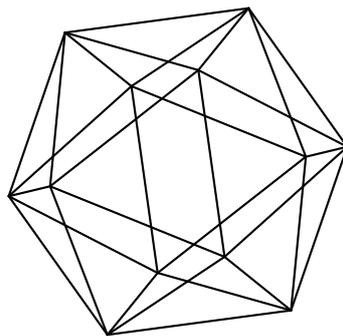


Max-Planck-Institut für Mathematik Bonn

Sur les symboles modulaires de Manin-Teitelbaum pour
 $\mathbf{F}_q(T)$

by

Cécile Armana



Sur les symboles modulaires de Manin-Teitelbaum pour $\mathbf{F}_q(T)$

Cécile Armana

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

SUR LES SYMBOLES MODULAIRES DE MANIN–TEITELBAUM POUR $\mathbf{F}_q(T)$

par

Cécile Armana

Résumé. — Les symboles modulaires pour le sous-groupe $\Gamma_0(\mathfrak{n})$ de $\mathrm{GL}_2(\mathbf{F}_q[T])$ définis par Teitelbaum possèdent une présentation par un nombre fini de générateurs et leurs relations. Dans ce travail, on utilise cette présentation pour obtenir un énoncé d’indépendance linéaire d’opérateurs de Hecke dans les symboles modulaires. Pour cela, on exprime d’abord l’action des opérateurs de Hecke en termes des générateurs de Manin–Teitelbaum. Puis, si \mathfrak{n} est premier de degré impair, on résout complètement les relations pour obtenir une base explicite de générateurs. On déduit de ces énoncés un résultat de non-annulation de fonctions L de certaines formes automorphes primitives pour $\mathbf{F}_q(T)$.

Abstract. — Modular symbols for the subgroup $\Gamma_0(\mathfrak{n})$ of $\mathrm{GL}_2(\mathbf{F}_q[T])$, as defined by Teitelbaum, have a presentation given by a finite number of generators and relations among them. In this work, we use this presentation to get a statement of linear independence for Hecke operators on modular symbols. For that purpose, we first give formulas for the action of Hecke operators in terms of Manin–Teitelbaum generators. Then, if \mathfrak{n} is a prime of odd degree, we completely solve the relations and get an explicit basis of generators. We derive a non-vanishing statement for L -functions of certain primitive automorphic forms for $\mathbf{F}_q(T)$.

1. Introduction

Soient $A = \mathbf{F}_q[T]$ l’anneau de polynômes sur un corps fini \mathbf{F}_q à q éléments en l’indéterminée T et $K = \mathbf{F}_q(T)$ son corps des fractions. Dans [30], J. Teitelbaum a développé une théorie de symboles modulaires de poids 2 pour un sous-groupe de congruence Γ de $\mathrm{GL}_2(A)$. Parmi ses applications, citons des formules pour les valeurs spéciales de fonctions L de certaines formes automorphes pour K au centre de symétrie [28, 29, 30] ainsi qu’une conjecture de zéro exceptionnel pour les courbes elliptiques sur K [30], qui a été établie par Hauer et Longhi [11] (voir aussi Pál [22] pour un résultat similaire démontré indépendamment).

Teitelbaum a donné une présentation de ces symboles modulaires par un nombre fini de générateurs et leurs relations dans un formalisme analogue à celui de Manin [14]. Soit

Classification mathématique par sujets (2010). — 11F67 (primaire) ; 11F75, 11G09 (secondaire).

$\Gamma_0(\mathfrak{n}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(A) \mid c \in \mathfrak{n} \right\}$ pour un idéal non nul \mathfrak{n} de A . Sur l'anneau fini A/\mathfrak{n} , considérons la droite projective $\mathbf{P}^1(A/\mathfrak{n})$ dont on note les éléments $(u : v)$. Le groupe $\mathbf{M}_{\mathfrak{n}}$ des symboles modulaires pour $\Gamma_0(\mathfrak{n})$ à valeurs dans \mathbf{Z} est isomorphe au quotient du groupe abélien libre $\mathbf{Z}[\mathbf{P}^1(A/\mathfrak{n})]$ par les relations

$$(1) \quad \begin{aligned} (u : v) + (-v : u) &= 0 \\ (u : v) + (v : -u - v) + (-u - v : u) &= 0 \\ (u : v) - (du : d'v) &= 0 \end{aligned}$$

pour $d, d' \in \mathbf{F}_q^\times$ et $(u : v) \in \mathbf{P}^1(A/\mathfrak{n})$. Les générateurs correspondants de $\mathbf{M}_{\mathfrak{n}}$ sont notés $\xi(u : v)$ et appelés *symboles de Manin–Teitelbaum*. Dans ce travail, on utilise la présentation pour établir un énoncé d'indépendance linéaire d'opérateurs de Hecke dans $\mathbf{M}_{\mathfrak{n}}$ (théorème 1.3). Ce faisant, on obtient des résultats d'intérêt indépendant concernant la présentation. L'énoncé d'indépendance linéaire intervient dans une étude de la torsion des modules de Drinfeld de rang 2 qui devrait faire l'objet d'un autre article.

1.1. Action de Hecke sur les symboles de Manin–Teitelbaum. — L'opérateur de Hecke $T_{\mathfrak{m}}$, pour \mathfrak{m} idéal non nul de A , est un endomorphisme de $\mathbf{M}_{\mathfrak{n}}$. L'énoncé suivant exprime son action en termes de symboles de Manin–Teitelbaum.

Théorème 1.1. — *Pour tout idéal \mathfrak{m} et $(u : v) \in \mathbf{P}^1(A/\mathfrak{n})$, on a*

$$T_{\mathfrak{m}} \xi(u : v) = \sum_{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{S}_{\mathfrak{m}}} \xi(au + cv : bu + dv)$$

où $\mathcal{S}_{\mathfrak{m}}$ est l'ensemble fini des matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ à coefficients dans A avec $\deg a > \deg b$, $\deg d > \deg c$, $(ad - bc) = \mathfrak{m}$, a et d unitaires et la somme est restreinte aux matrices telles que $(au + cv : bu + dv)$ est défini dans $\mathbf{P}^1(A/\mathfrak{n})$.

L'énoncé et sa preuve sont à rapprocher de ceux de Merel [18] pour les symboles modulaires sur \mathbf{Q} qui font suite aux travaux de Manin [14] et Mazur [15] sur les matrices de Heilbronn. L'ensemble $\mathcal{S}_{\mathfrak{m}}$ étant indépendant de \mathfrak{n} , le théorème 1.1 entraîne une loi de réciprocité pour les courbes elliptiques sur K (proposition 5.6).

D'un point de vue algorithmique, le théorème 1.1 fournit une méthode pour calculer l'action des opérateurs de Hecke sur $\mathbf{M}_{\mathfrak{n}}$ (voir la section 5.3).

1.2. Base explicite de symboles de Manin–Teitelbaum. —

Théorème 1.2. — *Soit \mathfrak{n} un idéal premier de degré impair $d \geq 3$. Les symboles de Manin–Teitelbaum $\xi(0 : 1)$ et $\xi(u : v)$, pour u et v polynômes unitaires de A , premiers entre eux tels que $\deg v < \deg u < d/2$, forment une base de $\mathbf{M}_{\mathfrak{n}}$ sur \mathbf{Z} .*

C'est un cas particulier du théorème 6.4 qui précise que la famille est libre si d est pair. La démarche consiste à résoudre les relations de Manin–Teitelbaum de façon explicite dans une variante de l'espace des symboles modulaires (proposition 6.3). En particulier, on donne dans le théorème 6.6 l'expression de tout symbole de Manin–Teitelbaum dans la base quand d est impair. Les théorèmes 1.2 et 6.6 n'ont pas d'analogues pour les symboles modulaires sur \mathbf{Q} . Ils simplifient le calcul des symboles modulaires pour $\mathbf{F}_q(T)$ sur machine puisque les relations de Manin–Teitelbaum sont résolues.

Cette base permet de retrouver la formule pour le genre de la courbe modulaire de Drinfeld associée à $\Gamma_0(\mathfrak{n})$ (remarque 6.5). Comme autre corollaire, on décrit le groupe des symboles paraboliques comme module pour l'algèbre de Hecke : si \mathfrak{n} est premier de degré 3, il est isomorphe à l'idéal d'Eisenstein *via* un homomorphisme d'enroulement dans l'esprit de Mazur (section 8).

La base explicite remplace avantageusement la présentation de Teitelbaum. Cela incite à étudier son existence dans des situations plus générales (\mathfrak{n} de degré pair ou non premier, autres sous-groupes de congruence, poids supérieur).

1.3. Indépendance linéaire d'opérateurs de Hecke dans \mathbf{M}_n . — Soit $\mathbf{H}_n(\mathbf{C})$ le \mathbf{C} -espace vectoriel des cochaînes harmoniques paraboliques pour $\Gamma_0(\mathfrak{n})$ à valeurs dans \mathbf{C} . D'après Drinfeld, il s'identifie à un certain espace de formes automorphes paraboliques pour K (voir la section 3.2 pour des rappels). Pour F dans $\mathbf{H}_n(\mathbf{C})$, la fonction L notée $L(F, s)$ est un polynôme en q^{-s} pour la variable complexe s . Elle satisfait une équation fonctionnelle dont le centre de symétrie est $s = 1$.

Teitelbaum a mis en évidence un accouplement, compatible aux opérateurs de Hecke et parfait sur \mathbf{C} , entre $\mathbf{H}_n(\mathbf{C})$ et le sous-espace des symboles modulaires paraboliques $\mathbf{M}_n^0(\mathbf{C})$. La forme linéaire $F \mapsto (q-1)L(F, 1)$ sur $\mathbf{H}_n(\mathbf{C})$ définit alors un symbole modulaire \mathbf{e} dans $\mathbf{M}_n^0(\mathbf{C})$ (voir section 7.1). Par analogie avec la situation classique, on l'appelle *élément d'enroulement*. De la formule du théorème 1.1 et de la famille libre du théorème 6.4, on déduit un énoncé d'indépendance linéaire d'opérateurs de Hecke en \mathbf{e} .

Théorème 1.3. — *Si \mathfrak{n} est premier de degré ≥ 3 et r est la partie entière de $(\deg(\mathfrak{n}) - 3)/2$, alors la famille $T_{\mathfrak{m}}\mathbf{e}$, pour \mathfrak{m} de degré r , est libre sur \mathbf{Z} .*

C'est un cas particulier du théorème 7.12. Il est à rapprocher d'énoncés de Merel (proposition 3 de [19]), Parent (proposition 1.9 de [24]) et VanderKam (théorème 0.1 de [31]) pour les symboles modulaires sur \mathbf{Q} . Dans le cas classique, de telles estimations jouent un rôle central dans la preuve d'une borne uniforme pour la torsion des courbes elliptiques sur les corps de nombres ([19], [24] pour une version explicite).

Mentionnons une application du théorème 1.3 aux formes automorphes sur K . Lorsque \mathfrak{n} est premier, l'espace $\mathbf{H}_n(\mathbf{C})$ possède une base \mathcal{F}_n de formes propres pour tous les $T_{\mathfrak{m}}$ et normalisées. À \mathfrak{n} fixé, on minore le nombre de formes de \mathcal{F}_n dont la fonction L ne s'annule pas en $s = 1$.

Théorème 1.4. — *Soit \mathfrak{n} un idéal premier de degré ≥ 3 . On a*

$$\#\{F \in \mathcal{F}_n \mid L(F, 1) \neq 0\} \geq \frac{(q^2 - 1)^{1/2}}{q^2} (\#\mathcal{F}_n)^{1/2}.$$

L'exposant $1/2$ pour la dimension de l'espace est meilleur que ceux de Parent ($1/6$) et VanderKam ($1/2 + \varepsilon$ pour tout $\varepsilon > 0$) pour les formes modulaires classiques. Pour ces dernières, la théorie analytique des nombres fournit même des estimations linéaires en la dimension de l'espace, comme dans Kowalski–Michel [13] et Iwaniec–Sarnak [12]. Sur $\mathbf{F}_q(T)$, on peut s'attendre à une borne linéaire, dont on ne dispose pas actuellement à ma connaissance.

2. Notations

Soient q une puissance d'un nombre premier p et \mathbf{F}_q (resp. \mathbf{F}_p) un corps fini à q (resp. p) éléments. On munit l'anneau $A = \mathbf{F}_q[[T]]$ en l'indéterminée T du degré usuel \deg avec la convention $\deg 0 = -\infty$. Le *degré* d'un idéal non nul de A est celui de l'un de ses générateurs. On appellera *premiers de A* les idéaux premiers non nuls de A .

Soit $K = \mathbf{F}_q(T)$ le corps des fractions de A . On distingue sa place non-archimédienne ∞ donnée par $\pi = 1/T$. Par la suite, la notation ∞ désignera aussi un bout ou une pointe de l'arbre de Bruhat–Tits mais, d'après le contexte, il n'y aura pas de confusion possible. Le complété $K_\infty = \mathbf{F}_q((\pi))$ de K pour ∞ est muni de la valeur absolue $|\cdot|$ normalisée par $|T| = q$.

Le schéma en groupes $\mathrm{GL}(2)$ est noté G et son centre Z . Sauf mention contraire, Γ désigne le sous-groupe de congruence $\Gamma_0(\mathfrak{n})$ pour un idéal propre \mathfrak{n} de A .

Pour P, Q dans A , (P) est l'idéal engendré par P et $P \mid Q$ signifie P divise Q . Les lettres gothiques désigneront des idéaux de A .

3. Cochaînes harmoniques paraboliques

Soit $O_\infty = \mathbf{F}_q[[\pi]]$ l'anneau des entiers π -adiques. Le sous-groupe d'Iwahori \mathcal{I} est formé des matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ de $G(O_\infty)$ avec $c \equiv 0 \pmod{\pi}$.

3.1. L'arbre de Bruhat–Tits \mathcal{T} . — Soit \mathcal{T} l'arbre de Bruhat–Tits de $\mathrm{PGL}(2, K_\infty)$ (voir [26] ou [10]). C'est le graphe $(q+1)$ -régulier dont l'ensemble des sommets est $X(\mathcal{T}) = G(K_\infty)/G(O_\infty) \cdot Z(K_\infty)$, celui des arêtes orientées est $Y(\mathcal{T}) = G(K_\infty)/\mathcal{I} \cdot Z(K_\infty)$ et l'application canonique $Y(\mathcal{T}) \rightarrow X(\mathcal{T})$ associe à chaque arête son origine.

