Module supersingulier et homologie des courbes modulaires

Marusia Rebolledo *

Résumé

Nous étudions ici le groupe libre engendré par les classes d'isomorphisme de courbes elliptiques supersingulières en caractéristique non nulle. Nous comparons ce $\mathbb{Z}$-module appelé *module supersingulier* à un autre module de Hecke : l'homologie de la courbe modulaire $X_0(p)$. Nous donnons une interprétation de la formule de Gross pour les valeurs spéciales des fonctions L de formes modulaires dans ce contexte. Nous obtenons en application une formule pour la somme des carrés des nombres de plongements optimaux des ordres quadratiques dans une algèbre de quaternions définie.

We study here the free group generated by isomorphism classes of supersingular elliptic curves in positive characteristic. We compare this $\mathbb{Z}$-module called *supersingular module* to another one : the homology of the modular curve $X_0(p)$. We give an interpretation of Gross formula for special values of L-functions of modular forms in this context. As an application, we obtain a formula for the sum of the squares of the optimal embeddings numbers of quadratic orders in a definite quaternion algebra.

Introduction

Soient $p > 3$ un nombre premier et $\bar{\mathbb{F}}_p$ une clôture algébrique de $\mathbb{F}_p$. L'ensemble $\mathcal{S}$ des classes d'isomorphismes de courbes elliptiques supersingulières sur $\bar{\mathbb{F}}_p$ est fini : on le note $\mathcal{S} = \{x_0, \ldots, x_g\}$. Nous appelons *module supersingulier* le $\mathbb{Z}$-module libre engendré par $\mathcal{S}$, c'est-à-dire

$$\mathcal{P} = \mathbb{Z}[\mathcal{S}] = \oplus_{i=0}^{g} \mathbb{Z}.x_i.$$

*L'auteur est accueilli comme chercheur post-doctorant à l'Université de Milan : Dip. di Matematica, Università degli Studi di Milano, via C. Saldini 50, 20133 Milano, Italia *mel : rebolledo@mat.unimi.it* *Mathematics Subject Classification (2004) :* 11F67, 11G, 11R52 *Mots clefs* : courbes elliptiques, symboles modulaires, fonctions L.

Soit $\mathcal{P}^0$ le sous-groupe de $\mathcal{P}$ constitué des éléments de degré nul. On munit $\mathcal{P}$ de l'accouplement bilinéaire non dégénéré $\langle\ ,\ \rangle : \mathcal{P} \times \mathcal{P} \longrightarrow \mathbb{Z}$ défini par

$$\langle x_i, x_j \rangle = w_i \delta_{i,j} \qquad (0 \leq i, j \leq g)$$

où $\delta_{i,j}$ est le symbole de Kronecker et $w_i = |\mathrm{Aut}(E_i)|/2$ ($E_i \in x_i,\ 0 \leq i \leq g$).

Soient $X_0(p)$ la courbe modulaire sur $\mathbb{Q}$ classifiant les courbes elliptiques généralisées munies d'un sous-groupe d'ordre p et $J_0(p)$ sa jacobienne (voir par exemple [1]). Soit $\mathbb{T} \subset \mathrm{End}(J_0(p))$ le sous-anneau engendré par les endomorphismes T_m ($m \geq 1$) de $J_0(p)$ déduits des correspondances de Hecke sur $X_0(p)$ par fonctorialité de Picard. Les réalisations géométriques de $\mathcal{P}$ et $\mathcal{P}^0$ rappelées en 3.1 confèrent à $\mathcal{P}^0$ une structure de $\mathbb{T}$-module fidèle. Les opérateurs T_m ($m \geq 1$) sur $\mathcal{P}^0$ sont autoadjoints pour l'accouplement $\langle\ ,\ \rangle$.

Soit $\mathcal{H} = H_1(X, \mathbb{Z})$ le premier groupe d'homologie singulière absolue de la surface de Riemann $X = X_0(p)(\mathbb{C})$. Notons $\mathbf{c}$ l'involution sur $\mathcal{H}$ déduite de la conjugaison complexe sur $X_0(p)$ et $\mathcal{H}^+$ (resp. $\mathcal{H}^-$) le sous-groupe de $\mathcal{H}$ invariant (resp. anti-invariant) sous l'action de $\mathbf{c}$. Les correspondances de Hecke sur $X_0(p)$ définissent une action de $\mathbb{T}$ sur $\mathcal{H}$ qui commute avec $\mathbf{c}$ et laisse donc stables $\mathcal{H}^+$ et $\mathcal{H}^-$ (voir le paragraphe 2.3). Les opérateurs T_m ($m \geq 1$) sont autoadjoints pour l'accouplement $\bullet : \mathcal{H}^+ \times \mathcal{H}^- \longrightarrow \mathbb{Z}$ défini par le produit d'intersection.

Enfin, notons $\mathrm{S}_2(\Gamma_0(p))$ l'ensemble des formes paraboliques de poids 2 pour $\Gamma_0(p)$ et $\mathcal{M}^0$ le $\mathbb{Z}$-module constitué des éléments de $\mathrm{S}_2(\Gamma_0(p))$ dont le développement de Fourier à l'infini est à coefficients entiers. Les correspondances de Hecke sur $X_0(p)$ déterminent une action fidèle de $\mathbb{T}$ sur $\mathrm{S}_2(\Gamma_0(p))$ qui laisse stable $\mathcal{M}^0$ et les opérateurs $T_m, m \geq 1$ sont autoadjoints pour le produit scalaire de Petersson $(\ ,\ )$. Signalons également qu'il y a un isomorphisme canonique de $\mathbb{T}$-modules entre $\mathcal{M}^0$ et $\mathrm{Hom}(\mathbb{T}, \mathbb{Z})$ (voir le paragraphe 1).

Pour A un anneau et M un $\mathbb{Z}$-module, notons $M_A = M \otimes A$. Les $\mathbb{T}_\mathbb{Q}$-modules $\mathcal{M}^0_\mathbb{Q}$, $\mathcal{P}^0_\mathbb{Q}$, $\mathcal{H}^+_\mathbb{Q}$ et $\mathcal{H}^-_\mathbb{Q}$ sont libres de rang 1. Soit $\bar{\mathbb{Q}}$ une clôture algébrique de $\mathbb{Q}$. Les $\bar{\mathbb{Q}}$-droites propres sous l'action de $\mathbb{T}$ sont en correspondance bijective, cependant il n'existe pas d'isomorphisme explicite. La théorie de Manin [8], rappelée en 2.1, donne une présentation de l'homologie $\mathcal{H}$ par générateurs et relations. En dépit des descriptions explicites de $\mathcal{P}$ et $\mathcal{H}$, aucun isomorphisme général n'a, à notre connaissance, été exhibé entre $\mathcal{P}^0_\mathbb{Q}$ d'une part, et $\mathcal{H}^+_\mathbb{Q}$ ou $\mathcal{H}^-_\mathbb{Q}$ d'autre part. L'algèbre $\mathbb{T}$ agit par dualité sur $\check{\mathcal{P}}^0 = \mathrm{Hom}(\mathcal{P}^0, \mathbb{Z})$. Nous comparons ici les $\mathbb{T}$-modules $\mathcal{P}^0 \otimes_\mathbb{T} \check{\mathcal{P}}^0$ et $\mathcal{H}^+ \otimes_\mathbb{T} \mathcal{H}^-$.

