme

$$\begin{array}{rcl} \varphi^{(d)} : X_0(\mathfrak{n})_K^{(d)} & \longrightarrow & J_0(\mathfrak{n}) \\ D & \longmapsto & \text{classe de } (D - d(\infty)). \end{array}$$

Soient $\mathfrak{n}$ un idéal premier de A et J un quotient optimal de $J_0(\mathfrak{n})$ défini sur K. Par composition de $\varphi^{(d)}$ avec la projection canonique $\pi : J_0(\mathfrak{n}) \to J$, on obtient un morphisme de variétés algébriques sur K

$$u^{(d)} : X_0(\mathfrak{n})_K^{(d)} \longrightarrow J.$$

Soit $\mathcal{J}$ le modèle de Néron de J sur $A[1/\mathfrak{n}]$. Par propriété universelle, $u^{(d)}$ se prolonge de façon unique en un morphisme de schémas sur $A[1/\mathfrak{n}]$

$$u^{(d)} : X_0(\mathfrak{n})^{(d)} \longrightarrow \mathcal{J}.$$

Notons $\infty^{(d)}$ la section $\mathrm{Spec}(A[1/\mathfrak{n}]) \to X_0(\mathfrak{n})^{(d)}$ déduite de ∞. Si $\mathfrak{l}$ est un idéal maximal de A distinct de $\mathfrak{n}$, on note $\infty_{\mathfrak{l}}^{(d)}$ la restriction de $\infty^{(d)}$ à la fibre spéciale en $\mathfrak{l}$. On notera φ (resp. u) pour $\varphi^{(1)}$ (resp. $u^{(1)}$). Enfin, on pose $w = w_{\mathfrak{n}}$.

Proposition 5.8. *Soit $\mathfrak{l}$ un idéal premier de A distinct de $\mathfrak{n}$. La spécialisation en $\mathfrak{l}$*

$$J(K)_{\mathrm{tors}} \simeq \mathcal{J}(A[1/\mathfrak{n}]) \longrightarrow J(\mathbf{F}_{\mathfrak{l}})$$

est un homomorphisme de groupes injectif.

Démonstration. Notons v cet homomorphisme. Son noyau est un groupe fini. La variété abélienne $J_0(\mathfrak{n})$ a bonne réduction en $\mathfrak{l}$ (car $\mathfrak{l} \neq \mathfrak{n}$), donc il en est de même de J d'après le critère de Néron-Ogg-Shafarevich. Comme p est la caractéristique de $\mathbf{F}_{\mathfrak{l}}$, le noyau de v est alors un p-groupe. De plus, la composante p-primaire de $J(K)_{\mathrm{tors}}$ est triviale d'après la proposition 5.4. Ainsi, v est injectif. □

On pourra comparer l'énoncé suivant avec le corollaire 4.3 [Maz78], le lemme 3.2 et le théorème 3.3 de [Kam92b].

Théorème 5.9. *Soit $\mathfrak{l}$ un idéal maximal de A. Soit $\mathfrak{n}$ un idéal premier de A, distinct de $\mathfrak{l}$, de degré $> d \deg \mathfrak{l}$ tels que les conditions suivantes sont vérifiées :*

(i) $J(K)$ est fini ;

(ii) $u^{(d)} : X_0(\mathfrak{n})^{(d)} \to \mathcal{J}$ est une immersion formelle en $\infty_{\mathfrak{l}}^{(d)}$.

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

Démonstration. Supposons qu'il existe un entier d vérifiant $d \deg \mathfrak{l} < \deg \mathfrak{n}$, une extension L de K de degré d et un point dans $Y_1(\mathfrak{n})(L)$. Par l'interprétation modulaire, ce point correspond à la classe de L^{alg}-isomorphisme d'un couple (ϕ, P), où ϕ est un module de Drinfeld sur L de rang 2 et $P \in ({}^{\phi}L)_{\mathrm{tors}}$ est un point d'ordre $\mathfrak{n}$. Considérons le couple donné par ϕ et le sous-A-module cyclique de $({}^{\phi}L)_{\mathrm{tors}}$ d'ordre $\mathfrak{n}$ engendré par P. Ce couple définit un point $x \in X_0(\mathfrak{n})(L)$. Soient $s = [L : K]_{\mathrm{sep}}$ et $p^e = [L : K]_{\mathrm{ins}}$

($e \geq 0$) les degrés séparables et inséparables de l'extension L/K. Notons $\sigma_1, \ldots, \sigma_s$ les s plongements de L dans K^{alg} fixant K. Le diviseur $\sum_{i=1}^{s} p^e \sigma_i(x)$ de $X_0(\mathfrak{n})_{K^{\mathrm{sep}}}$ est K-rationnel et de degré $p^e \cdot s = d$. Il définit un point K-rationnel y' de $X_0(\mathfrak{n})^{(d)}$. Comme $X_0(\mathfrak{n})^{(d)}$ est propre sur $A[1/\mathfrak{n}]$, il se prolonge en une section du morphisme structurel $X_0(\mathfrak{n})^{(d)} \to \mathrm{Spec}(A[1/\mathfrak{n}])$, notée y'.

Comme $d \deg \mathfrak{l} < \deg \mathfrak{n}$, d'après le corollaire 1.21, en toute place $\mathfrak{L}$ de L au-dessus de $\mathfrak{l}$, ϕ a réduction stable de rang 1, et P ne définit pas un point entier d'un modèle stable de ϕ. Par la proposition 4.5, on a $x_{\mathfrak{L}} = 0_{\mathfrak{L}}$ pour toute place $\mathfrak{L}$ au-dessus de $\mathfrak{l}$, donc $y'_{\mathfrak{l}} = 0_{\mathfrak{l}}^{(d)}$. En posant $y = w(y')$, on a alors

$$y_{\mathfrak{l}} = \infty_{\mathfrak{l}}^{(d)} \tag{5.1}$$

puisque w échange les pointes. Posons $z = u^{(d)}(y) \in \mathcal{J}(A[1/\mathfrak{n}]) \subset J(K)$. La spécialisation en $\mathfrak{l}$ de z vérifie

$$z_{\mathfrak{l}} = 0_{\mathfrak{l}}.$$

Comme $J(K)$ est fini, z est nul d'après la proposition 5.8. On a donc $u^{(d)}(y) = u^{(d)}(\infty)$ dans $\mathcal{J}(A[1/\mathfrak{n}])$. Par ailleurs, y et $\infty^{(d)}$ ont même spécialisation en $\mathfrak{l}$ d'après (5.1). Appliquons la propriété d'immersion formelle (proposition 5.7) à $u^{(d)}$ en $\infty_{\mathfrak{l}}^{(d)}$: les sections y et $\infty^{(d)}$ sont égales. On a donc $y = \infty^{(d)}$, $y' = 0^{(d)}$ et $x = 0$. Cela contredit le fait que x n'est pas une pointe de $X_0(\mathfrak{n})_K$. □

***Remarque* 5.10.** Pour $\mathfrak{n}$ premier, il existe des quotients optimaux de $J_0(\mathfrak{n})$ vérifiant la condition (i) : par exemple, le quotient d'Eisenstein [Tam95, Pál05], les quotients d'enroulement et raffiné du chapitre 3. Le quotient d'enroulement devrait être, d'après la conjecture de Birch et Swinnerton-Dyer, le plus grand quotient de $J_0(\mathfrak{n})$ défini sur K vérifiant (i).

5.4 Application au cas où $\mathfrak{n}$ est de degré 3 ou 4

Revenons sur les situations examinées aux paragraphes 3.5 et 4.4. Les résultats de cette section sont basés sur des variantes de l'argument de Mazur, ne faisant intervenir ni les symboles modulaires, ni la propriété d'immersion formelle.

5.4.1 Torsion de degré 3 des modules de Drinfeld

Théorème 5.11. *Soit $\mathfrak{n}$ un idéal premier de A de degré 3. Pour toute extension L de K de degré ≤ 2, la courbe modulaire de Drinfeld $Y_1(\mathfrak{n})$ n'a pas de point L-rationnel. En particulier, il n'existe pas de module de Drinfeld sur L de rang 2 ayant un point L-rationnel dont l'ordre est un idéal premier de degré 3.*

Démonstration. On démontre en fait le résultat suivant : si $\mathfrak{n}$ est un idéal premier de A de degré ≥ 3 tel que $J_0(\mathfrak{n}) = J_{\mathbf{e}}(\mathfrak{n})$, la courbe $Y_1(\mathfrak{n})$ n'a pas de point défini sur une extension de K de degré $< \deg \mathfrak{n}$. La condition $J_0(\mathfrak{n}) = J_{\mathbf{e}}(\mathfrak{n})$ se produit si et seulement si $\mathfrak{n}$ est de degré 3, d'après le théorème 3.19.

Supposons qu'il existe un entier d vérifiant $1 \leq d < \deg \mathfrak{n}$, une extension L de K de degré d et un point x dans $Y_1(\mathfrak{n})(L)$. Fixons une place $\mathfrak{l}$ de A de degré 1 et procédons

comme dans la démonstration du théorème 5.9. On obtient un point K-rationnel y de $Y_0(\mathfrak{n})^{(d)}$, qui s'étend en une section y du morphisme structurel $X_0(\mathfrak{n})^{(d)} \to \mathrm{Spec}(A[1/\mathfrak{n}])$, et dont la spécialisation en $\mathfrak{l}$ vérifie

$$\varphi^{(d)}(y)_{\mathfrak{l}} = 0_{\mathfrak{l}}.$$

Comme $J_{\mathbf{e}}(\mathfrak{n}) = J_0(\mathfrak{n})$, $J_0(\mathfrak{n})(K)$ est fini donc $\varphi^{(d)}(y)$ est nul d'après la proposition 5.8 (voir aussi la remarque 5.5 (iii)). Le diviseur $D = \sum_{i=1}^{s} p^e \sigma_i(x) - d(\infty)$ est principal sur K^{alg}, donc sur une extension finie purement inséparable $\widetilde{K}$ de K. Il existe alors une fonction rationnelle non nulle f sur $X_0(\mathfrak{n})_{\widetilde{K}}$ dont D est le diviseur. Elle admet un unique pôle en ∞ d'ordre d, car $y \neq \infty^{(d)}$. Rappelons que le genre g de $X_0(\mathfrak{n})_{\widetilde{K}}$ est donné par l'une des formules

$$g = g(X_0(\mathfrak{n})) = \begin{cases} \frac{q^{\deg \mathfrak{n}} - q^2}{q^2-1} & \text{si } \deg \mathfrak{n} \text{ est pair ;} \\ \frac{q^{\deg \mathfrak{n}} - q}{q^2-1} & \text{si } \deg \mathfrak{n} \text{ est impair} \end{cases}$$

(prop. 1.23). En particulier, si $\deg \mathfrak{n} \geq 3$, on a $\deg(\mathfrak{n}) - 1 \leq g$. Comme $d \leq \deg(\mathfrak{n}) - 1$, f est régulière en dehors de ∞ et possède un pôle en ∞ d'ordre $\leq g$. Cela contredit le fait que ∞ n'est pas un point de Weierstrass de $X_0(\mathfrak{n})_{\widetilde{K}}$ (proposition 4.42).