Les bouts de \mathcal{T} sont les classes d'équivalence de demi-droites de \mathcal{T} (*i.e.* de suites infinies d'arêtes adjacentes indexées par \mathbf{N}) où deux demi-droites sont dites équivalentes si elles diffèrent d'un nombre fini d'arêtes. Les bouts sont en bijection naturelle avec $\mathbf{P}^1(K_\infty)$. Cette bijection est toutefois non canonique : nous la fixons en prenant la convention du paragraphe 1.6 de [10]. Comme \mathcal{T} est un arbre, deux bouts donnés définissent une unique géodésique (c'est-à-dire un unique chemin sans aller-retour) les reliant dans \mathcal{T} . Le bout $\infty = (1 : 0) \in \mathbf{P}^1(K)$ est représenté par la demi-droite donnée par les images de $\left\{ \begin{pmatrix} \pi^k & 0 \\ 0 & 1 \end{pmatrix} \right\}_{k \geq 0}$ dans $Y(\mathcal{T})$. De même, le bout $0 = (0 : 1)$ est représenté par $\left\{ \begin{pmatrix} \pi^k & 0 \\ 0 & 1 \end{pmatrix} \right\}_{k \leq 0}$.

Le groupe $G(K_\infty)$ opère par multiplication à gauche sur \mathcal{T} . Soit Γ un sous-groupe de congruence de $G(A)$. Il opère sur \mathcal{T} en préservant la structure simpliciale et on définit alors le graphe quotient $\Gamma \backslash \mathcal{T}$, dont l'ensemble des sommets est $\Gamma \backslash X(\mathcal{T})$ et celui des arêtes orientées est $\Gamma \backslash Y(\mathcal{T})$. D'après Serre [26, II, théorème 9], le graphe $\Gamma \backslash \mathcal{T}$ est la réunion, disjointe sur les arêtes, d'un graphe fini et d'un ensemble fini de demi-droites disjointes indexées par les éléments de $\Gamma \backslash \mathbf{P}^1(K)$. On appelle ces demi-droites les *pointes* de $\Gamma \backslash \mathcal{T}$ et on note **ptes** leur ensemble. Pour la détermination explicite de tels « domaines fondamentaux » de $\Gamma \backslash \mathcal{T}$, on pourra consulter Gekeler [3] et Gekeler–Nonnengardt [9].

3.2. Les cochaînes harmoniques paraboliques. — Soit R un anneau commutatif. Les cochaînes harmoniques paraboliques pour $\Gamma = \Gamma_0(\mathfrak{n})$ à valeurs dans R sont des fonctions $Y(\mathcal{T}) \rightarrow R$ vérifiant des propriétés d'alternance et d'harmonicité, invariantes par Γ et à support fini modulo Γ (voir par exemple [10, section 3] pour leur définition).

On note $\mathbf{H}_n(R)$, ou encore $\mathbf{H}(R)$, leur R -module ; lorsque $R = \mathbf{Z}$, on le note \mathbf{H}_n ou encore \mathbf{H} .

Soit g le nombre de cycles indépendants du graphe $\Gamma \setminus \mathcal{T}$. Il coïncide avec le genre de la courbe modulaire de Drinfeld X_Γ associée à Γ ([1, théorème 2], [10, section 4]). Si R est sans torsion sur \mathbf{Z} , on a un isomorphisme canonique $\mathbf{H} \otimes_{\mathbf{Z}} R \simeq \mathbf{H}(R)$ entre R -modules libres de rang g . Dans le cas où n est premier de degré d , les formules suivantes de Gekeler donnent la valeur de g :

$$(2) \quad g = \begin{cases} \frac{q^d - q^2}{q^2 - 1} & \text{si } d \text{ est pair ;} \\ \frac{q^d - q}{q^2 - 1} & \text{si } d \text{ est impair} \end{cases}$$

(théorème 3.4.18 de [2]). En particulier, il est non nul dès que $d \geq 3$.

Rappelons comment $\mathbf{H}_n(\mathbf{C})$ s'identifie à un espace de formes automorphes paraboliques, d'après Drinfeld ([1, proposition 10.3], [10, section 4]). Soient \mathbf{A}_K l'anneau des adèles de K , \mathbf{O} son anneau des entiers et $\mathbf{O} = \mathbf{O}_f \times \mathbf{O}_\infty$. On note D_n le diviseur positif de K associé à l'idéal n . Considérons le sous-groupe ouvert $\mathcal{K}_0(n)_f = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid c \equiv 0 \pmod{D_n} \right\}$ de $G(\mathbf{O}_f)$. Le théorème d'approximation forte pour K identifie alors $\mathbf{H}_n(\mathbf{C})$ à l'espace des fonctions

$$G(K) \backslash G(\mathbf{A}_K) / (\mathcal{K}_0(n)_f \times \mathcal{I} \cdot \mathbf{Z}(K_\infty)) \longrightarrow \mathbf{C}$$

qui sont paraboliques et spéciales en ∞ , au sens de Drinfeld.

Toute cochaîne F de $\mathbf{H}(\mathbf{C})$ admet un développement de Fourier indexé par les idéaux de A (voir Weil [32] et Tan [28] pour un point de vue adélique, Gekeler [2, 6] pour un point de vue en la place ∞). Sa fonction L notée $L(F, s)$ est définie comme la série de Dirichlet associée aux coefficients de Fourier. C'est une fonction de la variable complexe s qui converge absolument dans le demi-plan des s de partie réelle > 1 . Rappelons l'expression comme transformée de Mellin qui se déduit de son produit eulérien. Soit w_n l'involution de $\mathbf{H}(\mathbf{C})$ définie par

$$(w_n F)(e) = F \left(\begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix} e \right) \quad (F \in \mathbf{H}(\mathbf{C}), e \in Y(\mathcal{T}))$$

où N est le générateur unitaire de n .

Proposition 3.1. — *Pour tout $s \in \mathbf{C}$ de partie réelle > 1 , on a*

$$(3) \quad L(F, s) = \frac{1}{q-1} \sum_{k \in \mathbf{Z}} F \left(\begin{pmatrix} \pi^k & 0 \\ 0 & 1 \end{pmatrix} \right) q^{(2-k)(s-1)}.$$

Cette formule définit un unique prolongement holomorphe de $L(F, s)$ à \mathbf{C} . Il vérifie

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

De plus, la somme de (3) est finie et $L(F, s)$ est un polynôme en q^{-s} de degré $\leq \deg(n) - 3$.

Pour ces résultats, on peut consulter Weil [32, VII théorème 2], Tan [28, proposition 2 et équation 3.4], Tan–Rockmore [29, proposition 1] pour une présentation adélique et Gekeler [6, section 3] en la place ∞ . En particulier, $L(F, s)$ a un zéro d'ordre impair si $w_n F = +F$ et un zéro d'ordre pair (ou pas de zéro) si $w_n F = -F$. Lorsque n est premier et F primitive, $L(F, s)$ est même un polynôme en q^{-s} de degré $\deg(n) - 3$ et de terme constant 1 ([28, p. 305]).

La valeur en $s = 1$ est essentiellement donnée en sommant les valeurs de F le long de la géodésique de \mathcal{T} reliant les bouts 0 et ∞ :

$$(4) \quad L(F, 1) = \frac{1}{q-1} \sum_{k \in \mathbf{Z}} F \left(\begin{pmatrix} \pi^k & 0 \\ 0 & 1 \end{pmatrix} \right)$$

(la somme ne porte que sur un nombre fini de termes).

3.3. Les opérateurs de Hecke. — L'espace $\mathbf{H}(\mathbf{C})$ est muni d'un produit de Petersson $(\ , \)_\mu$ provenant de celui sur les formes automorphes. On peut voir les éléments de $\mathbf{H}(\mathbf{C})$ comme des fonctions à support fini sur les arêtes du graphe $\Gamma \backslash \mathcal{T}$: le produit de Petersson correspond alors à la norme L^2 sur l'ensemble discret des arêtes, en prenant pour volume d'une arête \tilde{e} la quantité $\frac{1}{2}[\Gamma_e : \Gamma \cap \mathbf{Z}(K)]^{-1}$ (pour une arête e de \mathcal{T} au-dessus de \tilde{e} et Γ_e son stabilisateur pour Γ). Le produit de Petersson est un produit scalaire hermitien sur $\mathbf{H}(\mathbf{C})$ et à valeurs entières sur \mathbf{H} .

Soit \mathfrak{m} un idéal premier à \mathfrak{n} . L'opérateur de Hecke $T_{\mathfrak{m}}$ est un endomorphisme de $\mathbf{H}(\mathbf{C})$ qui provient d'une correspondance à coefficients entiers sur $Y(\Gamma \backslash \mathcal{T})$ (section 9 de [10]) et stabilise la structure entière \mathbf{H} . La formule suivante le définit :

$$(5) \quad (T_{\mathfrak{m}}F)(e) = \sum_{\substack{a,b,d \in A \\ (ad)=\mathfrak{m}, (a)+\mathfrak{n}=A \\ \deg b < \deg d, a \text{ et } d \text{ unitaires}}} F \left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} e \right) \quad (F \in \mathbf{H}(\mathbf{C}), e \in Y(\mathcal{T})).$$

Ces opérateurs commutent et sont hermitiens pour $(\ , \)_\mu$. On note \mathbf{T} la sous-algèbre commutative de $\text{End}(\mathbf{H}(\mathbf{C}))$ engendrée sur \mathbf{Z} par les $T_{\mathfrak{m}}$, pour \mathfrak{m} premier à \mathfrak{n} . C'est l'*algèbre de Hecke*. Pour \mathfrak{m} non premier à \mathfrak{n} , la formule (5) définit encore un opérateur noté $T_{\mathfrak{m}}$ qui commute aux autres mais n'est plus nécessairement hermitien. L'involution $w_{\mathfrak{n}}$ est hermitienne pour le produit de Petersson et commute à $T_{\mathfrak{m}}$ pour \mathfrak{m} premier à \mathfrak{n} .

Par la suite, on s'intéressera essentiellement à la situation où \mathfrak{n} est premier. Alors les endomorphismes $-w_{\mathfrak{n}}$ et $T_{\mathfrak{n}}$ coïncident. De plus, l'espace $\mathbf{H}(\mathbf{C})$ se décompose en somme directe orthogonale, pour $(\ , \)_\mu$, de sous-espaces propres de dimension 1 pour tous les opérateurs de Hecke. En particulier, il existe une base orthonormée de $\mathbf{H}(\mathbf{C})$ constituée de formes propres pour tous les opérateurs et normalisées (*i.e.* le coefficient de Fourier associé à l'idéal A est égal à 1). Ce sont les *formes primitives*.

4. Symboles modulaires de Teitelbaum

Le lecteur est invité à consulter [30] pour plus de détails.

4.1. Les symboles modulaires. — Soit M le groupe abélien des diviseurs de degré nul à support dans $\mathbf{P}^1(K)$. Le sous-groupe de congruence Γ , qui opère par transformations linéaires à gauche sur $\mathbf{P}^1(K)$, donne une structure de Γ -module sur M . Soit R un anneau commutatif. On munit le R -module $M \otimes_{\mathbf{Z}} R$ de l'action induite de Γ . Le R -module des *symboles modulaires pour Γ à valeurs dans R* est le groupe abélien $\mathbf{M}_{\mathfrak{n}}(R) = H_0(\Gamma, M \otimes_{\mathbf{Z}} R)$ muni de sa structure canonique de R -module. Il est engendré par les classes $[r, s]$ des diviseurs $(s) - (r)$ pour r et s dans $\mathbf{P}^1(K)$. Pour simplifier, on pose $\mathbf{M}_{\mathfrak{n}}(R) = \mathbf{M}(R)$; lorsque $R = \mathbf{Z}$, on le note $\mathbf{M}_{\mathfrak{n}}$ ou encore \mathbf{M} .

Considérons le groupe B_Γ 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 $[r, s] \mapsto (\Gamma s) - (\Gamma r)$ donne par linéarité une application *bord* surjective $M_\Gamma(R) \rightarrow B_\Gamma(R)$. Le sous-groupe des *symboles modulaires paraboliques* est son noyau, noté $\mathbf{M}_n^0(R)$ (ou $\mathbf{M}^0(R)$). Lorsque $R = \mathbf{Z}$, on le note \mathbf{M}_n^0 ou encore \mathbf{M}^0 . On a les isomorphismes canoniques $\mathbf{M} \otimes_{\mathbf{Z}} R \simeq \mathbf{M}(R)$ et, lorsque R est sans torsion sur \mathbf{Z} , $\mathbf{M}^0 \otimes_{\mathbf{Z}} R \simeq \mathbf{M}^0(R)$.

Soient $H_1(\Gamma \backslash \mathcal{T}, \mathbf{ptes}, \mathbf{Z})$ le premier groupe d'homologie relative aux pointes du graphe quotient $\Gamma \backslash \mathcal{T}$ et $H_1(\Gamma \backslash \mathcal{T}, \mathbf{Z})$ son sous-groupe des cycles. En regardant r et s comme des bouts rationnels de l'arbre \mathcal{T} , il existe une unique géodésique de l'arbre \mathcal{T} qui les relie. Considérons l'application qui associe au symbole modulaire $[r, s]$ la projection de cette géodésique dans le graphe $\Gamma \backslash \mathcal{T}$. Elle est bien définie et s'étend par linéarité en un homomorphisme de groupes abéliens $\mathbf{M} \rightarrow H_1(\Gamma \backslash \mathcal{T}, \mathbf{ptes}, \mathbf{Z})$.

Proposition 4.1 ([30] p. 277). — *L'application précédente induit les isomorphismes de groupes*

$$\begin{aligned} \mathbf{M}/\mathbf{M}_{\text{tors}} &\xrightarrow{\simeq} H_1(\Gamma \backslash \mathcal{T}, \mathbf{ptes}, \mathbf{Z}) \\ \mathbf{M}^0/(\mathbf{M}^0)_{\text{tors}} &\xrightarrow{\simeq} H_1(\Gamma \backslash \mathcal{T}, \mathbf{Z}). \end{aligned}$$

Soit h le nombre de pointes du graphe $\Gamma \backslash \mathcal{T}$. Il coïncide avec le nombre de pointes de la courbe modulaire de Drinfeld X_Γ associée à Γ . Pour des formules donnant h , on se réfère à la section 6 de [8]. D'après la proposition, les dimensions des \mathbf{Q} -espaces vectoriels $\mathbf{M}(\mathbf{Q})$ et $\mathbf{M}^0(\mathbf{Q})$ sont donc respectivement $g + h - 1$ et g .

Lorsque n est premier de degré impair (resp. pair), la torsion de \mathbf{M} est nulle (resp. cyclique d'ordre $q + 1$) (voir la remarque p. 278 de [30]).

