Une base explicite de symboles modulaires sur les corps de fonctions

Cécile Armana*

2 novembre 2011

Résumé

Modular symbols for the subgroup $\Gamma_0(\mathfrak{n})$ of $\mathrm{GL}_2(\mathbf{F}_q[T])$ have been defined by Teitelbaum. They have a presentation given by a finite number of generators and relations, in a formalism similar to Manin's for classical modular symbols. We completely solve the relations and get an explicit basis of generators when $\mathfrak{n}$ is a prime ideal of odd degree. As an application, we give a non-vanishing statement for L-functions of certain automorphic cusp forms for $\mathbf{F}_q(T)$. The main statement also provides a key-step for a result towards the uniform boundedness conjecture for Drinfeld modules of rank 2.

1 Introduction

Soient $A = \mathbf{F}_q[T]$ l'anneau de polynômes sur un corps fini $\mathbf{F}_q$ à q éléments et $K = \mathbf{F}_q(T)$ son corps des fractions. Dans [32], J. Teitelbaum a introduit les symboles modulaires de poids 2 pour un sous-groupe de congruence de $\mathrm{GL}_2(A)$. Parmi leurs applications, mentionnons des formules pour les valeurs spéciales de fonctions L de certaines formes automorphes pour K [31, 33, 32] et une conjecture de zéro exceptionnel pour les courbes elliptiques sur K (énoncée dans [32], établie indépendamment par Hauer–Longhi [13] et Pál [24]).

Soit $\Gamma_0(\mathfrak{n})$ le sous-groupe de $\mathrm{GL}_2(A)$ formé des matrices triangulaires supérieures modulo un idéal non nul $\mathfrak{n}$ de A. On note $\mathbf{M}_\mathfrak{n}$ le groupe abélien des symboles modulaires pour $\Gamma_0(\mathfrak{n})$ à coefficients dans $\mathbf{Z}$ (sa définition sera rappelée plus loin). Teitelbaum a donné une présentation de $\mathbf{M}_\mathfrak{n}$ par un nombre fini de générateurs et leurs relations, que nous rappelons. Considérons la droite projective $\mathbf{P}^1(A/\mathfrak{n})$ sur l'anneau fini $A/\mathfrak{n}$; on note ses éléments $(u : v)$. D'après Teitelbaum, le groupe abélien $\mathbf{M}_\mathfrak{n}$ est alors isomorphe au quotient du groupe abélien libre $\mathbf{Z}[\mathbf{P}^1(A/\mathfrak{n})]$ par les relations

$$\begin{aligned} (u : v) + (-v : u) &= 0 \\ (u : v) + (v : -u - v) + (-u - v : u) &= 0 \\ (u : v) - (\delta_1 u : \delta_2 v) &= 0 \end{aligned} \tag{1}$$

*Université de Franche–Comté, Laboratoire de Mathématiques de Besançon, CNRS UMR 6623, Faculté des Sciences et Techniques, 16 route de Gray, 25030 Besançon, France – cecile.armana@univ-fcomte.fr

pour tout $\delta_1, \delta_2 \in \mathbf{F}_q^\times$ et $(u : v) \in \mathbf{P}^1(A/\mathfrak{n})$. Notons ξ l'isomorphisme du quotient vers $\mathbf{M}_\mathfrak{n}$. Les générateurs $\xi(u : v)$ de $\mathbf{M}_\mathfrak{n}$ sont appelés *symboles de Manin–Teitelbaum*. Cette présentation finie est en tout point similaire à celle donnée par Manin [16] pour les symboles modulaires classiques associés à $\mathrm{SL}_2(\mathbf{Z})$.

Les symboles modulaires, classiques ou sur K, correspondent essentiellement au premier groupe d'homologie relative aux pointes d'une courbe modulaire (ou ici du graphe combinatoire $\Gamma_0(\mathfrak{n})\backslash\mathcal{T}$, où $\mathcal{T}$ est l'arbre de Bruhat–Tits de $\mathrm{PGL}_2(\mathbf{F}_q((1/T)))$, qui est apparenté à la courbe modulaire de Drinfeld $X_0(\mathfrak{n})$). Or une particularité des relations (1) est d'avoir une forme indépendante de $\mathfrak{n}$. Ainsi les présentations à la Manin décrivent ces groupes d'homologie sans la connaissance préalable d'un domaine fondamental pour le sous-groupe de congruence. Ces présentations se prêtent particulièrement bien à l'implémentation des symboles modulaires sur machine. Elles constituent le socle d'algorithmes de calcul des formes modulaires ou automorphes qui leurs correspondent (voir Cremona [2] et Stein [29] pour un aperçu dans le cas des symboles et formes modulaires classiques).

1.1 Base explicite de symboles de Manin–Teitelbaum

Dorénavant, prenons $\mathfrak{n} = \mathfrak{p}$ premier. Dans ce travail, nous résolvons complètement la présentation de $\mathbf{M}_\mathfrak{p}$ dans un cas assez général ($\mathfrak{p}$ de degré impair) et explicitons une base de $\mathbf{M}_\mathfrak{p}$ extraite des générateurs.

Théorème 1.1. *Soit $\mathfrak{p}$ un idéal de A de degré impair d. Les symboles de Manin–Teitelbaum $\xi(1 : 0)$ et $\xi(u : v)$, où u et v parcourent les polynômes unitaires de A, premiers entre eux et tels que $\deg v < \deg u < d/2$, forment une base de $\mathbf{M}_\mathfrak{p}$ sur $\mathbf{Z}$.*

C'est un cas particulier du théorème 5.16. Il est complété par le théorème 5.18, qui exprime n'importe quel symbole de Manin–Teitelbaum dans cette base. Ces deux énoncés peuvent donc se substituer à la présentation de Teitelbaum. De plus, en retirant $\xi(1 : 0)$ de la liste, on obtient une base du sous-espace parabolique $\mathbf{M}_\mathfrak{p}^0$. Dans le cas où d est pair, mentionnons que la famille du théorème 1.1 est libre mais ne possède pas suffisamment d'éléments pour être une base.

Pour les symboles modulaires de poids 2 pour $\Gamma_0(n) \subset \mathrm{SL}_2(\mathbf{Z})$, Manin a donné une présentation très similaire comme quotient sans torsion du $\mathbf{Z}$-module libre $\mathbf{Z}[\mathbf{P}^1(\mathbf{Z}/n\mathbf{Z})]$ par des relations à deux et trois termes ([16, th. 2.7]). Cependant on ne sait la résoudre qu'au cas par cas, c'est-à-dire en fixant une valeur numérique pour n. Les théorèmes 1.1 et 5.18 n'ont donc pas d'équivalents pour les symboles modulaires classiques et témoignent d'une situation nettement plus favorable sur les corps de fonctions.

La base donnée par le théorème 1.1 ne dépend que de $d = \deg \mathfrak{p}$. De fait, sa démonstration passe par un « modèle » de $\mathbf{M}_\mathfrak{p}$ dans lequel nous sommes capables de résoudre les relations (il s'agit de remplacer $\mathbf{P}^1(A/\mathfrak{p})$ par une troncature de la droite projective $\mathbf{P}^1(A)$). On met aussi en évidence une décomposition naturelle de $\mathbf{M}_\mathfrak{p}$ en somme directe de sous-espaces explicites qui ne dépendent que de d (section 5.2) ; là encore, on ne connaît pas de résultat analogue pour les symboles modulaires classiques. Cette construction et la preuve du théorème 1.1 sont présentées dans la section 5. On utilisera de façon essentielle l'inégalité $\deg(u + v) \leq \max(\deg u, \deg v)$ pour $u, v \in A$, qui est de nature non-archimédienne.

Ces arguments ne semblent donc pas s'adapter de façon naïve à la pré sentation de Manin des symboles modulaires classiques (cf. remarque 5.6).

La restriction dans le théorème 1.1 aux niveaux premiers $\mathfrak{p}$ de degré impair est de nature technique. Le mécanisme de la preuve est suffisamment général pour fournir des énoncés de même nature si $\deg \mathfrak{p}$ est pair, $\mathfrak{p}$ non premier ou encore pour d'autres sous-groupes de congruences de $\mathrm{GL}_2(A)$, au prix de certaines complications.

Passons aux premières applications des théorèmes 1.1 et 5.18. D'abord ils devraient simplifier le calcul des symboles modulaires pour $\mathbf{F}_q(T)$ sur machine car ils dispensent de l'étape préliminaire de résolution de la présentation. D'un point de vue théorique, la base explicite donne aussi la structure de $\mathbf{M}_{\mathfrak{p}}^0$ comme module pour l'algèbre de Hecke lorsque $\deg \mathfrak{p} = 3$: il est isomorphe à l'idéal d'Eisenstein (proposition 8.2).

1.2 Indépendance linéaire d'opérateurs de Hecke dans $\mathbf{M}_{\mathfrak{p}}$ et non annulation de fonctions L

Soit $\mathbf{H}_{\mathfrak{p}}(\mathbf{C})$ l'espace vectoriel des cochaînes harmoniques paraboliques pour $\Gamma_0(\mathfrak{p})$ à valeurs dans $\mathbf{C}$. D'après Drinfeld et le théorème d'approximation forte ([3, proposition 10.3], [12, section 4]), il correspond à un certain espace de formes automorphes pour K, que nous décrivons maintenant. Notons $\mathbf{A}$ l'anneau des adèles de K, $\mathbf{O}$ son anneau des entiers, $\mathbf{O} = \mathbf{O}_f \times O_\infty$ avec $O_\infty = \mathbf{F}_q[[1/T]]$. Soit $\mathcal{K}_0(\mathfrak{p})_f$ le sous-groupe ouvert compact des matrices de $\mathrm{GL}_2(\mathbf{O}_f)$ qui sont triangulaires supérieures modulo $D_{\mathfrak{p}}$, où $D_{\mathfrak{p}}$ est le diviseur positif de K associé à $\mathfrak{p}$. Soient $\mathcal{I}$ le sous-groupe d'Iwahori de $\mathrm{GL}_2(O_\infty)$ et $\mathrm{Z}(K_\infty)$ le centre de $\mathrm{GL}_2(K_\infty)$ avec $K_\infty = \mathbf{F}_q((1/T))$. Alors $\mathbf{H}_{\mathfrak{p}}(\mathbf{C})$ s'identifie à l'espace des fonctions

$$\mathrm{GL}_2(K)\backslash \mathrm{GL}_2(\mathbf{A})/(\mathcal{K}_0(\mathfrak{p})_f \times \mathcal{I} \cdot \mathrm{Z}(K_\infty)) \to \mathbf{C}$$

qui sont paraboliques et spéciales en ∞, au sens de Drinfeld. Pour F dans $\mathbf{H}_{\mathfrak{p}}(\mathbf{C})$, la fonction $L(F, s)$ est un polynôme en q^{-s} ($s \in \mathbf{C}$). Elle satisfait une équation fonctionnelle dont le centre de symétrie est $s = 1$. Ces formes automorphes donnent lieu à un théorème de modularité pour les courbes elliptiques sur K, conséquence des travaux de Grothendieck, Deligne, Jacquet–Langlands et Drinfeld, pour lequel on renvoie à [12].

Teitelbaum a mis en évidence un accouplement entre $\mathbf{H}_{\mathfrak{p}}(\mathbf{C})$ et le sous-espace parabolique $\mathbf{M}_{\mathfrak{p}}^0(\mathbf{C}) = \mathbf{M}_{\mathfrak{p}}^0 \otimes_{\mathbf{Z}} \mathbf{C}$. Il est compatible aux opérateurs de Hecke et parfait sur $\mathbf{C}$. La forme linéaire $F \mapsto (q-1)L(F, 1)$ sur $\mathbf{H}_{\mathfrak{p}}(\mathbf{C})$ définit alors un symbole modulaire $\mathbf{e}$ dans $\mathbf{M}_{\mathfrak{p}}^0(\mathbf{C})$. Par analogie avec [18], on l'appelle *élément d'enroulement* (cf. section 7.1, notamment pour un exemple).

Dans la section 6, on exprime l'action des opérateurs de Hecke $T_{\mathfrak{m}}$, où $\mathfrak{m}$ est un idéal de A, uniquement en termes de symboles de Manin–Teitelbaum (théorème 6.1). Cette formule, conjointement à la famille libre de symboles modulaires du théorème 5.16, donne un énoncé d'indépendance linéaire d'opérateurs de Hecke en l'élément d'enroulement.

Théorème 1.2. *Si $\mathfrak{p}$ est de degré ≥ 3 et r est la partie entière de $(\deg(\mathfrak{p}) - 3)/2$, alors la famille $\{T_{\mathfrak{m}}\mathbf{e}\}_{\deg \mathfrak{m} \leq r}$ est libre sur $\mathbf{Z}$.*

C'est un cas particulier du théorème 7.10. Cet énoncé est à rapprocher de Merel [21, prop. 3], Parent [26, prop. 1.9] et VanderKam [34, th. 0.1] pour les symboles modulaires

classiques. De telles estimations ont joué un rôle central dans la borne uniforme pour la torsion des courbes elliptiques sur les corps de nombres ([21], [26] pour une version effective).

De même, le théorème 7.10 est l'argument-clé d'un résultat vers une borne uniforme pour la torsion des modules de Drinfeld de rang 2, conjecturée par Poonen. En suivant l'approche de Mazur et Merel, le théorème 7.102 permet d'établir une propriété d'immersion formelle puis une borne uniforme sous certaines conditions (essentiellement une dualité entre formes modulaires de Drinfeld et algèbre de Hecke). Ce résultat est paru séparément dans [1].

Précisons les différences de méthode avec l'indépendance linéaire d'opérateurs de Hecke classiques prouvée dans [26, prop. 1.9]. L'argument combinatoire de Parent utilisait un graphe encodant les relations de Manin. Sa transposition à $\mathbf{F}_q(T)$ semble poser quelque difficulté par la présence des relations $(u : v) - (\delta_1 u : \delta_2 v)$ (de fait, la preuve s'adapte sans encombre pour $q = 2$ et, moyennant un raffinement, à $q \in \{3, 5\}$ mais nous n'avons pu l'étendre au-delà). Nos théorèmes 1.1 et 1.2 reposent eux aussi sur la présentation de Manin mais le mécanisme de la preuve est complètement différent, peut-être plus simple. Parent avait aussi recours, pour conclure, à un résultat de théorie analytique des nombres tandis qu'ici nos arguments restent de nature purement algébrique.

Une autre conséquence du théorème 1.2 que nous souhaitons mettre en évidence concerne la non-annulation de fonctions L des formes automorphes paraboliques de Drinfeld. Puisque $\mathfrak{p}$ est premier, l'espace $\mathbf{H}_!(\mathbf{C})$ possède une base $\mathcal{F}_\mathfrak{p}$ de formes primitives pour l'algèbre de Hecke. On minore le nombre de celles dont la fonction L ne s'annule pas en $s = 1$.

Théorème 1.3. *Si $\mathfrak{p}$ est de degré ≥ 3 et r est la partie entière de $(\deg(\mathfrak{p}) - 3)/2$, on a*

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

Sa preuve sera donnée fin de section 7. 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 [15] et Iwaniec–Sarnak [14]. Pour les formes automorphes de $\mathbf{H}_!(\mathbf{C})$, on peut s'attendre à une borne linéaire, dont on ne dispose pas actuellement à notre 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.