□

Le théorème confirme partiellement la conjecture 1.14 de Schweizer sur la structure du module des points K-rationnels d'un module de Drinfeld. Par ailleurs, une démonstration alternative du théorème 5.11, utilisant la propriété d'immersion formelle, sera donnée en 5.5.4.

Signalons qu'il existe quelques cas isolés pour lesquels on sait que la courbe $Y_0(\mathfrak{n})$ (et donc la courbe $Y_1(\mathfrak{n})$) n'a pas de point K-rationnel, avec $\mathfrak{n}$ composé de degré 3 : il s'agit de $q = 2$ et $\mathfrak{n} = (T(T^2+T+1))$, (T^3) et $(T^2(T+1))$ (lemme 1.3 de [Sch03]). Schweizer m'a signalé aussi les cas $(q = 3, \mathfrak{n} = (T(T-1)(T+1)))$, $(q = 3, \mathfrak{n} = T^2(T-1))$ et $(q = 4, \mathfrak{n}$ produit de trois facteurs linéaires distincts), pour lesquels la démonstration est similaire.

Une variante de la démonstration précédente fournit le résultat partiel suivant concernant les points K-rationnels de $Y_0(\mathfrak{n})$, lorsque $\mathfrak{n}$ est de degré 3.

Proposition 5.12. *Soit $\mathfrak{n}$ un idéal premier de degré 3. Soit ϕ un module de Drinfeld sur K de rang 2 possédant une $\mathfrak{n}$-isogénie cyclique K-rationnelle. Alors ϕ a bonne réduction potentielle en tout idéal premier distinct de $\mathfrak{n}$.*

Démonstration. On pourra comparer les arguments suivants avec ceux du corollaire 4.3 de [Maz78]. Soit un module de Drinfeld ϕ sur K de rang 2 possédant une $\mathfrak{n}$-isogénie cyclique K-rationnelle $C_{\mathfrak{n}}$. Par l'interprétation modulaire, il correspond à un point y dans $Y_0(\mathfrak{n})(K)$. Notons encore y son prolongement en une section du morphisme structurel de $X_0(\mathfrak{n}) \to \mathrm{Spec}(A[1/\mathfrak{n}])$.

Supposons qu'il existe un idéal premier $\mathfrak{l}$ de A distinct de $\mathfrak{n}$ en lequel ϕ n'a pas bonne réduction potentielle. Par la proposition 1.6, ϕ a réduction potentiellement stable de rang 1 donc la spécialisation $y_{\mathfrak{l}}$ est une pointe de $X_0(\mathfrak{n})_{\mathbf{F}_{\mathfrak{l}}}$. L'involution w permute

les pointes ∞ et 0 de $X_0(\mathfrak{n})$ et $\infty_{\mathfrak{l}}$ et $0_{\mathfrak{l}}$ de $X_0(\mathfrak{n})_{\mathbf{F}_{\mathfrak{l}}}$. Quitte à remplacer y par $w(y)$, on peut donc supposer que y n'est pas une pointe et que

$$\varphi(y)_{\mathfrak{l}} = 0_{\mathfrak{l}}.$$

La fin de la démonstration est alors similaire à celle du théorème 5.11 dans le cas $d = 1$. □

***Remarque* 5.13.** Lorsque $\mathfrak{n}$ est de degré ≤ 3, la courbe $Y_0(\mathfrak{n})$ a une infinité de points de degré 2 sur K. En effet :

(i) si $\mathfrak{n}$ est de degré 1 ou 2, la courbe $X_0(\mathfrak{n})$ est de genre nul et possède un point rationnel (la pointe ∞) ;

(ii) si $\deg \mathfrak{n} = 3$, la courbe $X_0(\mathfrak{n})$ est hyperelliptique d'après le corollaire 3.8 de [Gek86b].

Signalons que Schweizer a complété cette étude et obtenu une liste exhaustive des idéaux $\mathfrak{n}$ pour lesquels la courbe $X_0(\mathfrak{n})$ a une infinité de points quadratiques sur $\mathbf{F}_q(T)$ ([Sch01] th. 5.3). Sa preuve utilise le théorème de Hrushovski (ex-conjecture de Mordell-Lang pour les variétés abéliennes sur les corps de fonctions).

5.4.2 Torsion de degré 4 des modules de Drinfeld

Soit $\mathcal{C}$ une courbe projective lisse sur un corps k. La *gonalité de $\mathcal{C}$ sur k*, notée $\gamma_{\mathcal{C},k}$, est le plus petit degré possible d'une application k-rationnelle dominante (c'est-à-dire non constante) de $\mathcal{C}$ dans $\mathbf{P}^1_k$. Si k' est une extension de k, on a $\gamma_{\mathcal{C},k} \geq \gamma_{\mathcal{C},k'}$. Les courbes de gonalité 1 (resp. 2) sont celles de genre 0 (resp. les courbes elliptiques ou hyperelliptiques).

Proposition 5.14 (Schweizer [Sch03] lemme 2.2)**.** *Soit $\mathfrak{n}$ un idéal premier de A. Soit $\widetilde{K}$ une extension finie purement inséparable de K. La gonalité de la courbe modulaire de Drinfeld $X_0(\mathfrak{n})_{\widetilde{K}}$ sur $\widetilde{K}$ vérifie*

$$\gamma_{X_0(\mathfrak{n}),\widetilde{K}} \geq \frac{q^{\deg \mathfrak{n}}}{(q^2+1)(q+1)} + 1.$$

Rappelons que $\mathbf{H}(\mathbf{C})$ désigne l'espace de formes automorphes introduit dans la section 2.1.2.

Théorème 5.15. *Soit $\mathfrak{n}$ un idéal premier vérifiant la propriété : toute forme propre de $\mathbf{H}(\mathbf{C})$ est de rang ≤ 1. Soit L une extension de K, de degré*

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

Alors la courbe $Y_1(\mathfrak{n})$ n'a pas de point L-rationnel.

En particulier, soient $\mathfrak{n}$ un idéal premier de degré 4 et L une extension de K de degré $\leq d$, où

$$d = \begin{cases} 1 & \text{si } q = 2, 3\ ; \\ 2 & \text{si } q = 4, 5\ ; \\ 3 & \text{si } q \geq 7. \end{cases}$$

Alors la courbe $Y_1(\mathfrak{n})$ n'a pas de point L-rationnel. En d'autres termes, il n'existe pas de module de Drinfeld sur L de rang 2 ayant un point L-rationnel dont l'ordre est premier de degré 4.

Démonstration. Supposons qu'il existe un entier $d < \min\left(\deg \mathfrak{n}, \frac{1}{2}\left(\frac{q^{\deg \mathfrak{n}}}{(q^2+1)(q+1)} + 1\right)\right)$, une extension L de K de degré d et un point x dans $Y_1(\mathfrak{n})(L)$. Fixons une place $\mathfrak{l}$ de A de degré 1 et procédons comme dans la démonstration du théorème 5.9. Soient $s = [L : K]_{\text{sep}}$ et $p^e = [L : K]_{\text{ins}}$ ($e \geq 0$) les degrés séparables et inséparables de l'extension L/K et $\sigma_1, \ldots, \sigma_s$ les s plongements de L dans K^{alg} fixant K. Le diviseur $\sum_{i=1}^{s} p^e \sigma_i(x)$ de $X_0(\mathfrak{n})_{K^{\text{sep}}}$ définit un point K-rationnel y' de $Y_0(\mathfrak{n})^{(d)}$, qui s'étend en une section y' du morphisme structurel $X_0(\mathfrak{n})^{(d)} \to \operatorname{Spec}(A[1/\mathfrak{n}])$, et dont la spécialisation en $\mathfrak{l}$ vérifie $y'_{\mathfrak{l}} = 0_{\mathfrak{l}}^{(d)}$. En posant $y = w(y')$, on a

$$y_{\mathfrak{l}} = \infty_{\mathfrak{l}}^{(d)}.$$

Considérons le morphisme

$$\begin{array}{rcl} g : X_0(\mathfrak{n})_K^{(d)} & \longrightarrow & J_0(\mathfrak{n}) \\ D & \longmapsto & \text{classe de } (D - w(D) + d(0) - d(\infty)). \end{array}$$

L'image de g est anti-invariante par w, donc contenue dans $J_0(\mathfrak{n})_-$. Rappelons que $J_0(\mathfrak{n})_-$ est isogène, sur K, à $J_0(\mathfrak{n})^- = J_{\mathbf{e}}(\mathfrak{n})$ (proposition 3.24). En particulier, le groupe $J_0(\mathfrak{n})_-(K)$ est fini, donc $g(y)$ est d'ordre fini dans $J_0(\mathfrak{n})(K)$. D'après le résultat de spécialisation (proposition 5.8), $g(y)$ est nul dans $J_0(\mathfrak{n})(K)$. Le diviseur

$$y - w(y) + d(0) - d(\infty) = \sum_{i=1}^{s} p^e w(\sigma_i(x)) - \sum_{i=1}^{s} p^e \sigma_i(x) + d(0) - d(\infty)$$

est alors principal sur K^{alg}, donc sur une extension finie purement inséparable $\widetilde{K}$ de K. De plus, il est non nul : en effet, comme x provient d'un module de Drinfeld et w échange les pointes, on a $\sigma_i(x) \neq 0$ et $w(\sigma_i(x)) \neq \infty$ pour tout $1 \leq i \leq s$. Il existe donc une fonction $\widetilde{K}$-rationnelle de $X_0(\mathfrak{n})_{\widetilde{K}}$ dont c'est le diviseur. Cette fonction définit un morphisme $f : X_0(\mathfrak{n})_{\widetilde{K}} \to \mathbf{P}^1_{\widetilde{K}}$. Le degré de f étant égal à la somme des indices de ramification aux points de $f^{-1}(0)$, on en déduit $\deg f = \sum_{i=1}^{s} p^e + d = 2d$. On a donc, par définition de la gonalité et en appliquant la proposition 5.14,

$$2d \geq \gamma_{X_0(\mathfrak{n}),\widetilde{K}} \geq \frac{q^{\deg \mathfrak{n}}}{(q^2+1)(q+1)} + 1,$$

ce qui contredit l'hypothèse initiale sur d. Donc pour toute extension L de K de degré

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

la courbe $Y_1(\mathfrak{n})$ n'a pas de point L-rationnel.