L'accouplement $\langle\ ,\ \rangle$ restreint à $\mathcal{P}^0 \times \mathcal{P}^0$ définit un homomorphisme injectif de $\mathbb{T}$-modules de $\mathcal{P}^0$ dans $\check{\mathcal{P}}^0$ et identifie $\check{\mathcal{P}}^0$ à un sous-$\mathbb{T}$-module de $\mathcal{P}^0_\mathbb{Q}$. L'accouplement canonique $\mathcal{P}^0 \times \check{\mathcal{P}}^0 \longrightarrow \mathbb{Z}$ étend donc l'accouplement $\langle\ ,\ \rangle$ et sera encore noté $\langle\ ,\ \rangle$. Soient

$$\theta^0 : \mathcal{P}^0 \otimes_{\mathbb{T}} \check{\mathcal{P}}^0 \longrightarrow \mathrm{Hom}(\mathbb{T}, \mathbb{Z}) \cong \mathcal{M}^0 \quad \text{et} \quad \psi : \mathcal{H}^+ \otimes_{\mathbb{T}} \mathcal{H}^- \longrightarrow \mathrm{Hom}(\mathbb{T}, \mathbb{Z}) \cong \mathcal{M}^0$$

les homomorphismes de $\mathbb{T}$-modules qui se déduisent des accouplements bilinéaires.

Pour M et N deux $\mathbb{Z}$-modules, $a > 0$ un entier et $f : M \longrightarrow N$ un homomorphisme de $\mathbb{Z}$-modules, notons $M\big[\frac{1}{a}\big] = M \otimes \mathbb{Z}\big[\frac{1}{a}\big]$ et $f\big[\frac{1}{a}\big] = f \otimes 1 : M\big[\frac{1}{a}\big] \longrightarrow N\big[\frac{1}{a}\big]$ l'homomorphisme obtenu par extension des scalaires à $\mathbb{Z}\left[\frac{1}{a}\right]$. Emerton [2] a montré que $\theta^0\left[\frac{1}{2}\right]$ est un isomorphisme de $\mathbb{T}\left[\frac{1}{2}\right]$-modules. Les résultats de Mazur [9] nous permettent de montrer au paragraphe 4.3 que $\psi\left[\frac{1}{2}\right]$ l'est également. En particulier, après extension des scalaires à $\mathbb{Q}$, nous obtenons des isomorphismes de $\mathbb{T}_{\mathbb{Q}}$-modules libres de rang 1 dont nous décrivons ci-après des générateurs respectifs.

Soit $a_E = \sum_{i=0}^{g} \frac{x_i}{w_i} \in \mathcal{P}_{\mathbb{Q}}$ l'*élément d'Eisenstein* (voir 4.1). L'élément

$$\Delta_2^0 = \sum_{i=0}^{g} \frac{1}{w_i}\, x_i \otimes_{\mathbb{Q}} x_i - \frac{12}{p-1}\, a_E \otimes_{\mathbb{Q}} a_E$$

est alors dans $\mathcal{P}_{\mathbb{Q}}^0 \otimes_{\mathbb{Q}} \mathcal{P}_{\mathbb{Q}}^0$. Notons $\bar{\Delta}_2^0$ son image par la surjection canonique $\mathcal{P}_{\mathbb{Q}}^0 \otimes_{\mathbb{Q}} \mathcal{P}_{\mathbb{Q}}^0 \twoheadrightarrow \mathcal{P}_{\mathbb{Q}}^0 \otimes_{\mathbb{T}_{\mathbb{Q}}} \mathcal{P}_{\mathbb{Q}}^0$.

Notons $\mathfrak{H}$ le demi-plan de Poincaré et $\bar{\mathfrak{H}} = \mathfrak{H} \cup \mathbb{P}^1(\mathbb{Q})$. La surface de Riemann X s'identifie à $\Gamma_0(p)\backslash\bar{\mathfrak{H}}$. Pour x un entier premier à p, la classe d'homologie $\{0, 1/x\}$ de l'image dans X d'une géodésique de $\bar{\mathfrak{H}}$ d'origine 0 et d'extrémité $1/x$ ne dépend que de la classe de x modulo p et définit un élément de $\mathcal{H}$ que l'on notera $\xi^0(x)$ (voir la section 2.1). Considérons l'élément de $\mathcal{H}_{\mathbb{Q}} \otimes_{\mathbb{T}_{\mathbb{Q}}} \mathcal{H}_{\mathbb{Q}}$ suivant :

$$\bar{\Lambda}_2 = \frac{1}{6} \sum_{x \in \mathbb{F}_p^* \backslash \{1\}} \left(\xi^0\left(\frac{1}{1-x}\right) \otimes_{\mathbb{T}_{\mathbb{Q}}} \xi^0(x) - \xi^0(x) \otimes_{\mathbb{T}_{\mathbb{Q}}} \xi^0\left(\frac{1}{1-x}\right)\right).$$

Notons $\bar{\Lambda}_2^0$ son image par l'homomorphisme canonique de $\mathbb{T}_{\mathbb{Q}}$-modules

$$\frac{1}{4}(1+\mathbf{c}) \otimes_{\mathbb{T}_{\mathbb{Q}}} (1-\mathbf{c})\ :\ \mathcal{H}_{\mathbb{Q}} \otimes_{\mathbb{T}_{\mathbb{Q}}} \mathcal{H}_{\mathbb{Q}} \longrightarrow \mathcal{H}_{\mathbb{Q}}^+ \otimes_{\mathbb{T}_{\mathbb{Q}}} \mathcal{H}_{\mathbb{Q}}^-.$$

Théorème 1 *Les éléments $\bar{\Delta}_2^0$ et $\bar{\Lambda}_2^0$ sont des générateurs respectifs des $\mathbb{T}_{\mathbb{Q}}$-modules libres $\mathcal{P}_{\mathbb{Q}}^0 \otimes_{\mathbb{T}_{\mathbb{Q}}} \mathcal{P}_{\mathbb{Q}}^0$ et $\mathcal{H}_{\mathbb{Q}}^+ \otimes_{\mathbb{T}_{\mathbb{Q}}} \mathcal{H}_{\mathbb{Q}}^-$ et on a*

$$\theta_{\mathbb{Q}}^0(\bar{\Delta}_2^0) = \psi_{\mathbb{Q}}(\bar{\Lambda}_2^0).$$

Ces générateurs sont liés aux accouplements au sens de la proposition 3. Si ce fait est trivial pour $\bar{\Delta}_2^0$, cela l'est moins pour $\bar{\Lambda}_2^0$ et requiert un calcul (voir 2.2) faisant appel aux résultats fondamentaux de Manin [8] et Merel [10] rappelés en 2.1.