Soient $K = \mathbf{F}_q(T)$ le corps des fractions de A et ∞ 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, ou encore le point à l'infini dans $\mathbf{P}^1$, mais d'après le contexte il n'y aura pas de confusion possible. Soit $K_\infty = \mathbf{F}_q((\pi))$ le complété de K en ∞.

Le schéma en groupes GL(2) est noté G et son centre Z. Dans les sections 3, 4 (rappels) et 6 (action de Hecke sur les symboles de Manin–Teitelbaum), on travaillera avec le sous-groupe de congruence $\Gamma_0(\mathfrak{n}) \subset \mathrm{G}(A)$ pour un idéal propre $\mathfrak{n}$ de A. Ailleurs on supposera en outre $\mathfrak{n} = \mathfrak{p}$ idéal *premier*. On notera parfois Γ ce sous-groupe de congruence.

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

3.1 L'arbre de Bruhat–Tits

Soit $O_\infty = \mathbf{F}_q[[\pi]]$ l'anneau des entiers π-adiques. Le sous-groupe d'Iwahori $\mathcal{I}$ de $\mathrm{G}(O_\infty)$ est formé des matrices qui sont triangulaires supérieures modulo π. L'arbre de Bruhat–Tits $\mathcal{T}$ de $\mathrm{PGL}_2(K_\infty)$ est le graphe $(q+1)$-régulier dont l'ensemble des sommets est $X(\mathcal{T}) = \mathrm{G}(K_\infty)/\mathrm{G}(O_\infty)\cdot\mathrm{Z}(K_\infty)$, celui des arêtes orientées est $Y(\mathcal{T}) = \mathrm{G}(K_\infty)/\mathcal{I}\cdot\mathrm{Z}(K_\infty)$ et la surjection canonique $Y(\mathcal{T}) \to X(\mathcal{T})$ associe à chaque arête son origine ([28, 12]).

Les bouts de $\mathcal{T}$ sont en bijection avec $\mathbf{P}^1(K_\infty)$. Cette bijection est toutefois non canonique : on prendra la convention de [12, 1.6]. Le bout $\infty = (1:0) \in \mathbf{P}^1(K)$ est alors représenté par la demi-droite donnée par les images de $\{\left(\begin{smallmatrix}\pi^k & 0\\ 0 & 1\end{smallmatrix}\right)\}_{k\le 0}$ dans $Y(\mathcal{T})$; de même, $0 = (0:1)$ est représenté par $\{\left(\begin{smallmatrix}\pi^k & 0\\ 0 & 1\end{smallmatrix}\right)\}_{k\ge 0}$.

Le groupe $\mathrm{G}(K_\infty)$ opère par multiplication à gauche sur $\mathcal{T}$. Tout sous-groupe de congruence Γ de $\mathrm{G}(A)$ opère sur $\mathcal{T}$ en préservant la structure simpliciale. On dispose alors du 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 [28, II, théorème 9], ce 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 et 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 [5] et Gekeler–Nonnengardt [11].

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 certaines fonctions sur les arêtes de $\mathcal{T}$ se factorisant en applications $\Gamma\backslash Y(\mathcal{T}) \to R$ à support fini (voir [12, section 3] pour leur définition). Leur R-module sera noté $\mathbf{H}_\mathfrak{n}(R)$, ou encore $\mathbf{H}(R)$; lorsque $R = \mathbf{Z}$, on le note $\mathbf{H}_\mathfrak{n}$ ou encore $\mathbf{H}$.

Soit g le nombre de cycles indépendants du graphe $\Gamma\backslash\mathcal{T}$, qui est aussi le genre de la courbe modulaire de Drinfeld X_Γ associée à Γ ([3, théorème 2], [12, 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. Les formules suivantes de Gekeler donnent la valeur de g si $\mathfrak{n}$ est premier

de degré d :

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

([4, th. 3.4.18]) ; en particulier, g est non nul dès que $d \geq 3$.

Toute cochaîne F de $\mathbf{H}(\mathbf{C})$ a un développement de Fourier de coefficients $c_F(m)$ pour m parcourant les idéaux positifs de K (voir Weil [35] ou Tan [31] pour un point de vue adélique, Gekeler [4, 8] pour un point de vue en la place ∞). La fonction $L(F,s)$ de la variable complexe s est définie comme la série de Dirichlet associée $L(F,s) = \sum_m c_F(m) q^{(1-s)\deg m}$ (cf. [31, (1.10)] ; dans [33] p. 109, $L_f(\chi)$ avec $\chi = \chi_s = (m \mapsto q^{-s\deg m})$). Notons $M(F,s) = \sum_{k\in\mathbf{Z}} F\left(\left(\begin{smallmatrix}\pi^k & 0\\ 0 & 1\end{smallmatrix}\right)\right) q^{-ks}$ la transformée de Mellin de F ($s \in \mathbf{C}$ et la somme est en fait finie).

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

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

La fonction $L(F,s)$ est un polynôme non nul en q^{-s} de degré $\leq \deg(\mathfrak{n}) - 3$. Elle possède un prolongement holomorphe à $\mathbf{C}$ ainsi qu'une équation fonctionnelle pour $L(F,s)$ dont le centre de symétrie est $s = 1$.

Pour cet énoncé on renvoie à [31] Prop. 2, Eq. (3.4) et le corollaire p. 305 (le niveau de F y est noté $N = \mathfrak{n}\cdot\infty$) ; voir aussi [8, (3.4)–(3.6)] avec la convention $s = 0$ pour centre de symétrie. Ainsi, la valeur spéciale $L(F,1)$ est donnée à un facteur près par la somme, finie, des valeurs de F le long de l'unique géodésique de l'arbre $\mathcal{T}$ qui relie les bouts 0 et ∞ :

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

(voir aussi [31, prop. 2], [8, 3.6], [32, (4)]).

3.3 Les opérateurs de Hecke

L'espace $\mathbf{H}(\mathbf{C})$ est muni d'un produit de Petersson $(\cdot,\cdot)_\mu$ 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 $\frac{1}{2}[\Gamma_e : \Gamma \cap \mathrm{Z}(K)]^{-1}$ (e est une arête de $\mathcal{T}$ au-dessus de $\tilde{e}$ et Γ_e son stabilisateur sous Γ). C'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 4.9 de [12]) et stabilise la structure entière $\mathbf{H}$. On peut le définir par la formule suivante :

$$(T_\mathfrak{m} F)(e) = \sum_{\substack{a,b,d\in A \\ (ad)=\mathfrak{m},\ (a)+\mathfrak{n}=A \\ \deg b<\deg d,\ a \text{ et } d \text{ unitaires}}} F\left(\begin{pmatrix}a & b\\ 0 & d\end{pmatrix} e\right) \qquad (F \in \mathbf{H}(\mathbf{C}), e \in Y(\mathcal{T})). \tag{4}$$

Ces opérateurs commutent et sont hermitiens pour $(\cdot,\cdot)_\mu$. L'algèbre $\mathbf{T}$ dite *de Hecke* est la sous-algèbre commutative de $\mathrm{End}(\mathbf{H}(\mathbf{C}))$ engendrée sur $\mathbf{Z}$ par les $T_\mathfrak{m}$, pour $\mathfrak{m}$ premier à $\mathfrak{n}$. Pour $\mathfrak{m}$ non premier à $\mathfrak{n}$, la formule (4) définit encore un opérateur, noté $T_\mathfrak{m}$, qui commute aux autres mais n'est plus nécessairement hermitien.

Soit $w_\mathfrak{n}$ l'involution de $\mathbf{H}(\mathbf{C})$ définie par

$$(w_\mathfrak{n} F)(e) = F\left(\begin{pmatrix} 0 & -1 \\ n & 0 \end{pmatrix} e\right) \qquad (F \in \mathbf{H}(\mathbf{C}), e \in Y(\mathcal{T}))$$

où n est le générateur unitaire de $\mathfrak{n}$. Elle est hermitienne pour $(\cdot,\cdot)_\mu$ et commute à $T_\mathfrak{m}$ pour $\mathfrak{m}$ premier à $\mathfrak{n}$.

Par la suite, on travaillera essentiellement avec $\Gamma = \Gamma_0(\mathfrak{p})$ pour $\mathfrak{p}$ premier. Dans ce cas les endomorphismes $-w_\mathfrak{p}$ et $T_\mathfrak{p}$ coïncident. De plus, l'espace $\mathbf{H}(\mathbf{C})$ se décompose en somme directe orthogonale pour $(\cdot,\cdot)_\mu$ 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 primitives, c'est-à-dire propres pour tous les $T_\mathfrak{m}$ et normalisées (*i.e.* le coefficient de Fourier associé à l'idéal A est égal à 1).

4 Symboles modulaires pour $\mathbf{F}_q(T)$

Excepté pour le paragraphe 4.3, cette section est constituée de rappels de [32], auquel on renvoie 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 $\Gamma = \Gamma_0(\mathfrak{n})$, qui opère à gauche par homographies sur $\mathbf{P}^1(K)$, munit M d'une structure de Γ-module. 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 $\mathbf{M}_\mathfrak{n}(R) = H_0(\Gamma, M \otimes_\mathbf{Z} R)$ avec sa structure canonique de R-module. Il est engendré par les classes $[r,s]$ des diviseurs $(s)-(r)$ pour r, s dans $\mathbf{P}^1(K)$. Pour simplifier, on note aussi cet espace $\mathbf{M}(R)$ et, lorsque $R = \mathbf{Z}$, simplement $\mathbf{M}_\mathfrak{n}$ ou $\mathbf{M}$.

Considérons le groupe B des diviseurs de degré nul à support dans $\Gamma\backslash\mathbf{P}^1(K)$ et soit $B(R) = B \otimes_\mathbf{Z} R$. L'application $[r,s] \mapsto (\Gamma s) - (\Gamma r)$ donne par linéarité une application de bord $\mathbf{M}_\mathfrak{n}(R) \to B(R)$ surjective. Le sous-groupe des *symboles modulaires paraboliques* est son noyau, noté $\mathbf{M}^0_\mathfrak{n}(R)$. Pour simplifier, on le note aussi $\mathbf{M}^0(R)$ et, lorsque $R = \mathbf{Z}$, simplement $\mathbf{M}^0_\mathfrak{n}$ ou $\mathbf{M}^0$. On a les isomorphismes canoniques $\mathbf{M} \otimes_\mathbf{Z} R \simeq \mathbf{M}(R)$ et, si 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 (pour ces notions nous renvoyons à [28], ch. 2, II.8). Soient r et s des bouts dans $\mathbf{P}^1(K)$. Il existe alors une unique géodésique de l'arbre $\mathcal{T}$ allant de r à s. L'application qui associe au symbole modulaire $[r,s]$ l'image dans $\Gamma\backslash\mathcal{T}$ de cette géodésique est bien définie. Elle s'étend par linéarité en un homomorphisme de groupes abéliens $\mathbf{M} \to H_1(\Gamma\backslash\mathcal{T}, \mathbf{ptes}, \mathbf{Z})$.

Proposition 4.1 ([32, p. 277]). *L'application précédente induit les isomorphismes de groupes* $\mathbf{M}/\mathbf{M}_{\mathrm{tors}} \xrightarrow{\simeq} H_1(\Gamma\backslash\mathcal{T}, \mathbf{ptes}, \mathbf{Z})$ *et* $\mathbf{M}^0/(\mathbf{M}^0)_{\mathrm{tors}} \xrightarrow{\simeq} H_1(\Gamma\backslash\mathcal{T}, \mathbf{Z})$.

Soit h le nombre de pointes du graphe $\Gamma\backslash\mathcal{T}$, qui est aussi le nombre de pointes de la courbe modulaire de Drinfeld X_Γ associée à Γ (pour des formules donnant h, on renvoie à [10, sec. 6]). D'après la proposition, $\mathbf{M}(\mathbf{Q})$ et $\mathbf{M}^0(\mathbf{Q})$ ont pour dimensions respectives $g+h-1$ et g sur $\mathbf{Q}$. Enfin, lorsque $\mathfrak{n}$ est premier de degré impair (resp. pair), la torsion de $\mathbf{M}$ est nulle (resp. cyclique d'ordre $q+1$) (cf. [32, p. 278]).

4.2 L'accouplement avec les cochaînes

Soit $\mathfrak{m}$ un idéal premier à $\mathfrak{n}$. À partir de la correspondance sur $Y(\Gamma\backslash\mathcal{T})$ qui a servi à définir $T_\mathfrak{m}$ sur les cochaînes, on définit un opérateur de Hecke $T_\mathfrak{m}$ sur $\mathbf{M}(R)$. C'est l'endomorphisme de $\mathbf{M}(R)$ donné par

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

(les matrices agissent par homographies et la formule garde un sens pour $\mathfrak{m}$ non premier à $\mathfrak{n}$). De même, on définit l'involution $w_\mathfrak{n}$ de $\mathrm{End}(\mathbf{M}(R))$ par

$$w_\mathfrak{n}\,[r,s] = [-1/(nr), -1/(ns)] \qquad ([r,s]\in\mathbf{M}(R))$$

où n est le générateur unitaire de $\mathfrak{n}$. Tous ces opérateurs stabilisent le sous-espace parabolique.

Suivant [32, déf. 8], 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 la géodésique de $\mathcal{T}$ allant de r à s. Cette somme est bien définie et finie, par la parabolicité de F et la description de $\Gamma\backslash\mathcal{T}$ rappelée dans la section 3.1. On déduit une application R-bilinéaire $\langle\cdot,\cdot\rangle : \mathbf{M}(R)\times\mathbf{H}(R)\to R$ qui est compatible aux opérateurs de Hecke ([32, lem. 9]).

Théorème 4.2 (Teitelbaum). *L'accouplement d'intégration* $\langle\cdot,\cdot\rangle$ *fournit une suite exacte de* $\mathbf{Z}$*-modules*

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

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

(La suite exacte est le théorème 14 de [32] ; le deuxième énoncé se déduit par extension des scalaires à $\mathbf{Q}$.) On dispose donc d'un accouplement parfait $\mathbf{M}^0(\mathbf{C})\times\mathbf{H}(\mathbf{C})\to\mathbf{C}$. 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 $\mathrm{End}(\mathbf{M}^0(\mathbf{C}))$ engendrée par les $T_\mathfrak{m}$ avec $\mathfrak{m}$ premier à $\mathfrak{n}$. On notera encore $\mathbf{T}$ cette algèbre.

Enfin, d'après (3), la valeur spéciale de la fonction L s'exprime avec l'accouplement par $L(F,1) = \langle [0,\infty], F\rangle/(q-1)$ (voir aussi [32, th. 23]).

4.3 Symboles paraboliques comme cochaînes

Nous apportons un complément à la théorie de Teitelbaum en mettant en évidence un isomorphisme canonique entre d'une part les symboles paraboliques à torsion près, et d'autre part les cochaînes paraboliques. Il s'agit d'une comparaison de [32] et Gekeler–Nonnengardt [11]. Nous ne connaissons pas de construction similaire pour les symboles et formes modulaires classiques. Cet isomorphisme interviendra notamment dans l'exemple de la section 7.1.2.