Ce résultat s'applique au cas où $\mathfrak{n}$ est de degré 4, car toute forme propre de $\mathbf{H}(\mathbf{C})$ est alors de rang au plus 1, d'après le corollaire 2.18. En examinant la valeur du majorant,

on voit que $Y_1(\mathfrak{n})$ n'a pas de point L-rationnel, pour toute extension de K de degré $\leq d$, où

$$d = \begin{cases} 1 & \text{si } q = 2, 3 \text{ ;} \\ 2 & \text{si } q = 4, 5 \text{ ;} \\ 3 & \text{si } q \geq 7. \end{cases}$$

□

***Remarque* 5.16.** (i) Supposons $\mathfrak{n}$ premier de degré 3. Un argument similaire appliqué au morphisme

$$\begin{array}{rcl} X_0(\mathfrak{n})_K & \longrightarrow & J_0(\mathfrak{n}) \\ x & \longmapsto & \text{classe de } ((x) - (\infty)) \end{array}$$

permet de retrouver $Y_1(\mathfrak{n})(K) = \emptyset$ (en effet, on a alors $J_0(\mathfrak{n}) = J_0(\mathfrak{n})^- = J_{\mathbf{e}}(\mathfrak{n})$ et la courbe $Y_0(\mathfrak{n})$ est hyperelliptique, de gonalité 2).

(ii) Lorsque $\mathfrak{n}$ est de degré 4, le théorème 5.15 affirme que $Y_1(\mathfrak{n})$ n'a pas de point K-rationnel : cela confirme partiellement la conjecture 1.14 de Schweizer.

(iii) Nous n'avons pas eu l'occasion de vérifier si le théorème 5.15 s'applique à des courbes $Y_1(\mathfrak{n})$ avec $\deg \mathfrak{n} \geq 5$.

Une variante de la démonstration précédente, à la façon de la proposition 5.12, fournit le résultat partiel suivant concernant les points K-rationnels de $Y_0(\mathfrak{n})$, lorsque $\mathfrak{n}$ est de degré 4.

Proposition 5.17. *Soit $\mathfrak{n}$ un idéal premier de degré 4. Soit ϕ un module de Drinfeld sur K de rang 2 possédant une $\mathfrak{n}$-isogénie cyclique K-rationnelle. Alors ϕ a bonne réduction potentielle en tout idéal premier distinct de $\mathfrak{n}$.*

5.4.3 Isogénies K-rationnelles en degré ≥ 5

On rappelle que $\eta_{\mathfrak{l}}$ désigne l'élément $T_{\mathfrak{l}} - (q^{\deg \mathfrak{l}} + 1)$ de l'algèbre de Hecke $\mathbf{T}$, pour $\mathfrak{l}$ idéal premier non nul de A.

Théorème 5.18. *Soit $\mathfrak{n}$ un idéal premier de degré ≥ 5. Si $\deg \mathfrak{n} = 5$ (resp. $\deg \mathfrak{n} = 6$), on suppose $q \geq 4$ (resp. $q \geq 3$). Supposons que $\mathfrak{n}$ vérifie la propriété : toute forme propre de $\mathbf{H}(\mathbf{C})$ est de rang ≤ 1. Alors la courbe $Y_0(\mathfrak{n})$ n'a pas de point K-rationnel.*

Démonstration.

Lemme 5.19. *Soient $\mathfrak{n}$ un idéal premier de degré ≥ 4 et $\mathfrak{l}$ un idéal maximal distinct de $\mathfrak{n}$. Considérons l'application*

$$\begin{array}{rcl} X_0(\mathfrak{n})(K) & \longrightarrow & \mathrm{Div}^0(X_0(\mathfrak{n})(K)) \\ x & \longmapsto & \eta_{\mathfrak{l}}((x) - (w(x))). \end{array}$$

L'image réciproque du diviseur nul est $\{0, \infty\}$.

Démonstration. Soit $x \in X_0(\mathfrak{n})(K)$ vérifiant $\eta_{\mathfrak{l}}((x) - (w(x))) = 0$. Schweizer a établi la liste des points CM K-rationnels de $X_0(\mathfrak{n})$ lorsque $\deg \mathfrak{n} \geq 3$ ([Sch03], remarque 6) : ils ne correspondent qu'à des idéaux $\mathfrak{n}$ de degré 3. En particulier, x n'est pas un point CM de $X_0(\mathfrak{n})$, donc $w(x) \neq x$. Comme

$$T_{\mathfrak{l}}(x) + (q^{\deg \mathfrak{l}} + 1)(w(x)) = T_{\mathfrak{l}}(w(x)) + (q^{\deg \mathfrak{l}} + 1)(x) = 0,$$

on a nécessairement l'égalité de diviseurs $T_{\mathfrak{l}}(x) = (q^{\deg \mathfrak{l}} + 1)(x)$.

D'après l'inégalité de Ramanujan-Petersson pour les formes automorphes de $\mathbf{H}(\mathbf{C})$, les valeurs propres de $T_{\mathfrak{l}}$ opérant sur $\mathbf{H}(\mathbf{C})$ sont des entiers algébriques de valeur absolue $\leq 2q^{\frac{\deg \mathfrak{l}}{2}}$. Les valeurs propres de $\eta_{\mathfrak{l}}$ sont donc non nulles. L'opérateur $\eta_{\mathfrak{l}}$ opérant sur $\mathbf{H}(\mathbf{C})$ est alors inversible dans $\mathbf{T} \otimes_{\mathbf{Z}} \mathbf{Q} \subset \mathrm{End}_K(J_0(\mathfrak{n})) \otimes_{\mathbf{Z}} \mathbf{Q}$. De $\eta_{\mathfrak{l}}(x) = \eta_{\mathfrak{l}}(\infty) = 0$, on déduit $\eta_{\mathfrak{l}}((x) - (\infty)) = 0$ donc $(x) - (\infty) = 0$ dans $J_0(\mathfrak{n})(K) \otimes_{\mathbf{Z}} \mathbf{Q}$. Ainsi, la classe du diviseur K-rationnel $(x) - (\infty)$ est de torsion dans $J_0(\mathfrak{n})(K)$.

Rappelons que le sous-groupe $J_0(\mathfrak{n})(K)_{\mathrm{tors}}$ coïncide avec le sous-groupe cuspidal de $J_0(\mathfrak{n})(K)$ (théorème 3.7). Ce dernier étant annulé par $1 + w$, le groupe $J_0(N)(K)_{\mathrm{tors}}$ est contenu dans $J_0(\mathfrak{n})_-(K)$. Notons ∞^+ l'unique pointe de la courbe $X_0(\mathfrak{n})_K^+ = w \backslash X_0(\mathfrak{n})_K$. Considérons le diagramme commutatif

$$\begin{tikzcd} X_0(\mathfrak{n})_K \arrow[r, "\varphi"] \arrow[d, "\pi"'] & J_0(\mathfrak{n}) \arrow[d, "\pi_*"] \\ X_0(\mathfrak{n})_K^+ \arrow[r, "\varphi^+"] & J_0(\mathfrak{n})^+, \end{tikzcd}$$

où π est la projection, φ l'application qui à P associe la classe de $(P) - (\infty)$, π_* l'application déduite de π par fonctorialité d'Albanese, φ^+ l'application qui à P^+ associe la classe de $(P^+) - (\infty^+)$. D'après ce qui précède, le diviseur $(\pi_* \circ \varphi)(x)$ est nul dans $J_0(\mathfrak{n})^+(K)$. Par ailleurs, la courbe $X_0(\mathfrak{n})_K$ n'est pas hyperelliptique d'après Schweizer, car $\deg \mathfrak{n} > 3$ (([Sch97] th. 20). Donc le genre de $X_0(\mathfrak{n})_K^+$ est > 0, et le morphisme d'Albanese φ^+ est injectif. D'après le diagramme, on en déduit $x^+ = \infty^+$, c'est-à-dire $x \in \{0, \infty\}$. □

Supposons que $\mathfrak{n}$ vérifie les hypothèses du théorème et qu'il existe un point y dans $Y_0(\mathfrak{n})(K)$. Soit $\mathfrak{l}$ une place de degré 1 de K. Considérons les morphismes

$$\begin{array}{rcl} f : X_0(\mathfrak{n})_K & \longrightarrow & J_0(\mathfrak{n}) \\ x & \longmapsto & \text{classe de } ((x) - (w(x))) \end{array}$$

et

$$h = \eta_{\mathfrak{l}} \circ f = (T_{\mathfrak{l}} - (q+1)) \circ f : X_0(\mathfrak{n})_K \to J_0(\mathfrak{n}).$$

L'image de f est anti-invariante par w, donc contenue dans $J_0(\mathfrak{n})_-$. Rappelons que $J_0(\mathfrak{n})_-$ est isogène sur K à $J_0(\mathfrak{n})^- = J_{\mathbf{e}}(\mathfrak{n})$ d'après la proposition 3.24. En particulier, le groupe $J_0(\mathfrak{n})_-(K)$ est fini. Le sous-groupe $J_0(\mathfrak{n})(K)_{\mathrm{tors}}$ coïncide avec le sous-groupe cuspidal de $J_0(\mathfrak{n})(K)$ (théorème 3.7). Par ailleurs, $\eta_{\mathfrak{l}}$ annule le diviseur $(0) - (\infty)$. Donc $h(X_0(\mathfrak{n})(K)) = \{0\}$ et, en particulier, $h(y)$ est nul. Le diviseur

$$D = T_{\mathfrak{l}}(y) + (q+1)(w(y)) - T_{\mathfrak{l}}(w(y)) - (q+1)(y)$$

est principal sur K, et non nul d'après le lemme 5.19. Il existe donc une fonction K-rationnelle de $X_0(\mathfrak{n})_K$ dont D est le diviseur. Cette fonction définit un morphisme $X_0(\mathfrak{n})_K \to \mathbf{P}^1_K$, de degré $2(q+1)$. Par définition de la gonalité et en appliquant la proposition 5.14, on a

$$2(q+1) \geq \gamma_{X_0(\mathfrak{n}),K} \geq \gamma_{X_0(\mathfrak{n}),\widetilde{K}} \geq \frac{q^{\deg \mathfrak{n}}}{(q^2+1)(q+1)} + 1.$$

Ceci est impossible si l'une des conditions suivantes est vérifiée :

$$\begin{cases} \deg \mathfrak{n} = 5 \text{ et } q \geq 4 \text{ ;} \\ \deg \mathfrak{n} = 6 \text{ et } q \geq 3 \text{ ;} \\ \deg \mathfrak{n} \geq 7. \end{cases}$$

□

Nous n'avons pas eu l'occasion de vérifier si cette proposition s'applique à des courbes $Y_0(\mathfrak{n})$ avec $\deg \mathfrak{n} \geq 5$.