L'intérêt de la comparaison entre $\mathcal{P}$ et $\mathcal{H}$ réside en particulier dans le fait qu'on sait lire sur l'homologie les valeurs spéciales de fonctions L alors qu'on ne sait *a priori* pas le faire sur le module supersingulier.

Soient $-D < 0$ un discriminant quadratique imaginaire premier à p et ε_D le caractère non trivial de $\mathrm{Gal}(\mathbb{Q}(\sqrt{-D})/\mathbb{Q})$. Pour f une forme primitive de poids 2 pour $\Gamma_0(p)$, la forme parabolique $f \otimes \varepsilon_D$ est alors primitive de niveau pD^2. Notons e l'élément d'enroulement de Mazur (resp. e_D l'élément d'enroulement tordu par ε_D)(voir [9] p. 136 et le paragraphe 5.2 ci-dessous). C'est l'antécédent par l'isomorphisme $\mathbb{T}$-linéaire de $\mathbb{R}$-espaces vectoriels $\mathcal{H}_{\mathbb{R}} \xrightarrow{\sim} \mathrm{Hom}_{\mathbb{C}}(\mathrm{S}_2(\Gamma_0(p)), \mathbb{C})$ rappelé en 2.3.2, de la forme linéaire qui à une forme primitive f associe $-L(f,1)$ (resp. $i\sqrt{D}\ L(f \otimes \varepsilon_D, 1)$). On a en fait $e \in \mathcal{H}_{\mathbb{Q}}^+$ et $e_D \in \mathcal{H}_{\mathbb{Q}}^-$. La formule de Gross-Zhang nous permet de déterminer la *D-ième forme parabolique de Gross* $\mathbf{g}_D = \psi_{\mathbb{Q}}(e \otimes_{\mathbb{T}_{\mathbb{Q}}} e_D)$.

Notons $\mathcal{O}_{-D}$ l'ordre quadratique de discriminant $-D$ et $u(-D)$ l'ordre de $\mathcal{O}_{-D}^*/\langle \pm 1 \rangle$. Pour $i \in \{0, \ldots, g\}$, $R_i = \mathrm{End}(E_i)$ ($E_i \in x_i$) est un ordre maximal de l'algèbre de quaternions ramifiée en p et l'infini ; on note $h_i(-D)$ le nombre de plongements optimaux de $\mathcal{O}_{-D}$ dans R_i modulo conjugaison par R_i^*. Nous appelons *D-ième élément de Gross* l'élément[1]

$$\gamma_D = \frac{1}{2u(-D)} \sum_{i=0}^{g} h_i(-D) x_i \in \mathcal{P}_{\mathbb{Q}}. \tag{1}$$

Posons $\gamma_D^0 = \gamma_D - \frac{12}{p-1} \deg(\gamma_D) a_E \in \mathcal{P}_{\mathbb{Q}}^0$. Nous obtenons comme corollaire de la formule de Gross-Zhang [4, 20] le théorème suivant démontré en 5.2

Théorème 2 *On a dans $\mathcal{M}_{\mathbb{Q}}^0$ l'égalité*

$$\theta_{\mathbb{Q}}^0(\gamma_D^0 \otimes_{\mathbb{T}_{\mathbb{Q}}} \gamma_D^0) = \psi_{\mathbb{Q}}(e \otimes_{\mathbb{T}_{\mathbb{Q}}} e_D).$$

En d'autres termes, la D-ième forme parabolique de Gross $\mathbf{g}_D$ a pour développement de Fourier à l'infini

$$\sum_{m \geq 1} \langle \gamma_D^0, T_m \gamma_D^0 \rangle\, q^m = \sum_{m \geq 1} e \bullet T_m e_D\, q^m \ ;$$

ou encore

$$\langle \gamma_D^0, t\gamma_D^0 \rangle = e \bullet t e_D \quad (t \in \mathbb{T}_{\mathbb{Q}}).$$

[1] Cet élément, introduit par Gross, est noté e_D dans [4]. Nous choisissons la notation γ_D dans le souci de ne pas confondre cet élément avec l'élément d'enroulement tordu.

Le calcul des coefficients du développement de Fourier de $\mathbf{g}_D$ conduit à des formules du même type que la formule d'Eichler (voir [4] (1.12))

$$\sum_{i=0}^{g} h_i(-D) = \left(1 - \left(\frac{-D}{p}\right)\right) h(-D).$$

En calculant le premier coefficient nous obtenons en 5.3 la formule énoncée ci-dessous. Soit $r > 0$ un entier premier à p. Notons $\mathrm{M}_2(\mathbb{Z})_r$ l'ensemble des matrices de taille 2×2 à coefficients entiers et de déterminant r, et

$$\mathcal{X}'_r = \{M = \left(\begin{smallmatrix} u & v \\ w & t \end{smallmatrix}\right) \in \mathrm{M}_2(\mathbb{Z})_r \,;\, u > v \geq 0,\ 0 \leq w < t, (w,t) = 1\}. \qquad (2)$$

Pour $M \in \mathcal{X}'_r$, notons b_M l'unique entier modulo r solution[2] du système

$$(S_r) \begin{cases} b_M & \equiv \frac{u}{(w,r)} \left(\frac{w}{(w,r)}\right)^{-1} \pmod{\frac{r}{(w,r)}} \\ b_M & \equiv \frac{v}{(t,r)} \left(\frac{t}{(t,r)}\right)^{-1} \pmod{\frac{r}{(t,r)}}. \end{cases} \qquad (3)$$

Pour u, v deux entiers premiers entre eux, $v > 0$, on note $S(u,v)$ leur somme de Dedekind.

Théorème 3 *On a*

$$\begin{aligned} \sum_{i=0}^{g} h_i(-D)^2 w_i &= 4u(-D)^2 \sum_{k=1}^{p-1} \sum_{\substack{M = \left(\begin{smallmatrix} u & v \\ w & t \end{smallmatrix}\right) \in \mathcal{X}'_D \\ w \equiv tk \mod p}} \varepsilon_D(b_M) \left(\frac{k_* - k}{p} - 12\frac{S(k,p)}{p-1}\right) \\ &\quad + \frac{48}{p-1} h(-D)^2, \end{aligned}$$

où, pour $k \in \{1, \ldots, p-1\}$, k_* désigne l'unique entier de $\{1, \ldots, p-1\}$ tel que $kk_* \equiv -1 \pmod{p}$.

Nous ne savons actuellement pas simplifier cette formule mais espérons que l'approche proposée en 5.3.4 pour le calcul de $e \bullet e_D$ conduira à une telle simplification.

[2]Notons $\delta = \left(\frac{r}{(w,r)}, \frac{r}{(t,r)}\right)$. On a $\delta = \frac{r}{(w,r)(t,r)}$ car $(w,t) = 1$. Comme, par hypothèse, $wv \equiv ut \pmod{r}$, on a l'égalité $\frac{u}{(w,r)} \left(\frac{w}{(w,r)}\right)^{-1} \equiv \frac{v}{(t,r)} \left(\frac{t}{(t,r)}\right)^{-1} \pmod{\delta}$. Ceci prouve que (S_r) a une solution modulo r. Cette solution est unique car le plus petit commun multiple de $\frac{r}{(w,r)}$ et $\frac{r}{(t,r)}$ est égal à r.