Commençons par rappeler le lien existant entre cochaînes paraboliques pour Γ et cycles du graphe $\Gamma\backslash\mathcal{T}$, d'après [11]. Soit $n(\tilde{e}) = n(e)$ l'indice de $\Gamma \cap \mathrm{Z}(K)$ 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

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

est bien défini, injectif et de conoyau fini ([12, 3.2.5]). Comme $\Gamma = \Gamma_0(\mathfrak{n})$, il est même bijectif : c'est un résultat profond de Gekeler–Nonnengardt sur la structure du graphe $\Gamma\backslash\mathcal{T}$ ([11, th. 3.3]).

Notation 4.3. On désigne par $\overline{\mathbf{M}^0}$ le quotient maximal sans torsion $\mathbf{M}^0/(\mathbf{M}^0)_{\mathrm{tors}}$.

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

$$\alpha : \overline{\mathbf{M}^0} \xrightarrow{\simeq} \mathbf{H}.$$

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

Démonstration. L'isomorphisme α entre les $\mathbf{Z}$-modules $\overline{\mathbf{M}^0}$ et $\mathbf{H}$ est obtenu en composant j avec celui 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 $Y(\Gamma\backslash\mathcal{T})$:

$$\varphi(\tilde{e}) = \#\{e \in c \mid e \text{ se projette sur } \tilde{e}\} - \#\{e \in c \mid \bar{e} \text{ se projette sur } \tilde{e}\}$$

(où $\bar{e}$ désigne l'arête opposée de e). En d'autres termes, $\varphi(\tilde{e}) = m(\tilde{e}) - m(\overline{\tilde{e}})$. Cette fonction est alternée, c'est-à-dire $\varphi(\overline{\tilde{e}}) = -\varphi(\tilde{e})$. L'accouplement entre $[r, s]$ et une cochaîne $G \in \mathbf{H}$ est alors

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

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 $x \in \overline{\mathbf{M}^0}$. Par ce qui précède et la compatibilité de $\langle \cdot, \cdot \rangle$ aux opérateurs de Hecke, on voit que la cochaîne $\alpha(T_{\mathfrak{m}} x) - T_{\mathfrak{m}} \alpha(x)$ 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. □

Remarque 4.5. – *Via* l'isomorphisme α, la suite exacte du théorème 4.2 revient à $0 \to \mathbf{H} \xrightarrow{i} \mathrm{Hom}(\mathbf{H}, \mathbf{Z}) \to \Phi_\infty \to 0$. Gekeler l'avait aussi établie de manière indépendante ([7, cor. 2.11]) comme conséquence de l'uniformisation analytique de la jacobienne de X_Γ par Gekeler–Reversat [12].

– Bien que l'espace des symboles modulaires soit canoniquement isomorphe à $\mathbf{H}$ à torsion près, il conserve son intérêt car la présentation de Manin, dont nous ferons un usage essentiel, ne semble pas avoir été établie directement sur les cochaînes.

– Une base de $\mathbf{H}$ peut s'obtenir par une méthode combinatoire reposant sur la détermination du graphe $\Gamma\backslash\mathcal{T}$ (voir Gekeler–Nonnengardt [5, 22, 11]). Grâce à leur présentation finie rappelée ci-après, les symboles modulaires permettent de déterminer une base d'un espace isomorphe à $\mathbf{H}$, *via* α, sans connaître précisément $\Gamma\backslash\mathcal{T}$.

4.4 La présentation finie

Considérons la droite projective $\mathbf{P}^1(A/\mathfrak{n})$. Ses éléments 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 $(w) + \mathfrak{n} = A$ et $(u_1, v_1) \equiv (wu_2, wv_2) \bmod \mathfrak{n}$. On note $(u : v)$ la classe de (u, v).

Le sous-groupe $\Gamma_0(\mathfrak{n})$, qui opère par multiplication à gauche sur $\mathrm{G}(A)$, est d'indice fini et on a une bijection $\Gamma_0(\mathfrak{n})\backslash\mathrm{G}(A) \to \mathbf{P}^1(A/\mathfrak{n})$ donnée par $\Gamma_0(\mathfrak{n})\left(\begin{smallmatrix} a & b \\ u & v \end{smallmatrix}\right) \mapsto (u : v)$ (noter qu'on peut toujours choisir un représentant (u, v) de $(u : v)$ avec u et v premiers entre eux). Considérons l'application

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

où $g = \left(\begin{smallmatrix} a & b \\ u & v \end{smallmatrix}\right) \in \mathrm{G}(A)$ 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 ([32, lem. 16]). On appelle les $\xi(u : v)$ les *symboles de Manin–Teitelbaum* et ils engendrent $\mathbf{M}$. La droite $\mathbf{P}^1(A/\mathfrak{n})$ est munie d'une action naturelle à droite de $\mathrm{G}(A)$. Posons dans $\mathrm{G}(\mathbf{F}_q)$:

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

Ces matrices sont d'ordre respectivement 4 (ou 2 si $p = 2$) et 3. La présentation suivante se déduit de [32], énoncés pp. 283–286 et théorème 21.

1. Teitelbaum a adopté la convention inverse $[g\infty, g0]$; nous avons choisi celle qui semble être la plus courante pour les symboles modulaires classiques.

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 le sous-module engendré par les relations*

$$\begin{aligned}(x) + (x\sigma)\\ (x) + (x\tau) + (x\tau^2)\\ (x) - (x\delta)\end{aligned}$$

pour toute matrice δ diagonale dans $\mathrm{G}(\mathbf{F}_q)$ et $x \in \mathbf{P}^1(A/\mathfrak{n})$.

Ces relations sont celles (1) données dans l'introduction.

Remarque 4.7. Notons Δ le sous-groupe de $\mathrm{G}(\mathbf{F}_q)$ formé des matrices $\left(\begin{smallmatrix}\lambda & 0\\ 0 & 1\end{smallmatrix}\right)$ pour $\lambda \in \mathbf{F}_q^\times$. De façon équivalente, le troisième ensemble de relations peut être remplacé par

$$(x) - (x\delta) \qquad \text{pour } \delta \in \Delta, x \in \mathbf{P}^1(A/\mathfrak{n}).$$

5 Une base explicite de symboles de Manin–Teitelbaum

5.1 Une variante de l'espace des symboles modulaires

Notation 5.1. Considérons la droite projective $\mathbf{P}^1(A)$. Ses éléments sont les classes d'équivalence de couples $(u, v) \in A \times A$ avec $(u) + (v) = A$, 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 $(u : v) \in \mathbf{P}^1(A/\mathfrak{n})$.

Pour e entier ≥ 0, on note $\mathbf{P}^1(A)_e$ l'ensemble des $\{u : v\} \in \mathbf{P}^1(A)$ avec $\deg u \leq e$ et $\deg v \leq e$.

Commençons par un lemme de dénombrement.

Lemme 5.2. *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 et b dans $\mathbf{N}$. 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 si $e > 0$.*

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 $(u, v) \in A \times A$ 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 degrés respectivement $i - h$ et $i + l - h$, il existe $N_{i-h,i+l-h}$ tels couples. Ainsi on a, pour tout $l \geq 0$ et $i \geq 0$,

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

Prenons x et y des indéterminées. En multipliant l'égalité précédente par $x^i y^{i+l}$, sommant sur $i \geq 0$ et $l \geq 0$ puis arrangeant l'expression obtenue, 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. Notons $F_{a,b}$ l'ensemble des $(u,v) \in A \times A$ 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, φ est aussi injective donc bijective. De plus, il est clair que

$$\#F_{a,b} = \sum_{i=0}^{a}\sum_{j=0}^{b} N_{i,j}.$$

En substituant les expressions de $N_{i,j}$ obtenues précédemment, on obtient

$$\#\mathbf{P}^1(A)_{a,b} = \#F_{a,b} = (q^{a+b+1}-1)/(q-1).$$

Enfin l'ensemble $\mathbf{P}^1(A)_e$ est réunion disjointe de $\{\lambda u : v\}$ pour $(u,v) \in F_{e,e}$, $\lambda \in \mathbf{F}_q^\times$, et des deux éléments $\{1:0\}$ et $\{0:1\}$. Donc $\mathbf{P}^1(A)_e$ est de cardinal $q^{2e+1}+1$.

□

Dans ce qui suit, $\mathfrak{p}$ est un idéal *premier* de A, de degré noté d.

Lemme 5.3. *Supposons $e < d/2$. L'application canonique*

$$\begin{array}{ccc} \mathbf{P}^1(A)_e & \longrightarrow & \mathbf{P}^1(A/\mathfrak{p}) \\ \{u:v\} & \longmapsto & (u:v) \end{array}$$

est injective.

Démonstration. 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 $\mathfrak{p}$. Comme ce polynôme est de degré $\leq 2e < d = \deg \mathfrak{p}$, 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. Ainsi 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 est injective. □

On constate que l'ensemble $\mathbf{P}^1(A)_e$ est stable par l'action à droite des matrices σ, τ et $\delta \in \Delta$. L'objet suivant est donc bien défini.

Notation 5.4. Si R est un anneau commutatif, on note $M_e(R)$ le quotient du R-module libre $R[\mathbf{P}^1(A)_e]$ par le sous-module engendré par les éléments $(x)+(x\sigma)$, $(x)+(x\tau)+(x\tau^2)$ et $(x)-(x\delta)$ pour $\delta \in \Delta$ et $x \in \mathbf{P}^1(A)_e$. On appelle respectivement ces éléments les *relations à deux termes*, *trois termes* et *diagonales*.

Jusqu'à la fin de la section 5.1 on compare l'espace des symboles modulaires à $M_e(R)$ pour certaines valeurs de e.

5.1.1 Cas d impair

Proposition 5.5. *Supposons $d = \deg \mathfrak{p}$ impair. L'application du lemme 5.3 induit une bijection $\mathbf{P}^1(A)_{(d-1)/2} \to \mathbf{P}^1(A/\mathfrak{p})$ ainsi qu'un isomorphisme $M_{(d-1)/2}(R) \simeq \mathbf{M}_{\mathfrak{p}}(R)$.*

Démonstration. L'application étant injective par le lemme 5.3, on obtient sa bijectivité par un dénombrement. D'après le lemme 5.2 avec $a = b = (d-1)/2$, l'ensemble $\mathbf{P}^1(A)_{(d-1)/2}$ a (q^d+1) éléments. Comme $\mathfrak{p}$ est premier, il en est de même de l'ensemble $\mathbf{P}^1(A/\mathfrak{p})$. Donc l'application est bijective. Par ailleurs, elle est aussi équivariante sous l'action de σ, τ et Δ. L'isomorphisme se déduit alors de la définition de $M_{(d-1)/2}(R)$ et de la présentation finie (théorème 4.6 et remarque 4.7). □

Remarque 5.6. La matrice τ opère sur $\mathbf{P}^1(A)_e$ car on dispose de l'inégalité

$$\deg(u+v) \leq \max(\deg u, \deg v)$$

pour $u, v \in A$. La construction du « modèle » $M_{(d-1)/2}(R)$ de $\mathbf{M}_{\mathfrak{p}}(R)$ est donc possible car la norme $|x| = q^{\deg(x)}$ $(x \in A)$ associée à la place ∞ de K est non-archimédienne. Manin a donné une présentation finie des symboles modulaires de poids 2 pour $\Gamma_0(n) \subset \mathrm{SL}_2(\mathbf{Z})$, similaire au théorème 4.6 : c'est le quotient sans torsion du $\mathbf{Z}$-module libre $\mathbf{Z}[\mathbf{P}^1(\mathbf{Z}/n\mathbf{Z})]$ par des relations à deux et trois termes ([16, th. 2.7]). Une adaptation naïve de notre démarche, en remplaçant la norme $|\cdot|$ par la valeur absolue sur $\mathbf{R}$, ne semble donc pas permettre de résoudre la présentation de Manin des symboles modulaires classiques.

5.1.2 Cas d pair

Notation 5.7. Dans cette partie uniquement on suppose d pair et on pose $e = d/2$. On note P_e (resp. S_e) le sous-ensemble de $\mathbf{P}^1(A)_e$ formé des $\{u : v\}$ avec $\deg v \leq e-1$ (resp. $\deg u = e$ et $\deg v \leq e-1$). On a donc la partition $P_e = \mathbf{P}^1(A)_{e-1} \sqcup S_e$.

Lemme 5.8. *L'application canonique*

$$\begin{array}{rccc} \pi : & P_e & \longrightarrow & \mathbf{P}^1(A/\mathfrak{p}) \\ & \{u:v\} & \longmapsto & (u:v) \end{array}$$

est bijective.

Démonstration. L'injectivité s'obtient par un argument similaire à celui du lemme 5.3. Prouvons la bijectivité par un dénombrement. Soit E l'ensemble réunion de $(0,1) \in A \times A$ et des couples $(u,v) \in A \times A$ avec u unitaire, u et v premiers entre eux, $\deg u \leq e$ et $\deg v \leq e-1$. On voit facilement que E et P_e sont en bijection. De plus, outre $(1,0)$ et $(0,1)$, l'ensemble E est constitué des $(u, \lambda v)$ avec $\lambda \in \mathbf{F}_q^\times$, u et v unitaires premiers entre eux, $\deg u \leq e$, $\deg v \leq e-1$. Par le lemme 5.2, son cardinal est alors

$$2 + (q-1) \sum_{0 \leq i \leq e-1} \sum_{0 \leq j \leq e} N_{i,j} = q^{2e} + 1.$$

Or l'ensemble $\mathbf{P}^1(A/\mathfrak{p})$ a aussi $q^{2e}+1$ éléments. Donc π est bijective. □

Remarquons que les matrices σ et τ n'opèrent pas sur l'ensemble P_e (plus précisement, elles opèrent sur $\mathbf{P}^1(A)_{e-1}$ mais pas sur S_e). Contrairement au cas d impair, on ne peut donc considérer le quotient de $R[P_e]$ par les relations induites par ces matrices. Le lemme suivant suffit à contourner ce problème.