5.5 Étude du cas général

Soit $\mathfrak{n}$ un idéal premier de A. On pose $S = \mathrm{Spec}(A[1/\mathfrak{n}])$ et $X = X_0(\mathfrak{n})$ sur S. Le morphisme

$$\varphi^{(d)} : X^{(d)} \longrightarrow \mathcal{J}_0(\mathfrak{n}),$$

qui envoie $\infty^{(d)}$ sur 0, définit une application entre les espaces cotangents

$$(\varphi^{(d)})^* : \mathrm{Cot}\, \mathcal{J}_0(\mathfrak{n}) \longrightarrow \mathrm{Cot}_{\infty^{(d)}} X^{(d)}.$$

5.5.1 Espace cotangent en 0 à la jacobienne

Rappelons que, d'après la proposition 4.13, on a un isomorphisme canonique

$$\Theta : \mathrm{Cot}(\mathcal{J}_0(\mathfrak{n})) \xrightarrow{\sim} \mathbf{S}(A[1/\mathfrak{n}]).$$

L'énoncé suivant s'en déduit par changement de base (proposition 4.10).

Corollaire 5.20. *Soit $\mathfrak{l}$ un idéal premier de A distinct de $\mathfrak{n}$. Alors on a un isomorphisme canonique*

$$\mathrm{Cot}(\mathcal{J}_0(\mathfrak{n})_{\mathbf{F}_\mathfrak{l}}) \xrightarrow{\sim} \mathbf{S}(\mathbf{F}_\mathfrak{l}).$$

5.5.2 Espace cotangent en 0 au quotient raffiné

Jusqu'à la fin de ce texte, sauf mention contraire, nous supposons l'hypothèse (H_I), page 76, vérifiée.

Reprenons les notations de la section 3.6. L'homomorphisme de variétés abéliennes sur K

$$\pi : J_0(\mathfrak{n}) \longrightarrow J'_{\mathbf{e}}(\mathfrak{n})$$

se prolonge de façon unique, par propriété universelle des modèles de Néron, en un homomorphisme de schémas sur S

$$\pi : \mathcal{J}_0(\mathfrak{n}) \longrightarrow \mathcal{J}'_{\mathbf{e}}(\mathfrak{n}).$$

Notons $\pi^* : \operatorname{Cot} \mathcal{J}'_{\mathbf{e}}(\mathfrak{n}) \to \operatorname{Cot} \mathcal{J}_0(\mathfrak{n})$ le morphisme induit sur les espaces cotangents en 0. Tout élément t de $\mathbf{T}$ est un endomorphisme de $J_0(\mathfrak{n})$ sur K, qui se prolonge de façon unique en un endomorphisme de $\mathcal{J}_0(\mathfrak{n})$ noté t. Notons t^* l'endomorphisme de $\operatorname{Cot} \mathcal{J}_0(\mathfrak{n})$ déduit par passage aux espaces cotangents. Si $\mathscr{I}$ est un idéal de $\mathbf{T}$, on notera $\operatorname{Cot} \mathcal{J}_0(\mathfrak{n})[\mathscr{I}]$ le sous-espace de $\operatorname{Cot} \mathcal{J}_0(\mathfrak{n})$ annulé par $\{t^* \mid t \in \mathscr{I}\}$.

Lemme 5.21. *L'image de π^* contient* $\operatorname{Cot} \mathcal{J}_0(\mathfrak{n})[\widetilde{I}_{\mathbf{e}}]$.

Démonstration. Par l'hypothèse (H_I), il existe $\widetilde{t} \in \widetilde{I}_{\mathbf{e}}$ et $\widehat{t} \in \widehat{I}$ vérifiant $1 = \widetilde{t} + \widehat{t}$ dans $\mathbf{T} \subset \operatorname{End}_K(J_0(\mathfrak{n}))$. Comme $\widehat{t} \in \widehat{I}$, on a $\widehat{t}I = 0$ et donc la factorisation

$$\begin{tikzcd} J_0(\mathfrak{n}) \arrow[r, "\widehat{t}"] \arrow[d, "\pi"] & J_0(\mathfrak{n}) \\ J'_{\mathbf{e}}(\mathfrak{n}) \arrow[ur] & \end{tikzcd}.$$

Par propriété universelle des modèles de Néron, ce diagramme se prolonge en

$$\begin{tikzcd} \mathcal{J}_0(\mathfrak{n}) \arrow[r, "\widehat{t}"] \arrow[d, "\pi"] & \mathcal{J}_0(\mathfrak{n}). \\ \mathcal{J}'_{\mathbf{e}}(\mathfrak{n}) \arrow[ur] & \end{tikzcd}$$

On a donc le diagramme commutatif suivant entre espaces cotangents

$$\begin{tikzcd} \operatorname{Cot} \mathcal{J}_0(\mathfrak{n}) \arrow[r] \arrow[dr, "\widehat{t}^*"'] & \operatorname{Cot} \mathcal{J}'_{\mathbf{e}}(\mathfrak{n}) \arrow[d, "\pi^*"] \\ & \operatorname{Cot} \mathcal{J}_0(\mathfrak{n}). \end{tikzcd}$$

En particulier, l'image de π^* contient $\widehat{t}^*(\operatorname{Cot} \mathcal{J}_0(\mathfrak{n})[\widetilde{I}_{\mathbf{e}}])$. La relation $1 = \widetilde{t} + \widehat{t}$ est encore valable dans $\operatorname{End}_S(\mathcal{J}_0(\mathfrak{n}))$, donc

$$\widehat{t}^*(\operatorname{Cot} \mathcal{J}_0(\mathfrak{n})[\widetilde{I}_{\mathbf{e}}]) = (1 - \widetilde{t})^*(\operatorname{Cot} \mathcal{J}_0(\mathfrak{n})[\widetilde{I}_{\mathbf{e}}]) = \operatorname{Cot} \mathcal{J}_0(\mathfrak{n})[\widetilde{I}_{\mathbf{e}}].$$

On a montré que l'image de π^* contient $\operatorname{Cot} \mathcal{J}_0(\mathfrak{n})[\widetilde{I}_{\mathbf{e}}]$. □

L'énoncé qui suit se déduit directement du lemme précédent.

Proposition 5.22. *Soit $\mathfrak{l}$ un idéal maximal de A distinct de $\mathfrak{n}$. Si l'application*

$$(\operatorname{Cot} \mathcal{J}_0(\mathfrak{n})_{\mathbf{F}_\mathfrak{l}})[\widetilde{I}_{\mathbf{e}}] \longrightarrow \operatorname{Cot} X^{(d)}_{\mathbf{F}_\mathfrak{l}}$$

est surjective, alors le morphisme $u^{(d)} : X^{(d)}_S \to \mathcal{J}'_{\mathbf{e}}(\mathfrak{n})$ est une immersion formelle en $\infty^{(d)}_\mathfrak{l}$.

***Remarque* 5.23.** L'hypothèse minimale dont nous aurons besoin par la suite est en fait la suivante : il existe un idéal saturé I de $\mathbf{T}$ tel que

(i) $I_{\mathbf{e}} \subset I \subset \widetilde{I_{\mathbf{e}}}$;

(ii) Soit $\mathcal{J}_I$ le modèle de Néron de la variété abélienne quotient $J_0(\mathfrak{n})/IJ_0(\mathfrak{n})$. L'image de l'application $\operatorname{Cot}\mathcal{J}_I \to \operatorname{Cot}\mathcal{J}_0(\mathfrak{n})$ contient $\operatorname{Cot}\mathcal{J}_0(\mathfrak{n})[I]$.

Cette hypothèse est plus faible que (H_I) et que l'hypothèse *(H2)* de l'introduction.

5.5.3 Espace cotangent en $\infty^{(d)}$ à $X^{(d)}$

D'après la proposition 4.3, le complété formel de X le long de la section ∞ est isomorphe, *via* le module de Tate-Drinfeld, au spectre formel de $A[1/\mathfrak{n}][[t^{q-1}]]$. En d'autres termes, X admet la coordonnée formelle locale $s = t^{q-1}$ en ∞. L'espace cotangent à X en la section ∞ est alors isomorphe, comme $A[1/\mathfrak{n}]$-module, à $sA[1/\mathfrak{n}][[s]]/s^2A[1/\mathfrak{n}][[s]]$; il est de libre de rang 1, de base ds.

Le schéma X^d admet alors les coordonnées formelles locales $s_1, \ldots, s_d$. Par construction du produit symétrique, les fonctions symétriques élémentaires :

$$\sigma_1 = s_1 + \ldots + s_d, \ \ldots, \ \sigma_d = s_1 \cdots s_d$$

sont des coordonnées formelles locales de $X^{(d)}$ en $\infty^{(d)}$. Donc le $A[1/\mathfrak{n}]$-module $\operatorname{Cot}_{\infty^{(d)}} X^{(d)}$ est libre de rang d et admet pour base $d\sigma_1, \ldots, d\sigma_d$.

5.5.4 Application entre espaces cotangents

On pourra comparer l'énoncé suivant avec la proposition 3.1 de [Kam92b].