Structure de l'article. Nous faisons dans les trois premiers paragraphes, quelques rappels succincts qui n'ont pas la prétention d'être exhaustifs mais permettent de fixer les notations et résultats utilisés par la suite. Les résultats énoncés dans l'introduction sont démontrés dans les paragraphes 4 et 5.

Notations. Outre les notations indiquées au cours du texte, on désignera par n le numérateur et par δ le dénominateur de $(p-1)/12$. Pour $m \geq 1$ un entier, on note $\sigma'(m)$ la somme des diviseurs de m premiers à p.

Remerciements. Je remercie chaleureusement L. Merel d'avoir guidé mes recherches pendant ma thèse et de m'avoir fait part de précieux commentaires lors de la rédaction de cet article.

1 Formes modulaires et algèbre de Hecke

Soit $\widetilde{\mathbb{T}}$ l'algèbre engendrée par l'action classique des opérateurs de Hecke sur le $\mathbb{C}$-espace vectoriel $\mathrm{M}_2(\Gamma_0(p))$ des formes modulaires de poids 2 pour $\Gamma_0(p)$ (voir par exemple [14] 4.5). L'action de $\widetilde{\mathbb{T}}$ sur $\mathrm{M}_2(\Gamma_0(p))$ est fidèle et laisse stable le sous-espace $\mathrm{S}_2(\Gamma_0(p))$ des formes paraboliques. L'algèbre $\mathbb{T}$ définie dans l'introduction, vue comme sous-anneau de $\mathrm{End}(\mathrm{S}_2(\Gamma_0(p)))$, est le quotient de $\widetilde{\mathbb{T}}$ qui agit fidèlement sur $\mathrm{S}_2(\Gamma_0(p))$. Par abus de notation, on désigne de la même façon un opérateur de Hecke dans $\widetilde{\mathbb{T}}$ ou son image dans le quotient $\mathbb{T}$ de $\widetilde{\mathbb{T}}$. Les opérateurs T_m ($m \geq 1$) sont caractérisés par les relations classiques (voir [14] théorème 4.5.13). Remarquons que l'opérateur T_p agit sur $\mathrm{M}_2(\Gamma_0(p))$ comme $-w_p$ où w_p est l'opérateur d'Atkin-Lehner[3] sur $X_0(p)$.

Notons $\sum_{m\geq 0} a_m(f)q^m$ le développement de Fourier à l'infini d'un élément $f \in \mathrm{M}_2(\Gamma_0(p))$. Considérons le $\mathbb{Z}$-module $\mathcal{M}$ (resp. $\mathcal{N}$) des formes modulaires $f \in \mathrm{M}_2(\Gamma_0(p))$ telles que $a_0(f) \in \frac{1}{2}\mathbb{Z}$ et $a_m(f) \in \mathbb{Z}$ pour $m \geq 1$ (resp. $a_0(f) \in \mathbb{Q}$ et $a_m(f) \in \mathbb{Z}$ pour $m \geq 1$). Le groupe $\mathcal{M}^0$ est alors le sous-$\mathbb{Z}$-module des formes paraboliques dans $\mathcal{M}$ ou $\mathcal{N}$ indifféremment.

L'action de $\widetilde{\mathbb{T}}$ sur $\mathrm{M}_2(\Gamma_0(p))$ laisse stables $\mathcal{M}$, $\mathcal{N}$ et $\mathcal{M}^0$. L'action de $\widetilde{\mathbb{T}}$ sur $\mathcal{M}$ est fidèle et l'action de $\widetilde{\mathbb{T}}$ sur $\mathcal{M}^0$ se factorise par $\mathbb{T}$. L'accouplement défini par $\langle f, T\rangle = a_1(f \mid T)$ induit un isomorphisme de $\widetilde{\mathbb{T}}$-modules (resp. de $\mathbb{T}$-modules)

$$\mathcal{N} \xrightarrow{\sim} \mathrm{Hom}(\widetilde{\mathbb{T}}, \mathbb{Z}) \quad (\text{resp. } \mathcal{M}^0 \xrightarrow{\sim} \mathrm{Hom}(\mathbb{T}, \mathbb{Z}))$$

[3] Un calcul élémentaire montre en effet que, pour $f \in \mathrm{M}_2(\Gamma_0(p))$, on a $f|_{T_p w} = \mathrm{Tr}\ f - f$, où $\mathrm{Tr}\ f$ est la trace de f pour l'action de $\Gamma_0(p)\backslash\mathrm{SL}_2(\mathbb{Z})$. Or $\mathrm{Tr}\ f$ est une forme modulaire de poids 2 pour $\mathrm{SL}_2(\mathbb{Z})$ donc est nulle.

(voir par exemple [2] proposition 1.3). Le conoyau de l'homomorphisme injectif de $\widetilde{\mathbb{T}}$-modules $\mathcal{M} \hookrightarrow \mathcal{N}$ est isomorphe à $\mathbb{Z}/\delta\mathbb{Z}$ (*loc. cit.* proposition 1.1).

Notons $\omega_f = 2i\pi f(z)dz$ la forme différentielle sur $X_0(p)$ associée à une forme modulaire f. Conformément à la convention adoptée par Gross [4], on normalise le produit scalaire de Petersson d'une forme parabolique f et d'une forme modulaire g de la façon suivante

$$(f,g) = \iint_X \omega_f \wedge i\,\overline{\omega}_g = 8\pi^2 \iint_{\Gamma_0(p)\backslash\mathfrak{H}} f(z)\overline{g(z)}dxdy. \tag{4}$$

Les opérateurs de Hecke sont autoadjoints pour (,).

2 Homologie des courbes modulaires

Soient $Y_0(p)$ l'ouvert affine de $X_0(p)$, $Y = Y_0(p)(\mathbb{C}) = \Gamma_0(p)\backslash\mathfrak{H}$ la surface de Riemann associée et $J = J_0(p)(\mathbb{C})$ la jacobienne de $X = X_0(p)(\mathbb{C})$. Notons $\varpi : \mathfrak{H} \cup \mathbb{P}^1(\mathbb{Q}) \twoheadrightarrow X$ la surjection canonique et $\mathrm{ptes} = \varpi(\mathbb{P}^1(\mathbb{Q}))$ l'ensemble des pointes de X.