4.2. L'accouplement avec les cochaînes. — Soit \mathfrak{m} un idéal premier à n . L'opérateur de Hecke $T_{\mathfrak{m}}$ est un endomorphisme de $\mathbf{M}(R)$ provenant de la correspondance sur $Y(\Gamma \backslash \mathcal{T})$ qui a servi à définir $T_{\mathfrak{m}}$ sur les cochaînes. La formule suivante le définit et garde un sens pour \mathfrak{m} non premier à n :

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

De même, on définit l'involution w_n de $\text{End}(\mathbf{M}(R))$ par

$$w_n[r, s] = [-1/(Nr), -1/(Ns)] \quad ([r, s] \in \mathbf{M}(R))$$

où N est le générateur unitaire de n . Tous ces opérateurs stabilisent le sous-espace parabolique.

Notation 4.2 (définition 8 de [30]). — Pour $F \in \mathbf{H}(R)$ et $[r, s] \in \mathbf{M}(R)$, on pose $\langle [r, s], F \rangle = \sum_{e \in c} F(e)$ où c est l'unique géodésique de \mathcal{T} reliant le bout r au bout s . Cette somme, qui est bien définie, est même finie par la parabolicité de F et la description de $\Gamma \backslash \mathcal{T}$ rappelée en section 3.1.

Par linéarité, on déduit une application R -bilinéaire $\langle \cdot, \cdot \rangle : \mathbf{M}(R) \times \mathbf{H}(R) \rightarrow R$ qui est compatible aux opérateurs de Hecke ([30, lemme 9]).

Théorème 4.3 (Teitelbaum). — *L'accouplement $\langle \cdot, \cdot \rangle$ fournit une suite exacte de groupes*

$$\begin{array}{ccccccc} 0 & \longrightarrow & (\mathbf{M}^0)_{\text{tors}} & \longrightarrow & \mathbf{M}^0 & \longrightarrow & \text{Hom}(\mathbf{H}, \mathbf{Z}) \longrightarrow \Phi_\infty \longrightarrow 0 \\ & & & & m \longmapsto & & (F \mapsto \langle m, F \rangle) \end{array}$$

où Φ_∞ est le groupe des composantes connexes de la fibre spéciale du modèle de Néron de la jacobienne de la courbe modulaire de Drinfeld X_Γ en la place ∞ . En particulier, on a un accouplement parfait de \mathbf{Q} -espaces vectoriels

$$\langle \cdot, \cdot \rangle : \mathbf{M}^0(\mathbf{Q}) \times \mathbf{H}(\mathbf{Q}) \longrightarrow \mathbf{Q}.$$

La suite exacte est le théorème 14 de [30]. On déduit le deuxième énoncé en étendant les scalaires à \mathbf{Q} .

On dispose donc d'un accouplement parfait $\mathbf{M}^0(\mathbf{C}) \times \mathbf{H}(\mathbf{C}) \rightarrow \mathbf{C}$. Il permet d'identifier les opérateurs de Hecke sur $\mathbf{M}^0(\mathbf{C})$ et $\mathbf{H}(\mathbf{C})$, et plus généralement l'algèbre de Hecke \mathbf{T} à la sous \mathbf{Z} -algèbre de $\text{End}(\mathbf{M}^0(\mathbf{C}))$ engendrée par les T_m avec m premier à n . On notera encore \mathbf{T} cette algèbre.

Enfin, d'après l'équation (4), la valeur spéciale $L(F, 1)$ d'une cochaîne harmonique $F \in \mathbf{H}(\mathbf{C})$ est reliée au symbole modulaire $[0, \infty]$ par

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

(voir aussi le théorème 23 de [30]).

4.3. Symboles paraboliques comme cochaînes. — On apporte un complément à la théorie de Teitelbaum en exhibant un isomorphisme canonique entre symboles paraboliques, à torsion près, et cochaînes paraboliques. Il s'agit d'une comparaison de [30] et du travail de Gekeler et Nonnengardt [9].

Commençons par rappeler le lien existant entre cochaînes paraboliques pour Γ et cycles du graphe $\Gamma \backslash \mathcal{T}$, d'après Gekeler et Nonnengardt. Soit $n(\tilde{e}) = n(e)$ l'indice de $\Gamma \cap \mathbf{Z}(K)$ dans Γ_e , pour une arête e de \mathcal{T} d'image \tilde{e} dans $\Gamma \backslash \mathcal{T}$. L'homomorphisme de \mathbf{Z} -modules

$$\begin{array}{ccc} j : H_1(\Gamma \backslash \mathcal{T}, \mathbf{Z}) & \longrightarrow & \mathbf{H} \\ \varphi & \longmapsto & (e \mapsto n(e)\varphi(\tilde{e})) \end{array}$$

est bien défini, injectif et de conoyau fini ([10, 3.2.5]). Comme $\Gamma = \Gamma_0(n)$, il est même bijectif : c'est un résultat profond sur la structure de $\Gamma \backslash \mathcal{T}$ ([9, théorème 3.3]).

Lemme 4.4. — *On a un isomorphisme canonique de \mathbf{T} -modules*

$$\alpha : \mathbf{M}^0 / (\mathbf{M}^0)_{\text{tors}} \xrightarrow{\cong} \mathbf{H}.$$

Notons i l'injection $\mathbf{H} \hookrightarrow \text{Hom}(\mathbf{H}, \mathbf{Z})$ provenant du produit de Petersson. Alors $i \circ \alpha$ est l'injection $\mathbf{M}^0 / (\mathbf{M}^0)_{\text{tors}} \hookrightarrow \text{Hom}(\mathbf{H}, \mathbf{Z})$ provenant de l'accouplement $\langle \cdot, \cdot \rangle$.

Démonstration. — L'isomorphisme α s'obtient en composant j avec l'isomorphisme de la proposition 4.1 (Teitelbaum). Prouvons que $i \circ \alpha$ est induit par $\langle \cdot, \cdot \rangle$ en le vérifiant sur les générateurs $[r, s]$ de \mathbf{M}^0 avec $s \in \Gamma r$. Notons c la géodésique de \mathcal{T} reliant r à s , \tilde{c}

sa projection dans $\Gamma \backslash \mathcal{T}$ et $m(\tilde{e})$ le nombre d'arêtes de c au-dessus de $\tilde{e} \in \tilde{c}$. L'image de $[r, s]$ dans $H_1(\Gamma \backslash \mathcal{T}, \mathbf{Z})$ s'identifie à la fonction suivante sur $Y(\Gamma \backslash \mathcal{T})$:

$$\varphi(\tilde{e}) = \begin{cases} m(\tilde{e}) & \text{si } \tilde{e} \text{ appartient à } \tilde{c} \\ -m(\tilde{e}) & \text{si l'arête opposée de } \tilde{e} \text{ appartient à } \tilde{c} \\ 0 & \text{sinon.} \end{cases}$$

Elle est alternée, c'est-à-dire que la valeur de φ sur l'arête opposée à \tilde{e} est $-\varphi(\tilde{e})$. L'accouplement entre $[r, s]$ et une cochaîne $G \in \mathbf{H}$ est alors

$$\langle [r, s], G \rangle = \sum_{\tilde{e} \in \tilde{c}} m(\tilde{e})G(\tilde{e}) = \sum_{\tilde{e} \in \tilde{c}} \varphi(\tilde{e})G(\tilde{e}) = \frac{1}{2} \sum_{\tilde{e} \in Y(\Gamma \backslash \mathcal{T})} \varphi(\tilde{e})G(\tilde{e})$$

la dernière égalité provenant de l'alternance de φ et G . En posant $F = j(\varphi) = \alpha([r, s])$, on obtient

$$\langle [r, s], G \rangle = \frac{1}{2} \sum_{\tilde{e} \in Y(\Gamma \backslash \mathcal{T})} \frac{1}{n(\tilde{e})} F(\tilde{e})G(\tilde{e}) = (F, G)_\mu.$$

Soit $x \in \mathbf{M}^0/(\mathbf{M}^0)_{\text{tors}}$. En utilisant ce qui précède et la compatibilité de $\langle \cdot, \cdot \rangle$ aux opérateurs de Hecke, on voit que la cochaîne $\alpha(T_{\mathbf{m}}x) - T_{\mathbf{m}}\alpha(x)$ est orthogonale pour $(\cdot, \cdot)_\mu$ à \mathbf{H} . Par extension des scalaires, elle est orthogonale à $\mathbf{H}(\mathbf{C})$ donc nulle. Ainsi, α est Hecke-équivariant. \square

Remarque 4.5. — — Via l'isomorphisme α , le théorème 4.3 sur l'accouplement revient à la suite exacte

$$0 \longrightarrow \mathbf{H} \xrightarrow{i} \text{Hom}(\mathbf{H}, \mathbf{Z}) \longrightarrow \Phi_\infty \longrightarrow 0.$$

Gekeler l'avait déjà établie de manière indépendante (corollaire 2.11 de [5]) comme conséquence de l'uniformisation analytique de la jacobienne de X_Γ donnée dans [10].

- Bien qu'on ait l'isomorphisme $\alpha : \mathbf{M}^0/(\mathbf{M}^0)_{\text{tors}} \xrightarrow{\cong} \mathbf{H}$, la construction de Teitelbaum conserve son intérêt car la présentation finie, dont nous ferons un usage essentiel, ne semble pas avoir été établie directement sur les cochaînes.
- Pour calculer une base de \mathbf{H} , on dispose d'une méthode combinatoire naturelle qui repose sur la détermination du graphe $\Gamma \backslash \mathcal{T}$ (voir Gekeler et Nonnengardt [3, 20, 9]). Les symboles modulaires sur $\mathbf{F}_q(T)$ permettent de déterminer une base d'un espace isomorphe, *via* α , en évitant le calcul préliminaire de $\Gamma \backslash \mathcal{T}$.

4.4. La présentation finie. — Considérons la droite projective $\mathbf{P}^1(A/\mathfrak{n})$. Ce sont les classes d'équivalence de couples $(u, v) \in A \times A$ avec $(u) + (v) + \mathfrak{n} = A$, deux tels couples (u_1, v_1) et (u_2, v_2) étant équivalents s'il existe $w \in A$ avec $(w) + \mathfrak{n} = A$, $u_1 \equiv wu_2 \pmod{\mathfrak{n}}$ et $v_1 \equiv wv_2 \pmod{\mathfrak{n}}$. On note $(u : v)$ la classe de (u, v) .

Le sous-groupe $\Gamma_0(\mathfrak{n})$, qui opère par multiplication à gauche sur $G(A)$, est d'indice fini. On a alors une bijection

$$\begin{aligned} \Gamma_0(\mathfrak{n}) \backslash G(A) &\longrightarrow \mathbf{P}^1(A/\mathfrak{n}) \\ \Gamma_0(\mathfrak{n}) \begin{pmatrix} a & b \\ u & v \end{pmatrix} &\longmapsto (u : v) \end{aligned}$$

(noter qu'on peut toujours choisir un représentant (u, v) de $(u : v)$ avec u et v premiers entre eux). Considérons l'application

$$\begin{aligned} \mathbf{P}^1(A/\mathfrak{n}) &\longrightarrow \mathbf{M} \\ (u : v) &\longmapsto [g0, g\infty] = [b/v, a/u] \end{aligned}$$

où $g = \begin{pmatrix} a & b \\ u & v \end{pmatrix} \in G(A)$ est une matrice relevant $(u : v)$ par la bijection précédente⁽¹⁾. Elle est bien définie et se prolonge par \mathbf{Z} -linéarité en un homomorphisme surjectif

$$\xi : \mathbf{Z}[\mathbf{P}^1(A/\mathfrak{n})] \longrightarrow \mathbf{M}$$

où la surjectivité provient d'un développement en fractions continuées (lemme 16 de [30]). On appelle les $\xi(u : v)$ les *symboles de Manin–Teitelbaum*. Ils engendrent \mathbf{M} . Posons dans $G(\mathbf{F}_q)$:

$$\sigma = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \tau = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}.$$

Ces matrices sont d'ordre respectivement 4 (ou 2 si $p = 2$) et 3. La présentation suivante se déduit des énoncés pp. 283–286 et du théorème 21 de [30].

Théorème 4.6 (Teitelbaum). — *Le R -module $\mathbf{M}(R)$ est isomorphe au quotient du R -module libre $R[\mathbf{P}^1(A/\mathfrak{n})]$ par les relations (1) (données dans l'introduction).*

5. L'action de Hecke sur les symboles modulaires de Manin–Teitelbaum

Soit $M_2(A)$ l'ensemble des matrices $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ avec a, b, c, d dans A . Pour $(u : v) \in \mathbf{P}^1(A/\mathfrak{n})$, on pose $(u : v)M = (au + cv : bu + dv)$ si cela a un sens dans $\mathbf{P}^1(A/\mathfrak{n})$. La formule du théorème 1.1, que nous allons démontrer, s'écrit alors

$$T_{\mathfrak{m}} \xi(u : v) = \sum_{\substack{M \in \mathcal{S}_{\mathfrak{m}} \\ (u:v)M \text{ bien défini}}} \xi((u : v)M).$$

Appliquée au symbole modulaire $[0, \infty] = \xi(0 : 1)$, elle donne

$$T_{\mathfrak{m}} [0, \infty] = \sum_{\substack{\deg a > \deg b, \deg d > \deg c \\ (ad-bc)=\mathfrak{m}, (c)+(d)+\mathfrak{n}=A \\ a \text{ et } d \text{ unitaires}}} \xi(c : d).$$

Ces formules pourraient être prolongées dans différentes directions : aux involutions $w_{\mathfrak{m}}$ (pour $\mathfrak{n} \subset \mathfrak{m}$), à d'autres ensembles de matrices ou d'autres sous-groupes de congruence, dans l'esprit de [18] pour les symboles modulaires sur \mathbf{Q} . Dans la section 5.2, on donne la liste des éléments de $\mathcal{S}_{\mathfrak{m}}$ lorsque \mathfrak{m} est de petit degré.

⁽¹⁾Teitelbaum a adopté la convention inverse $[g\infty, g0]$; nous préférons suivre celle habituellement utilisée pour les symboles modulaires sur \mathbf{Q} .

5.1. Démonstration du théorème 1.1. — Elle repose sur des idées de Merel [18] (voir aussi la démonstration du lemme 2 de [19]).

Lemme 5.1. — *L'ensemble de matrices \mathcal{S}_m est fini.*

Démonstration. — Soit $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ appartenant à \mathcal{S}_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, $(ad - bc) = m$ donc $\deg a$ et $\deg d$ valent au plus $\deg m$. Comme a, b, c et d sont à coefficients dans le corps fini \mathbf{F}_q , cela ne laisse qu'un nombre fini de possibilités pour ces polynômes. \square

Le groupe $G(A)$ opère à droite sur l'ensemble $M_2(A)_m$ des matrices de $M_2(A)$ dont le déterminant engendre m . Notons $M_2(A)_m/G(A)$ l'ensemble des classes. On commence par en exhiber un système de représentants. Soit P le générateur unitaire de m . Pour la suite, on notera que toute matrice de \mathcal{S}_m a pour déterminant P .