Proposition 5.24. *Le morphisme* $(\varphi^{(d)})^* : \operatorname{Cot}\mathcal{J}_0(\mathfrak{n}) \to \operatorname{Cot}_{\infty^{(d)}} X^{(d)}$ *correspond,* via *l'isomorphisme* Θ *de la proposition 4.13, à l'homomorphisme de* $A[1/\mathfrak{n}]$*-modules*

$$\begin{array}{rcl} \mathbf{S}(A[1/\mathfrak{n}]) & \longrightarrow & A[1/\mathfrak{n}]^d \\ f & \longmapsto & (-b_1(f), b_2(f), \ldots, , (-1)^d b_d(f)), \end{array}$$

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

Démonstration. Posons $\Omega^1 = \Omega^1_{X/S}$. On a un isomorphisme canonique

$$\beta : H^0(X, \Omega^1) \simeq H^0(X^{(d)}, \Omega^1)$$

([Mil86] prop. 5.3). Soit $v : H^0(X^{(d)}, \Omega^1) \to \operatorname{Cot}_{\infty^{(d)}}(X^{(d)})$ le morphisme qui, à une section, associe sa restriction au fibré cotangent de $\infty^{(d)}$ dans $X^{(d)}$. Considérons le diagramme suivant.

$$\begin{tikzcd}
\operatorname{Cot}(\mathcal{J}_0(\mathfrak{n})) \arrow[r, "(\varphi^{(d)})^*"] \arrow[d, "\Theta"', "\sim"] & \operatorname{Cot}_{\infty^{(d)}}(X^{(d)}) \arrow[r, "\sim"] & A[1/\mathfrak{n}]^d \\
\mathbf{S}(A[1/\mathfrak{n}]) \arrow[d, "\beta"', "\sim"] & & \\
H^0(X^{(d)}, \Omega^1) \arrow[uur, "v"] & &
\end{tikzcd}$$

Le triangle est commutatif d'après le lemme 2.1 de [Maz78]. Explicitons le morphisme $v \circ \beta$. Soit $f \in \mathbf{S}(A[1/\mathfrak{n}])$ une forme modulaire, de t-développement $\sum_{i\geq 1} b_i t^{1+i(q-1)}$. D'après le lemme 4.8, le développement formel de f en ∞ est $-\sum_{i\geq 1} b_i s^{i-1} ds$. L'image de f dans $H^0(X^d, \Omega^1)$, par le morphisme canonique, est une différentielle régulière globale, de développement formel

$$-\sum_{i=1}^{d} \sum_{k\geq 1} b_k s_i^{k-1} ds_i$$

(signalons qu'à partir de cette étape, les calculs menés dans la proposition 3.2 de [Kam92a] ne sont plus valables en caractéristique non nulle). Posons $U_j = \sum_{i=1}^{d} s_i^j ds_i$ ($j \geq 0$). On a alors

$$\sum_{i=1}^{d} \sum_{k\geq 1} b_k s_i^{k-1} ds_i = \sum_{k\geq 1} b_k U_{k-1}. \tag{5.2}$$

L'image de f par $v \circ \beta$ s'obtient en prenant l'image de f dans $H^0(X^{(d)}, \Omega^1)$ et en considérant la partie linéaire de son développement.

Lemme 5.25. *Soient $\sigma_1 = s_1 + \ldots + s_d, \cdots, \sigma_d = s_1 \cdots s_d$ les polynômes symétriques élémentaires en les indéterminées $s_1, \ldots, s_d$ et $U_j = \sum_{i=1}^{d} s_i^j ds_i$. Alors on a*

(i) pour tout $1 \leq m \leq d-1$, $\sigma_m U_0 - \sigma_{m-1} U_1 + \ldots + (-1)^m U_m = d\sigma_{m+1}$;

(ii) pour tout $m \geq d$, $(-1)^d \sigma_d U_{m-d} + \ldots - \sigma_1 U_{m-1} + U_m = 0$.

Ces égalités ont lieu dans le module des différentielles $\Omega^1_{A[1/\mathfrak{n}, s_1, \ldots, s_d]/A[1/\mathfrak{n}]}$.

Démonstration. (i) C'est le lemme 5.4 de [Mil86].

(ii) Supposons $m \geq d$. Les relations de Newton donnent

$$s_i^d - \sigma_1 s_i^{d-1} + \ldots + (-1)^d \sigma_d = 0 \qquad (1 \leq i \leq d).$$

En multipliant cette égalité par $s_i^{m-d}\, ds_i$ et en sommant sur i ($1 \leq i \leq d$), on obtient la seconde relation.

□

En évaluant en l'infini les différentielles du lemme, on a les égalités dans $\mathrm{Cot}_{\infty^{(d)}} X^{(d)}$:

$$\begin{array}{rcll} (-1)^m U_m & = & d\sigma_{m+1} & (1 \leq m \leq d-1) \\ U_m & = & 0 & (m \geq d). \end{array}$$

On substitue dans l'expression (5.2) et on obtient finalement

$$(v \circ \beta)(f) = -\sum_{k=1}^{d} (-1)^{k+1} b_k d\sigma_k \quad \in \mathrm{Cot}_{\infty^{(d)}} X^{(d)}.$$

□

Si $\mathscr{I}$ est un idéal de l'algèbre de Hecke $\mathbf{T}$, on note $\mathbf{S}(\mathbf{F}_\mathfrak{l})[\mathscr{I}]$ le sous-$\mathbf{T}$-module de $\mathbf{S}(\mathbf{F}_\mathfrak{l})$ annulé par $\mathscr{I}$.

Théorème 5.26. *Supposons que l'application linéaire*

$$\begin{array}{rcl} \mathbf{S}(\mathbf{F}_{\mathfrak{l}})[\widetilde{I}_{\mathbf{e}}] & \longrightarrow & \mathbf{F}_{\mathfrak{l}}^d \\ f & \longmapsto & (b_1(f), \ldots, b_d(f)) \end{array}$$

est surjective. Alors le morphisme $u^{(d)} : X^{(d)} \to \mathcal{J}'_{\mathbf{e}}(\mathfrak{n})$ *est une immersion formelle en* $\infty_{\mathfrak{l}}^{(d)}$.

Démonstration. Le corollaire 5.20 identifie les espaces vectoriels $\mathbf{S}(\mathbf{F}_{\mathfrak{l}})$ et $\mathrm{Cot}(\mathcal{J}_0(\mathfrak{n})_{\mathbf{F}_{\mathfrak{l}}})$. D'après l'hypothèse de l'énoncé et la proposition 5.24, l'application linéaire

$$\mathrm{Cot}(\mathcal{J}_0(\mathfrak{n})_{\mathbf{F}_{\mathfrak{l}}})[\widetilde{I}_{\mathbf{e}}] \longrightarrow \mathrm{Cot}(X_{\mathbf{F}_{\mathfrak{l}}}^{(d)}),$$

déduite de $(\varphi^{(d)})^*$ par restriction à $\mathrm{Cot}(\mathcal{J}_0(\mathfrak{n})_{\mathbf{F}_{\mathfrak{l}}})[\widetilde{I}_{\mathbf{e}}]$, est surjective. D'après la proposition 5.22, cela suffit à prouver que $u^{(d)}$ est une immersion formelle en $\infty_{\mathfrak{l}}^{(d)}$. □

Signalons une démonstration alternative du théorème 5.11, qui repose sur le résultat suivant.

Proposition 5.27. *Si* $\mathfrak{n}$ *est un idéal premier de degré* 3*, le morphisme* $u^{(q)} : X_0(\mathfrak{n})^{(q)} \to \mathcal{J}_{\mathbf{e}}(\mathfrak{n})$ *est une immersion formelle en* $\infty_{\mathfrak{l}}^{(q)}$.

Démonstration. Comme $\deg \mathfrak{n} = 3$, le quotient d'enroulement est $J_0(\mathfrak{n})$, donc

$$u^{(q)} = \varphi^{(q)} : X_0(\mathfrak{n})^{(q)} \to \mathcal{J}_0(\mathfrak{n}).$$

Comme $\deg \mathfrak{n} = 3$, d'après la proposition 4.47, l'application

$$\begin{array}{rcl} \mathbf{S}(\mathbf{F}_{\mathfrak{l}}) & \longrightarrow & \mathbf{F}_{\mathfrak{l}}^q \\ f & \longmapsto & (b_1(f), \ldots, b_q(f)) \end{array}$$

est surjective. Donc $u^{(q)}$ est une immersion formelle en $\infty_{\mathfrak{l}}^{(q)}$ d'après la proposition 5.24, ce qui achève la démonstration.

Signalons qu'il est possible de déduire cet énoncé du théorème 5.26 précédent. Comme $\deg \mathfrak{n} = 3$, l'idéal $I_{\mathbf{e}}$ est nul. Démontrons $d_{\mathbf{e}}\widetilde{I}_{\mathbf{e}} \subset p\mathbf{T}$. Soit $t \in \widetilde{I}_{\mathbf{e}}$. Le symbole modulaire $d_{\mathbf{e}}t\mathbf{e}$ appartient à $p\mathbf{M}^0$. Comme $\deg \mathfrak{n} = 3$, d'après le théorème 2.64, il existe $\theta \in I_E$ vérifiant $d_{\mathbf{e}}t\mathbf{e} = p\theta\mathbf{e}$. L'endomorphisme $d_{\mathbf{e}}t - p\theta$ de $\mathbf{M}^0$, qui annule $\mathbf{e}$, est nul. L'algèbre de Hecke agissant fidèlement sur $\mathbf{M}^0$, on a $d_{\mathbf{e}}t = p\theta$ dans $\mathbf{T}$. Donc $d_{\mathbf{e}}t \in pI_E \subset p\mathbf{T}$ et l'assertion $d_{\mathbf{e}}\widetilde{I}_{\mathbf{e}} \subset p\mathbf{T}$ est démontrée. Comme la caractéristique p de $\mathbf{F}_{\mathfrak{l}}$ est première à $d_{\mathbf{e}}$, on en déduit

$$\mathbf{S}(\mathbf{F}_{\mathfrak{l}})[\widetilde{I}_{\mathbf{e}}] = \mathbf{S}(\mathbf{F}_{\mathfrak{l}})[d_{\mathbf{e}}\widetilde{I}_{\mathbf{e}}] \supset \mathbf{S}(\mathbf{F}_{\mathfrak{l}})[p\mathbf{T}] = \mathbf{S}(\mathbf{F}_{\mathfrak{l}})$$

donc $\mathbf{S}(\mathbf{F}_{\mathfrak{l}})[\widetilde{I}_{\mathbf{e}}] = \mathbf{S}(\mathbf{F}_{\mathfrak{l}})$. Le théorème 5.26 assure alors que $u^{(q)}$ est une immersion formelle. □

Deuxième démonstration du théorème 5.11. Soient $\mathfrak{n}$ un idéal premier de degré 3 et $\mathfrak{l}$ un idéal premier de A de degré 1. Appliquons la méthode de Mazur (théorème 5.9). D'abord, comme $\deg \mathfrak{n} = 3$, on a $J_{\mathbf{e}}(\mathfrak{n}) = J_0(\mathfrak{n})$ et cette variété abélienne n'a qu'un nombre fini de points rationnels d'après le théorème 3.11. Ensuite, la proposition 5.27 assure que le morphisme $u^{(2)} : X_0(\mathfrak{n})^{(2)} \to \mathcal{J}_{\mathbf{e}}(\mathfrak{n}) = \mathcal{J}_0(\mathfrak{n})$ est une immersion formelle en $\infty_{\mathfrak{l}}^{(2)}$ (c'est vrai *a fortiori* pour $u^{(q)}$). D'après le théorème 5.9, la courbe $Y_1(\mathfrak{n})$ n'a pas de point L-rationnel pour toute extension L de K de degré 2. □

5.5.5 Critère de Kamienny pour le quotient raffiné

Soit $\mathfrak{l}$ un idéal premier maximal de A distinct de $\mathfrak{n}$.