2.1 La théorie de Manin

Reprenons les notations de [10] : soient $\mathcal{H}^{\mathrm{ptes}} = H_1(X, \mathrm{ptes}\,; \mathbb{Z})$, $\mathcal{H}_{\mathrm{ptes}} = H_1(Y\,; \mathbb{Z})$ et $\mathcal{H} = H_1(X\,; \mathbb{Z})$. On a une injection et une surjection canoniques

$$\alpha^{\mathrm{ptes}} : \mathcal{H} \hookrightarrow \mathcal{H}^{\mathrm{ptes}} \quad \text{et} \quad \alpha_{\mathrm{ptes}} : \mathcal{H}_{\mathrm{ptes}} \twoheadrightarrow \mathcal{H}.$$

Les produits d'intersection définissent des accouplements parfaits

$$\mathcal{H}^{\mathrm{ptes}} \times \mathcal{H}_{\mathrm{ptes}} \longrightarrow \mathbb{Z} \quad \text{et} \quad \mathcal{H} \times \mathcal{H} \longrightarrow \mathbb{Z}$$

que nous noterons tous deux $\bullet$. Ces accouplements sont compatibles à α_{ptes} et α^{ptes} *i.e.* on a

$$\alpha^{\mathrm{ptes}}(x) \bullet y = x \bullet \alpha_{\mathrm{ptes}}(y) \quad (y \in \mathcal{H}_{\mathrm{ptes}},\ x \in \mathcal{H}).$$

De plus, l'accouplement $\bullet : \mathcal{H} \times \mathcal{H} \longrightarrow \mathbb{Z}$ est antisymétrique.

Désormais, nous identifierons $\mathcal{H}$ à son image par α^{ptes} dans $\mathcal{H}^{\mathrm{ptes}}$.

Pour x et y dans $\mathbb{P}^1(\mathbb{Q})$, notons $\{x, y\}$ la classe dans $\mathcal{H}^{\mathrm{ptes}}$ de l'image dans X d'un chemin géodésique de x à y dans $\bar{\mathfrak{H}}$. Le groupe $\mathcal{H}$, identifié à un sous-groupe de $\mathcal{H}^{\mathrm{ptes}}$, est le noyau de l'application *bord* β définie par

$$\begin{array}{rccl} \beta\ : & \mathcal{H}^{\mathrm{ptes}} & \longrightarrow & \mathbb{Z}[\mathrm{ptes}] \\ & \{x,y\} & \longmapsto & (\Gamma_0(p).y) - (\Gamma_0(p).x). \end{array}$$

Soit $g \in \mathrm{SL}_2(\mathbb{Z})$. La classe $\{g0, g\infty\} \in \mathcal{H}^{\mathrm{ptes}}$ ne dépend que de la classe de g dans $\Gamma_0(p)\backslash\mathrm{SL}_2(\mathbb{Z})$. On définit alors l'application

$$\begin{array}{rcrcl} \xi^0 & : & \mathbb{Z}[\Gamma_0(p)\backslash\mathrm{SL}_2(\mathbb{Z})] & \longrightarrow & \mathcal{H}^{\mathrm{ptes}} \\ & & \Gamma_0(p).g & \longmapsto & \{g0, g\infty\}. \end{array}$$

Nous noterons indifféremment $\Gamma_0(p)g$ ou g pour désigner la classe de l'élément g de $\mathrm{SL}_2(\mathbb{Z})$ modulo $\Gamma_0(p)$, le contexte suffisant à distinguer un élément de sa classe modulo $\Gamma_0(p)$.

Considérons les éléments de $\mathrm{SL}_2(\mathbb{Z})$ d'ordres respectifs 4 et 6

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

On note $\mathcal{E}_{\Gamma_0(p)}$ l'ensemble des éléments de $\mathbb{Z}[\Gamma_0(p)\backslash\mathrm{SL}_2(\mathbb{Z})]$ de la forme $\sum_g \lambda_g\, g$ avec, pour tout $g \in \Gamma_0(p)\backslash\mathrm{SL}_2(\mathbb{Z})$,

$$\lambda_g + \lambda_{g\sigma} = 0 \quad \text{et} \quad \lambda_g + \lambda_{g\tau} + \lambda_{g\tau^2} = 0.$$

Dans la suite, lorsque cela n'est pas précisé, les sommes portent sur $\Gamma_0(p)\backslash\mathrm{SL}_2(\mathbb{Z})$.

Posons $\rho = e^{2i\pi/3}$, $R = \varpi\,(\mathrm{SL}_2(\mathbb{Z})\rho)$ et $I = \varpi\,(\mathrm{SL}_2(\mathbb{Z})i)$. Pour tout $g \in \Gamma_0(p)\backslash\mathrm{SL}_2(\mathbb{Z})$, on note $[gi, g\rho]$ la classe dans $H_1(Y, R\cup I\,;\,\mathbb{Z})$ de l'image dans Y d'un chemin géodésique reliant gi à $g\rho$ dans $\mathfrak{H}$. Soit $x = \sum_g \lambda_g\, g \in \mathcal{E}_{\Gamma_0(p)}$. La classe

$$\sum_{g\in\Gamma_0(p)\backslash\mathrm{SL}_2(\mathbb{Z})} \lambda_g[gi, g\rho]$$

est un élément de $\mathcal{H}_{\mathrm{ptes}}$ vu comme un sous-groupe de $H_1(Y, R\cup I\,;\,\mathbb{Z})$ (voir [10]). Cela définit une application :

$$\begin{array}{rcrcl} \xi_0 & : & \mathcal{E}_{\Gamma_0(p)} & \longrightarrow & \mathcal{H}_{\mathrm{ptes}} \\ & & \sum_g \lambda_g g & \longmapsto & \sum_g \lambda_g[gi, g\rho]. \end{array}$$

Théorème 4 (Manin, Merel) *1. Pour $g \in \Gamma_0(p)\backslash\mathrm{SL}_2(\mathbb{Z})$ et $\sum_h \mu_h\, h \in \mathcal{E}_{\Gamma_0(p)}$, on a*

$$\xi^0(g) \bullet \xi_0\left(\sum \mu_h h\right) = \mu_g.$$

2. L'application ξ_0 est un isomorphisme de groupes.

3. L'application $\xi^0 = \mathbb{Z}[\Gamma_0(p)\backslash\mathrm{SL}_2(\mathbb{Z})] \longrightarrow \mathcal{H}^{\mathrm{ptes}}$ est surjective. Pour tout $g \in \Gamma_0(p)\backslash\mathrm{SL}_2(\mathbb{Z})$, on a les relations dites relations de Manin *:*

$$\xi^0(g) + \xi^0(g\sigma) = 0 \quad \textit{et} \quad \xi^0(g) + \xi^0(g\tau) + \xi^0(g\tau^2) = 0.$$