Lemme 5.9. *Les matrices σ, τ et celles de Δ opèrent sur $\pi(\mathbf{P}^1(A)_{e-1})$ et sur $\pi(S_e)$.*

Démonstration. Par la bijection du lemme 5.8, on écrit $\mathbf{P}^1(A/\mathfrak{p})$ comme la réunion disjointe $\mathbf{P}^1(A/\mathfrak{p}) = \pi(\mathbf{P}^1(A)_{e-1}) \sqcup \pi(S_e)$. Les matrices considérées opèrent sur $\mathbf{P}^1(A/\mathfrak{p})$ et $\pi(\mathbf{P}^1(A)_{e-1})$ (pour ce dernier, car elles opèrent déjà sur $\mathbf{P}^1(A)_{e-1}$ et π est équivariant par ces matrices). Elles opèrent donc aussi sur l'ensemble $\pi(S_e)$. □

Proposition 5.10. *L'application $\mathbf{P}^1(A)_{e-1} \subset P_e \xrightarrow{\pi} \mathbf{P}^1(A/\mathfrak{p})$ induit un homomorphisme injectif $M_{e-1}(R) \to \mathbf{M}_{\mathfrak{p}}(R)$.*

Démonstration. Notons $i : R[\mathbf{P}^1(A)_{e-1}] \to R[\mathbf{P}^1(A/\mathfrak{p})]$ l'homomorphisme injectif déduit de $\mathbf{P}^1(A)_{e-1} \hookrightarrow \mathbf{P}^1(A/\mathfrak{p})$. Si S est un ensemble fini sur lequel opèrent σ, τ et Δ, on notera $Rel(S)$ le sous-module de $R[S]$ engendré par les relations à deux termes, trois termes et diagonales correspondant à ces matrices. Il s'agit de montrer que tout élément de $R[\mathbf{P}^1(A)_{e-1}]$ dont l'image par i est dans $Rel(\mathbf{P}^1(A/\mathfrak{p}))$ est lui-même dans $Rel(\mathbf{P}^1(A)_{e-1})$. L'image par la bijection π de la partition de P_e donne $\mathbf{P}^1(A/\mathfrak{p}) = \pi(\mathbf{P}^1(A)_{e-1}) \sqcup \pi(S_e)$. On a donc la décomposition en somme directe

$$R[\mathbf{P}^1(A/\mathfrak{p})] = R[\pi(\mathbf{P}^1(A)_{e-1})] \oplus R[\pi(S_e)].$$

Par ailleurs, d'après le lemme 5.9, les sous-modules $Rel(\pi(\mathbf{P}^1(A)_{e-1}))$ et $Rel(\pi(S_e))$ sont bien définis et on a $Rel(\mathbf{P}^1(A/\mathfrak{p})) = Rel(\pi(\mathbf{P}^1(A)_{e-1})) \oplus Rel(\pi(S_e))$. Donc l'intersection de $Rel(\mathbf{P}^1(A/\mathfrak{p}))$ et $R[\pi(\mathbf{P}^1(A)_{e-1})]$ est $Rel(\pi(\mathbf{P}^1(A)_{e-1}))$. Par injectivité de i, l'assertion est démontrée. □

5.1.3 Cas général

Dans l'énoncé suivant, nous ne faisons plus d'hypothèse de parité sur $d = \deg \mathfrak{p}$. Les propositions 5.5 et 5.10 ont mis en évidence un plongement de $M_e(R)$ dans l'espace de symboles modulaires $\mathbf{M}_{\mathfrak{p}}(R)$ pour certaines valeurs maximales de e. On étend ces résultats aux valeurs inférieures de e.

Lemme 5.11. *Supposons $e < d/2$. L'application du lemme 5.3 induit un homomorphisme injectif $M_e(R) \to \mathbf{M}_{\mathfrak{p}}(R)$.*

Démonstration. Les propositions 5.5 et 5.10 l'ont déjà démontré pour les valeurs maximales entières de e (c'est-à-dire $(d-1)/2$ si d est impair, $(d-2)/2$ si d est pair). Il suffit alors de prouver que, pour tout $e' \leq e$, l'homomorphisme canonique $M_{e'}(R) \to M_e(R)$ est injectif. Écrivons $\mathbf{P}^1(A)_e$ comme réunion disjointe de $\mathbf{P}^1(A)_{e'}$ et de l'ensemble S des couples $\{u : v\} \in \mathbf{P}^1(A)_e$ avec ($\deg u > e'$ ou $\deg v > e'$). On vérifie facilement que S est stable par l'action des matrices σ, τ et celles de Δ. Cela entraîne les sommes directes $R[\mathbf{P}^1(A)_e] = R[\mathbf{P}^1(A)_{e'}] \oplus R[S]$ et $Rel(\mathbf{P}^1(A)_e) = Rel(\mathbf{P}^1(A)_{e'}) \oplus Rel(S)$ avec les notations de la preuve de la proposition 5.10. Donc $Rel(\mathbf{P}^1(A)_e) \cap R[\mathbf{P}^1(A)_{e'}] = Rel(\mathbf{P}^1(A)_{e'})$. L'injectivité est démontrée. □

5.2 Décomposition naturelle en sous-espaces

Notation 5.12. Soit $k \geq 0$. Notons C_k l'ensemble des $\{u : v\} \in \mathbf{P}^1(A)_k$ avec u ou v de degré k. Si $k \geq 1$, C_k est le complémentaire de $\mathbf{P}^1(A)_{k-1}$ dans $\mathbf{P}^1(A)_k$ et on constate qu'il est stable par l'action de σ, τ et Δ. Notons ainsi $N_k(R)$ le R-module quotient de $R[C_k]$ par le sous-module engendré par $(x)+(x\sigma)$, $(x)+(x\tau)+(x\tau^2)$ et $(x)-(x\delta)$ pour $x \in C_k$, $\delta \in \Delta$. On l'identifie à un sous-module de $M_k(R)$.

Si $k < (\deg \mathfrak{p})/2$, notons $\mathbf{N}_{\mathfrak{p},k}(R)$ l'image de $N_k(R)$ dans $\mathbf{M}_\mathfrak{p}(R)$ par l'injection du lemme 5.11. En d'autres termes, $\mathbf{N}_{\mathfrak{p},k}(R)$ est le sous-module engendré par les symboles modulaires $\xi(u : v)$ avec u, v premiers entre eux, de degrés $\leq k$ et ($\deg u = k$ ou $\deg v = k$).

Proposition 5.13. *1. Pour $e \geq 0$, on a $M_e(R) = \bigoplus_{0 \leq k \leq e} N_k(R)$.*

2. Soit $\mathfrak{p}$ premier de degré d. Les sous-modules $\mathbf{N}_{\mathfrak{p},k}(R)$ pour $0 \leq k < d/2$ sont en somme directe. De plus, si d est impair, on a

$$\mathbf{M}_\mathfrak{p}(R) = \bigoplus_{0 \leq k \leq (d-1)/2} \mathbf{N}_{\mathfrak{p},k}(R).$$

En particulier, $\mathbf{M}_\mathfrak{p}(R) = \mathbf{N}_{\mathfrak{p},0}(R)$ si $\mathfrak{p}$ est de degré 1.

Démonstration. 1. Pour $k \geq 1$, la partition $\mathbf{P}^1(A)_k = \mathbf{P}^1(A)_{k-1} \sqcup C_k$ entraîne

$$\mathbf{P}^1(A)_e = \mathbf{P}^1(A)_0 \sqcup \bigsqcup_{1 \leq k \leq e} C_k = \bigsqcup_{0 \leq k \leq e} C_k$$

(car $\mathbf{P}^1(A)_0 = C_0$). On en déduit $M_e(R) = \bigoplus_{0 \leq k \leq e} N_k(R)$.

2. La décomposition de $M_e(R)$ et son plongement dans $\mathbf{M}_\mathfrak{p}(R)$ (lemme 5.11) assurent que la somme des $\mathbf{N}_{\mathfrak{p},k}(R)$ est directe. Son égalité avec $\mathbf{M}_\mathfrak{p}(R)$ pour d impair découle du point 1 et de l'isomorphisme $M_{(d-1)/2}(R) \simeq \mathbf{M}_\mathfrak{p}(R)$ (proposition 5.5).

□

5.3 La base explicite

On exhibe maintenant une base de chaque sous-espace $N_k(R)$.

Notation 5.14. Posons

$$\begin{aligned}
C^> &= \{\{u : v\} \in C_k \mid \deg u = k > \deg v\} \\
C^< &= \{\{u : v\} \in C_k \mid \deg u < \deg v = k\} \\
C^= &= \{\{u : v\} \in C_k \mid \deg u = \deg v = k\} \\
C_\bullet &= \{\{u : v\} \in C^= \mid \lambda_u + \lambda_v = 0\} \\
C^\bullet &= \{\{u : v\} \in C^= \mid \lambda_u + \lambda_v \neq 0\}
\end{aligned}$$

où λ_u (resp. λ_v) est le coefficient dominant de u (resp. v). Noter que, u et v étant non nuls ($k \geq 0$), ces coefficients sont bien définis. Enfin $C^{>+}$ désignera le sous-ensemble des $\{u : v\} \in C^>$ avec u unitaire, et v unitaire si non nul.

On a les partitions $C_k = C^> \sqcup C^< \sqcup C^=$ et $C^= = C_\bullet \sqcup C^\bullet$. De plus, la matrice σ est une bijection de C_k qui stabilise $C^=$ et permute $C^>$ et $C^<$. La matrice τ est une bijection de C_k qui permute de façon cyclique les ensembles $C_\bullet$, $C^>$ et $C^<$ dans cet ordre. Enfin les matrices de Δ sont des bijections de $C^>$, $C^<$ et $C^=$.

Notons que l'ensemble $C^>$ ne contient d'élément de la forme $\{u : 0\}$ que si $k = 0$, auquel cas $C^> = C^{>+} = \{\{1 : 0\}\}$, $C^= = \{\{1 : \lambda\} \mid \lambda \in \mathbf{F}_q^\times\}$ et $C_\bullet = \{\{1 : -1\}\}$.

Proposition 5.15. *Soit $k \geq 0$. L'ensemble $C^{>+}$ fournit une base de $N_k(R)$ sur R. En particulier, ce module est libre de rang q^{2k-1} si $k > 0$, et 1 si $k = 0$.*

Démonstration. Commençons par établir que $C^{>+}$ est génératrice. Par les relations diagonales sur $C^>$, il suffit de voir que $C^>$ engendre $N_k(R)$. Comme σ permute $C^>$ et $C^<$, par les relations à deux termes sur $C^>$, tout élément de $C^<$ est congru dans $N_k(R)$ à l'opposé d'un élément de $C^>$. Ainsi, l'ensemble $C^> \sqcup C^=$ engendre $N_k(R)$. Maintenant, éliminons $C^=$ de la liste des générateurs. Rappelons que τ permute $C_\bullet$, $C^>$ et $C^<$. Donc, par les relations à trois termes sur $C_\bullet$, tout élément de $C_\bullet$ est congru dans $N_k(R)$ à l'opposé de la somme d'un élément de $C^>$ et d'un élément de $C^<$. Cela montre que $N_k(R)$ est engendré par $C^> \sqcup C^\bullet$. Enfin, tout élément $\{u : v\}$ de $C^\bullet$ est congru à un élément de $C_\bullet$ dans $N_k(R)$ par la relation diagonale $\{u : v\} - \{u : v\} \left(\begin{smallmatrix} -\lambda_v\lambda_u^{-1} & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Par ce qui précède, $N_k(R)$ est engendré par $C^>$ donc par $C^{>+}$, comme annoncé.

Pour simplifier, posons dans $R[C_k]$:

$$s(x) = (x) + (x\sigma), \quad t(x) = (x) + (x\tau) + (x\tau^2), \quad d_\delta(x) = (x) - (x\delta)$$

pour $x \in C_k$ et $\delta \in \Delta$. Notons $\mathcal{R}$ le sous-module de $R[C_k]$ engendré par les éléments suivants :

- $\star$ $d_\delta(x)$ pour $(x, \delta) \in (C^> \sqcup C_\bullet) \times \Delta$;
- $\star$ $s(x)$ pour $x \in C^>$ (ou, ce qui revient au même, dans $C^<$) ;
- $\star$ $t(x)$ pour $x \in C_\bullet$ (ou, ce qui revient au même, dans $C^>$ ou $C^<$).

Il contient toutes les relations utilisées pour démontrer que $C^{>+}$ est génératrice. Comme $d_\delta(x) = -d_{\delta^{-1}}(x\delta)$, le module $\mathcal{R}$ contient aussi $d_\delta(x)$ pour $(x, \delta) \in C^\bullet \times \Delta$ tels que $x\delta \in C_\bullet$.

Dorénavant le symbole $\equiv$ désigne une égalité dans $R[C_k]/\mathcal{R}$. On a

$$x = d_\delta(x) + t(x\delta) - (x\delta\tau) - (x\delta\tau^2).$$

Cette équation pour $\delta = \left(\begin{smallmatrix} -\lambda_v\lambda_u^{-1} & 0 \\ 0 & 1 \end{smallmatrix}\right)$ entraîne la relation suivante pour tout $x = \{u : v\} \in C^\bullet$

$$x \equiv -\{\lambda_u v : w\} - \{w : -\lambda_v u\} \tag{5}$$

en posant $w = \lambda_v u - \lambda_u v$. On propose d'établir que $\mathcal{R}$ coïncide avec le sous-module engendré par toutes les relations dans $R[C_k]$, c'est-à-dire le noyau de l'homomorphisme $R[C_k] \to N_k(R)$.

Commençons par voir que les relations diagonales sur $C^<$ sont dans $\mathcal{R}$. Soient $\delta = \left(\begin{smallmatrix} \lambda & 0 \\ 0 & 1 \end{smallmatrix}\right)$ et $\delta' = \left(\begin{smallmatrix} \lambda^{-1} & 0 \\ 0 & 1 \end{smallmatrix}\right)$ dans Δ. Dans $\mathrm{G}(\mathbf{F}_q)$ on a l'égalité $-\lambda\sigma\delta'\sigma = \delta$ d'où pour tout $x \in C^<$,

$$(x) - (x\delta) = s(x) - d_{\delta'}(x\sigma) - s(x\sigma\delta').$$

Comme σ permute $C^<$ et $C^>$, l'élément $x\sigma$ est dans $C^>$. De même, $x\sigma\delta'$ est dans $C^>$. Donc $(x) - (x\delta) \equiv 0$ et l'affirmation est démontrée.

Démontrons maintenant que $\mathcal{R}$ contient $d_\delta(x)$ pour $(x, \delta) \in C^\bullet \times \Delta$ tels que $x\delta \in C^\bullet$. Soient $x = \{u : v\} \in C^\bullet$ et $\delta = \left(\begin{smallmatrix} \lambda & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Comme $x\delta \in C^\bullet$, on déduit de la formule (5)

$$\begin{aligned} x &\equiv -\{\lambda_u v : w\} - \{w : -\lambda_v u\} \\ x\delta &\equiv -\{\lambda\lambda_u v : \lambda w\} - \{\lambda w : -\lambda\lambda_v u\} \equiv -\{\lambda_u v : w\} - \{w : -\lambda_v u\} \end{aligned}$$

la dernière congruence provenant d'une égalité dans $\mathbf{P}^1(A)$. Donc $d_\delta(x) = (x) - (x\delta)$ appartient à $\mathcal{R}$. Ainsi on a établi que $\mathcal{R}$ contient toutes les relations diagonales.