Proposition 5.2. — *Les matrices $m(a, b) = \begin{pmatrix} a & b \\ 0 & P/a \end{pmatrix}$ avec $a \mid P$, a unitaire et $\deg a > \deg b$, forment un système de représentants de $M_2(A)_m/G(A)$. De plus, ce sont les seuls éléments $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ de \mathcal{S}_m avec $c = 0$.*

Démonstration. — Soit $M \in M_2(A)_m$. On commence par trouver une matrice triangulaire supérieure dans la classe de M . L'action à gauche du groupe $G(A)$ sur $\mathbf{P}^1(K)$ est transitive. Il existe donc $\gamma \in G(A)$ telle que $\gamma\infty = M^{-1}\infty$. Dans $M_2(A)_m$, on a alors $M' = M\gamma = \begin{pmatrix} a & b \\ 0 & \lambda P/a \end{pmatrix}$ avec $a \mid P$, $b \in A$ et $\lambda \in \mathbf{F}_q^\times$. Quitte à remplacer M' par $M' \begin{pmatrix} \alpha^{-1} & 0 \\ 0 & \alpha\lambda^{-1} \end{pmatrix}$ où $\alpha \in \mathbf{F}_q^\times$ est le coefficient dominant de a , on peut supposer $M' = \begin{pmatrix} a & b \\ 0 & P/a \end{pmatrix}$ avec a unitaire. Enfin, un calcul élémentaire montre que deux telles matrices $\begin{pmatrix} a & b \\ 0 & P/a \end{pmatrix}$ et $\begin{pmatrix} a' & b' \\ 0 & P/a' \end{pmatrix}$ sont dans la même classe pour $G(A)$ si et seulement si $a = a'$ et $b' \equiv b \pmod{a}$. On peut donc choisir b de telle sorte que $\deg a > \deg b$. La dernière assertion de l'énoncé provient de la définition de \mathcal{S}_m . \square

Proposition 5.3. — *Soit $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{S}_m$ avec $c \neq 0$ (c'est-à-dire $M\infty \neq \infty$). Il existe une unique matrice $M' \in \mathcal{S}_m \cap MG(A)$ telle que $M'0 = M\infty$.*

Soit $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{S}_m$ avec $b \neq 0$ (c'est-à-dire $M0 \neq 0$). Il existe une unique matrice $M' \in \mathcal{S}_m \cap MG(A)$ telle que $M'\infty = M0$.

Démonstration. — On démontre le résultat pour $c \neq 0$, le cas $b \neq 0$ étant similaire. Commençons par l'existence. Soit $\alpha \in \mathbf{F}_q^\times$ le coefficient dominant de c . Le quotient de la division euclidienne de d par $\alpha^{-1}c$ est un polynôme unitaire Q vérifiant $\deg c > \deg(cQ - ad)$. Posons

$$M' = M \begin{pmatrix} Q & \alpha^{-1} \\ -\alpha & 0 \end{pmatrix} = \begin{pmatrix} aQ - \alpha b & \alpha^{-1}a \\ cQ - \alpha d & \alpha^{-1}c \end{pmatrix} \in M_2(A)_m.$$

Comme $\deg Q \geq 0$, on a $\deg(aQ - \alpha b) = \deg(aQ) > \deg(\alpha^{-1}a)$. De plus, $\alpha^{-1}c$ et $aQ - \alpha b$ sont unitaires. Donc la matrice M' appartient à l'ensemble \mathcal{S}_m et vérifie $M'0 = a/c = M\infty$.

Passons à l'unicité. Soit une matrice $M'' \in \mathcal{S}_m \cap MG(A)$ avec $M''0 = M\infty$. Il suffit de montrer que $M^{-1}M''$ est déterminée de façon unique par M . Comme $M^{-1}M''$ est de déterminant 1 et envoie 0 sur ∞ , on a $M^{-1}M'' = \begin{pmatrix} Q & \alpha^{-1} \\ -\alpha & 0 \end{pmatrix}$ avec $\alpha \in \mathbf{F}_q^\times$ et $Q \in A$, d'où

$M'' = \begin{pmatrix} aQ - \alpha b & \alpha^{-1}a \\ cQ - \alpha d & \alpha^{-1}c \end{pmatrix}$. De plus, M'' étant dans \mathcal{S}_m , le polynôme $\alpha^{-1}c$ est unitaire donc α est le coefficient dominant de c . Il reste à montrer que Q est déterminé de façon unique par la matrice M . Comme $M'' \in \mathcal{S}_m$, le polynôme Q vérifie $\deg c > \deg(cQ - \alpha d)$. Donc Q est le quotient de la division euclidienne de αd par c et il est déterminé de façon unique par les polynômes c et d , donc par M . \square

Démonstration du théorème 1.1. — Prenons un représentant (u, v) de $(u : v)$ dans $A \times A$ avec u et v premiers entre eux. Il existe donc une matrice $g = \begin{pmatrix} x & y \\ u & v \end{pmatrix} \in G(A)$ telle que $\xi(u : v) = [g0, g\infty]$. Soit $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{S}_m$. On commence par relever $(au + cv : bu + dv)$ en une matrice de $G(A)$. Comme $gM \in M_2(A)_m$, il existe δ et β , avec $\delta \mid P$, δ unitaire et $\deg \beta < \deg \delta$, tels que $gM \in m(\delta, \beta)G(A)$ d'après la proposition 5.2. Comme $m(\delta, \beta)^{-1}gM \in G(A)$, on a

$$\begin{aligned} [m(\delta, \beta)^{-1}gM0, m(\delta, \beta)^{-1}gM\infty] &= \xi(\delta(au + cv)/P : \delta(bu + dv)/P) \\ &= \xi(au + cv : bu + dv) \end{aligned}$$

si P/δ est inversible dans A/\mathfrak{n} . Pour simplifier, posons $C(\delta, \beta) = m(\delta, \beta)G(A)$. Par la proposition 5.2, on en déduit l'égalité des sommes, finies d'après le lemme 5.1 :

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

Ce symbole modulaire ne dépend que du diviseur D suivant, à support dans $\mathbf{P}^1(K)$:

$$D = \sum_{\substack{\deg \beta < \deg \delta, \delta \mid P, \delta \text{ unitaire} \\ (P/\delta) + \mathfrak{n} = A \\ M \in g^{-1}C(\delta, \beta) \cap \mathcal{S}_m}} (m(\delta, \beta)^{-1}gM0) - (m(\delta, \beta)^{-1}gM\infty).$$

Si M vérifie $M0 \neq 0$, d'après la proposition 5.3, il existe une unique matrice $M' \in \mathcal{S}_m \cap MG(A)$ telle que $M'\infty = M0$. De plus, $M'\infty$ est distinct de ∞ (sinon on aurait $M0 = \infty = b/d$, donc $d = 0$ ce que l'inégalité $\deg d > \deg b$ exclut). On a donc l'égalité des diviseurs

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

En utilisant l'unicité dans la proposition 5.3, il ne reste dans D que

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

Cela se traduit par l'égalité de symboles modulaires

$$\sum_{\substack{M \in \mathcal{S}_m \\ (u:v)M \text{ bien défini}}} \xi((u:v)M) = \sum_{\substack{\deg \beta < \deg \delta \\ \delta | P, \delta \text{ unitaire} \\ (P/\delta) + n = A}} \left[m(\delta, \beta)^{-1} g_0, m(\delta, \beta)^{-1} g_\infty \right].$$

Enfin, comme $g_0 = y/v$ et $g_\infty = x/u$, on reconnaît $T_m[y/v, x/u] = T_m \xi(u:v)$ au membre de droite. \square

5.2. Exemples d'ensembles \mathcal{S}_m . — La lettre P continue à désigner le générateur unitaire de l'idéal \mathfrak{m} . Si \mathfrak{m} est de degré 1, l'ensemble \mathcal{S}_m est formé des $2q$ matrices $\begin{pmatrix} P & \lambda \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ \lambda & P \end{pmatrix}$, pour $\lambda \in \mathbf{F}_q$. D'après le théorème 1.1, l'action de T_m est alors donnée par

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

Si \mathfrak{m} est de degré 2, l'ensemble \mathcal{S}_m est donné explicitement par l'énoncé suivant.

Proposition 5.4. — Soit \mathfrak{m} l'idéal engendré par $P = T^2 + mT + n$ ($m, n \in \mathbf{F}_q$). Posons

$$M_1(b) = \begin{pmatrix} P & b \\ 0 & 1 \end{pmatrix}, \quad M_2(b) = \begin{pmatrix} 1 & 0 \\ b & P \end{pmatrix} \quad (b \in A, \deg b \leq 1)$$

$$M_3(\alpha, b, c) = \begin{pmatrix} T + \alpha & b \\ c & T + m - \alpha \end{pmatrix} \quad (\alpha, b, c \in \mathbf{F}_q).$$

Soit \mathcal{R} l'ensemble des racines de P dans \mathbf{F}_q . Alors \mathcal{S}_m est formé des matrices

$$M_1(b), M_2(b) \quad (b \in A, \deg b \leq 1)$$

$$M_3(-x, b, c) \quad (x \in \mathcal{R}, b, c \in \mathbf{F}_q \text{ avec } b = 0 \text{ ou } c = 0)$$

$$M_3(\alpha, b, -P(-\alpha)/b) \quad (\alpha \in \mathbf{F}_q, \alpha \notin \mathcal{R}, b \in \mathbf{F}_q^\times).$$

Si \mathcal{R} possède zéro (resp. un, resp. deux) élément(s), alors \mathcal{S}_m est de cardinal $3q^2 - q$ (resp. $3q^2$, resp. $3q^2 + q$).

Démonstration. — Soit $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{S}_m$. On a $\deg P = \deg a + \deg d = 2$. Si $\deg a = 2$, alors $d = 1$. Comme $\deg c < \deg d$, c est alors nul. La matrice est donc de la forme $M_1(b)$ avec $\deg b \leq 1$. Le cas $\deg d = 2$ se traite de façon similaire et correspond aux matrices $M_2(b)$. Supposons $\deg a = \deg d = 1$. Alors b et c sont constants. Écrivons $a = T + \alpha$ et $d = T + \delta$ avec $\alpha, \delta \in \mathbf{F}_q$. La condition $\det M = T^2 + mT + n$ équivaut au système d'équations : $\alpha + \delta = m$ et $\alpha\delta - bc = n$. Cela revient à dire que α et δ sont racines dans \mathbf{F}_q de l'équation $P(-x) = -bc$. La conclusion suit. \square

5.3. Un exemple numérique. — On illustre, sur un exemple, l'utilisation du théorème 1.1 pour calculer la matrice d'un opérateur de Hecke dans une base de symboles modulaires. Fixons \mathfrak{n} . On commence par trouver une base de $\mathbf{M}_n(\mathbf{Q})$ constituée de symboles modulaires de Manin–Teitelbaum : on établit la liste des générateurs c'est-à-dire des éléments de $\xi(\mathbf{P}^1(A/\mathfrak{n}))$, puis on résout le système linéaire sur \mathbf{Q} donné par les relations de Manin–Teitelbaum (théorème 4.6). Lorsque \mathfrak{n} est premier de degré impair, on peut avantageusement remplacer ces calculs par la base explicite qui sera exposée dans la section 6 (théorèmes 6.4 et 6.6).

La méthode usuelle pour déterminer la matrice de l'opérateur $T_{\mathfrak{m}}$ dans la base consiste à calculer l'image par $T_{\mathfrak{m}}$ de chaque élément de la base, en utilisant la définition de $T_{\mathfrak{m}}$, puis à exprimer le résultat en termes de symboles de Manin–Teitelbaum à l'aide de développements en fractions continuées. Un exemple est traité dans [30] pp. 287–288. Le théorème 1.1 fournit une nouvelle méthode pour calculer cette matrice :

1. on détermine l'ensemble de matrices $\mathcal{S}_{\mathfrak{m}}$;
2. on écrit la matrice de $T_{\mathfrak{m}}$ dans cette base à l'aide du théorème 1.1 et des relations de Manin–Teitelbaum.

Cette méthode se prête particulièrement bien aux calculs à \mathfrak{m} fixé pour différentes valeurs de \mathfrak{n} , puisque l'ensemble $\mathcal{S}_{\mathfrak{m}}$ ne dépend pas de \mathfrak{n} . À titre d'exemple, considérons $q = 5$ et l'idéal premier $\mathfrak{n} = (T^3 + T + 1)$. Le \mathbf{Z} -module \mathbf{M} possède 126 symboles de Manin–Teitelbaum desquels on extrait la base $\{\xi(1 : 0), \xi(T + a : 1) \mid a \in \mathbf{F}_5\}$. Pour $\mathfrak{m} = (T^3 + 3T + 3)$, l'ensemble $\mathcal{S}_{\mathfrak{m}}$ est formé de 450 matrices. Par la méthode ci-dessus, la matrice de $T_{\mathfrak{m}}$ dans cette base est, pour l'action à gauche sur les vecteurs colonnes,

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

5.4. Une loi de réciprocité de Manin. — On déduit du théorème 1.1 une loi de réciprocité à la Manin pour les courbes elliptiques sur $K = \mathbf{F}_q(T)$. L'énoncé s'appuie sur le théorème de modularité pour ces courbes elliptiques. Pour des résultats analogues sur \mathbf{Q} , on se réfère à Manin [14, théorème 7.3], Mazur [15] et Merel [17, théorème 4].

Lemme 5.5. — *Soit $F \in \mathbf{H}(\mathbf{C})$ une cochaîne parabolique non nulle et propre pour $T_{\mathfrak{m}}$ de valeur propre $a_{\mathfrak{m}}$. L'application*

$$\begin{aligned} l_F : \mathbf{P}^1(A/\mathfrak{n}) &\longrightarrow \mathbf{C} \\ x &\longmapsto \langle \xi(x), F \rangle. \end{aligned}$$

n'est pas identiquement nulle et vérifie pour tout $x \in \mathbf{P}^1(A/\mathfrak{n})$

$$a_{\mathfrak{m}} l_F(x) = \sum_{\substack{M \in \mathcal{S}_{\mathfrak{m}} \\ xM \text{ bien défini}}} l_F(xM).$$

Démonstration. — Comme F est non nulle et l'accouplement est parfait sur \mathbf{C} , il existe au moins un élément parmi les générateurs $\{\xi(x)\}$ de $\mathbf{M}^0(\mathbf{C})$ avec $\langle \xi(x), F \rangle \neq 0$. Enfin, pour tout $x \in \mathbf{P}^1(A/\mathfrak{n})$, on a d'après le théorème 1.1

$$\sum_{\substack{M \in \mathcal{S}_{\mathfrak{m}} \\ xM \text{ bien défini}}} l_F(xM) = \langle T_{\mathfrak{m}} \xi(x), F \rangle = \langle \xi(x), T_{\mathfrak{m}} F \rangle = \langle \xi(x), a_{\mathfrak{m}} F \rangle = a_{\mathfrak{m}} l_F(x).$$

□

Proposition 5.6. — Soit E une courbe elliptique sur K , de conducteur $\mathfrak{n} \cdot (\infty)$ avec réduction multiplicative déployée en la place ∞ et \mathfrak{n} idéal non nul de A . Il existe une application

$$l_E : \mathbf{P}^1(A/\mathfrak{n}) \longrightarrow \mathbf{Q}$$

et un élément λ_E de $\mathbf{P}^1(A/\mathfrak{n})$ tels qu'on ait, pour tout \mathfrak{p} premier avec $\mathfrak{n} \not\subset \mathfrak{p}$,

$$q^{\deg \mathfrak{p}} + 1 - \#E(\mathbf{F}_{\mathfrak{p}}) = \sum_{M \in \mathcal{S}_{\mathfrak{p}}} l_E(\lambda_E M)$$

où $E(\mathbf{F}_{\mathfrak{p}})$ est le groupe des points à valeurs dans $\mathbf{F}_{\mathfrak{p}} = A/\mathfrak{p}$ de la réduction de E modulo \mathfrak{p} .