Démonstration. Voir [8] et [11]. $\square$

On rappelle que $\mathrm{SL}_2(\mathbb{Z})$ agit à droite sur $\mathbb{P}^1(\mathbb{F}_p)$: pour $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ et $[u:v] \in \mathbb{P}^1(\mathbb{F}_p)$, $[u:v]\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = [au+cv : bu+dv]$. Notons $\bar{c}$ la classe modulo p d'un entier c. L'application

$$\begin{array}{rccc} \iota \ : & \Gamma_0(p)\backslash\mathrm{SL}_2(\mathbb{Z}) & \longrightarrow & \mathbb{P}^1(\mathbb{F}_p) \\ & \Gamma_0(p).\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) & \longmapsto & [\bar{c}:\bar{d}] \end{array}$$

est un isomorphisme de groupes compatible avec l'action à droite de $\mathrm{SL}_2(\mathbb{Z})$ sur $\Gamma_0(p)\backslash\mathrm{SL}_2(\mathbb{Z})$ et $\mathbb{P}^1(\mathbb{F}_p)$. Notons encore ξ^0 l'homomorphisme de groupes de $\mathbb{Z}[\mathbb{P}^1(\mathbb{F}_p)]$ vers $\mathcal{H}^{\mathrm{ptes}}$ obtenu en composant ξ^0 et l'isomorphisme $\mathbb{Z}[\mathbb{P}^1(\mathbb{F}_p)] \xrightarrow{\sim} \mathbb{Z}[\Gamma_0(p)\backslash\mathrm{SL}_2(\mathbb{Z})]$ déduit de ι^{-1}. On a donc par définition

$$\xi^0([\bar{c}:\bar{d}]) = \left\{\frac{b}{d}, \frac{a}{c}\right\} \quad \text{où} \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

Passons à un système non homogène de coordonnées, c'est-à-dire notons $\infty = [1:0] \in \mathbb{P}^1(\mathbb{F}_p)$ et $c/d = [\bar{c}:\bar{d}] = [\bar{c}\bar{d}^{-1}:1]$ pour c et d deux entiers tels que $d \not\equiv 0 \pmod p$. Pour k un entier premier à p, en considérant la matrice $\left(\begin{smallmatrix} 1 & 0 \\ k & 1 \end{smallmatrix}\right)$, on obtient

$$\xi^0(k) = \left\{0, \frac{1}{k}\right\}$$

qui est un élément de $\mathcal{H}$. Par ailleurs, en considérant les matrices $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ et $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$, on obtient $\xi^0(0) = \{0,\infty\} = -\xi^0(\infty)$.

Les relations de Manin peuvent s'écrire ($x \in \mathbb{P}^1(\mathbb{F}_p)$)

$$\xi^0(x) + \xi^0\left(-\frac{1}{x}\right) = 0 \text{ et } \xi^0(x) + \xi^0\left(\frac{1}{1-x}\right) + \xi^0\left(1-\frac{1}{x}\right) = 0.$$

Remarquons que cela donne en particulier $\xi^0(1) = 0 = \xi^0(-1)$.

2.2 Calculs préliminaires

Considérons le morphisme de groupes $\alpha^{\mathrm{ptes}} \circ \alpha_{\mathrm{ptes}} : \mathcal{H}_{\mathrm{ptes}} \longrightarrow \mathcal{H}^{\mathrm{ptes}}$.

Théorème 5 *Pour tout $u = \sum_g \lambda_g g \in \mathcal{E}_{\Gamma_0(p)}$, on a*

$$\alpha^{\mathrm{ptes}} \circ \alpha_{\mathrm{ptes}}(\xi_0(u)) = \frac{1}{6} \sum_{g \in \Gamma_0(p)\backslash\mathrm{SL}_2(\mathbb{Z})} (\lambda_{g\tau} - \lambda_{g\tau^2})\, \xi^0(g).$$

Démonstration. Pour cette démonstration, généralisons nos notations pour les symboles modulaires. Pour u et v dans $(\mathrm{SL}_2(\mathbb{Z})\rho) \cup (\mathrm{SL}_2(\mathbb{Z})i) \cup \mathbb{P}^1(\mathbb{Q})$, on note $\{u, v\}$ la classe dans $H_1(X, R \cup I \cup \mathrm{ptes}\,; \mathbb{Z})$ de l'image dans X d'un chemin géodésique reliant u à v dans $\mathfrak{H}$.

Observons qu'on a des injections canoniques

$$\mathcal{H} \hookrightarrow \mathcal{H}^{\mathrm{ptes}} \hookrightarrow H_1(X, R \cup I \cup \mathrm{ptes}\,; \mathbb{Z}).$$

On identifie ainsi $\mathcal{H}$ et $\mathcal{H}^{\mathrm{ptes}}$ à des sous-groupes de $H_1(X, R \cup I \cup \mathrm{ptes}\,; \mathbb{Z})$. Nous allons établir l'égalité du théorème 5 dans $H_1(X, R \cup I \cup \mathrm{ptes}\,; \mathbb{Z})$. Dans ce groupe, on a

$$\alpha^{\mathrm{ptes}} \circ \alpha_{\mathrm{ptes}}\,(\xi_0(u)) = \sum_{g \in \Gamma_0(p) \backslash \mathrm{SL}_2(\mathbb{Z})} \{gi, g\rho\}.$$

Comme $-I \in \Gamma_0(p)$, l'image de σ (resp. τ) dans $\Gamma_0(p) \backslash \mathrm{SL}_2(\mathbb{Z})$ est d'ordre 2 (resp. 3). On a

$$\begin{aligned}
\sum_g \lambda_g \{gi, g\rho\} &= \sum_g \lambda_g \{gi, g\infty\} - \sum_h \lambda_h \{h\rho, h\infty\} \\
&= \frac{1}{2} \sum_g (\lambda_g \{gi, g\infty\} + \lambda_{g\sigma} \{g\sigma i, g\sigma\infty\}) - \frac{1}{3} \sum_h \lambda_h \{h\rho, h\infty\} \\
&\quad - \frac{1}{3} \sum_h (\lambda_{h\tau} \{h\tau\rho, h\tau\infty\} + \lambda_{h\tau^2} \{h\tau^2\rho, h\tau^2\infty\}).
\end{aligned}$$

Or $\sigma i = i$, $\sigma\infty = 0$, $\tau\rho = \rho$, $\tau\infty = 0$, $\lambda_{g\sigma} = -\lambda_g$ et $\lambda_h = -\lambda_{h\tau} - \lambda_{h\tau^2}$. Par conséquent, on a

$$\begin{aligned}
\sum_g \lambda_g \{gi, g\rho\} &= \frac{1}{2} \sum_g (\lambda_g \{gi, g\infty\} - \lambda_g \{gi, g0\}) - \frac{1}{3} \sum_h (\lambda_{h\tau} + \lambda_{h\tau^2}) \{h\infty, h\rho\} \\
&\quad - \frac{1}{3} \sum_h (\lambda_{h\tau} \{h\rho, h0\} + \lambda_{h\tau^2} \{h\rho, h\tau 0\}) \\
&= \frac{1}{2} \sum_g \lambda_g \{g0, g\infty\} - \frac{1}{3} \sum_g \lambda_{g\tau} \{g\infty, g0\} - \frac{1}{3} \sum_g \lambda_{g\tau^2} \{g\infty, g\tau 0\}.
\end{aligned}$$

Donc on a

$$\begin{aligned}
\sum_g \lambda_g \{gi, g\rho\} &= -\frac{1}{2} \sum_g \lambda_{g\tau} \{g0, g\infty\} - \frac{1}{2} \sum_g \lambda_{g\tau^2} \{g0, g\infty\} \\
&\quad + \frac{1}{3} \sum_g \lambda_{g\tau} \{g0, g\infty\} + \frac{1}{3} \sum_g \lambda_{g\tau^2} \{g0, g\infty\} \\
&\quad + \frac{1}{3} \sum_g \lambda_{g\tau^2} \{g\tau 0, g\tau\infty\}.
\end{aligned}$$