Montrons ensuite que $\mathcal{R}$ contient $t(x)$ pour tout $x \in C^\bullet$. Par (5) et bijectivité de τ sur $C^\bullet$, on obtient

$$\begin{aligned} x\tau = \{v : -u - v\} &\equiv -\{-\lambda_v(u + v) : w\} - \{w : (\lambda_u + \lambda_v)v\} \\ x\tau^2 = \{-u - v : u\} &\equiv -\{-(\lambda_u + \lambda_v)u : w\} - \{w : \lambda_u(u + v)\}\,. \end{aligned}$$

En utilisant des relations diagonales sur $C^>$ et $C^<$ (elles sont dans $\mathcal{R}$), on a

$$\begin{aligned} x &\equiv -\{v : w\} - \{w : u\} \\ x\tau &\equiv -\{u + v : w\} - \{w : v\} \\ x\tau^2 &\equiv -\{u : w\} - \{w : u + v\}\,. \end{aligned}$$

Or des relations à deux termes et diagonales sur $C^>$ donnent

$$\{w : u\} \equiv -\{u : w\}\,, \quad \{w : v\} \equiv -\{v : w\}\,, \quad \{w : u + v\} \equiv -\{u + v : w\}\,.$$

Donc $t(x) = (x) + (x\tau) + (x\tau^2)$ appartient à $\mathcal{R}$ pour $x \in C^\bullet$. Afin de conclure, il reste à voir que $\mathcal{R}$ contient $s(x)$ pour $x \in C^=$. Posons $\sigma' = \sigma\left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ et $s'(x) = (x) + (x\sigma')$. On a la relation $s(x) = s'(x) + d_{\left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)}(x\sigma)$. Soit $x = \{u : v\} \in C^=$. Comme $x\sigma \in C^=$ et $\mathcal{R}$ contient toutes les relations diagonales sur $C^=$, $\mathcal{R}$ contient $s(x)$ si et seulement s'il contient $s'(x)$. On propose d'établir $s'(x) \in \mathcal{R}$ en distinguant deux cas. D'abord, supposons $x \in C^\bullet$. D'après (5), on a $x \equiv -\{\lambda_u v : w\} - \{w : -\lambda_v u\}$. L'élément $x\sigma' = \{v : u\}$ est aussi dans $C^\bullet$ et donc congru à $-\{\lambda_v u : w\} - \{w : -\lambda_u v\} \in R[C^>] + R[C^<]$. Par des relations à deux termes sur $C^>$ (ou $C^<$) on voit que $classeA\lambda_v uw \equiv -\{w : -\lambda_v u\}$ et $\{w : -\lambda_u v\} \equiv -\{\lambda_u v : w\}$. Donc $s'(x) = (x) + (x\sigma')$ appartient à $\mathcal{R}$. Supposons ensuite $x \in C_\bullet$. On a

$$x \equiv -(x\tau) - (x\tau^2) \equiv -\{v : -u - v\} - \{-u - v : u\}\,.$$

L'élément $x\sigma'$ appartient aussi à $C_\bullet$ et il est congru à

$$-\{u : -u - v\} - \{-u - v : v\} \in R[C^>] + R[C^<].$$

Par des relations à deux termes et diagonales sur $C^>$ (ou $C^<$), on voit que

$$\{u : -u - v\} \equiv -\{-u - v : u\} \quad \text{et} \quad \{-u - v : v\} \equiv -\{v : -u - v\}\,.$$

Donc $s'(x)$ appartient à $\mathcal{R}$. Ainsi $\mathcal{R}$ contient $s(x)$ pour $x \in C^{=}$.

En conclusion, $\mathcal{R}$ est le noyau de $R[C_k] \to N_k(R)$. Auparavant on a établi la surjectivité de l'application $R[C^{>+}] \to N_k(R)$. Donc $C^{>+}$ fournit une base de $N_k(R)$ dès que $R[C^{>+}] \cap \mathcal{R} = \{0\}$, ce qu'on se propose de prouver maintenant.

Soit z dans cette intersection. Comme z est dans $\mathcal{R}$, il s'écrit $z = a + b + c + d$ où a, resp. b, resp. c, resp. d, est une combinaison linéaire de $d_\delta(x)$ ($x \in C^{>}$, $\delta \in \Delta$), resp. $s(x)$ ($x \in C^{>}$), resp. $t(x)$ ($x \in C_\bullet$), resp. $d_\delta(x)$ ($x \in C_\bullet, \delta \in \Delta$). Nous allons préciser l'expression de d. Pour cela, considérons l'application

$$\begin{array}{rcl} f : C_\bullet \times (\Delta - \{\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)\}) & \longrightarrow & C^\bullet \\ (x, \delta) & \longmapsto & x\delta. \end{array}$$

Elle est bien définie : un calcul montre que pour $x \in C_\bullet$, $x\delta$ est dans $C_\bullet$ si et seulement si δ est l'identité. De plus, tout $\{u : v\} \in C^\bullet$ a pour antécédent $(\{-\lambda_v u : \lambda_u v\}, \left(\begin{smallmatrix}-\lambda_v^{-1}\lambda_u & 0\\0&1\end{smallmatrix}\right))$, donc f est surjective. Enfin, supposons $f(x_1, \delta_1) = f(x_2, \delta_2)$; comme $x_1 = x_2\delta_2\delta_1^{-1}$ est dans $C_\bullet$, on a nécessairement $\delta_2\delta_1^{-1} = \left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$ d'où $(x_1, \delta_1) = (x_2, \delta_2)$. Ainsi f est bijective. Maintenant le terme d s'écrit de façon générale

$$d = \sum_{x \in C_\bullet, \delta \neq \left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)} r_{x,\delta}((x) - (x\delta))$$

avec $r_{x,\delta} \in R$. D'après ce qui précède, le coefficient de $y \in C^\bullet$ dans le diviseur d est donc $-r_{f^{-1}(y)}$ où $f^{-1}(y)$ est l'antécédent de y par f. Or σ permute $C^{>}$ et $C^{<}$, et τ permute de façon cyclique $C_\bullet$, $C^{>}$ et $C^{<}$. Donc les supports de z, a, b et c ne contiennent aucun élément de $C^\bullet$. Il doit en être de même du support de d. Donc, pour tout $y \in C^\bullet$, le coefficient $r_{f^{-1}(y)}$ est nul. Par bijectivité de f, les coefficients $r_{x,\delta}$ sont nuls pour tout $x \in C_\bullet$ et $\delta \neq \left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$. Ainsi le terme d est nul et $z = a + b + c$. Par suite, les supports de z, a et b ne contiennent aucun élément de $C_\bullet$. En écrivant $c = \sum_{x \in C_\bullet} \mu_x t(x)$, l'intersection du support de c avec $C_\bullet$ est précisément $\{x \in C_\bullet \mid \mu_x \neq 0\}$. Donc c est nul et $z = a + b$. De même, les supports de z et a ne contenant aucun élément de $D^{<}$, le terme b est nul. Enfin, le support de z ne contient aucun élément du complémentaire de $C^{>+}$ dans $C^{>}$, donc a est nul. Cela démontre que $C^{>+}$ donne une base de $N_k(R)$.

Si $k > 0$, par le lemme 5.2, cette base possède $\sum_{0 \leq j \leq k-1} N_{k,j} = q^{2k-1}$ éléments. Si $k = 0$, elle possède un seul élément, $\{1 : 0\}$. Ce sont les rangs annoncés. □

Le théorème principal 1.1 découle de l'énoncé suivant.

Théorème 5.16. *Soit $\mathfrak{p}$ un idéal premier de degré d.*

1. *Soit $1 \leq k < d/2$. Les symboles modulaires $\xi(u : v)$, pour u, v polynômes unitaires de A, premiers entre eux avec $k = \deg u > \deg v$, forment une base de $\mathbf{N}_{\mathfrak{p},k}(R)$. Le symbole modulaire $\xi(1 : 0)$ est une base de $\mathbf{N}_{\mathfrak{p},0}(R)$.*
2. *La famille constituée de $\xi(1 : 0)$ (non parabolique) et de tous les $\xi(u : v)$ (paraboliques), pour u, v polynômes unitaires premiers entre eux de A avec $\deg v < \deg u < d/2$, est libre dans $\mathbf{M}_\mathfrak{p}(R)$. De plus si d est impair, c'est une base de $\mathbf{M}_\mathfrak{p}(R)$ qu'on notera $\mathcal{B}$.*

Démonstration. C'est un corollaire du lemme 5.11 et des propositions 5.13 et 5.15. Les seules affirmations non démontrées sont que $\xi(u:v)$ est parabolique et $\xi(1:0)$ ne l'est pas. L'argument est classique. Comme $\mathfrak{p}$ est premier, il n'y a que deux pointes correspondant à 0 et ∞. Il est facile de voir que $\xi(1:0) = [\infty, 0]$ n'est pas parabolique. Passons à $\xi(u:v)$. Comme u et v sont premiers entre eux, il existe une matrice $\left(\begin{smallmatrix} b & -a \\ u & v \end{smallmatrix}\right)$ dans $\mathrm{G}(A)$ et alors

$$\xi(u:v) = [-a/v, b/u] = [-a/v, 0] - [b/u, 0].$$

Prouvons que les deux derniers symboles modulaires sont paraboliques. Soit P un générateur de $\mathfrak{p}$. Le polynôme P étant irréductible, v est premier à aP. Il existe alors α, β dans A avec $\alpha v + \beta a P = 1$. La matrice $g = \left(\begin{smallmatrix} \alpha & -a \\ \beta P & v \end{smallmatrix}\right)$ est dans $\Gamma_0(\mathfrak{p})$ et vérifie $g0 = -a/v$. Donc $[-a/v, 0]$ est parabolique. On procède de même avec $[b/u, 0]$. □

Remarque 5.17.
- Si $\mathfrak{p}$ est de degré 1, le module $\mathbf{M}_{\mathfrak{p}}(R)$ a donc pour base $\xi(1:0)$.
- Si $d \geq 3$, le sous-espace parabolique $\mathbf{M}^0_{\mathfrak{p}}(R)$ est non nul et l'énoncé en donne une famille libre (et même une base si $\deg \mathfrak{p}$ est impair).
- L'énoncé du théorème reste valable en remplaçant $\xi(1:0)$ par $\xi(0:1)$, ou la condition $\deg u > \deg v$ par $\deg u < \deg v$.
- Si d est impair, on retrouve la formule (2) de Gekeler pour le genre. En effet, cette base explicite $\mathcal{B}$ de $\mathbf{M}_{\mathfrak{p}}$ possède $1 + (q^d - q)/(q^2 - 1)$ éléments (d'après la proposition 5.15 et le théorème 5.16) et par ailleurs, on sait d'après Teitelbaum que le rang doit être $g + 1$ (car $h = 2$ lorsque $\mathfrak{p}$ est premier). Notre construction de la base $\mathcal{B}$ fournit en fait une interprétation arithmétique de la formule pour le genre.
- Avec le théorème 5.16, on retrouve aussi le fait que $\mathbf{M}_{\mathfrak{p}}$ est sans torsion sur $\mathbf{Z}$ si $\mathfrak{p}$ est de degré impair.

Lorsque d est impair, la première partie de la preuve de la proposition 5.15 donne même l'expression de tout symbole de Manin–Teitelbaum dans la base $\mathcal{B}$.

Théorème 5.18. *Soit $\mathfrak{p}$ un idéal premier de degré impair d. Soit $x \in \mathbf{P}^1(A/\mathfrak{p})$. D'après la proposition 5.5, on peut écrire $x = (u:v)$ avec u, v premiers entre eux dans A de degrés $< d/2$.*
- *Si $v = 0$ alors $\xi(x) = \xi(1:0)$. Si $u = 0$ alors $\xi(x) = -\xi(1:0)$. Si u et v sont constants non nuls, alors $\xi(x) = 0$.*
- *Supposons u et v non constants. Soient λ_u et λ_v leurs coefficients dominants respectifs.*
  - *Si $\deg u > \deg v$ alors $\xi(x) = \xi(u/\lambda_u : v/\lambda_v)$.*
  - *Si $\deg u < \deg v$ alors $\xi(x) = -\xi(v/\lambda_v : u/\lambda_u)$.*
  - *Supposons $\deg u = \deg v$. Notons $w = \lambda_v u - \lambda_u v$ ($\neq 0$) et λ_w son coefficient dominant. Alors*

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

Sous les hypothèses de l'énoncé, tout symbole de Manin–Teitelbaum s'écrit donc comme combinaison linéaire d'au plus deux éléments de la base $\mathcal{B}$. C'est une façon particulièrement économe de stocker les données relatives à cette base, qui pourrait avoir un intérêt pour l'implémentation sur machine.

Si $\deg \mathfrak{p}$ est impair, on a l'isomorphisme $\alpha : \mathbf{M}_{\mathfrak{p}}^0 \xrightarrow{\simeq} \mathbf{H}_{\mathfrak{p}}$ du lemme 4.4. Le théorème 5.16 fournit alors une base de l'espace des cochaînes paraboliques, qui est explicite en un certain sens.

Corollaire 5.19. *Soit $\mathfrak{p}$ premier de degré impair d. La famille de cochaînes paraboliques $\alpha(\xi(u:v))$, où u et v sont unitaires premiers entre eux tels que $\deg v < \deg u < d/2$, est une base de $\mathbf{H}_{\mathfrak{p}}$ sur $\mathbf{Z}$.*

Remarque 5.20. Gekeler avait donné une base explicite de $\mathbf{H}_{\mathfrak{n}}$ si $\mathfrak{n}$ est de degré 3, non nécessairement premier ([5, section 5], [9, section 6]). Dans le paragraphe 7.1.2, on la comparera sur un exemple avec celle obtenue au corollaire 5.19. Si ces bases coïncident de façon générale, le théorème 5.16 pourrait alors être vu comme un prolongement du travail de Gekeler à $\mathfrak{p}$ premier quelconque de degré impair.

6 L'action de Hecke sur les symboles de Manin–Teitelbaum

Dans cette section, on travaille dans l'espace $\mathbf{M}_{\mathfrak{n}}$ de symboles modulaires avec $\mathfrak{n}$ idéal quelconque de A. On exprime l'action de l'opérateur de Hecke $T_{\mathfrak{m}}$ en termes de symboles de Manin–Teitelbaum.

Théorème 6.1. *Pour tout idéal $\mathfrak{m}$ et $(u:v) \in \mathbf{P}^1(A/\mathfrak{n})$, on a*

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

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

Soit $M_2(A)$ l'ensemble des matrices 2×2 à coefficients dans A. Pour une telle matrice $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ et $(u:v) \in \mathbf{P}^1(A/\mathfrak{n})$, 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 se récrit alors

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

L'énoncé et sa preuve sont à rapprocher de ceux de Merel [20] pour les symboles modulaires sur $\mathbf{Q}$ (voir aussi la démonstration de [21, lem. 2]) qui font suite aux travaux de Manin [16] et Mazur [17] sur les matrices de Heilbronn.

L'ensemble $\mathcal{S}_{\mathfrak{m}}$ étant indépendant de $\mathfrak{n}$, le théorème 6.1 entraîne une loi de réciprocité pour les courbes elliptiques sur K (proposition 6.6). Dans la section 6.2, on donne la liste des matrices de $\mathcal{S}_{\mathfrak{m}}$ lorsque $\mathfrak{m}$ est de petit degré.

Le théorème 6.1 fournit aussi un algorithme pour calculer la matrice de $T_{\mathfrak{m}}$ dans une base de $\mathbf{M}_{\mathfrak{n}}$ (dans [29, 3.4.2 et 8.3.2] sont discutés des algorithmes similaires pour les symboles modulaires classiques issus de [20]). Cette méthode se prête bien aux calculs à $\mathfrak{m}$ fixé pour différents sous-groupes de congruence $\Gamma_0(\mathfrak{n})$ du fait que $\mathcal{S}_{\mathfrak{m}}$ ne dépend pas de $\mathfrak{n}$.