Démonstration. — Soit E une telle courbe elliptique. D'après le théorème de modularité pour les courbes elliptiques sur K , qui fait suite aux travaux de Grothendieck, Jacquet–Langlands, Deligne et Drinfeld (discuté dans la section 8 de [10]), il existe F primitive dans $\mathbf{H}_{\mathfrak{n}}(\mathbf{Q})$ dont la valeur propre pour $T_{\mathfrak{p}}$ est $a_{\mathfrak{p}} = q^{\deg \mathfrak{p}} + 1 - \#E(\mathbf{F}_{\mathfrak{p}})$, pour tout \mathfrak{p} premier avec $\mathfrak{n} \not\subset \mathfrak{p}$. L'application l_F est alors à valeurs dans \mathbf{Q} et le lemme 5.5 assure qu'il existe $\lambda_E \in \mathbf{P}^1(A/\mathfrak{n})$ avec $l_F(\lambda_E) \neq 0$. On voit que $l_E = l_F/l_F(\lambda_E)$ vérifie la propriété souhaitée. \square

Du fait que l'ensemble $\mathcal{S}_{\mathfrak{p}}$ est indépendant de \mathfrak{n} , comme l'a remarqué Manin, la proposition s'apparente à une formule de réciprocité : elle relie les solutions modulo \mathfrak{p} d'une équation dépendant de \mathfrak{n} aux solutions modulo \mathfrak{n} d'une équation dépendant de \mathfrak{p} .

6. Une base explicite de symboles de Manin–Teitelbaum

Dans cette section, on suppose l'idéal \mathfrak{n} premier.

6.1. Une variante de l'espace des symboles modulaires. — Considérons la droite projective $\mathbf{P}^1(A)$. Ce sont les classes d'équivalence de couples $(u, v) \in A \times A$ avec $(u, v) \neq (0, 0)$, deux tels couples (u_1, v_1) et (u_2, v_2) étant équivalents s'il existe $\lambda \in A^\times = \mathbf{F}_q^\times$ tel que $(u_2, v_2) = (\lambda u_1, \lambda v_1)$. La classe de (u, v) sera notée $[u : v]$ afin de la distinguer de $(u : v) \in \mathbf{P}^1(A/\mathfrak{n})$.

Soit e un entier > 0 . Soit $\mathbf{P}^1(A)_e$ l'ensemble des $[u : v] \in \mathbf{P}^1(A)$ avec $\deg u \leq e$ et $\deg v \leq e$. On constate qu'il est stable par l'action à droite des matrices σ, τ et des matrices diagonales de $\mathbf{G}(\mathbf{F}_q)$. Si R est un anneau commutatif, on définit alors le quotient $M_e(R)$ du R -module libre $R[\mathbf{P}^1(A)_e]$ par le sous-module engendré par les relations $(z) + (z\sigma)$, $(z) + (z\tau) + (z\tau^2)$ et $(z) - (z\delta)$ pour δ diagonale dans $\mathbf{G}(\mathbf{F}_q)$.

Lemme 6.1. — 1. Soit $N_{i,j}$ le nombre de couples $(u, v) \in A \times A$ avec u, v unitaires premiers entre eux, $\deg u = i$ et $\deg v = j$ pour $i, j \geq 0$. On a

$$N_{i,j} = \begin{cases} (q-1)q^{i+j-1} & \text{si } \min(i, j) > 0 \\ q^{\max(i,j)} & \text{sinon.} \end{cases}$$

2. Soient $a, b \in \mathbf{N}$. L'ensemble des $[u : v] \in \mathbf{P}^1(A)$ avec u et v unitaires, $\deg u \leq a$ et $\deg v \leq b$ possède $(q^{a+b+1} - 1)/(q - 1)$ éléments. En particulier, $\mathbf{P}^1(A)_e$ possède $q^{2e+1} + 1$ éléments.

Démonstration. — 1. Par symétrie, il suffit d'établir ces formules pour $i \leq j$, ce qu'on fait à l'aide d'une fonction génératrice. Posons $l = j - i$ et calculons $N_{i,i+l}$. Le nombre de couples (u, v) avec u, v unitaires, $\deg u = i$, $\deg v = i + l$ est q^{2i+l} . Dénombrons ceux dont le pgcd unitaire w est de degré $0 \leq h \leq i$. Comme u/w et v/w sont unitaires, premiers entre eux, de degré respectivement $i - h$ et $i + l - h$, il y a $N_{i-h, i+l-h}$ tels couples. Ainsi on a, pour tout $l \geq 0$ et $i \geq 0$,

$$q^{2i+l} = \sum_{h=0}^i q^h N_{i-h, i+l-h}.$$

Soient x et y des indéterminées. En multipliant l'égalité précédente par $x^i y^{i+l}$, en sommant sur $i \geq 0$ et $l \geq 0$ et en arrangeant l'expression, on trouve

$$\sum_{i=0}^{+\infty} \sum_{l=0}^{+\infty} N_{i, i+l} x^i y^{i+l} = (1 - qxy) \sum_{i=0}^{+\infty} \sum_{l=0}^{+\infty} q^{2i+l} x^i y^{i+l}.$$

Par identification, on obtient $N_{i, i+l} = (q - 1)q^{2i+l-1}$ si $i > 0$ et $N_{0, l} = q^l$. Ce sont les formules annoncées.

2. Notons $\mathbf{P}^1(A)_{a,b}$ cet ensemble. Soit $F_{a,b}$ l'ensemble des couples $(u, v) \in A \times A$ avec u, v unitaires premiers entre eux, $\deg u \leq a$ et $\deg v \leq b$. L'application $\varphi : (u, v) \mapsto [u : v]$ est clairement une surjection de $F_{a,b}$ sur $\mathbf{P}^1(A)_{a,b}$. Comme on impose à u et v d'être unitaires, elle est aussi injective. Ainsi, φ est bijective. Il reste à dénombrer $F_{a,b}$. On a $\#F_{a,b} = \sum_{i=0}^a \sum_{j=0}^b N_{i,j}$. En remplaçant par les expressions de $N_{i,j}$ obtenues précédemment, on obtient $\#F_{a,b} = (q^{a+b+1} - 1)/(q - 1)$. \square

Proposition 6.2. — Soit \mathfrak{n} un idéal premier, de degré noté d .

1. Supposons $e < d/2$. L'application canonique

$$\begin{aligned} \mathbf{P}^1(A)_e &\longrightarrow \mathbf{P}^1(A/\mathfrak{n}) \\ [u : v] &\longmapsto (u : v) \end{aligned}$$

est injective. Elle induit un homomorphisme injectif $M_e(R) \rightarrow \mathbf{M}_{\mathfrak{n}}(R)$.

2. Si d est impair, alors on a une bijection $\mathbf{P}^1(A)_{(d-1)/2} \simeq \mathbf{P}^1(A/\mathfrak{n})$ et un isomorphisme $M_{(d-1)/2}(R) \xrightarrow{\simeq} \mathbf{M}_{\mathfrak{n}}(R)$.

Démonstration. — 1. Supposons $(u_1 : v_1) = (u_2 : v_2)$ pour des polynômes u_1, u_2, v_1, v_2 de degré $\leq e$ avec $(u_1) + (v_1) = (u_2) + (v_2) = A$. Alors $u_1 v_2 - u_2 v_1$ appartient à l'idéal \mathfrak{n} . Comme ce polynôme est de degré $\leq 2e < d$, il est nécessairement nul. Donc u_1 , qui divise $u_2 v_1$ et est premier à v_1 , divise u_2 . De même, u_2 divise u_1 . Donc il existe $\lambda \in \mathbf{F}_q^\times$ avec $u_2 = \lambda u_1$. On a alors $v_2 = \lambda v_1$ puis $[u_1 : v_1] = [u_2 : v_2]$. L'application canonique est injective.

L'homomorphisme $i : R[\mathbf{P}^1(A)_e] \rightarrow R[\mathbf{P}^1(A/\mathfrak{n})]$ est alors injectif. Rappelons que, d'après la présentation (théorème 4.6), $\mathbf{M}_{\mathfrak{n}}(R)$ est isomorphe au quotient du R -module libre $R[\mathbf{P}^1(A/\mathfrak{n})]$ par les relations de Manin–Teitelbaum. Pour l'injectivité de $M_e(R) \rightarrow \mathbf{M}_{\mathfrak{n}}(R)$, il s'agit de vérifier que tout élément x de $R[\mathbf{P}^1(A)_e]$ tel que $i(x)$ est dans les relations de Manin–Teitelbaum de $R[\mathbf{P}^1(A/\mathfrak{n})]$ est lui-même dans les relations de Manin–Teitelbaum de $R[\mathbf{P}^1(A)_e]$. Comme i est injective, il suffit

de voir que $i(x)$ est dans l'image des relations de $R[\mathbf{P}^1(A)_e]$. Mais cela résulte de l'équivariance de i par l'action de σ , τ et des matrices diagonales de $G(\mathbf{F}_q)$.

2. Posons $a = b = e = (d - 1)/2 \in \mathbf{N}$. D'après le lemme 6.1, $\mathbf{P}^1(A)_e$ est de cardinal $q^d + 1$. Comme il coïncide avec celui de $\mathbf{P}^1(A/n)$, l'application $\mathbf{P}^1(A)_e \rightarrow \mathbf{P}^1(A/n)$ est bijective. Donc $M_e(R) \rightarrow \mathbf{M}_n(R)$ est surjective et on conclut. \square

6.2. Une base explicite. — On résout maintenant les relations pour trouver une base explicite de $M_e(R)$ en suivant une idée de Merel. Soit $D_{>}$ l'ensemble des $[u : v] \in \mathbf{P}^1(A)_e$ avec u, v unitaires et $\deg u > \deg v$.

Proposition 6.3. — *Soit $e > 0$. L'ensemble $\{[1 : 0]\} \cup D_{>}$ fournit une base de $M_e(R)$ sur R . En particulier, ce module est libre de rang $1 + (q^{2e+1} - q)/(q^2 - 1)$.*

Démonstration. — Commençons par démontrer que la famille est génératrice. Posons

$$\begin{aligned} D' &= \{[u : v] \in \mathbf{P}^1(A)_e \mid \deg u < \deg v\} \\ D'' &= \{[u : v] \in \mathbf{P}^1(A)_e \mid \deg u > \deg v\} \\ E &= \{[u : v] \in \mathbf{P}^1(A)_e \mid \deg u = \deg v\} \end{aligned}$$

de sorte que $\mathbf{P}^1(A)_e = D' \sqcup D'' \sqcup E$. Il suffit de voir que D'' donne une famille génératrice : les relations diagonales appliquées à D'' permettront ensuite de ne garder que les éléments de $\{[1 : 0]\} \cup D_{>}$ comme générateurs de $M_e(R)$.

On constate que $\sigma(D') = D''$ et $\sigma(D'') = D'$. D'après les relations à deux termes sur D'' , $M_e(R)$ est donc engendré par $D'' \sqcup E$. Il reste à éliminer les éléments de E de la liste des générateurs.

Soit $E^* = \{[u : v] \in E \mid \lambda_u + \lambda_v = 0\}$ où λ_u (resp. λ_v) est le coefficient dominant de u (resp. v). Par une relation diagonale sur E , on peut toujours ramener un élément de E à un élément de E^* dans $M_e(R)$ (il suffit de considérer $[u : v] - [u : v] \begin{pmatrix} -\lambda_v & 0 \\ 0 & \lambda_u \end{pmatrix}$). De plus, sur E^* , on a $\tau(E^*) = D''$ et $\tau^2(E^*) = D'$. Donc tout élément de E^* s'écrit, dans $M_e(R)$, comme somme d'un élément de D'' et d'un élément de D' , donc somme d'éléments de D'' . Ainsi, $M_e(R)$ est engendré par D'' , donc par $\{[1 : 0]\} \cup D_{>}$.

Vérifions ensuite que toutes les relations de Manin–Teitelbaum ont été épuisées. On a déjà utilisé les relations diagonales sur D'' , les relations à deux termes sur D'' (ou, ce qui revient au même, sur D') et les relations à trois termes sur E^* (ou, ce qui revient au même, sur D' ou D'' , car $\tau(E^*) = D''$ et $\tau^2(E^*) = D'$). Notons \mathcal{R} le sous-module de $R[\mathbf{P}^1(A)_e]$ engendré par ces relations. On vérifie aisément que les relations diagonales sur D' sont engendrées par celles à deux termes et diagonales sur D'' , donc sont dans \mathcal{R} . Passons maintenant aux relations restantes sur E . D'après l'étude précédente, tout élément $[u : v]$ de E est somme de $[\lambda_u v : w] - [\lambda_v u : w]$ et d'un élément de \mathcal{R} , en posant $w = \lambda_v u - \lambda_u v$. Considérons l'application bien définie

$$\begin{aligned} \theta : \quad E &\longrightarrow R[\mathbf{P}^1(A)_e] \\ [u : v] &\longmapsto [\lambda_u v : w] - [\lambda_v u : w]. \end{aligned}$$

Comme $\sigma(E) = E$ et $\theta([u : v] \sigma) = -\theta([u : v])$, on voit que les relations à deux termes sur E sont dans \mathcal{R} . De même, toute matrice diagonale δ de $G(\mathbf{F}_q)$ stabilise E et satisfait

$\theta([u : v] \delta) = \theta([u : v])$. Donc les relations diagonales sur E appartiennent à \mathcal{R} . Enfin, on constate que τ stabilise $E - E^*$ et, pour $[u : v] \in E - E^*$,

$$\begin{aligned}\theta([u : v]) &= [\lambda_u v : w] - [\lambda_v u : w] \\ \theta([u : v] \tau) &= [\lambda_v(-u - v) : w] - [\lambda_{-u-v} v : w] \\ \theta([u : v] \tau^2) &= [\lambda_{-u-v} u : -w] - [\lambda_u(-u - v) : -w].\end{aligned}$$

En utilisant les relations diagonales (elles appartiennent à \mathcal{R}), on voit alors que $\theta([u : v]) + \theta([u : v] \tau) + \theta([u : v] \tau^2)$ est dans \mathcal{R} . Alors il en est de même pour la relation à trois termes sur $[u : v]$.