Comme $\sum_g \lambda_{g\tau^2}\{g\tau 0, g\tau\infty\} = \sum_g \lambda_{g\tau}\{g0, g\infty\}$, on a finalement

$$\sum_g \lambda_g\{gi, g\rho\} \quad = \quad -\frac{1}{6}\sum_g \lambda_{g\tau^2}\{g0, g\infty\} + \frac{1}{6}\sum_g \lambda_{g\tau}\{g0, g\infty\}.$$

On en déduit l'égalité annoncée. $\square$

Corollaire 1 *Pour tous $x = \sum_g \lambda_g g$ et $y = \sum_h \mu_h h$ dans $\mathcal{E}_{\Gamma_0(p)}$, on a dans $\mathcal{H}$:*

$$\alpha_{\mathrm{ptes}}(\xi_0(x)) \bullet \alpha_{\mathrm{ptes}}(\xi_0(y)) = \frac{1}{6}\sum_g (\lambda_{g\tau}\mu_g - \lambda_g \mu_{g\tau}).$$

Démonstration. La dualité de α^{ptes} et α_{ptes} et la proposition précédente justifient le calcul suivant :

$$\begin{aligned} \alpha_{\mathrm{ptes}}(\xi_0(x)) \bullet \alpha_{\mathrm{ptes}}(\xi_0(y)) \quad &= \psi(\xi_0(x)) \bullet \xi_0(y) \\ &= \tfrac{1}{6}\textstyle\sum_g (\lambda_{g\tau} - \lambda_{g\tau^2})\xi^0(g) \bullet \xi_0(y) \\ &= \tfrac{1}{6}\textstyle\sum_g (\lambda_{g\tau}\mu_g - \lambda_{g\tau^2}\mu_g) \\ &= \tfrac{1}{6}\textstyle\sum_g (\lambda_{g\tau}\mu_g - \lambda_g\mu_{g\tau}). \end{aligned}$$

$\square$

2.3 Algèbre de Hecke et conjugaison complexe

2.3.1 Action de la conjugaison complexe

L'involution $z \mapsto -\bar{z}$ de $\mathfrak{H}$ définit une involution sur $X = X_0(p)(\mathbb{C})$ qui laisse stable l'ensemble ptes et définit ainsi des involutions de $\mathcal{H}^{\mathrm{ptes}}$ et $\mathcal{H}_{\mathrm{ptes}}$. On note $\bar{x}$ l'image d'un cycle x sous l'action de cette involution appelée *conjugaison complexe.*

Un petit calcul (voir [8] ou [10] proposition 4) montre que l'action de la conjugaison complexe sur $\mathcal{H}^{\mathrm{ptes}}$ est donnée par $\overline{\xi^0(u)} = \xi^0(-u)$ $(u \in \mathbb{P}^1(\mathbb{F}_p))$. En particulier, le sous-groupe $\mathcal{H}$ de $\mathcal{H}^{\mathrm{ptes}}$ est stable sous cette action. L'involution $\mathbf{c}$ définie dans l'introduction n'est autre que la restriction de la conjugaison complexe à $\mathcal{H}$. Pour x, y dans $\mathcal{H}$, on a

$$\bar{x} \bullet \bar{y} = -x \bullet y. \tag{5}$$

Les sous-groupes $\mathcal{H}^+$ et $\mathcal{H}^-$ sont donc totalement isotropes. De plus $\mathcal{H}\left[\frac{1}{2}\right] = \mathcal{H}^+\left[\frac{1}{2}\right] \oplus \mathcal{H}^-\left[\frac{1}{2}\right]$. L'accouplement $\mathcal{H}^+\left[\frac{1}{2}\right] \times \mathcal{H}^-\left[\frac{1}{2}\right] \longrightarrow \mathbb{Z}\left[\frac{1}{2}\right]$ déduit de $\bullet$ par restriction à $\mathcal{H}^+ \times \mathcal{H}^-$ et extension des scalaires à $\mathbb{Z}\big[\frac{1}{2}\big]$ est parfait. En fait, on a $\mathcal{H}^+ = (1+\mathbf{c})\mathcal{H}$ et $\mathcal{H}^- = (1-\mathbf{c})\mathcal{H}$ (voir la proposition 5 de [12]). On note

$$\pi^+ = \frac{1}{2}(1+\mathbf{c}) : \mathcal{H}\big[\tfrac{1}{2}\big] \twoheadrightarrow \mathcal{H}^+\big[\tfrac{1}{2}\big] \quad \text{et} \quad \pi^- = \frac{1}{2}(1-\mathbf{c}) : \mathcal{H}\big[\tfrac{1}{2}\big] \twoheadrightarrow \mathcal{H}^-\big[\tfrac{1}{2}\big]$$

les surjections canoniques.

2.3.2 Action de l'algèbre de Hecke

Les correspondances de Hecke sur $X_0(p)$ laissent stable l'ensemble des pointes et définissent par conséquent une action de $\widetilde{\mathbb{T}}$ sur $\mathcal{H}_{\mathrm{ptes}}$ et $\mathcal{H}^{\mathrm{ptes}}$. Les opérateurs de Hecke $T_m,\ m \geq 1$ sont autoadjoints pour $\bullet : \mathcal{H}^{\mathrm{ptes}} \times \mathcal{H}_{\mathrm{ptes}} \longrightarrow \mathbb{Z}$ (voir par exemple [10] 2.2 lorsque $(m,p)=1$ et utiliser le fait que $T_p = -w_p$).

Le sous-groupe $\mathcal{H}$ de $\mathcal{H}^{\mathrm{ptes}}$ est stable sous l'action de $\widetilde{\mathbb{T}}$ et la surjection $\alpha_{\mathrm{ptes}}\ :\ \mathcal{H}_{\mathrm{ptes}} \longrightarrow \mathcal{H}$ est compatible avec cette action :

$$\alpha_{\mathrm{ptes}}(T_m(c)) = T_m \alpha_{\mathrm{ptes}}(c).$$

L'intégration sur les chemins définit l'accouplement non dégénéré suivant

$$\begin{array}{rcccl} [\ ,\ ] & : & \mathcal{H} \times H^0(X,\Omega^1) & \longrightarrow & \mathbb{C} \\ & & (c,\omega) & \longmapsto & [c,\omega] = \int_c \omega. \end{array} \tag{6}$$

L'image du morphisme injectif qui s'en déduit

$$\begin{array}{rcccl} F & : & \mathcal{H} & \longrightarrow & \mathrm{Hom}_{\mathbb{C}}(H^0(X,\Omega^1),\mathbb{C}) \\ & & c & \longmapsto & (\omega \mapsto \int_c \omega) \end{array} \tag{7}$$

s'identifie à $H_1(J,\mathbb{Z})$. L'isomorphisme $\mathcal{H} \cong H_1(J,\mathbb{Z})$ définit par transport de structure une action de $\mathbb{T}$ sur $\mathcal{H}$. Cette action coïncide avec la restriction à $\mathcal{H}$ de l'action de $\widetilde{\mathbb{T}}$ sur $\mathcal{H}^{\mathrm{ptes}}$.