6.1 Démonstration du théorème 6.1

Lemme 6.2. *L'ensemble de matrices $\mathcal{S}_\mathfrak{m}$ est fini.*

Démonstration. Soit $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ appartenant à $\mathcal{S}_\mathfrak{m}$. Comme $\deg a > \deg b$ et $\deg d > \deg c$, le degré de $ad - bc$ est égal à $\deg(ad) = \deg a + \deg d$. Or, $(ad - bc) = \mathfrak{m}$ donc $\deg a$ et $\deg d$ valent au plus $\deg \mathfrak{m}$. 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. □

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

Proposition 6.3. *Les matrices $m(a,b) = \left(\begin{smallmatrix} a & b \\ 0 & P/a \end{smallmatrix}\right)$ avec a divisant P, a unitaire et $\deg a > \deg b$, forment un système de représentants de $M_2(A)_\mathfrak{m}/\mathrm{G}(A)$. De plus, ce sont les seuls éléments $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ de $\mathcal{S}_\mathfrak{m}$ avec $c = 0$.*

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

Proposition 6.4. *Soit $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathcal{S}_\mathfrak{m}$. Si $c \neq 0$ (c'est-à-dire $M\infty \neq \infty$), il existe une unique matrice $M' \in \mathcal{S}_\mathfrak{m} \cap M\mathrm{G}(A)$ telle que $M'0 = M\infty$. Si $b \neq 0$ (c'est-à-dire $M0 \neq 0$), il existe une unique matrice $M' \in \mathcal{S}_\mathfrak{m} \cap M\mathrm{G}(A)$ 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 $\deg c > \deg(cQ - \alpha d)$. Posons

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

Comme $\deg Q > 0$, 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 $\mathcal{S}_\mathfrak{m}$ et vérifie $M'0 = a/c = M\infty$.

Passons à l'unicité. Soit une matrice $M'' \in \mathcal{S}_\mathfrak{m} \cap M\mathrm{G}(A)$ 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 $M^{-1}M'' = \left(\begin{smallmatrix} Q & \alpha^{-1} \\ -\alpha & 0 \end{smallmatrix}\right)$ avec $\alpha \in \mathbf{F}_q^\times$ et $Q \in A$, d'où $M'' = \left(\begin{smallmatrix} aQ-\alpha b & \alpha^{-1}a \\ cQ-\alpha d & \alpha^{-1}c \end{smallmatrix}\right)$. De plus, M'' étant dans $\mathcal{S}_\mathfrak{m}$, le polynôme $\alpha^{-1}c$ est unitaire donc α est le coefficient dominant de c. Il reste à montrer que Q est déterminé par la matrice M. Comme $M'' \in \mathcal{S}_\mathfrak{m}$, 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. □

Démonstration du théorème 6.1. Prenons un représentant (u, v) de $(u : v)$ dans $A \times A$ avec u et v premiers entre eux. Il existe donc une matrice $g = \left(\begin{smallmatrix} x & y \\ u & v \end{smallmatrix}\right) \in \mathrm{G}(A)$ telle que $\xi(u : v) = [g0, g\infty]$. Soit $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathcal{S}_{\mathfrak{m}}$. On commence par relever $(au+cv : bu+dv)$ en une matrice de $\mathrm{G}(A)$. Comme $gM \in M_2(A)_{\mathfrak{m}}$, il existe δ et β, avec $\delta \mid P$, δ unitaire et $\deg \beta < \deg \delta$, tels que $gM \in m(\delta, \beta)\mathrm{G}(A)$ d'après la proposition 6.3. Comme $m(\delta, \beta)^{-1} gM \in \mathrm{G}(A)$, on a

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

si P/δ est inversible dans $A/\mathfrak{n}$. Pour simplifier, posons $C(\delta, \beta) = m(\delta, \beta)\mathrm{G}(A)$. Par la proposition 6.3, on en déduit l'égalité des sommes, finies d'après le lemme 6.2 :

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

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

$$D = \sum_{\beta,\delta,M} (m(\delta,\beta)^{-1}gM\infty) - (m(\delta,\beta)^{-1}gM0)$$

où la somme est sur β, δ et M comme précédemment. Si M vérifie $M0 \neq 0$, d'après la proposition 6.4, il existe une unique matrice $M' \in \mathcal{S}_{\mathfrak{m}} \cap M\mathrm{G}(A)$ 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

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

En utilisant l'unicité dans la proposition 6.4, le diviseur D vaut

$$\begin{aligned}&\sum_{\beta,\delta}\left(\sum_{\substack{M \in g^{-1}C(\delta,\beta)\cap\mathcal{S}_{\mathfrak{m}}, \\ M\infty=\infty}} (m(\delta,\beta)^{-1}gM\infty) - \sum_{\substack{M \in g^{-1}C(\delta,\beta)\cap\mathcal{S}_{\mathfrak{m}}, \\ M0=0}} (m(\delta,\beta)^{-1}gM0)\right) \\ =&\sum_{\beta,\delta}\left((m(\delta,\beta)^{-1}g\infty) - (m(\delta,\beta)^{-1}g0)\right)\end{aligned}$$

(β, δ dans A avec $\deg\beta < \deg\delta$, δ unitaire divisant P et $(P/\delta)+\mathfrak{n} = A$). La dernière égalité provient du fait que chaque classe pour $\mathrm{G}(A)$ possède d'uniques représentants fixant 0 et ∞ respectivement (voir proposition 6.3). Donc on obtient l'égalité de symboles modulaires

$$\sum_{\substack{M \in \mathcal{S}_{\mathfrak{m}} \\ (u:v)M \text{ bien défini}}} \xi((u:v)M) = \sum_{\substack{\deg\beta < \deg\delta \\ \delta \mid P,\ \delta \text{ unitaire} \\ (P/\delta)+\mathfrak{n}=A}} \left[m(\delta,\beta)^{-1}g0, m(\delta,\beta)^{-1}g\infty\right].$$

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

6.2 Exemples d'ensembles $\mathcal{S}_{\mathfrak{m}}$

La lettre P continue à désigner le générateur unitaire de l'idéal $\mathfrak{m}$. Si $\mathfrak{m}$ est de degré 1, l'ensemble $\mathcal{S}_{\mathfrak{m}}$ est formé des $2q$ matrices $\left(\begin{smallmatrix} P & \lambda \\ 0 & 1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & 0 \\ \lambda & P \end{smallmatrix}\right)$, pour $\lambda \in \mathbf{F}_q$, et d'après le théorème 6.1, l'action de $T_{\mathfrak{m}}$ est alors donnée par

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

Si $\mathfrak{m}$ est de degré 2, on obtient facilement la liste suivante des matrices de $\mathcal{S}_{\mathfrak{m}}$.

Lemme 6.5. *Soit $\mathfrak{m}$ l'idéal engendré par $P = T^2 + mT + n$ $(m, n \in \mathbf{F}_q)$. Posons*

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

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

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

$$\begin{aligned} M_1(b), M_2(b) \qquad & (b \in A, \deg b \leq 1) \\ M_3(-x, b, c) \qquad & (x \in \mathcal{R},\ b, c \in \mathbf{F}_q \text{ avec } b = 0 \text{ ou } c = 0) \\ M_3(\alpha, b, -P(-\alpha)/b) \qquad & (\alpha \in \mathbf{F}_q, \alpha \notin \mathcal{R}, b \in \mathbf{F}_q^{\times}). \end{aligned}$$

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

6.3 Une loi de réciprocité de Manin

Cet énoncé est une conséquence directe du théorème 6.1 et du théorème de modularité pour les courbes elliptiques sur K.

Proposition 6.6. *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. Alors il existe une application $l_E : \mathbf{P}^1(A/\mathfrak{n}) \to \mathbf{Q}$ et un élément λ_E de $\mathbf{P}^1(A/\mathfrak{n})$ tels qu'on ait, pour tout $\mathfrak{p}$ premier avec $\mathfrak{n} \not\subset \mathfrak{p}$,*

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

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 $\mathfrak{p}$.

L'ensemble $\mathcal{S}_{\mathfrak{p}}$ étant indépendant de $\mathfrak{n}$, l'énoncé s'apparente à une loi de réciprocité comme l'a remarqué Manin : elle relie les solutions modulo $\mathfrak{p}$ d'une équation dépendant de $\mathfrak{n}$ aux solutions modulo $\mathfrak{n}$ d'une équation dépendant de $\mathfrak{p}$. Pour des résultats similaires sur $\mathbf{Q}$, on renvoie à Manin [16, th. 7.3], Mazur [17] et Merel [19, th. 4].

Démonstration. Soit E une telle courbe elliptique. D'après le théorème de modularité pour les courbes elliptiques sur K, corollaire des travaux de Grothendieck, Jacquet–Langlands, Deligne et Drinfeld (discuté dans [12, section 8]), 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 $\mathfrak{n} \not\subset \mathfrak{p}$. Considérons l'application

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

Elle n'est pas identiquement nulle. En effet, comme $F \neq 0$ et l'accouplement est parfait sur $\mathbf{Q}$, il existe au moins un générateur $\xi(x)$ de $\mathbf{M}^0(\mathbf{Q})$ avec $l_F(x) \neq 0$. Fixons un élément λ_E de $\mathbf{P}^1(A/\mathfrak{n})$ vérifiant $l_F(\lambda_E)) \neq 0$. Pour tout $x \in \mathbf{P}^1(A/\mathfrak{n})$, on a d'après le théorème 6.1 :

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

L'application $l_E = l_F / l_F(\lambda_E)$ satisfait alors la propriété souhaitée. □

7 Indépendance linéaire d'opérateurs de Hecke

Dans cette section on travaille avec $\mathbf{M}_{\mathfrak{p}}$, pour $\mathfrak{p}$ premier.

7.1 L'élément d'enroulement

7.1.1 Définition et propriétés

Définition 7.1. En s'inspirant de [18, 21], on appelle *élément d'enroulement* le symbole modulaire parabolique $\mathbf{e} \in \mathbf{M}^0_{\mathfrak{p}}(\mathbf{Q})$ correspondant à la forme linéaire $F \mapsto \langle [0, \infty], F \rangle$ sur $\mathbf{H}(\mathbf{Q})$ d'après le théorème 4.2.

En particulier, par la formule (3), on a pour toute cochaîne F de $\mathbf{H}(\mathbf{C})$

$$L(F, 1) = \frac{1}{q-1} \langle \mathbf{e}, F \rangle. \tag{6}$$

Rappelons que $\overline{\mathbf{M}^0_{\mathfrak{p}}}$ (noté aussi $\overline{\mathbf{M}^0}$) désigne le quotient sans torsion $\mathbf{M}^0_{\mathfrak{p}} / (\mathbf{M}^0_{\mathfrak{p}})_{\text{tors}}$. On l'identifie à un sous $\mathbf{Z}$-module de $\mathbf{M}^0(\mathbf{Q})$. Notons $\eta_{\mathfrak{m}} = T_{\mathfrak{m}} - (q^{\deg \mathfrak{m}} + 1)$ dans $\mathbf{T}$, pour tout premier $\mathfrak{m} \neq \mathfrak{p}$.

Lemme 7.2. *On a* $\eta_{\mathfrak{m}} [0, \infty] = \eta_{\mathfrak{m}} \mathbf{e}$ *dans* $(q-1)\overline{\mathbf{M}^0}$.

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

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

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

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

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 des symboles modulaires $\eta_{\mathfrak{m}}\,[0, \infty] \in \overline{\mathbf{M}^0}$ et $\eta_{\mathfrak{m}}\mathbf{e}$. Comme ils sont paraboliques d'après ce qui précède, ils sont égaux par perfection de $\langle \cdot, \cdot \rangle$ sur $\mathbf{Q}$. □

Définition 7.3 (voir aussi [23, 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, $\mathfrak{m} \neq \mathfrak{p}$.

Il n'est pas clair que cette définition coïncide avec donnée par A. Tamagawa [30, p. 230] comme annulateur du diviseur cuspidal. Par ailleurs d'après le lemme 7.2, $I_E\mathbf{e}$ est contenu dans $(q-1)\overline{\mathbf{M}^0}$. Afin de préciser le dénominateur de l'élément d'enroulement, on rappelle un théorème de Pál sur la structure de $\mathbf{T}/I_E$, analogue d'un énoncé célèbre de Mazur [18].

Théorème 7.4 (([25, th. 1.2]))**.** *Si* $\mathfrak{p}$ *est premier de degré* d*, le groupe abélien* $\mathbf{T}/I_E$ *est cyclique d'ordre*

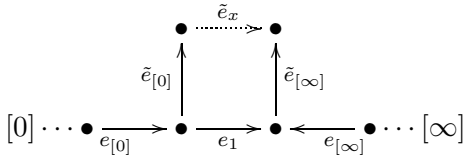
$$n_E(\mathfrak{p}) = \begin{cases} \frac{q^d-1}{q-1} & \text{si } d \text{ est impair ;} \\ \frac{q^d-1}{q^2-1} & \text{si } d \text{ est pair.} \end{cases}$$

Proposition 7.5. *Il existe un plus petit entier* $d_{\mathbf{e}} > 0$ *tel que* $d_{\mathbf{e}}\mathbf{e} \in \overline{\mathbf{M}^0}$*. On l'appelle* dénominateur *de* $\mathbf{e}$*. Il divise* $n_E(\mathfrak{p})$ *; en particulier, il est premier à* p*.*

Démonstration. Soit $\mathbf{e}'$ la classe de $\mathbf{e}$ dans $\mathbf{M}^0(\mathbf{Q})/\overline{\mathbf{M}^0}$. Comme $I_E\mathbf{e}$ est contenu dans $\overline{\mathbf{M}^0}$, l'application canonique $\mathbf{T} \to \mathbf{T}\mathbf{e}'$ passe au quotient en un homomorphisme surjectif de groupes abéliens $\mathbf{T}/I_E \to \mathbf{T}\mathbf{e}'$. D'après le théorème 7.4, $\mathbf{T}\mathbf{e}'$ est donc fini d'ordre divisant $n_E(\mathfrak{p})$. On en déduit que $\mathbf{e}'$ est d'ordre fini, divisant $n_E(\mathfrak{p})$, dans le groupe $\mathbf{M}^0(\mathbf{Q})/\overline{\mathbf{M}^0}$. Cet ordre est le dénominateur de $\mathbf{e}$. Il est premier à p car $p \nmid n_E(\mathfrak{p})$. □

7.1.2 Exemple de calcul de e et $d_{\mathbf{e}}$

Rappelons l'isomorphisme $\alpha : \mathbf{M}^0(\mathbf{Q}) \xrightarrow{\simeq} \mathbf{H}(\mathbf{Q})$ déduit du lemme 4.4. Pour $\mathfrak{p}$ premier de degré 3, on propose d'expliciter $\alpha(\mathbf{e})$ dans une base de $\mathbf{H}_{\mathfrak{p}}(\mathbf{Q})$. Notre calcul repose sur une description du graphe $\Gamma\backslash\mathcal{T}$ donnée par Gekeler. Ce graphe est de genre q et possède deux pointes notées $[0]$ et $[\infty]$. D'après [5, 5.3] et [9, section 6], en reprenant les notations de ce dernier, la structure de $\Gamma\backslash\mathcal{T}$ est :



où $\overset{\tilde{e}_x}{\dashrightarrow}$ désigne q arêtes indexées par $x \in \mathbf{F}_q$. De plus, la projection dans le groupe $H_1(\Gamma\backslash\mathcal{T}, \mathbf{ptes}, \mathbf{Z})$ 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

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

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 $\mathrm{Hom}(\mathbf{H}, \mathbf{Z})$. La forme linéaire $F \mapsto \langle [0,\infty] \, , F\rangle$ s'écrit $\sum_{x\in\mathbf{F}_q} \varphi_x^{'}$. 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 la relation $(\alpha(\mathbf{e}), \cdot)_\mu = \sum_{x\in\mathbf{F}_q} \varphi_x^{'}$. En calculant le volume de chaque arête du graphe à l'aide de [5, lem. 5.6] ou [9, sec. 6], 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

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

En particulier, si $\mathfrak{p}$ est premier de degré 3, le dénominateur $d_{\mathbf{e}}$ est exactement $n_E(\mathfrak{p})$.