Pour déterminer le rang de $M_e(R)$, on dénombre $D_{>}$. Cet ensemble est en bijection avec les couples $(u, v) \in A \times A$ avec u, v unitaires, premiers entre eux et $\deg v < \deg u \leq e$. Avec les notations du lemme 6.1, il y a $\sum_{i=1}^e \sum_{j=0}^{i-1} N_{i,j}$, c'est-à-dire $(q^{2e+1} - q)/(q^2 - 1)$, tels couples. \square

L'énoncé suivant se déduit des propositions 6.2 et 6.3 et entraîne le théorème 1.2.

Théorème 6.4. — *Soit \mathfrak{n} un idéal premier, de degré noté d . Les symboles modulaires $\xi(1 : 0)$ et $\xi(u : v)$ pour $u, v \in A$ unitaires premiers entre eux avec $\deg v < \deg u < d/2$ forment :*

- une famille libre de $\mathbf{M}_n(R)$;
- une base \mathcal{B} de $\mathbf{M}_n(R)$ si d est impair.

Remarque 6.5. — Si d est impair, on retrouve la formule (2) de Gekeler pour le genre. En effet, \mathbf{M}_n est alors de rang $1 + (q^d - q)/(q^2 - 1)$ sur \mathbf{Z} (d'après les propositions 6.2 et 6.3) et on sait, d'après Teitelbaum, que ce rang doit être $1 + g$. On retrouve aussi le fait que \mathbf{M}_n est sans torsion sur \mathbf{Z} (voir la remarque de Teitelbaum, p. 278 de [30]).

Lorsque d est impair, on a même résolu les relations de Manin–Teitelbaum de façon explicite. La preuve de la proposition 6.3 fournit l'énoncé qui suit.

Théorème 6.6. — *Soit \mathfrak{n} un idéal premier de degré impair, noté d . Pour tout $x \in \mathbf{P}^1(A/\mathfrak{n})$, la procédure suivante exprime le symbole modulaire $\xi(x)$ dans la base \mathcal{B} de $\mathbf{M}_n(R)$.*

- On écrit $x = (u : v)$ avec u, v dans A de degré $\leq (d - 1)/2$ et $(u) + (v) = A$ (proposition 6.2). Si $u \neq 0$ (resp. $v \neq 0$), notons λ_u (resp. λ_v) le coefficient dominant de u (resp. v).
- Si $\deg u > \deg v$, alors $\xi(x) = \begin{cases} \xi(1 : 0) & \text{si } v = 0 \\ \xi(u/\lambda_u : v/\lambda_v) & \text{sinon.} \end{cases}$
- Si $\deg u < \deg v$, alors $\xi(x) = \begin{cases} -\xi(1 : 0) & \text{si } u = 0 \\ -\xi(u/\lambda_u : v/\lambda_v) & \text{sinon.} \end{cases}$
- Supposons $\deg u = \deg v$. Notons $w = \lambda_v u - \lambda_u v$, λ_w le coefficient dominant de w et (w, v) (resp. (w, u)) le pgcd unitaire de w et v (resp. w et u). Alors

$$\xi(x) = \xi\left(\frac{v}{\lambda_v(v, w)} : \frac{w}{\lambda_w(v, w)}\right) - \xi\left(\frac{u}{\lambda_u(u, w)} : \frac{w}{\lambda_w(u, w)}\right).$$

En particulier, tout symbole de Manin–Teitelbaum s'écrit comme combinaison linéaire d'au plus deux éléments de la base \mathcal{B} .

Si $\deg \mathfrak{n}$ est impair, comme $\mathbf{M}_{\mathfrak{n}}^0$ est libre, on a un isomorphisme $\alpha : \mathbf{M}_{\mathfrak{n}}^0 \xrightarrow{\simeq} \mathbf{H}_{\mathfrak{n}}$ d'après le lemme 4.4. Le théorème 6.6 se traduit alors en une base de l'espace des cochaînes paraboliques, explicite en un certain sens.

Corollaire 6.7. — Soit \mathfrak{n} premier de degré impair $d \geq 3$. Les cochaînes paraboliques $\alpha(\xi(u : v))$, pour u et v unitaires, premiers entre eux et tels que $\deg v < \deg u < d/2$, forment une base de $\mathbf{H}_{\mathfrak{n}}$ sur \mathbf{Z} .

Remarque 6.8. — Gekeler a déjà donné une base explicite de $\mathbf{H}_{\mathfrak{n}}$ si \mathfrak{n} est de degré 3, non nécessairement premier ([3, section 6] et [7, section 6]). Au paragraphe 7.1.2, on la comparera sur un exemple avec celle du corollaire 6.7. Si ces bases coïncident, le théorème 6.4 pourrait alors être vu comme un prolongement du travail de Gekeler, pour \mathfrak{n} premier quelconque.

7. Indépendance linéaire d'opérateurs de Hecke dans $\mathbf{M}_{\mathfrak{n}}$

Dans cette section, on suppose l'idéal \mathfrak{n} premier.

7.1. L'élément d'enroulement \mathbf{e} . —

7.1.1. *Définition et propriétés.* —

Définition 7.1. — En s'inspirant de [16, 19], on appelle *élément d'enroulement* le symbole modulaire parabolique $\mathbf{e} \in \mathbf{M}_{\mathfrak{n}}^0(\mathbf{Q})$ qui correspond à la forme linéaire $F \mapsto \langle [0, \infty], F \rangle$ sur $\mathbf{H}(\mathbf{Q})$ d'après le théorème 4.3.

Notation 7.2. — On pose $\eta_{\mathfrak{m}} = T_{\mathfrak{m}} - (q^{\deg \mathfrak{m}} + 1)$ dans \mathbf{T} , pour tout premier $\mathfrak{m} \neq \mathfrak{n}$.

Lemme 7.3. — On a $\eta_{\mathfrak{m}}[0, \infty] = \eta_{\mathfrak{m}}\mathbf{e}$ dans $(q - 1)\mathbf{M}^0$.

Démonstration. — Soit P (resp. N) le générateur unitaire de \mathfrak{m} (resp. \mathfrak{n}). Les idéaux \mathfrak{n} et \mathfrak{m} étant premiers distincts, on a par définition des opérateurs de Hecke

$$\eta_{\mathfrak{m}}[0, \infty] = \sum_{\substack{b \in A, b \neq 0 \\ \deg b < \deg P}} [b/P, 0].$$

Par ailleurs, le symbole modulaire $[b/P, 0]$ est parabolique car $(bN, P) = 1$. Enfin, pour tout $\lambda \in \mathbf{F}_q^\times$, on a $[\lambda b/P, 0] = [b/P, 0]$. Donc

$$\eta_{\mathfrak{m}}[0, \infty] = (q - 1) \sum_{\deg b < \deg P, b \text{ unitaire}} [b/P, 0] \in (q - 1)\mathbf{M}^0.$$

Par l'accouplement $\langle \cdot, \cdot \rangle$, les symboles modulaires $[0, \infty]$ et \mathbf{e} définissent la même forme linéaire sur les cochaînes. Par compatibilité de $\langle \cdot, \cdot \rangle$ à Hecke, il en est de même de $\eta_{\mathfrak{m}}[0, \infty]$ et $\eta_{\mathfrak{m}}\mathbf{e}$. Ces symboles étant paraboliques d'après ce qui précède, ils sont égaux par perfection de $\langle \cdot, \cdot \rangle$ sur \mathbf{Q} . \square

Définition 7.4 (voir aussi [21, 7.10]). — L'idéal d'Eisenstein I_E est l'idéal de \mathbf{T} engendré par les éléments $\eta_{\mathfrak{m}}$ pour \mathfrak{m} premier, $\mathfrak{m} \neq \mathfrak{n}$.

Il n'est pas clair que cette définition coïncide avec de A. Tamagawa [27, p. 230] comme annulateur du diviseur cuspidal. D'après le lemme 7.3, $I_E \mathbf{e}$ est contenu dans $(q-1)\mathbf{M}^0$. On rappelle le résultat suivant de Pál concernant la structure de \mathbf{T}/I_E , analogue d'un célèbre énoncé de Mazur [16].

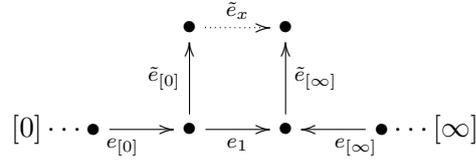
Théorème 7.5 ([23, théorème 1.2]). — *Pour \mathbf{n} premier, le groupe abélien \mathbf{T}/I_E est cyclique d'ordre*

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

Proposition 7.6. — *Il existe un plus petit entier $d_{\mathbf{e}} > 0$ tel que $d_{\mathbf{e}} \mathbf{e} \in \mathbf{M}^0$. On l'appelle dénominateur de \mathbf{e} . Il divise $n_E(\mathbf{n})$; en particulier, il est premier à p .*

Démonstration. — Soit \mathbf{e}' la classe de \mathbf{e} dans $\mathbf{M}^0(\mathbf{Q})/\mathbf{M}^0$. Comme $I_E \mathbf{e} \subset \mathbf{M}^0$, l'homomorphisme canonique de groupes abéliens $\mathbf{T} \rightarrow \mathbf{T}\mathbf{e}'$ passe au quotient en un homomorphisme surjectif $\mathbf{T}/I_E \rightarrow \mathbf{T}\mathbf{e}'$. D'après le théorème 7.5, $\mathbf{T}\mathbf{e}'$ est donc fini d'ordre divisant $n_E(\mathbf{n})$. On en déduit que \mathbf{e}' est d'ordre fini, divisant $n_E(\mathbf{n})$, dans le groupe $\mathbf{M}^0(\mathbf{Q})/\mathbf{M}^0$. Cet ordre est le dénominateur de \mathbf{e} . Il est premier à p car $p \nmid n_E(\mathbf{n})$. \square

7.1.2. *Un exemple de calcul de \mathbf{e} .* — Rappelons l'isomorphisme issu du paragraphe 4.3 : $\mathbf{M}^0(\mathbf{Q}) \xrightarrow{\alpha} \mathbf{H}(\mathbf{Q})$. Pour \mathbf{n} premier de degré 3, on propose d'expliciter $\alpha(\mathbf{e})$ dans une base de $\mathbf{H}(\mathbf{Q})$. Notre calcul repose sur une description précise du graphe $\Gamma \backslash \mathcal{T}$ donnée par Gekeler. Le graphe est de genre q et possède deux pointes $[0]$ et $[\infty]$. D'après [3, 5.3] et [7, section 6], en reprenant les notations de ce dernier, sa structure est la suivante :



où \tilde{e}_x désigne q arêtes indexées par $x \in \mathbf{F}_q$. On vérifie que la projection dans $H_1(\Gamma \backslash \mathcal{T}, \mathbf{pts}, \mathbf{Z})$ de la géodésique de \mathcal{T} reliant le bout 0 au bout ∞ passe successivement par les arêtes $e_{[0]}$, e_1 et l'arête opposée de $e_{[\infty]}$. Suivant Gekeler, pour $x \in \mathbf{F}_q$, on note φ_x l'unique élément de \mathbf{H} vérifiant

$$\varphi_x(\tilde{e}_{[\infty]}) = -1, \quad \varphi_x(\tilde{e}_y) = \delta_{xy} \quad (y \in \mathbf{F}_q)$$

où δ est le symbole de Kronecker. Alors $\{\varphi_x\}_{x \in \mathbf{F}_q}$ est une base de \mathbf{H} . Notons $\{\varphi'_x\}_x$ la base duale de $\text{Hom}(\mathbf{H}, \mathbf{Z})$. La forme linéaire $F \mapsto \langle [0, \infty], F \rangle$ s'écrit $\sum_{x \in \mathbf{F}_q} \varphi'_x$. Nous exprimons maintenant la cochaîne $\alpha(\mathbf{e}) \in \mathbf{H}(\mathbf{Q})$ dans la base $\{\varphi_x\}_x$. Elle est déterminée de façon unique par

$$(\alpha(\mathbf{e}), \cdot)_\mu = \sum_{x \in \mathbf{F}_q} \varphi'_x.$$

En calculant le volume de chaque arête du graphe à l'aide du lemme 5.6 de [3] ou de la section 6 de [7], on déduit que la matrice du produit de Petersson dans la base $\{\varphi_x\}_x$

est $I + (q + 1)J$, où I est la matrice identité et J la matrice dont tous les coefficients sont égaux à 1 (elles sont carrées de taille q). Un calcul d'algèbre linéaire donne alors

$$\alpha(\mathbf{e}) = \frac{1}{q^2 + q + 1} \sum_{x \in \mathbf{F}_q} \varphi_x \in \mathbf{H}(\mathbf{Q}).$$

Remarquons que le dénominateur de \mathbf{e} est exactement $n_E(\mathbf{n})$.

Maintenant, sur un exemple, on exprime \mathbf{e} dans la base explicite de symboles du théorème 1.2. Cela nous permettra de comparer cette base à celle de Gekeler évoquée dans la remarque 6.8.

Exemple 7.7 ($q = 2$ et $\mathbf{n} = (T^3 + T + 1)$ idéal premier). — L'espace \mathbf{M}^0 a pour base $\{\xi(T : 1), \xi(T + 1 : 1)\}$. Pour \mathfrak{p} idéal de degré 1, de générateur unitaire P , on a $\eta_{\mathfrak{p}}\mathbf{e} = -(q - 1)\xi(P : 1)$ (voir la preuve du lemme 7.3). Cela donne

$$(6) \quad \eta_{T}\mathbf{e} = (T_{(T)} - 3)\mathbf{e} = -\xi(T : 1).$$

Par ailleurs, la matrice de l'opérateur $T_{(T)}$ dans la base est $\begin{pmatrix} -3 & 2 \\ -1 & 1 \end{pmatrix}$. On déduit de (6) :

$$\mathbf{e} = \frac{1}{7}(\xi(T : 1) + \xi(T + 1 : 1)).$$

Avec les notations précédentes, la base de Gekeler pour \mathbf{H} est $\{\varphi_0, \varphi_1\}$. Notons i l'injection $\mathbf{H} \rightarrow \text{Hom}(\mathbf{H}, \mathbf{Z})$ donnée par le produit de Petersson et $v = i \circ \alpha : \mathbf{M} \rightarrow \text{Hom}(\mathbf{H}, \mathbf{Z})$. Si \mathfrak{p} est de degré 1, on a $v(\xi(P : 1)) = -\eta_{\mathfrak{p}}^t(v(\mathbf{e})) = -\eta_{\mathfrak{p}}^t(\varphi'_0 + \varphi'_1)$, où $\eta_{\mathfrak{p}}^t$ désigne l'application transposée de $\eta_{\mathfrak{p}}$. Par ailleurs, les matrices des opérateurs $T_{(T)}$ et $T_{(T+1)}$ dans $\{\varphi_0, \varphi_1\}$ sont respectivement $\begin{pmatrix} -3 & -1 \\ 2 & 1 \end{pmatrix}$ et $\begin{pmatrix} 2 & -1 \\ -2 & -2 \end{pmatrix}$ d'après Gekeler ([3, 6.10]). On en déduit $v(\xi(T : 1)) = 4\varphi'_0 + 3\varphi'_1$ et $v(\xi(T + 1 : 1)) = 3\varphi'_0 + 4\varphi'_1$. Comme la matrice du produit de Petersson est $\begin{pmatrix} 4 & 3 \\ 3 & 4 \end{pmatrix}$, on a alors $\alpha(\xi(T : 1)) = \varphi_0$ et $\alpha(\xi(T + 1 : 1)) = \varphi_1$. La base de Gekeler coïncide donc avec celle du corollaire 6.7.