Proposition 5.28. *Supposons les deux conditions suivantes vérifiées :*

(i) L'homomorphisme de $\mathbf{F}_\mathfrak{l}$-espaces vectoriels

$$\begin{array}{rcl} \mathbf{T} \otimes_{\mathbf{Z}} \mathbf{F}_\mathfrak{l} & \longrightarrow & \mathrm{Hom}(\mathbf{S}(\mathbf{F}_\mathfrak{l}), \mathbf{F}_\mathfrak{l}) \\ t & \longmapsto & (f \mapsto b_1(tf)) \end{array}$$

est un isomorphisme ;

(ii) Soient $t_1, \ldots, t_d$ des éléments de $\mathbf{T} \otimes_{\mathbf{Z}} \mathbf{F}_\mathfrak{l}$ vérifiant $b_i = b_1 \circ t_i$ $(1 \leq i \leq d)$. Leurs images dans $\mathbf{T}/\widetilde{I}_{\mathbf{e}} \otimes_{\mathbf{Z}} \mathbf{F}_\mathfrak{l}$ sont $\mathbf{F}_\mathfrak{l}$-linéairement indépendantes.

Alors le morphisme $u^{(d)} : X^{(d)} \to \mathcal{J}'_{\mathbf{e}}(\mathfrak{n})$ est une immersion formelle en $\infty_\mathfrak{l}^{(d)}$.

De plus, la condition (i) est vérifiée lorsque $\deg \mathfrak{n} = 3$. La condition (ii) est vérifiée dans les situations suivantes : $(1 \leq d \leq q, \deg \mathfrak{n} \geq 5)$ et $(d = 1, \deg \mathfrak{n} \geq 3)$.

La première condition de l'énoncé n'est autre que l'hypothèse $(H_{\mathbf{F}_\mathfrak{l}})$, étudiée au chapitre 4.

Démonstration. Considérons le diagramme commutatif suivant, dans lequel les lignes sont des suites exactes de $\mathbf{F}_\mathfrak{l}$-espaces vectoriels :

$$\begin{tikzcd} 0 \arrow[r] & \mathbf{S}(\mathbf{F}_\mathfrak{l})[\widetilde{I}_{\mathbf{e}}] \arrow[r] \arrow[d, "a"'] & \mathbf{S}(\mathbf{F}_\mathfrak{l}) \arrow[r] \arrow[d, "b"', "\sim"] & \mathbf{S}(\mathbf{F}_\mathfrak{l})/\mathbf{S}(\mathbf{F}_\mathfrak{l})[\widetilde{I}_{\mathbf{e}}] \arrow[r] \arrow[d, "c"'] & 0 \\ 0 \arrow[r] & \mathrm{Hom}(\mathbf{T}/\widetilde{I}_{\mathbf{e}} \otimes_{\mathbf{Z}} \mathbf{F}_\mathfrak{l}, \mathbf{F}_\mathfrak{l}) \arrow[r] & \mathrm{Hom}(\mathbf{T} \otimes_{\mathbf{Z}} \mathbf{F}_\mathfrak{l}, \mathbf{F}_\mathfrak{l}) \arrow[r] & \mathrm{Hom}(\widetilde{I}_{\mathbf{e}} \otimes_{\mathbf{Z}} \mathbf{F}_\mathfrak{l}, \mathbf{F}_\mathfrak{l}) \arrow[r] & 0. \end{tikzcd}$$

L'application b est un isomorphisme d'après l'hypothèse (i). Une chasse au diagramme montre que a est injectif et $\mathrm{Ker}(c) = \mathrm{Coker}(a)$. Démontrons que c est injectif. Soit $f \in \mathbf{S}(\mathbf{F}_\mathfrak{l})$ vérifiant

$$b_1(tf) = 0 \qquad (t \in \widetilde{I}_{\mathbf{e}} \otimes_{\mathbf{Z}} \mathbf{F}_\mathfrak{l}).$$

Soit $s \in \widetilde{I}_{\mathbf{e}}$. Prouvons $sf = 0$. Comme b est surjectif, il existe $t_j \in \mathbf{T} \otimes_{\mathbf{Z}} \mathbf{F}_\mathfrak{l}$ vérifiant l'identité de formes linéaires $b_j = b_1 \circ t_j$ sur $\mathbf{S}(\mathbf{F}_\mathfrak{l})$ pour tout $j \geq 1$. On a alors

$$b_j(sf) = b_1(t_j sf) = 0 \qquad (j \geq 1),$$

car $t_j s \in \widetilde{I}_{\mathbf{e}} \otimes_{\mathbf{Z}} \mathbf{F}_\mathfrak{l}$. Par le principe du t-développement (proposition 4.9), la forme modulaire sf est donc nulle. On a montré que a est un isomorphisme. Donc le morphisme dual

$$\mathbf{T}/\widetilde{I}_{\mathbf{e}} \otimes_{\mathbf{Z}} \mathbf{F}_\mathfrak{l} \longrightarrow \mathrm{Hom}(M(\mathbf{F}_\mathfrak{l})[\widetilde{I}_{\mathbf{e}}], \mathbf{F}_\mathfrak{l}) \tag{5.3}$$

est un isomorphisme.

D'après le théorème 5.26, $u^{(d)}$ est une immersion formelle en $\infty_\mathfrak{l}^{(d)}$ si les restrictions de $b_1, \ldots, b_d$ à $M(\mathbf{F}_\mathfrak{l})[\widetilde{I}_{\mathbf{e}}]$ sont $\mathbf{F}_\mathfrak{l}$-linéairement indépendantes. Par l'isomorphisme (5.3), cette indépendance linéaire résulte de l'indépendance linéaire des images de $t_1, \ldots, t_d$ dans $\mathbf{T}/\widetilde{I}_{\mathbf{e}} \otimes_{\mathbf{Z}} \mathbf{F}_\mathfrak{l}$, qui est vérifiée d'après (ii). Cela démontre la première affirmation.

Si $\deg \mathfrak{n} = 3$, la condition (i) est vérifiée d'après le théorème 4.51.

Supposons $d = 1$ et $\deg \mathfrak{n} \geq 3$. L'hypothèse (ii) revient à dire que $t_1 = T_1$ est non nul dans $\mathbf{T}/\widetilde{I}_{\mathbf{e}} \otimes_{\mathbf{Z}} \mathbf{F}_{\mathfrak{l}}$. Par restriction des scalaires, il suffit de montrer que T_1 est non nul dans le $\mathbf{F}_p$-espace vectoriel $\mathbf{T}/\widetilde{I}_{\mathbf{e}}$. Or, d'après le théorème 2.60, comme $\deg \mathfrak{n} \geq 3$, $\widetilde{\mathbf{e}}$ est non nul dans $\mathbf{T}\widetilde{\mathbf{e}}$ donc $T_1 \neq 0$ dans $\mathbf{T}/\widetilde{I}_{\mathbf{e}}$.

Supposons $\deg \mathfrak{n} \geq 5$ et montrons que (ii) est vérifiée pour $d = q$. Les éléments $\theta_1, \ldots, \theta_q \in \mathbf{T} \otimes_{\mathbf{Z}} A$ du théorème 4.34 vérifient $b_i = b_1 \circ \theta_i$ $(1 \leq i \leq q)$ dans $\mathrm{Hom}(\mathbf{S}(A[1/\mathfrak{n}]), A[1/\mathfrak{n}])$. Par extension des scalaires, l'égalité est encore vérifiée dans $\mathrm{Hom}(\mathbf{S}(\mathbf{F}_{\mathfrak{l}}), \mathbf{F}_{\mathfrak{l}})$. Soient $t_1, \ldots, t_q$ les images de $\theta_1, \ldots, \theta_q$ dans $\mathbf{T} \otimes_{\mathbf{Z}} \mathbf{F}_{\mathfrak{l}}$. Il s'agit de démontrer que les images de $t_1, \ldots, t_q$ dans $\mathbf{T}/\widetilde{I}_{\mathbf{e}} \otimes_{\mathbf{Z}} \mathbf{F}_{\mathfrak{l}}$ sont $\mathbf{F}_{\mathfrak{l}}$-linéairement indépendantes. D'après le lemme 4.35, cela revient à montrer que les images de $T_{P_1}, \ldots, T_{P_q}$ dans $\mathbf{T}/\widetilde{I}_{\mathbf{e}} \otimes_{\mathbf{Z}} \mathbf{F}_{\mathfrak{l}}$ sont $\mathbf{F}_{\mathfrak{l}}$-linéairement indépendantes. Par restriction des scalaires, il suffit de montrer que les images de $T_{P_1}, \ldots, T_{P_q}$ dans $\mathbf{T}/\widetilde{I}_{\mathbf{e}}$ sont $\mathbf{F}_p$-linéairement indépendantes. Appliquons le théorème 2.60 : comme $\deg \mathfrak{n} \geq 5$, les symboles modulaires $T_{P_1}\widetilde{\mathbf{e}}, \ldots, T_{P_q}\widetilde{\mathbf{e}}$ sont $\mathbf{F}_p$-linéairement indépendants dans $\mathbf{T}\widetilde{\mathbf{e}}$. L'affirmation est donc démontrée. □

***Remarque* 5.29.** Supposons qu'il existe un ensemble de polynômes $\mathscr{E} = \{Q_1, \ldots, Q_d\}$ de A de degrés r fixé et une matrice $M \in \mathrm{GL}(d, \mathbf{F}_{\mathfrak{l}})$ tels qu'on ait l'égalité de vecteurs dans $(\mathbf{T} \otimes_{\mathbf{Z}} \mathbf{F}_{\mathfrak{l}})^d$

$$\begin{pmatrix} t_1 \\ \vdots \\ t_d \end{pmatrix} = M \begin{pmatrix} T_{Q_1} \\ \vdots \\ T_{Q_d} \end{pmatrix}.$$

Alors, d'après le théorème 2.60, l'hypothèse (ii) est vérifiée si $d > q$ et $\deg \mathfrak{n} \geq 2r + 3$.