Maintenant, sur un exemple, on exprime $\mathbf{e}$ dans la base explicite du théorème 1.1. Cela permettra de comparer cette base à celle de Gekeler évoquée dans la remarque 5.20.

Exemple 7.6 ($q = 2$ et $\mathfrak{p} = (T^3 + T + 1)$ idéal premier)**.** Nous avons vu qu'une base de l'espace $\mathbf{M}_{\mathfrak{p}}^0$ est $\{\xi(T:1), \xi(T+1:1)\}$. Pour $\mathfrak{m}$ idéal de degré 1, de générateur unitaire m, on a $\eta_{\mathfrak{m}}\mathbf{e} = -(q-1)\xi(m:1)$ (voir la preuve du lemme 7.2). Cela donne

$$\eta_T \mathbf{e} = (T_{(T)} - 3)\mathbf{e} = -\xi(T:1). \tag{7}$$

Par ailleurs, la matrice de l'opérateur $T_{(T)}$ dans la base est $\left(\begin{smallmatrix} -3 & -1 \\ 2 & 1 \end{smallmatrix}\right)$. De (7), on déduit

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

Avec les notations précédentes, la base de Gekeler pour $\mathbf{H}$ est $\{\varphi_0, \varphi_1\}$. Notons i l'injection $\mathbf{H} \to \mathrm{Hom}(\mathbf{H}, \mathbf{Z})$ donnée par le produit de Petersson et $v = i \circ \alpha : \mathbf{M} \to \mathrm{Hom}(\mathbf{H}, \mathbf{Z})$. Si $\mathfrak{m}$ est de degré 1, on a $v(\xi(m:1)) = -\eta_{\mathfrak{m}}^t(v(\mathbf{e})) = -\eta_{\mathfrak{m}}^t(\varphi_0^{'} + \varphi_1^{'})$, où $\eta_{\mathfrak{m}}^t$ désigne l'application transposée de $\eta_{\mathfrak{m}}$. Par ailleurs, les matrices des opérateurs $T_{(T)}$ et $T_{(T+1)}$ dans $\{\varphi_0, \varphi_1\}$ sont respectivement $\left(\begin{smallmatrix} -3 & -1 \\ 2 & 1 \end{smallmatrix}\right)$ et $\left(\begin{smallmatrix} 2 & 1 \\ -2 & -2 \end{smallmatrix}\right)$ d'après [5, 6.8] [2]. 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 $\left(\begin{smallmatrix} 4 & 3 \\ 3 & 4 \end{smallmatrix}\right)$, on a alors $\alpha(\xi(T:1)) = \varphi_0$ et $\alpha(\xi(T+1:1)) = \varphi_1$. Sur cet exemple, la base de Gekeler coïncide donc avec celle du corollaire 5.19.

2. Dans cette référence, les opérateurs de Hecke agissent à droite. Les matrices de l'exemple (6.10) sont donc les transposées des nôtres.

7.2 Indépendance linéaire d'opérateurs de Hecke en l'élément d'enroulement

On établit l'énoncé sur $[0,\infty]$ puis on le relève à $\mathbf{e}$.

Proposition 7.7. *Soient R un anneau commutatif intègre dans lequel $q-1$ est non nul et $r \geq 0$ un entier. Si $\deg \mathfrak{p} \geq 2r+1$, la famille $\{T_\mathfrak{m}[0,\infty]\}_{\deg \mathfrak{m} \leq r}$ est libre sur R dans $\mathbf{M}_\mathfrak{p}(R)$.*

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

$$\sum_{\deg \mathfrak{m} \leq r} \lambda_\mathfrak{m} T_\mathfrak{m}[0,\infty] = 0 \tag{8}$$

avec $\lambda_\mathfrak{m} \in R$. Montrons que $\lambda_\mathfrak{n} = 0$ pour tout $\mathfrak{n}$ de degré r. L'hypothèse de récurrence permettra alors de conclure. Le théorème 6.1 appliqué à $[0,\infty] = \xi(0:1)$ donne

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

où la dernière égalité provient de $\xi(c:d) = -\xi(-d:c) = -\xi(d:c)$. Par ailleurs, $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathcal{S}_\mathfrak{m}$ si et seulement si $\left(\begin{smallmatrix} a & \lambda^{-1}b \\ \lambda c & d \end{smallmatrix}\right) \in \mathcal{S}_\mathfrak{m}$ pour tout $\lambda \in \mathbf{F}_q^\times$. Puisque $\xi(d:\lambda c) = \xi(d:c)$ on a donc

$$T_\mathfrak{m}[0,\infty] = -k\xi(1:0) - (q-1) \sum_{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathcal{S}_\mathfrak{m},\ c \text{ unitaire},\ (c)+(d)+\mathfrak{p}=A} \xi(d:c) \tag{9}$$

où k est le nombre de relèvements de $(0:1)$ en matrices de $\mathcal{S}_\mathfrak{m}$. 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 $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathcal{S}_\mathfrak{m}$. Notons n le générateur unitaire de $\mathfrak{n}$. Des considérations élémentaires montrent que $(d:c) = (n:1)$ pour un $(d,c) \in u_\mathfrak{m}$ (avec $\deg \mathfrak{m} \leq r$) si et seulement si $\mathfrak{m} = \mathfrak{n}$ et $(d,c) = (n,1)$ dans $A \times A$. En isolant le terme en $\xi(n:1)$ dans (8) à l'aide de (9), on obtient alors

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

avec k' et $\alpha_{d,c}$ dans R et $v_r = (\cup_{\deg \mathfrak{m} \leq r} u_\mathfrak{m}) - \{(n,1)\}$. 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 $r < \deg(\mathfrak{p})/2$ donc les symboles modulaires

$$\{\xi(1:0), \xi(n:1)\} \cup \{\xi(d:c) \mid (d,c) \in v_r, (d)+(c) = A\}$$

forment une sous-famille de celle, libre, du théorème 5.16. Le théorème appliqué à R donne $(q-1)\lambda_\mathfrak{n} = 0$. Comme $q-1$ est non nul dans l'anneau intègre R, on conclut $\lambda_\mathfrak{n} = 0$. □

Remarque 7.8. D'après la relation (9), l'énoncé de la proposition n'est plus vrai si la caractéristique de R divise $q-1$.

On donne des énoncés de relèvement en caractéristique 0 et p (la caractéristique de K). Notons $\widetilde{\mathbf{e}}$ la classe de $d_{\mathbf{e}}\mathbf{e}$ dans $\overline{\mathbf{M}^0_{\mathfrak{p}}}/p\overline{\mathbf{M}^0_{\mathfrak{p}}}$.

Lemme 7.9. *1. Supposons la famille $\{T_{\mathfrak{m}}\,[0,\infty]\}_{\deg\mathfrak{m}\leq r+1}$ libre sur $\mathbf{Z}$ dans $\mathbf{M}_{\mathfrak{p}}$. Alors la famille $\{T_{\mathfrak{m}}\mathbf{e}\}_{\deg\mathfrak{m}\leq r}$ est libre sur $\mathbf{Z}$.*

2. Supposons la famille $\{T_{\mathfrak{m}}\,[0,\infty]\}_{\deg\mathfrak{m}\leq r+1}$ libre sur $\mathbf{F}_p$ dans $\mathbf{M}_{\mathfrak{p}}(\mathbf{F}_p)$. Alors la famille $\{T_{\mathfrak{m}}\widetilde{\mathbf{e}}\}_{\deg\mathfrak{m}\leq r}$ est libre sur $\mathbf{F}_p$ dans $\overline{\mathbf{M}^0_{\mathfrak{p}}}/p\overline{\mathbf{M}^0_{\mathfrak{p}}}$.

Démonstration. Supposons qu'il existe $\lambda_{\mathfrak{m}}\in\mathbf{Z}$ pour $\deg\mathfrak{m}\leq r$ avec $\sum_{\mathfrak{m}}\lambda_{\mathfrak{m}}T_{\mathfrak{m}}\mathbf{e}=0$. Fixons un idéal $\mathfrak{n}$ de A de degré 1. En appliquant l'élément $\eta_{\mathfrak{n}}$ de l'anneau commutatif $\mathbf{T}$, on obtient $\sum_{\mathfrak{m}}\lambda_{\mathfrak{m}}T_{\mathfrak{m}}\eta_{\mathfrak{n}}\mathbf{e}=0$. Puis, d'après le lemme 7.2, on a l'égalité dans $\overline{\mathbf{M}^0_{\mathfrak{p}}}$

$$\sum_{\mathfrak{m}}\lambda_{\mathfrak{m}}T_{\mathfrak{m}}T_{\mathfrak{n}}\,[0,\infty]-(q+1)\sum_{\mathfrak{m}}\lambda_{\mathfrak{m}}T_{\mathfrak{m}}\,[0,\infty]=0. \tag{10}$$

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

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

En particulier $T_{\mathfrak{m}}T_{\mathfrak{n}}$ est la somme de $T_{\mathfrak{m}\mathfrak{n}}$ et d'une combinaison linéaire sur $\mathbf{Z}$ d'opérateurs $T_{\mathfrak{r}}$ où $\deg\mathfrak{r}<\deg(\mathfrak{m}\mathfrak{n})$ c'est-à-dire $\deg\mathfrak{r}\leq r$. De (10) on déduit une expression de $\lambda_{\mathfrak{m}}T_{\mathfrak{m}\mathfrak{n}}\,[0,\infty]$ dans $\overline{\mathbf{M}^0_{\mathfrak{p}}}$ comme combinaison linéaire de $(T_{\mathfrak{r}}\,[0,\infty])_{\deg\mathfrak{r}\leq r}$. Supposons $\mathfrak{m}$ de degré r. Par hypothèse, la famille $\{T_{\mathfrak{m}}\,[0,\infty]\}_{\deg\mathfrak{m}\leq r+1}$ étant libre dans $\mathbf{M}_{\mathfrak{p}}$, son image dans $\mathbf{M}_{\mathfrak{p}}/(\mathbf{M}_{\mathfrak{p}})_{\mathrm{tors}}$ est aussi libre sur $\mathbf{Z}$. Comme $\deg(\mathfrak{m}\mathfrak{n})=r+1$, le coefficient $\lambda_{\mathfrak{m}}$ est donc nul pour tout $\mathfrak{m}$ de degré r. En reportant dans (10) et en appliquant le même raisonnement à $\mathfrak{m}$ de degré $r-1$, puis $r-2$, et ainsi de suite, on trouve $\lambda_{\mathfrak{m}}=0$ pour tout $\mathfrak{m}$ de degré $\leq r$. Ainsi la famille est libre.

Passons à $\mathbf{F}_p$. Supposons qu'on ait $\sum_{\mathfrak{m}}\lambda_{\mathfrak{m}}T_{\mathfrak{m}}\widetilde{\mathbf{e}}=0$ dans $\overline{\mathbf{M}^0_{\mathfrak{p}}}/p\overline{\mathbf{M}^0_{\mathfrak{p}}}$ pour $\lambda_{\mathfrak{m}}\in\mathbf{Z}$. Un raisonnement similaire au précédent affirme que l'élément

$$\sum_{\mathfrak{m}}\lambda_{\mathfrak{m}}d_{\mathbf{e}}T_{\mathfrak{m}}\eta_{\mathfrak{n}}[0,\infty]=\sum_{\mathfrak{m}}\lambda_{\mathfrak{m}}d_{\mathbf{e}}T_{\mathfrak{m}}\eta_{\mathfrak{n}}\mathbf{e}$$

est dans $p\overline{\mathbf{M}^0_{\mathfrak{p}}}$, qui s'injecte dans $p\overline{\mathbf{M}_{\mathfrak{p}}}$, en notant $\overline{\mathbf{M}_{\mathfrak{p}}}=\mathbf{M}_{\mathfrak{p}}/(\mathbf{M}_{\mathfrak{p}})_{\mathrm{tors}}$. Par ailleurs, $\mathfrak{p}$ étant premier, le groupe $(\mathbf{M}_{\mathfrak{p}})_{\mathrm{tors}}$ est trivial ou cyclique d'ordre $(q+1)$ ([32, p. 278]) donc d'ordre premier à p. Il y a donc un isomorphisme canonique $\mathbf{M}_{\mathfrak{p}}/p\mathbf{M}_{\mathfrak{p}}\simeq\overline{\mathbf{M}_{\mathfrak{p}}}/p\overline{\mathbf{M}_{\mathfrak{p}}}$. Donc l'image de $\sum_{\mathfrak{m}}\lambda_{\mathfrak{m}}d_{\mathbf{e}}T_{\mathfrak{m}}\eta_{\mathfrak{n}}[0,\infty]$ est nulle dans le $\mathbf{F}_p$-espace vectoriel $\mathbf{M}_{\mathfrak{p}}/p\mathbf{M}_{\mathfrak{p}}$. Par ailleurs, le dénominateur $d_{\mathbf{e}}$ étant premier à p (proposition 7.5), cela revient à $\sum_{\mathfrak{m}}\lambda_{\mathfrak{m}}T_{\mathfrak{m}}\eta_{\mathfrak{n}}[0,\infty]=0$ dans $\mathbf{M}_{\mathfrak{p}}/p\mathbf{M}_{\mathfrak{p}}=\mathbf{M}_{\mathfrak{p}}(\mathbf{F}_p)$. La fin de l'argument est similaire à celui sur $\mathbf{Z}$. □

Théorème 7.10. *Soient $\mathfrak{p}$ un idéal premier de degré ≥ 3 et r la partie entière de $(\deg(\mathfrak{p})-3)/2$.*

1. Les symboles modulaires $\{T_{\mathfrak{m}}\mathbf{e}\}_{\deg\mathfrak{m}\leq r}$ sont libres sur $\mathbf{Z}$ dans $\mathbf{T}\mathbf{e}\subset\mathbf{M}^0_{\mathfrak{p}}(\mathbf{Q})$.

2. Les symboles modulaires $\{T_{\mathfrak{m}}\widetilde{\mathbf{e}}\}_{\deg \mathfrak{m}\leq r}$ *sont libres sur* $\mathbf{F}_p$ *dans* $\overline{\mathbf{M}^0_{\mathfrak{p}}}/p\overline{\mathbf{M}^0_{\mathfrak{p}}}$.