7.2. Indépendance linéaire dans le module de Hecke engendré par \mathbf{e} . — L'énoncé d'indépendance linéaire est établi sur $[0, \infty]$ puis relevé à \mathbf{e} .

Notation 7.8. — Pour un entier $r \geq 0$, on note A_r (resp. $A_{\leq r}$) l'ensemble des idéaux non nuls de degré r (resp. $\leq r$) de A .

Proposition 7.9. — Soient R un anneau commutatif intègre dans lequel $q - 1$ est non nul et $r \geq 0$ un entier. Si $\deg \mathbf{n} \geq 2r + 1$, la famille $\{T_{\mathfrak{m}}[0, \infty]\}_{\mathfrak{m} \in A_{\leq r}}$ est libre sur R dans $\mathbf{M}(R)$.

Démonstration. — On procède par récurrence sur r . Comme $\mathbf{n} \neq A$, le symbole modulaire $[0, \infty]$ est non nul, ce qui démontre l'affirmation pour $r = 0$. Supposons l'énoncé vérifié pour $r - 1$ et l'existence d'une relation

$$(7) \quad \sum_{\mathfrak{m} \in A_{\leq r}} \lambda_{\mathfrak{m}} T_{\mathfrak{m}}[0, \infty] = 0$$

avec $\lambda_{\mathfrak{m}} \in R$. Montrons que $\lambda_{\mathfrak{p}} = 0$ pour tout \mathfrak{p} dans A_r . L'hypothèse de récurrence permettra alors de conclure. Appliquons la formule du théorème 1.1 et utilisons $\xi(c :$

$d) = -\xi(d : c)$, égalité qui provient des relations à deux termes et diagonales. On obtient

$$T_{\mathfrak{m}}[0, \infty] = - \sum_{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{S}_{\mathfrak{m}, (c)+(d)+\mathfrak{n}=A}} \xi(d : c).$$

Par ailleurs, $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{S}_{\mathfrak{m}}$ si et seulement si $\begin{pmatrix} a & \lambda^{-1}b \\ \lambda c & d \end{pmatrix} \in \mathcal{S}_{\mathfrak{m}}$ pour tout $\lambda \in \mathbf{F}_q^\times$. On a donc

$$T_{\mathfrak{m}}[0, \infty] = n\xi(1 : 0) - (q-1) \sum_{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{S}_{\mathfrak{m}, c \text{ unitaire}, (c)+(d)+\mathfrak{n}=A}} \xi(d : c)$$

pour un $n \in R$. Remarquons que la condition sur la caractéristique de R empêche $T_{\mathfrak{m}}[0, \infty]$ d'être proportionnel à $\xi(1 : 0)$ pour tout \mathfrak{m} .

Notons $u_{\mathfrak{m}}$ l'ensemble des $(d, c) \in A \times A$ avec c unitaire tels qu'il existe a, b dans A avec $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{S}_{\mathfrak{m}}$. Notons P le générateur unitaire de \mathfrak{p} . Des considérations élémentaires montrent que $(d : c) = (P : 1)$ pour un $(d, c) \in u_{\mathfrak{m}}$ (avec $\mathfrak{m} \in A_{\leq r}$) si et seulement si $\mathfrak{m} = \mathfrak{p}$ et $(d, c) = (P, 1)$. En isolant l'unique terme en $\xi(P : 1)$ dans (7), on obtient alors

$$(q-1)\lambda_{\mathfrak{p}}\xi(P : 1) = n'\xi(1 : 0) + \sum_{(d,c) \in v'_r, (c)+(d)+\mathfrak{n}=A} \alpha_{d,c} \xi(d : c)$$

avec $v_r = \bigcup_{\mathfrak{m} \in A_{\leq r}} u_{\mathfrak{m}}$, $v'_r = v_r - \{(P, 1)\}$, et n' et $\alpha_{d,c}$ des éléments R . On constate que quitte à changer les coefficients $\alpha_{d,c}$ on peut aussi supposer d et c premiers entre eux. Par hypothèse, on a $r < \deg(\mathfrak{n})/2$ donc les symboles modulaires

$$\{\xi(1 : 0), \xi(P : 1)\} \cup \{\xi(d : c) \mid (d, c) \in v'_r, (d) + (c) = A\}$$

forment une sous-famille de celle, libre, du théorème 6.4. Le théorème appliqué à R donne $(q-1)\lambda_{\mathfrak{p}} = 0$. Comme $q-1$ est non nul dans R , on conclut $\lambda_{\mathfrak{p}} = 0$. \square

On donne des énoncés de relèvement en caractéristique 0 et p .

Notation 7.10. — Soit $\tilde{\mathfrak{e}}$ la classe de $d_{\mathfrak{e}}\mathfrak{e}$ dans $\mathbf{M}^0/p\mathbf{M}^0$.

Lemme 7.11. — 1. Supposons la famille $\{T_{\mathfrak{m}}[0, \infty]\}_{\mathfrak{m} \in A_{\leq r+1}}$ libre sur \mathbf{Z} dans \mathbf{M} .

Alors, pour tout entier $0 \leq r' \leq r$, la famille $\{T_{\mathfrak{m}}\mathfrak{e}\}_{\mathfrak{m} \in A_{r'}}$ est libre sur \mathbf{Z} .

2. Supposons la famille $\{T_{\mathfrak{m}}[0, \infty]\}_{\mathfrak{m} \in A_{\leq r+1}}$ libre sur \mathbf{F}_p dans $\mathbf{M}(\mathbf{F}_p)$. Alors, pour tout entier $0 \leq r' \leq r$, la famille $\{T_{\mathfrak{m}}\tilde{\mathfrak{e}}\}_{\mathfrak{m} \in A_{r'}}$ est libre sur \mathbf{F}_p dans $\mathbf{M}^0/p\mathbf{M}^0$.

Démonstration. — Supposons qu'il existe $\lambda_{\mathfrak{m}} \in \mathbf{Z}$, presque tous nuls pour $\mathfrak{m} \in A_{r'}$, avec $\sum_{\mathfrak{m}} \lambda_{\mathfrak{m}} T_{\mathfrak{m}}\mathfrak{e} = 0$. Fixons un idéal \mathfrak{p} de A de degré 1. En appliquant l'élément $\eta_{\mathfrak{p}}$ de l'anneau commutatif \mathbf{T} , on obtient $\sum_{\mathfrak{m}} \lambda_{\mathfrak{m}} T_{\mathfrak{m}}\eta_{\mathfrak{p}}\mathfrak{e} = 0$. Puis, comme $\eta_{\mathfrak{p}}\mathfrak{e} = \eta_{\mathfrak{p}}[0, \infty]$ d'après le lemme 7.3, on a

$$(8) \quad \sum_{\mathfrak{m} \in A_{r'}} \lambda_{\mathfrak{m}} T_{\mathfrak{m}} T_{\mathfrak{p}}[0, \infty] - (q^{\deg \mathfrak{p}} + 1) \sum_{\mathfrak{m} \in A_{r'}} \lambda_{\mathfrak{m}} T_{\mathfrak{m}}[0, \infty] = 0.$$

Les opérateurs $T_{\mathfrak{m}}$ satisfont aux propriétés usuelles ci-dessous (q est premier) :

$$\begin{aligned} T_{\mathfrak{m}} T_{\mathfrak{m}'} &= T_{\mathfrak{m}\mathfrak{m}'} && \text{si } \mathfrak{m} + \mathfrak{m}' = A \\ T_{\mathfrak{q}^i} T_{\mathfrak{q}} &= T_{\mathfrak{q}^{i+1}} + q^{\deg \mathfrak{q}} T_{\mathfrak{q}^{i-1}} && \text{si } \mathfrak{q} + \mathfrak{n} = A \\ T_{\mathfrak{q}^i} &= (T_{\mathfrak{q}})^i && \text{si } \mathfrak{q} + \mathfrak{n} \neq A. \end{aligned}$$

En particulier, $T_m T_p$ s'écrit comme somme de T_{mp} et d'une combinaison linéaire à coefficients dans \mathbf{Z} de T_τ où $\deg \tau < \deg(mp)$ c'est-à-dire $\tau \in A_{\leq r'}$. De (8), on déduit alors une expression dans laquelle le coefficient λ_m de $T_{mp}[0, \infty]$ est nul par hypothèse, pour tout $m \in A_{r'}$. Cela démontre que la famille est libre. Sur \mathbf{F}_p , on raisonne de la même manière en utilisant le fait que d_e est premier à p (proposition 7.6). \square

Théorème 7.12. — *Soit \mathfrak{n} un idéal premier de A de degré ≥ 3 . Soit r un entier vérifiant $0 \leq r \leq (\deg(\mathfrak{n}) - 3)/2$.*

1. *Les symboles modulaires $\{T_m \mathbf{e}\}_{m \in A_r}$ sont libres sur \mathbf{Z} dans $\mathbf{Te} \subset \mathbf{M}^0(\mathbf{Q})$.*
2. *Les symboles modulaires $\{T_m \tilde{\mathbf{e}}\}_{m \in A_r}$ sont libres sur \mathbf{F}_p dans $\mathbf{M}^0/p\mathbf{M}^0$.*

Démonstration. — Comme $\deg \mathfrak{n} \geq 2r + 3$, la famille $\{T_m[0, \infty]\}_{m \in A_{\leq r+1}}$ est libre sur \mathbf{Z} dans \mathbf{M} d'après la proposition 7.9. On relève le résultat dans \mathbf{Te} à l'aide du lemme 7.11. Le deuxième énoncé se prouve de façon similaire avec la proposition 7.9 pour $R = \mathbf{F}_p$. \square

Corollaire 7.13. — *Les affirmations suivantes sont équivalentes pour \mathfrak{n} premier :*

1. $\mathbf{e} \neq 0$;
2. $g > 0$;
3. $\deg \mathfrak{n} \geq 3$.

Démonstration. — L'équivalence de 2 et 3 découle de la formule (2) qui donne le genre en fonction de $\deg \mathfrak{n}$. Le théorème 7.12 pour $r = 0$ démontre $3 \Rightarrow 1$. Enfin, l'implication $1 \Rightarrow 2$ vient du fait que la dimension de $\mathbf{M}^0(\mathbf{Q})$ est g . \square

7.3. Non-annulation de fonctions L de formes automorphes. — On rappelle quelques résultats sur l'algèbre de Hecke issus de la théorie des formes automorphes. Comme \mathbf{H} est libre de type fini sur \mathbf{Z} et qu'on peut voir \mathbf{T} comme une sous-algèbre de $\text{End}(\mathbf{H})$, le \mathbf{Z} -module \mathbf{T} est libre de type fini. Soit $\mathcal{F}_\mathfrak{n}$ l'ensemble des formes primitives de $\mathbf{H}(\mathbf{C})$; on le notera aussi \mathcal{F} pour simplifier. On a supposé \mathfrak{n} premier donc elles constituent une base de $\mathbf{H}(\mathbf{C})$. Le groupe de Galois absolu de \mathbf{Q} opère sur \mathcal{F} via son action sur les coefficients de Fourier. Notons \mathcal{E} l'ensemble des orbites pour cette action. Pour $F \in \mathcal{F}$, soient $[F]$ l'orbite et $a_{[F]}$ l'idéal 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} .

Soit K_F le corps de nombres totalement réel engendré par les coefficients de Fourier de F . Le degré de K_F sur \mathbf{Q} coïncide avec le cardinal de l'orbite $[F]$. L'homomorphisme d'anneaux

$$\begin{array}{ccc} \mathbf{T} & \longrightarrow & K_F \\ t & \longmapsto & \frac{tF}{F} \end{array}$$

est de noyau $a_{[F]}$. Il induit un isomorphisme de \mathbf{Q} -algèbres $(\mathbf{T}/a_{[F]}) \otimes_{\mathbf{Z}} \mathbf{Q} \simeq K_F$. L'homomorphisme canonique de \mathbf{T} -modules $\varphi : \mathbf{T} \rightarrow \prod_{[F] \in \mathcal{E}} \mathbf{T}/a_{[F]}$ est injectif et son image est d'indice fini. Donc la \mathbf{Q} -algèbre $\mathbf{T} \otimes_{\mathbf{Z}} \mathbf{Q}$ est semi-simple et isomorphe au produit des K_F pour $[F] \in \mathcal{E}$. En particulier, l'algèbre \mathbf{T} est de rang g sur \mathbf{Z} .

Lemme 7.14. — *Le \mathbf{Z} -module \mathbf{Te} est libre de rang $\#\{F \in \mathcal{F} \mid L(F, 1) \neq 0\}$.*

Démonstration. — Ce module est clairement sans torsion et de type fini, donc libre. Soit $I_{\mathbf{e}}$ l'idéal annulateur de \mathbf{e} dans \mathbf{T} . L'application $t \mapsto t\mathbf{e}$ de \mathbf{T} dans \mathbf{T} donne un isomorphisme de \mathbf{Z} -modules $\mathbf{T}/I_{\mathbf{e}} \simeq \mathbf{T}\mathbf{e}$. Calculons le rang du quotient.