Théorème 5.30. *Supposons qu'il existe un idéal premier* $\mathfrak{l}$ *de degré* 1 *tel que l'homomorphisme de* $\mathbf{F}_{\mathfrak{l}}$*-espaces vectoriels*

$$\begin{array}{rcl} \mathbf{T} \otimes_{\mathbf{Z}} \mathbf{F}_{\mathfrak{l}} & \longrightarrow & \mathrm{Hom}(\mathbf{S}(\mathbf{F}_{\mathfrak{l}}), \mathbf{F}_{\mathfrak{l}}) \\ t & \longmapsto & (f \mapsto b_1(tf)) \end{array}$$

est un isomorphisme. Alors :

(i) la courbe $Y_1(\mathfrak{n})$ *n'a pas de point défini sur une extension de* K *de degré* $\leq q$ *lorsque* $\deg \mathfrak{n} \geq \max(q+1, 5)$ *; en particulier, la conjecture 1.16 est vraie pour* $d \leq q$ *;*

(ii) la courbe $Y_1(\mathfrak{n})$ *n'a pas de point* K*-rationnel lorsque* $\deg \mathfrak{n} \geq 3$.

Démonstration. Appliquons le théorème 5.9 à l'idéal premier $\mathfrak{l}$. Le quotient $J'_{\mathbf{e}}(\mathfrak{n})$ n'a qu'un nombre fini de points K-rationnels d'après la proposition 3.28.

Si $\deg \mathfrak{n} \geq \max(q+1, 5)$ (resp. ≥ 3), le morphisme $u^{(q)}$ (resp. u) est une immersion formelle en $\infty_{\mathfrak{l}}^{(d)}$ (resp. $\infty_{\mathfrak{l}}$) d'après la proposition 5.28. Donc $Y_1(\mathfrak{n})$ n'a pas de point défini sur une extension de K de degré $\leq q$ (resp. 1). □

***Remarque* 5.31.** Lorsque $\mathfrak{n}$ est de degré 3, le théorème 5.30 est inconditionnel. Cependant, il apporte un résultat sur les points K-rationnels, plus faible que celui obtenu précédemment par le théorème 5.11.

Signalons une variante de cet énoncé sur les points de $X_0(\mathfrak{n})$, qui est une généralisation de la proposition 5.12.

Proposition 5.32. *Supposons que l'homomorphisme de* $\mathbf{F}_{\mathfrak{l}}$*-espaces vectoriels*

$$\begin{array}{rcl} \mathbf{T} \otimes_{\mathbf{Z}} \mathbf{F}_{\mathfrak{l}} & \longrightarrow & \mathrm{Hom}(\mathbf{S}(\mathbf{F}_{\mathfrak{l}}), \mathbf{F}_{\mathfrak{l}}) \\ t & \longmapsto & (f \mapsto b_1(tf)) \end{array}$$

est un isomorphisme. Alors tout module de Drinfeld sur K *de rang* 2 *possédant une* $\mathfrak{n}$*-isogénie cyclique* K*-rationnelle a bonne réduction potentielle en* $\mathfrak{l}$*.*

Démonstration. Reprenons la démonstration de la proposition 5.12 et ses notations. On obtient un point $y \in X_0(\mathfrak{n})(A[1/\mathfrak{n}])$ qui n'est pas une pointe et dont la spécialisation vérifie

$$u(y)_{\mathfrak{l}} = 0_{\mathfrak{l}}.$$

Comme $\deg \mathfrak{n} \geq 3$, d'après la proposition 5.28, le morphisme $X_0(\mathfrak{n}) \to \mathcal{J}'_{\mathbf{e}}(\mathfrak{n})$ est une immersion formelle en $\infty_{\mathfrak{l}}$. On conclut comme dans la démonstration du théorème 5.9. $\square$

Bibliographie

[AM69] Michael F. Atiyah et Ian G. Macdonald : *Introduction to commutative algebra*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.

[BLR90] Siegfried Bosch, Werner Lütkebohmert et Michel Raynaud : *Néron models*, volume 21 de *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1990.

[DD99] Sinnou David et Laurent Denis : Isogénie minimale entre modules de Drinfel′d. *Math. Ann.*, 315(1):97–140, 1999.

[Del73] Pierre Deligne : Les constantes des équations fonctionnelles des fonctions L. *In Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pages 501–597. Lecture Notes in Math., Vol. 349. Springer, Berlin, 1973.

[Den92] Laurent Denis : Hauteurs canoniques et modules de Drinfel′d. *Math. Ann.*, 294(2):213–223, 1992.

[Den95] Laurent Denis : Problèmes diophantiens sur les t-modules. *J. Théor. Nombres Bordeaux*, 7(1):97–110, 1995. Les Dix-huitièmes Journées Arithmétiques (Bordeaux, 1993).

[DR73] Pierre Deligne et Michael Rapoport : Les schémas de modules de courbes elliptiques. *In Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pages 143–316. Lecture Notes in Math., Vol. 349. Springer, Berlin, 1973.

[Dri74] Vladimir G. Drinfel′d : Elliptic modules. *Mat. Sb. (N.S.)*, 94(136):594–627, 656, 1974.

[Dri87] Vladimir G. Drinfel′d : Two-dimensional l-adic representations of the Galois group of a global field of characteristic p and automorphic forms on GL(2). *Journal of Soviet Mathematics*, 36(1):93–105, 1987.

[Gek80] Ernst-Ulrich Gekeler : *Drinfeld-Moduln und modulare Formen über rationalen Funktionenkörpern*. Bonner Mathematische Schriften [Bonn Mathematical Publications], 119. Universität Bonn Mathematisches Institut, Bonn, 1980. Dissertation, Rheinische Friedrich-Wilhelms-Universität, Bonn, 1979.

[Gek85] Ernst-Ulrich Gekeler : Automorphe Formen über $\mathbf{F}_q(T)$ mit kleinem Führer. *Abh. Math. Sem. Univ. Hamburg*, 55:111–146, 1985.

[Gek86a] Ernst-Ulrich Gekeler : *Drinfel′d modular curves*, volume 1231 de *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1986.

[Gek86b] Ernst-Ulrich Gekeler : Über Drinfeldsche Modulkurven vom Hecke-Typ. *Compositio Math.*, 57(2):219–236, 1986.

[Gek88a] Ernst-Ulrich Gekeler : On power sums of polynomials over finite fields. *J. Number Theory*, 30(1):11–26, 1988.

[Gek88b] Ernst-Ulrich Gekeler : On the coefficients of Drinfel′d modular forms. *Invent. Math.*, 93(3):667–700, 1988.

[Gek91] Ernst-Ulrich Gekeler : On finite Drinfel′d modules. *J. Algebra*, 141(1):187–203, 1991.

[Gek95a] Ernst-Ulrich Gekeler : Analytical construction of Weil curves over function fields. *J. Théor. Nombres Bordeaux*, 7(1):27–49, 1995. Les Dix-huitièmes Journées Arithmétiques (Bordeaux, 1993).

[Gek95b] Ernst-Ulrich Gekeler : Improper Eisenstein series on Bruhat-Tits trees. *Manuscripta Math.*, 86(3):367–391, 1995.

[Gek97a] Ernst-Ulrich Gekeler : Jacquet-Langlands theory over K and relations with elliptic curves. *In Drinfeld modules, modular schemes and applications (Alden-Biesen, 1996)*, pages 224–257. World Sci. Publ., River Edge, NJ, 1997.

[Gek97b] Ernst-Ulrich Gekeler : On the cuspidal divisor class group of a Drinfeld modular curve. *Doc. Math.*, 2:351–374 (electronic), 1997.

[Gek01] Ernst-Ulrich Gekeler : Invariants of some algebraic curves related to Drinfeld modular curves. *J. Number Theory*, 90(1):166–183, 2001.

[GN95] Ernst-Ulrich Gekeler et Udo Nonnengardt : Fundamental domains of some arithmetic groups over function fields. *Internat. J. Math.*, 6(5):689–708, 1995.

[Gos79] David Goss : v-adic zeta functions, L-series and measures for function fields. *Invent. Math.*, 55(2):107–119, 1979. With an addendum.

[Gos80a] David Goss : The algebraist's upper half-plane. *Bull. Amer. Math. Soc. (N.S.)*, 2(3):391–415, 1980.

[Gos80b] David Goss : Modular forms for $\mathbf{F}_r[T]$. *J. Reine Angew. Math.*, 317:16–39, 1980.

[Gos80c] David Goss : π-adic Eisenstein series for function fields. *Compositio Math.*, 41(1):3–38, 1980.

[Gos82] David Goss : Kummer and Herbrand criterion in the theory of function fields. *Duke Math. J.*, 49(2):377–384, 1982.

[Gos96] David Goss : *Basic structures of function field arithmetic*, volume 35 de *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1996.

[GR96] Ernst-Ulrich Gekeler et Marc Reversat : Jacobians of Drinfeld modular curves. *J. Reine Angew. Math.*, 476:27–93, 1996.

[Gro60] Alexander Grothendieck : Éléments de géométrie algébrique. I. Le langage des schémas. *Inst. Hautes Études Sci. Publ. Math.*, (4):228, 1960.

[Gro67] Alexander Grothendieck : Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas IV. *Inst. Hautes Études Sci. Publ. Math.*, (32):361, 1967.

[GvdPRVG97] Ernst-Ulrich Gekeler, Marius van der Put, Marc Reversat et Jan Van Geel, éditeurs. *Drinfeld modules, modular schemes and applications*, River Edge, NJ, 1997. World Scientific Publishing Co. Inc.

[Har77] Robin Hartshorne : *Algebraic geometry.* Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52.

[Hru96] Ehud Hrushovski : The Mordell-Lang conjecture for function fields. *J. Amer. Math. Soc.*, 9(3):667–690, 1996.

[IS00] Henryk Iwaniec et Peter Sarnak : The non-vanishing of central values of automorphic L-functions and Landau-Siegel zeros. *Israel J. Math.*, 120(part A):155–177, 2000.

[Kam92a] Sheldon Kamienny : Torsion points on elliptic curves and q-coefficients of modular forms. *Invent. Math.*, 109(2):221–229, 1992.

[Kam92b] Sheldon Kamienny : Torsion points on elliptic curves over fields of higher degree. *Internat. Math. Res. Notices*, (6):129–133, 1992.

[Kat73] Nicholas M. Katz : p-adic properties of modular schemes and modular forms. *In Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pages 69–190. Lecture Notes in Mathematics, Vol. 350. Springer, Berlin, 1973.