Démonstration. Comme $\deg \mathfrak{p} \geq 2r+3$, la famille $\{T_{\mathfrak{m}}\,[0,\infty]\}_{\deg \mathfrak{m}\leq r+1}$ est libre sur $\mathbf{Z}$ dans $\mathbf{M}_{\mathfrak{p}}$ d'après la proposition 7.7. On relève le résultat dans $\mathbf{Te}$ à l'aide du lemme 7.9. Le deuxième énoncé se prouve de façon similaire avec la proposition 7.7 pour $R = \mathbf{F}_p$. □

Corollaire 7.11. *Les affirmations suivantes sont équivalentes pour* $\mathfrak{p}$ *premier :*

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

Démonstration. L'équivalence de 2 et 3 découle de la formule (2) qui donne le genre en fonction de $\deg \mathfrak{p}$. Le théorème 7.10 pour $r = 0$ démontre $3 \Rightarrow 1$. Enfin, l'implication $1 \Rightarrow 2$ vient du fait que la dimension de $\mathbf{M}^0_{\mathfrak{p}}(\mathbf{Q})$ est g. □

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 $\mathrm{End}(\mathbf{H})$, le $\mathbf{Z}$-module $\mathbf{T}$ est libre de type fini. Soit $\mathcal{F}$ l'ensemble des formes primitives de $\mathbf{H}(\mathbf{C})$ (on l'a noté $\mathcal{F}_{\mathfrak{p}}$ dans l'introduction). On a supposé $\mathfrak{p}$ 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 $(\mathbf{T}/a_{[F]}) \otimes_{\mathbf{Z}} \mathbf{Q} \simeq K_F$. Le morphisme canonique de $\mathbf{T}$-modules $\varphi : \mathbf{T} \to \prod_{[F]\in\mathcal{E}} \mathbf{T}/a_{[F]}$ 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 7.12. *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 $\mathbf{M}^0(\mathbf{Q})$ donne un isomorphisme de $\mathbf{Z}$-modules $\mathbf{T}/I_{\mathbf{e}} \simeq \mathbf{Te}$. Calculons le rang du quotient.

Notons $\mathcal{E}_{\mathbf{e}}$ 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

$$\bigcap_{[F]\in\mathcal{E}_{\mathbf{e}}} a_{[F]} = I_{\mathbf{e}}. \tag{11}$$

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 $\langle \mathbf{e}, F\rangle = 0$ par la formule (6). 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 $\mathbf{T} \to \prod_{[F]\in\mathcal{E}_{\mathbf{e}}} \mathbf{T}/a_{[F]}$ 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 à $\prod_{[F]\in\mathcal{E}_{\mathbf{e}}} K_F$. 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. □

On traduit alors l'indépendance linéaire du théorème 7.10 en le résultat annoncé de non-annulation de fonctions L.

Preuve du théorème 1.3. Le $\mathbf{Z}$-module $\mathbf{Te}$ est de rang $\#\{F \in \mathcal{F} \mid L(F,1) \neq 0\}$ par le lemme 7.12. Par ailleurs, d'après le théorème 7.10, il est de rang au moins égal au nombre de polynômes unitaires de A de degré $\leq r$ c'est-à-dire $\frac{q^{r+1}-1}{q-1}$. Enfin, la formule (2) pour $\#\mathcal{F} = g$ donne les inégalités $\frac{q^{r+1}-1}{q-1} \geq q^r \geq (q^2-1)^{1/2} g^{1/2}/q^2$. □

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

On travaille encore dans $\mathbf{M}_{\mathfrak{p}}$ avec $\mathfrak{p}$ premier. La définition suivante pourra être comparée à celles de Mazur [18] et Pál [25, rem. 5.7].

Définition 8.1. L'*homomorphisme d'enroulement* est l'homomorphisme de $\mathbf{T}$-modules

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

D'après le lemme 7.2, il est bien défini et l'involution $w_{\mathfrak{p}}$ opère par -1 sur son image car $w_{\mathfrak{p}}\,[0,\infty] = [\infty, 0]$

8.1 Homomorphisme d'enroulement en degré 3

Si $\mathfrak{p}$ est de degré 3, cet homomorphisme conjointement à la base explicite permet de décrire la structure du $\mathbf{T}$-module des symboles modulaires paraboliques. L'énoncé qui suit peut être rapproché de [18, th. 18.10] pour l'homomorphisme d'enroulement classique localisé en un nombre premier d'Eisenstein.

Proposition 8.2. *Soit $\mathfrak{p}$ premier de degré 3. Les symboles modulaires $\eta_{\mathfrak{n}}\mathbf{e}/(q-1)$, pour $\deg \mathfrak{n} = 1$, forment une base de $\mathbf{M}^0_{\mathfrak{p}}$ sur $\mathbf{Z}$. L'homomorphisme d'enroulement est un isomorphisme de $\mathbf{T}$-modules $I_E \simeq \mathbf{M}^0_{\mathfrak{p}}$.*

Démonstration. Comme $\mathfrak{p}$ est premier de degré impair, la torsion de $\mathbf{M}_\mathfrak{p}$ est nulle. L'homomorphisme d'enroulement est donc à valeurs dans $\overline{\mathbf{M}_\mathfrak{p}^0} = \mathbf{M}_\mathfrak{p}^0$ et le lemme 7.2 assure que $\eta_\mathfrak{n}\mathbf{e} = \eta_\mathfrak{n}[0,\infty]$ dans $\mathbf{M}_\mathfrak{p}^0$. Soit n le polynôme unitaire de degré 1 engendrant $\mathfrak{n}$. La preuve du lemme 7.2 donne $\eta_\mathfrak{n}[0,\infty] = -(q-1)\xi(n:1)$. De la base du théorème 1.1 on déduit alors la première affirmation de l'énoncé. L'homomorphisme d'enroulement, dont l'image contient une base de $\mathbf{M}_\mathfrak{p}^0$ sur $\mathbf{Z}$, est donc surjectif. Pour l'injectivité, il reste à voir que $I_\mathbf{e} \cap I_E = \{0\}$. En fait, l'idéal $I_\mathbf{e}$ est nul pour $\mathfrak{p}$ premier de degré 3. En effet, si F est primitive, la fonction $L(F,s)$ est alors un polynôme non nul en q^{-s} de degré ≤ 0, donc une constante non nulle (cf. proposition 3.1). D'après la description donnée en (11), l'idéal $I_\mathbf{e}$ est alors l'intersection de tous les idéaux premiers minimaux de $\mathbf{T}$, donc nul. □

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

Démonstration. Les deux modules sont isomorphes : cela provient de l'isomorphisme de $\mathbf{T}$-modules $\alpha : \mathbf{M}_\mathfrak{p}^0 \xrightarrow{\simeq} \mathbf{H}_\mathfrak{p}$. De plus, par la proposition 8.2, ils sont aussi isomorphes à I_E/pI_E.

Calculons le rang de I_E/pI_E sur $\mathbf{T}/p\mathbf{T}$. Le groupe $\mathbf{T}/I_E$ est fini d'ordre premier à p, d'après Pál (théorème 7.4). On en déduit $p\mathbf{T} + I_E = \mathbf{T}$. En effet, si ce n'est pas le cas, d'après le théorème de Krull, I_E et $p\mathbf{T}$ sont 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 contradictoire. Les idéaux $p\mathbf{T}$ et I_E étant étrangers, l'inclusion $I_E \hookrightarrow \mathbf{T}$ induit une surjection de $\mathbf{T}/p\mathbf{T}$-modules $I_E/pI_E \to \mathbf{T}/p\mathbf{T}$. On propose de voir que $I_E \cap p\mathbf{T} = pI_E$, ce qui prouvera que cette surjection est bijective (et I_E/pI_E sera alors de rang 1). Considérons un élément $x = pt$ de $I_E \cap p\mathbf{T}$, avec t dans $\mathbf{T}$. Comme x est d'image nulle dans $\mathbf{T}/I_E$, l'image de t est d'ordre 1 ou p dans ce quotient. Or, le groupe abélien $\mathbf{T}/I_E$ est d'ordre premier à p. Donc t appartient nécessairement à I_E. Cela démontre $I_E \cap p\mathbf{T} \subset pI_E$. L'autre inclusion est immédiate et conclut la démonstration. □

8.2 En degré supérieur

On peut voir que l'homomorphisme d'enroulement n'est plus surjectif dès que $d = \deg \mathfrak{p} \geq 4$. En effet notons V son image, qui est toujours contenue dans le sous-espace propre de $w_{\mathfrak{p}|\overline{\mathbf{M}_\mathfrak{p}^0}}$ pour la valeur propre -1. Si $V = \overline{\mathbf{M}_\mathfrak{p}^0}$ alors l'involution $w_\mathfrak{p}$ agit comme -1 sur $\overline{\mathbf{M}_\mathfrak{p}^0}$, donc sur $\mathbf{H}_\mathfrak{p}$ (lemme 4.4). Soit w l'involution d'Atkin–Lehner de la courbe modulaire de Drinfeld X associée à $\Gamma_0(\mathfrak{p})$ (cf. [6]). Elle induit un automorphisme de la jacobienne de X, défini sur K, qui serait alors $-\mathrm{id}$. La courbe X serait hyperelliptique. Mais d'après la classification de Schweizer [27, th. 20], cela ne se produit pas si $d \geq 4$.

Pour $d \geq 3$, on sait que la famille de symboles modulaires $\xi(n:1)$, pour n unitaire de degré 1, est libre (théorème 5.16). Comme dans la preuve de la proposition 8.2, on en déduit que $\mathbf{Q} \cdot V$ est toujours de dimension $\geq q$. On termine par un exemple pour $d = 4$ où cette minoration est optimale.

Exemple 8.4 ($q = 2$, $\mathfrak{p} = (T^4 + T + 1)$ idéal premier)**.** Dans la base suivante de $\mathbf{M}_\mathfrak{p}^0(\mathbf{Q})$

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

la matrice de $w_{\mathfrak{p}}$ 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 $w_{\mathfrak{p}}$ pour la valeur propre -1 est de dimension 2 et $\dim_{\mathbf{Q}} \mathbf{Q} \cdot V = 2$.

Remerciements Ce travail s'est développé à partir de ma thèse de doctorat préparée à l'Université Paris 7. Il a été complété lors de séjours à l'Institut des Hautes Études Scientifiques et au Max-Planck-Institut für Mathematik, que je remercie pour leur hospitalité. Je suis très reconnaissante à Loïc Merel pour ses remarques et un argument crucial dans la section 5. Enfin le rapporteur, par sa relecture minutieuse et ses nombreux commentaires, a sensiblement amélioré la présentation de ce travail : qu'il en soit chaleureusement remercié.

Références

[1] *C. Armana*, Torsion des modules de Drinfeld de rang 2 et formes modulaires de Drinfeld, Algebra Number Theory **6-6** (2012), 1239–1288.

[2] *J. Cremona*, Algorithms for modular elliptic curves, 2ème éd., Cambridge University Press, Cambridge 1997.

[3] *V. Drinfel'd*, Elliptic modules, Mat. Sb. (N.S.) **94(136)** (1974), 594–627, 656.

[4] *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.

[5] *E.–U. Gekeler*, Automorphe Formen über $\mathbf{F}_q(T)$ mit kleinem Führer, Abh. Math. Sem. Univ. Hamburg **55** (1985), 111–146.

[6] *E.–U. Gekeler*, Über Drinfeldsche Modulkurven vom Hecke-Typ, Compositio Math. **57** (1986), no. 2, 219–236.

[7] *E.–U. Gekeler*, Analytical construction of Weil curves over function fields, J. Théor. Nombres Bordeaux **7** (1995), no. 1, 27–49.

[8] *E.–U. Gekeler*, Improper Eisenstein series on Bruhat-Tits trees, Manuscripta Math. **86** (1995), no. 3, 367–391.

[9] *E.–U. Gekeler*, On the cuspidal divisor class group of a Drinfeld modular curve, Doc. Math. **2** (1997), 351–374.

[10] *E.–U. Gekeler*, Invariants of some algebraic curves related to Drinfeld modular curves, J. Number Theory **90** (2001), no. 1, 166–183.

[11] *E.–U. Gekeler* et *U. Nonnengardt*, Fundamental domains of some arithmetic groups over function fields, Internat. J. Math. **6** (1995), no. 5, 689–708.

[12] *E.–U. Gekeler* et *M. Reversat*, Jacobians of Drinfeld modular curves, J. Reine Angew. Math. **476** (1996), 27–93.

[13] *H. Hauer* et *I. Longhi*, Teitelbaum's exceptional zero conjecture in the function field case, J. Reine Angew. Math. **591** (2006), 149–175.

[14] *H. Iwaniec* et *P. Sarnak*, The non-vanishing of central values of automorphic L-functions and Landau-Siegel zeros, Israel J. Math. **120** (2000), no. part A, 155–177.

[15] *E. Kowalski* et *Ph. Michel*, The analytic rank of $J_0(q)$ and zeros of automorphic L-functions, Duke Math. J. **100** (1999), no. 3, 503–542.

[16] *Yu. Manin*, Parabolic points and zeta functions of modular curves, Izv. Akad. Nauk SSSR Ser. Mat. **36** (1972), 19–66.

[17] *B. Mazur*, Courbes elliptiques et symboles modulaires, Séminaire Bourbaki, 24ème année (1971/1972), Exp. No. 414, Lecture Notes in Math. **317**, Springer, Berlin, 1973, pp. 277–294.

[18] *B. Mazur*, Modular curves and the Eisenstein ideal, Inst. Hautes Études Sci. Publ. Math. (1977), no. 47, 33–186 (1978).

[19] *L. Merel*, Opérateurs de Hecke pour $\Gamma_0(N)$ et fractions continues, Ann. Inst. Fourier (Grenoble) **41** (1991), no. 3, 519–537.

[20] *L. Merel*, Universal Fourier expansions of modular forms, On Artin's conjecture for odd 2-dimensional representations, *Lecture Notes in Math.* **1585**, Springer, Berlin, 1994, pp. 59–94.

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

[22] *U. Nonnengardt*, Arithmetisch definierte graphen über rationalen funktionenkörpern, Diplomarbeit, Universität des Saarlandes, 1994.

[23] *A. Pál*, On the torsion of the Mordell-Weil group of the Jacobian of Drinfeld modular curves, Doc. Math. **10** (2005), 131–198.

[24] *A. Pál*, Proof of an exceptional zero conjecture for elliptic curves over function fields, Math. Z. **254** (2006), no. 3, 461–483.

[25] *A. Pál*, On the Eisenstein ideal of Drinfeld modular curves, Int. J. Number Theory **3** (2007), no. 4, 557–598.

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

[27] *A. Schweizer*, Hyperelliptic Drinfeld modular curves, in : Drinfeld modules, modular schemes and applications (Alden-Biesen, 1996), World Sci. Publ., River Edge, NJ, 1997, pp. 330–343.

[28] *J.–P. Serre*, Arbres, amalgames, SL_2, Astérisque **46**, 1977.

[29] *W. Stein*, Modular forms, a computational approach, Graduate Studies in Mathematics **79** (2007), American Mathematical Society, Providence, RI.

[30] *A. Tamagawa*, The Eisenstein quotient of the Jacobian variety of a Drinfel'd modular curve, Publ. Res. Inst. Math. Sci. **31** (1995), no. 2, 203–246.

[31] *K.–S. Tan*, Modular elements over function fields, J. Number Theory **45** (1993), no. 3, 295–311.

[32] *J. Teitelbaum*, Modular symbols for $\mathbf{F}_q(T)$, Duke Math. J. **68** (1992), no. 2, 271–295.

[33] *K.–S. Tan* et *D. Rockmore*, Computation of L-series for elliptic curves over function fields, J. Reine Angew. Math. **424** (1992), 107–135.

[34] *J. VanderKam*, Linear independence of Hecke operators in the homology of $X_0(N)$, J. London Math. Soc. (2) **61** (2000), no. 2, 349–358.

[35] *A. Weil*, Dirichlet series and automorphic forms, Lecture Notes in Mathematics **189**, Springer-Verlag, Berlin, 1971.