Soit $\mathcal{E}_{\mathbf{e}}$ l'ensemble des orbites $[F] \in \mathcal{E}$ telles que $L(F, 1) \neq 0$ (cette condition ne dépend que de $[F]$). On commence par montrer :

$$(9) \quad \bigcap_{[F] \in \mathcal{E}_{\mathbf{e}}} a_{[F]} = I_{\mathbf{e}}.$$

Soit t dans l'intersection. Pour tout $F \in \mathcal{F}$ vérifiant $L(F, 1) \neq 0$, on a $\langle t\mathbf{e}, F \rangle = \langle \mathbf{e}, tF \rangle = 0$. Par ailleurs, si $F \in \mathcal{F}$ vérifie $L(F, 1) = 0$, on a $\langle \mathbf{e}, F \rangle = 0$ donc $\langle t\mathbf{e}, F \rangle = 0$ car F est propre. Ainsi $t\mathbf{e}$ est orthogonal à \mathcal{F} et, comme l'accouplement est parfait, on en déduit $t\mathbf{e} = 0$. Cela démontre une inclusion. Pour l'autre, prenons t dans l'annulateur de \mathbf{e} et $F \in \mathcal{F}$ vérifiant $L(F, 1) \neq 0$. On a $\langle \mathbf{e}, tF \rangle = \langle t\mathbf{e}, F \rangle = 0$. Comme F est propre et $\langle \mathbf{e}, F \rangle \neq 0$, on en déduit $tF = 0$. Donc t appartient à $a_{[F]}$ pour tout $[F] \in \mathcal{E}_{\mathbf{e}}$.

L'homomorphisme canonique de \mathbf{Z} -modules $\mathbf{T} \rightarrow \prod_{[F] \in \mathcal{E}_{\mathbf{e}}} \mathbf{T}/a_{[F]}$ est de noyau $I_{\mathbf{e}}$ d'après ce qui précède, et son image est d'indice fini car il en est de même de φ . Donc le \mathbf{Q} -espace vectoriel $(\mathbf{T}/I_{\mathbf{e}}) \otimes_{\mathbf{Z}} \mathbf{Q}$ est isomorphe au produit $\prod_{[F] \in \mathcal{E}_{\mathbf{e}}} K_F$. Il est de dimension $\sum_{[F] \in \mathcal{E}_{\mathbf{e}}} [K_F : \mathbf{Q}] = \#\{F \in \mathcal{F} \mid L(F, 1) \neq 0\}$. Le \mathbf{Z} -module $\mathbf{T}/I_{\mathbf{e}}$ a le rang annoncé. \square

On traduit alors l'indépendance linéaire (théorème 7.12) en l'énoncé de non-annulation.

Preuve du théorème 1.4. — Soit $r \geq 0$ la partie entière de $(\deg(\mathbf{n}) - 3)/2$. Le \mathbf{Z} -module $\mathbf{T}\mathbf{e}$ est de rang $\#\{F \in \mathcal{F} \mid L(F, 1) \neq 0\}$ par le lemme 7.14. Par ailleurs, d'après le théorème 7.12, il est de rang $\geq \#A_r = q^r$. Enfin, la formule (2) pour $\#\mathcal{F} = g$ donne l'inégalité $q^r \geq (q^2 - 1)^{1/2} g^{1/2} / q^2$. \square

8. L'analogie de l'homomorphisme d'enroulement de Mazur

Dans cette section, l'idéal \mathbf{n} est encore premier. On pourra comparer la définition suivante à celle donnée par Pál dans la remarque 5.7 de [23].

Définition 8.1. — Suivant Mazur [16], on appelle *homomorphisme d'enroulement* l'homomorphisme de \mathbf{T} -modules

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

(bien défini d'après le lemme 7.3).

L'involution $w_{\mathbf{n}}$ opère comme -1 sur son image, d'après le lemme 7.3 et la relation $w_{\mathbf{n}}[0, \infty] = [\infty, 0]$. On étudie cet homomorphisme lorsque \mathbf{n} est de degré 3 puis on donne un exemple en degré supérieur.

8.1. Homomorphisme d'enroulement en degré 3. — L'énoncé qui suit donne la structure du \mathbf{T} -module \mathbf{M}^0 lorsque \mathbf{n} est premier de degré 3. Il peut être rapproché du théorème 18.10 de [16] pour l'homomorphisme d'enroulement classique localisé en un nombre premier d'Eisenstein.

Théorème 8.2. — Soit \mathfrak{n} premier de degré 3. Alors les symboles modulaires $\eta_{\mathfrak{p}\mathfrak{e}}/(q-1)$, pour \mathfrak{p} de degré 1, forment une base de \mathbf{M}^0 sur \mathbf{Z} . De plus, l'homomorphisme d'enroulement est un isomorphisme de \mathbf{T} -modules $I_E \simeq \mathbf{M}^0$.

Démonstration. — Soit P le générateur unitaire de \mathfrak{p} . Comme il est de degré 1, on a $\eta_{\mathfrak{p}\mathfrak{e}} = \eta_{\mathfrak{p}}[0, \infty] = -(q-1)\xi(P : 1)$ (voir la preuve du lemme 7.3). La base du théorème 1.2 donne alors la première affirmation. L'homomorphisme d'enroulement, dont l'image contient une base de \mathbf{M}^0 sur \mathbf{Z} , est donc surjectif. Pour l'injectivité, il reste à voir que $I_{\mathfrak{e}} \cap I_E = \{0\}$. En fait, l'idéal $I_{\mathfrak{e}}$ est nul pour \mathfrak{n} premier de degré 3. En effet, d'après les rappels de la section 3.2, la fonction $L(F, s)$ est alors constante égale à 1 pour F primitive. D'après la description donnée en (9), l'idéal $I_{\mathfrak{e}}$ est alors l'intersection de tous les idéaux premiers minimaux de \mathbf{T} , donc nul. \square

On en déduit la structure de Hecke des symboles paraboliques et des cochaînes harmoniques modulo p .

Corollaire 8.3. — Soit \mathfrak{n} premier de degré 3. Les $\mathbf{T}/p\mathbf{T}$ -modules $\mathbf{M}^0/p\mathbf{M}^0$ et $\mathbf{H}/p\mathbf{H}$ sont libres de rang 1. En particulier, l'action de $\mathbf{T}/p\mathbf{T}$ sur $\mathbf{H}/p\mathbf{H}$ est fidèle.

Démonstration. — Les deux modules considérés sont isomorphes : c'est une conséquence de l'isomorphisme de \mathbf{T} -modules $\alpha : \mathbf{M}^0 \xrightarrow{\simeq} \mathbf{H}$. De plus, par le théorème 8.2, ils sont aussi isomorphes à I_E/pI_E . Calculons leur rang.

Le groupe \mathbf{T}/I_E est fini d'ordre premier à p , d'après Pál (théorème 7.5). On en déduit que $p\mathbf{T} + I_E = \mathbf{T}$. En effet, supposons que I_E et $p\mathbf{T}$ soient contenus dans un idéal maximal \mathcal{M} de \mathbf{T} . On aurait une surjection canonique de \mathbf{T}/I_E dans le corps \mathbf{T}/\mathcal{M} de caractéristique p . Donc \mathbf{T}/\mathcal{M} serait fini d'ordre premier à p , ce qui est impossible. Les idéaux $p\mathbf{T}$ et I_E étant étrangers, l'inclusion $I_E \hookrightarrow \mathbf{T}$ induit un isomorphisme de $\mathbf{T}/p\mathbf{T}$ -modules $I_E/pI_E \simeq \mathbf{T}/p\mathbf{T}$. Donc I_E/pI_E est de rang 1. \square

8.2. En degré supérieur. — Soit V l'image de l'homomorphisme d'enroulement. Elle est contenue dans le sous-espace propre de $w_{\mathfrak{n}}|_{\mathbf{M}^0}$ pour la valeur propre -1 .

On peut voir que $V \subsetneq \mathbf{M}^0$ dès que $d = \deg(\mathfrak{n}) \geq 4$. En effet, supposons $V = \mathbf{M}^0$. Alors l'involution $w_{\mathfrak{n}}$ agit comme -1 sur \mathbf{M}^0 , donc sur \mathbf{H} . Soit w l'involution d'Atkin-Lehner de la courbe modulaire de Drinfeld X associée à $\Gamma_0(\mathfrak{n})$ (voir [4]). Elle induit un automorphisme de la jacobienne de X , défini sur K , qui serait alors -1 . La courbe X serait hyperelliptique. Mais d'après Schweizer [25, théorème 20], cela ne se produit pas si $d \geq 4$.

Pour $d \geq 3$, la famille $\xi(P : 1)$, pour P unitaire de degré 1, est libre (théorème 6.4). Comme dans la preuve du théorème 8.2, on en déduit que $\mathbf{Q} \cdot V$ est de dimension $\geq q$. On termine en donnant un exemple pour $d = 4$ où cette minoration est optimale.

Exemple 8.4 ($q = 2$, $\mathfrak{n} = (T^4 + T + 1)$ idéal premier). — L'espace $\mathbf{M}^0(\mathbf{Q})$ a pour base $\{\xi(T : 1), \xi(T + 1 : 1), \xi(T^2 : 1), \xi(T^2 + 1 : 1)\}$ et la matrice de $w_{\mathfrak{n}}$ est

$$\begin{pmatrix} -1 & 0 & 0 & -1 \\ 0 & -1 & -1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Le sous-espace propre de w_n pour la valeur propre -1 a pour base $\{\xi(T : 1), \xi(T+1 : 1)\}$. Donc $\mathbf{Q} \cdot V$ est de dimension 2.

Remerciements

La plupart des énoncés proviennent de ma thèse de doctorat de l'Université Paris 7. Ce travail a été approfondi à l'Universität des Saarlandes et au Centre de Recerca Matemàtica et sa rédaction achevée à l'Institut des Hautes Études Scientifiques et au Max-Planck-Institut für Mathematik. Je remercie ces institutions, ainsi qu'Ernst Gekeleler, pour leur hospitalité. Enfin, je suis très reconnaissante à Loïc Merel pour ses précieux commentaires ainsi qu'un argument crucial dans la section 6.

Références

- [1] V. G. DRINFELD : Elliptic modules. *Mat. Sb. (N.S.)*, 94(136):594–627, 656, 1974.
- [2] E.-U. 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.
- [3] E.-U. GEKELER : Automorphe Formen über $\mathbf{F}_q(T)$ mit kleinem Führer. *Abh. Math. Sem. Univ. Hamburg*, 55:111–146, 1985.
- [4] E.-U. GEKELER : Über Drinfeldsche Modulcurven vom Hecke-Typ. *Compositio Math.*, 57(2): 219–236, 1986.
- [5] E.-U. 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).
- [6] E.-U. GEKELER : Improper Eisenstein series on Bruhat-Tits trees. *Manuscripta Math.*, 86(3):367–391, 1995.
- [7] E.-U. GEKELER : On the cuspidal divisor class group of a Drinfeld modular curve. *Doc. Math.*, 2:351–374 (electronic), 1997.
- [8] E.-U. GEKELER : Invariants of some algebraic curves related to Drinfeld modular curves. *J. Number Theory*, 90(1):166–183, 2001.
- [9] E.-U. GEKELER et U. NONNENGARDT : Fundamental domains of some arithmetic groups over function fields. *Internat. J. Math.*, 6(5):689–708, 1995.
- [10] E.-U. GEKELER et M. REVERSAT : Jacobians of Drinfeld modular curves. *J. Reine Angew. Math.*, 476:27–93, 1996.
- [11] H. HAUER et I. LONGHI : Teitelbaum's exceptional zero conjecture in the function field case. *J. Reine Angew. Math.*, 591:149–175, 2006.
- [12] H. IWANIEC et P. SARNAK : The non-vanishing of central values of automorphic L -functions and Landau-Siegel zeros. *Israel J. Math.*, 120(part A):155–177, 2000.
- [13] E. KOWALSKI et P. MICHEL : The analytic rank of $J_0(q)$ and zeros of automorphic L -functions. *Duke Math. J.*, 100(3):503–542, 1999.
- [14] Y. I. MANIN : Parabolic points and zeta functions of modular curves. *Izv. Akad. Nauk SSSR Ser. Mat.*, 36:19–66, 1972.

- [15] B. MAZUR : Courbes elliptiques et symboles modulaires. *In Séminaire Bourbaki, 24^{ème} année (1971/1972), Exp. No. 414*, p. 277–294. Lecture Notes in Math., Vol. 317. Springer, Berlin, 1973.
- [16] B. MAZUR : Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, (47):33–186 (1978), 1977.
- [17] L. MEREL : Opérateurs de Hecke pour $\Gamma_0(N)$ et fractions continues. *Ann. Inst. Fourier (Grenoble)*, 41(3):519–537, 1991.
- [18] L. MEREL : Universal Fourier expansions of modular forms. *In On Artin's conjecture for odd 2-dimensional representations*, vol. 1585 de *Lecture Notes in Math.*, p. 59–94. Springer, Berlin, 1994.
- [19] L. MEREL : Bornes pour la torsion des courbes elliptiques sur les corps de nombres. *Invent. Math.*, 124(1-3):437–449, 1996.
- [20] U. NONNENGARDT : *Arithmetisch definierte Graphen über rationalen Funktionenkörpern*. Diplomarbeit, Universität des Saarlandes, 1994.
- [21] A. PÁL : On the torsion of the Mordell-Weil group of the Jacobian of Drinfeld modular curves. *Doc. Math.*, 10:131–198 (electronic), 2005.
- [22] A. PÁL : Proof of an exceptional zero conjecture for elliptic curves over function fields. *Math. Z.*, 254(3):461–483, 2006.
- [23] A. PÁL : On the Eisenstein ideal of Drinfeld modular curves. *Int. J. Number Theory*, 3(4): 557–598, 2007.
- [24] P. PARENT : Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres. *J. Reine Angew. Math.*, 506:85–116, 1999.
- [25] A. SCHWEIZER : Hyperelliptic Drinfeld modular curves. *In Drinfeld modules, modular schemes and applications (Alden-Biesen, 1996)*, p. 330–343. World Sci. Publ., River Edge, NJ, 1997.
- [26] J.-P. 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.
- [27] A. TAMAGAWA : The Eisenstein quotient of the Jacobian variety of a Drinfeld modular curve. *Publ. Res. Inst. Math. Sci.*, 31(2):203–246, 1995.
- [28] K.-S. TAN : Modular elements over function fields. *J. Number Theory*, 45(3):295–311, 1993.
- [29] K.-S. TAN et D. ROCKMORE : Computation of L -series for elliptic curves over function fields. *J. Reine Angew. Math.*, 424:107–135, 1992.
- [30] J. TEITELBAUM : Modular symbols for $\mathbf{F}_q(T)$. *Duke Math. J.*, 68(2):271–295, 1992.
- [31] J. VANDERKAM : Linear independence of Hecke operators in the homology of $X_0(N)$. *J. London Math. Soc. (2)*, 61(2):349–358, 2000.
- [32] A. WEIL : *Dirichlet series and automorphic forms*, vol. 189 de *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1971.

29 novembre 2010

CÉCILE ARMANA, Max-Planck-Institut für Mathematik – Vivatsgasse 7 – D-53111 Bonn – Allemagne
E-mail : armana@math.jussieu.fr