[KL89] Victor A. Kolyvagin et Dmitry Yu. Logachëv : Finiteness of the Shafarevich-Tate group and the group of rational points for some modular abelian varieties. *Algebra i Analiz*, 1(5):171–196, 1989.

[KM85] Nicholas M. Katz et Barry Mazur : *Arithmetic moduli of elliptic curves*, volume 108 de *Annals of Mathematics Studies.* Princeton University Press, Princeton, NJ, 1985.

[KM95] Sheldon Kamienny et Barry Mazur : Rational torsion of prime order in elliptic curves over number fields. *Astérisque*, 3(228):81–100, 1995. With an appendix by A. Granville, Columbia University Number Theory Seminar (New York, 1992).

[KT03] Kazuya Kato et Fabien Trihan : On the conjectures of Birch and Swinnerton-Dyer in characteristic $p > 0$. *Invent. Math.*, 153(3):537–592, 2003.

[Lan83] Serge Lang : *Fundamentals of Diophantine geometry.* Springer-Verlag, New York, 1983.

[Lee43] Herbert L. Lee : Power sums of polynomials in a Galois field. *Duke Math. J.*, 10:277–292, 1943.

[LK79] Knud Lønsted et Steven L. Kleiman : Basics on families of hyperelliptic curves. *Compositio Math.*, 38(1):83–111, 1979.

[Man69] Yuri I. Manin : The p-torsion of elliptic curves is uniformly bounded. *Izv. Akad. Nauk SSSR Ser. Mat.*, 33:459–465, 1969.

[Man72] Yuri I. Manin : Parabolic points and zeta functions of modular curves. *Izv. Akad. Nauk SSSR Ser. Mat.*, 36:19–66, 1972.

[Maz77] Barry Mazur : Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, (47):33–186 (1978), 1977.

[Maz78] Barry Mazur : Rational isogenies of prime degree (with an appendix by D. Goldfeld). *Invent. Math.*, 44(2):129–162, 1978.

[Mer94] Loïc Merel : Universal Fourier expansions of modular forms. *In On Artin's conjecture for odd* 2*-dimensional representations*, volume 1585 de *Lecture Notes in Math.*, pages 59–94. Springer, Berlin, 1994.

[Mer96] Loïc Merel : Bornes pour la torsion des courbes elliptiques sur les corps de nombres. *Invent. Math.*, 124(1-3):437–449, 1996.

[Mil68] James Milne : The Tate-Šafarevič group of a constant abelian variety. *Invent. Math.*, 6:91–105, 1968.

[Mil75] James Milne : On a conjecture of Artin and Tate. *Ann. of Math. (2)*, 102(3):517–533, 1975.

[Mil80] James Milne : *Étale cohomology*, volume 33 de *Princeton Mathematical Series*. Princeton University Press, Princeton, N.J., 1980.

[Mil86] James Milne : Jacobian varieties. *In Arithmetic geometry (Storrs, Conn., 1984)*, pages 167–212. Springer, New York, 1986.

[NY01] Viet NguyenKhac et Shin-ichiro Yamada : On d-gonality of Drinfel′d modular curves and strong uniform boundedness conjecture. *Proc. Japan Acad. Ser. A Math. Sci.*, 77(7):126–129, 2001.

[Oes] Joseph Oesterlé : Torsion des courbes elliptiques sur les corps de nombres. Non publié.

[Ogg78] Andrew P. Ogg : On the Weierstrass points of $X_0(N)$. *Illinois J. Math.*, 22(1):31–35, 1978.

[Pál05] Ambrus Pál : On the torsion of the Mordell-Weil group of the Jacobian of Drinfeld modular curves. *Doc. Math.*, 10:131–198 (electronic), 2005.

[Pál07a] Ambrus Pál : On the Eisenstein ideal of Drinfeld modular curves. *Int. J. Number Theory*, 3(4):557–598, 2007.

[Pál07b] Ambrus Pál : *On the torsion of Drinfeld modules of rank two.* Prépublication arXiv :0708.4243v2, 2007.

[Pap07] Mihran Papikian : Abelian subvarieties of Drinfeld Jacobians and congruences modulo the characteristic. *Math. Ann.*, 337(1):139–157, 2007.

[Par99] Pierre Parent : Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres. *J. Reine Angew. Math.*, 506:85–116, 1999.

[Poo95] Bjorn Poonen : Local height functions and the Mordell-Weil theorem for Drinfel′d modules. *Compositio Math.*, 97(3):349–368, 1995.

[Poo97] Bjorn Poonen : Torsion in rank 1 Drinfeld modules and the uniform boundedness conjecture. *Math. Ann.*, 308(4):571–586, 1997.

[Poo98] Bjorn Poonen : The classification of rational preperiodic points of quadratic polynomials over $\mathbf{Q}$: a refined conjecture. *Math. Z.*, 228(1):11–29, 1998.

[Ray70] Michel Raynaud : Spécialisation du foncteur de Picard. *Inst. Hautes Études Sci. Publ. Math.*, (38):27–76, 1970.

[Ray71] Michel Raynaud : Variétés abéliennes et géométrie rigide. *In Actes du Congrès International des Mathématiciens (Nice, 1970), Tome 1*, pages 473–477. Gauthier-Villars, Paris, 1971.

[Ray74] Michel Raynaud : Schémas en groupes de type $(p, \ldots, p)$. *Bull. Soc. Math. France*, 102:241–280, 1974.

[Rev00] Marc Reversat : On modular forms of characteristic $p > 0$. *J. Number Theory*, 84(2):214–229, 2000.

[Ros03] Michael Rosen : Formal Drinfeld modules. *J. Number Theory*, 103(2): 234–256, 2003.

[Sch82] Peter Schneider : Zur Vermutung von Birch und Swinnerton-Dyer über globalen Funktionenkörpern. *Math. Ann.*, 260(4):495–510, 1982.

[Sch97] Andreas Schweizer : Hyperelliptic Drinfeld modular curves. *In Drinfeld modules, modular schemes and applications (Alden-Biesen, 1996)*, pages 330–343. World Sci. Publ., River Edge, NJ, 1997.

[Sch01] Andreas Schweizer : Bielliptic Drinfeld modular curves. *Asian J. Math.*, 5(4):705–720, 2001.

[Sch03] Andreas Schweizer : On the uniform boundedness conjecture for Drinfeld modules. *Math. Z.*, 244(3):601–614, 2003.

[Sch04] Andreas Schweizer : On periodic points under the iteration of additive polynomials. *Manuscripta Math.*, 113(1):25–34, 2004.

[Ser77] Jean-Pierre Serre : *Arbres, amalgames,* SL_2. Société Mathématique de France, Paris, 1977. Avec un sommaire anglais, Rédigé avec la collaboration de Hyman Bass, Astérisque, No. 46.

[Shi92] Tetsuji Shioda : Some remarks on elliptic curves over function fields. *Astérisque*, (209):12, 99–114, 1992. Journées Arithmétiques, 1991 (Geneva).

[Tae06] Lenny Taelman : *Drinfeld modular curves have many points.* Prépublication arXiv :math/0602157v1, 2006.

[Tam95] Akio Tamagawa : The Eisenstein quotient of the Jacobian variety of a Drinfel′d modular curve. *Publ. Res. Inst. Math. Sci.*, 31(2):203–246, 1995.

[Tan93] Ki-Seng Tan : Modular elements over function fields. *J. Number Theory*, 45(3):295–311, 1993.

[Tat66] John Tate : On the conjectures of Birch and Swinnerton-Dyer and a geometric analog. *In Séminaire Bourbaki, Vol. 9*, pages Exp. No. 306, 415–440. Soc. Math. France, Paris, 1966.

[Tei91] Jeremy Teitelbaum : The Poisson kernel for Drinfeld modular curves. *J. Amer. Math. Soc.*, 4(3):491–511, 1991.

[Tei92a] Jeremy Teitelbaum : Modular symbols for $\mathbf{F}_q(T)$. *Duke Math. J.*, 68(2):271–295, 1992.

[Tei92b] Jeremy Teitelbaum : Rigid analytic modular forms : an integral transform approach. *In The arithmetic of function fields (Columbus, OH, 1991)*, volume 2 de *Ohio State Univ. Math. Res. Inst. Publ.*, pages 189–207. de Gruyter, Berlin, 1992.

[TR92] Ki-Seng Tan et Daniel Rockmore : Computation of L-series for elliptic curves over function fields. *J. Reine Angew. Math.*, 424:107–135, 1992.

[vdH06] Gert-Jan van der Heiden : Drinfeld modular curve and Weil pairing. *J. Algebra*, 299(1):374–418, 2006.

[Wei71] André Weil : *Dirichlet series and automorphic forms*, volume 189 de *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1971.

Index des notations

$d_{\mathbf{e}}$, 55

$\mathbf{e}$, 52
$\widetilde{\mathbf{e}}$, 55
$\eta_{\mathfrak{m}}$, 54

$\mathscr{F}$, 68

$g(X_0(\mathfrak{n}))$, 23

$\mathbf{H}$, 28
$\mathbf{H}(R)$, 28
(H_F), 104
(H_I), 76

$\widehat{I}$, 76
$I_{\mathbf{e}}$, 69
$\widetilde{I}_{\mathbf{e}}$, 76

$J_0(\mathfrak{n})$, 64
$J_0(\mathfrak{n})^-$, 68
$J_0(\mathfrak{n})_-$, 68
$J_0(\mathfrak{n})^+$, 68
$J_{\mathbf{e}}(\mathfrak{n})$, 69
$J'_{\mathbf{e}}(\mathfrak{n})$, 76

$\mathcal{M}_0(\mathfrak{n})$, 22
$\mathcal{M}_1(\mathfrak{n})$, 22
$\mathbf{M}$, 40
$\mathbf{M}(R)$, 40
$\mathbf{M}^0$, 40
$\mathbf{M}^0(R)$, 40

$n(\mathfrak{n})$, 66

$\mathscr{P}_r$, 55

$\mathbf{S}(R)$, 84

$\mathcal{T}$, 26

$\theta_1, \ldots, \theta_q$, 97
$T_{\mathfrak{m}}$, 33, 41, 65, 87, 88
$\mathbf{T}$, 33, 41, 67, 87

$w_{\mathfrak{m}}$, 33, 41, 64, 87

$X_0(\mathfrak{n})$, 23
$X_0(\mathfrak{n})^+_K$, 68
$X_1(\mathfrak{n})$, 23

$Y_0(\mathfrak{n})$, 22
$Y_1(\mathfrak{n})$, 22