L'action de l'algèbre de Hecke commute avec la conjugaison complexe. On en déduit une action de $\mathbb{T}$ sur $\mathcal{H}^+$ et $\mathcal{H}^-$.

3 Le module supersingulier

Pour les rappels qui suivent, nous nous inspirons des textes [4], [5], [2], [6], et [18]. Nous attirons l'attention sur le fait que les notations diffèrent quelque peu de celles adoptées par Emerton [2], notamment celles concernant l'algèbre de Hecke.

3.1 Réalisations géométriques et opérateurs de Hecke

L'ensemble $\mathcal{S} = \{x_0, \ldots, x_g\}$ des classes d'isomorphisme de courbes elliptiques supersingulières sur $\bar{\mathbb{F}}_p$ est muni d'une structure de schéma sur $\mathbb{F}_p$ de la façon suivante. Soient $X_0(p)_{\mathbb{Z}}$ la normalisation de $\mathbb{P}^1_{\mathbb{Z}}$ dans $X_0(p)$ via le morphisme composé $X_0(p) \longrightarrow X_0(1) \cong \mathbb{P}^1_{\mathbb{Z}}$. La fibre $X_0(p)_{\mathbb{F}_p}$ de $X_0(p)_{\mathbb{Z}}$ en p est constituée de deux copies de $\mathbb{P}^1_{\mathbb{F}_p}$ qui sont échangées par l'opérateur d'Atkin-Lehner w_p et se coupent transversalement. Les points doubles de $X_0(p)_{\mathbb{F}_p}$ sont en correspondance bijective avec les classes $x_0, \ldots, x_g$ et g n'est autre que le genre de $X_0(p)$.

Les correspondances de Hecke sur $X_0(p)$ s'étendent à $X_0(p)_{\mathbb{Z}_p}$ (voir [17] ou [1]). Par passage à la fibre en p et restriction à $\mathcal{S}$ on obtient une action de $\widetilde{\mathbb{T}}$ sur $\mathcal{P}$. L'action de $\widetilde{\mathbb{T}}$ sur la classe d'isomorphisme $[E]$ d'une courbe elliptique E supersingulière sur $\bar{\mathbb{F}}_p$ est donnée par (voir [17] ou [13] 1.2.1) :

$$T_m[E] = \sum_C [E/C] \quad (m \geq 1),$$

où C parcourt l'ensemble des sous-schémas en groupes finis d'ordre m de E. Lorsque p ne divise pas m, ces sous-schémas sont en correspondance bijective avec les sous-groupes d'ordre m de $E(\bar{\mathbb{F}}_p)$. Pour $m = p$, le seul sous-schéma en groupes fini d'ordre p de E est le noyau du morphisme de Frobenius

$$E \longrightarrow E^{(p)}.$$

On a donc

$$T_p([E]) = [E^{(p)}].$$

L'action de $\widetilde{\mathbb{T}}$ sur $\mathcal{P}$ est fidèle. Toute courbe elliptique supersingulière sur $\bar{\mathbb{F}}_p$ ayant $\sigma'(m)$ sous-schémas en groupes finis d'ordre m, le sous-groupe $\mathcal{P}^0$ de $\mathcal{P}$ est stable sous l'action de $\widetilde{\mathbb{T}}$. L'action de $\widetilde{\mathbb{T}}$ sur $\mathcal{P}^0$ se factorise par $\mathbb{T}$. Les opérateurs de Hecke sont autoadjoints pour $\langle\ ,\ \rangle$.

L'algèbre $\widetilde{\mathbb{T}}$ agit sur $\check{\mathcal{P}} = \mathrm{Hom}(\mathcal{P}, \mathbb{Z})$ par dualité. L'accouplement $\langle\ ,\ \rangle$ induit un homomorphisme injectif de $\widetilde{\mathbb{T}}$-modules de $\mathcal{P}$ dans $\check{\mathcal{P}}$ de conoyau isomorphe à $\mathbb{Z}/\delta\mathbb{Z}$ identifiant $\check{\mathcal{P}}$ au sous-$\widetilde{\mathbb{T}}$-module $\bigoplus_{i=0}^{g} \mathbb{Z}\frac{x_i}{w_i}$ de $\mathcal{P}_{\mathbb{Q}}$ (voir [4] ou [2] lemme 3.16). On fera désormais l'identification. L'homomorphisme injectif de $\mathbb{T}$-modules de $\mathcal{P}^0$ dans $\check{\mathcal{P}}^0$ induit par $\langle\ ,\ \rangle$ est de conoyau isomorphe à $\mathbb{Z}/n\mathbb{Z}$ (*loc. cit.*). L'accouplement canonique $\mathcal{P} \times \check{\mathcal{P}} \longrightarrow \mathbb{Z}$ étend donc l'accouplement $\langle\ ,\ \rangle$ et sera encore noté $\langle\ ,\ \rangle$.

Pour tout anneau A, on étendra l'homomorphisme *degré* $\deg : \mathcal{P} \longrightarrow \mathbb{Z}$ à $\mathcal{P}_A$ par linéarité.

3.2 Courbes elliptiques supersingulières et algèbres de quaternions

Pour tout $i \in \{0, \ldots, g\}$, fixons un représentant E_i de la classe x_i et notons $I_i = \mathrm{Hom}(E_i, E_0)$. Les anneaux $R_i = \mathrm{End}E_i$, $i \in \{0, \ldots, g\}$ sont des ordres maximaux de l'algèbre de quaternions $\mathcal{B} = R_0 \otimes \mathbb{Q}$ sur $\mathbb{Q}$ définie ramifiée en p et ∞. Toute classe de conjugaison des ordres maximaux de $\mathcal{B}$ est représentée par un élément de $\{R_0, \ldots, R_g\}$. Pour $i \in \{0, \ldots, g\}$, I_i est un idéal de $\mathcal{B}$ d'ordre à gauche R_0 et d'ordre à droite R_i. L'ensemble $\mathcal{C}_g(R_0)$ des classes d'idéaux à gauche de R_0 est fini et son cardinal est indépendant du choix de R_0 (voir [18]). L'application $E_i \mapsto I_i$ induit une bijection de $\mathcal{S}$ vers $\mathcal{C}_g(R_0)$.

Rappelons que $w_i = |R_i^*/\langle \pm 1 \rangle| = |\mathrm{Aut}(E_i)/\langle \pm 1 \rangle|$. On a

$$\prod_{i=0}^{g} w_i = \delta \quad \text{et} \quad \sum_{i=0}^{g} \frac{1}{w_i} = \frac{p-1}{12}.$$

La deuxième égalité est la *formule de masse d'Eichler*.

Notons $M_{i,j}$ l'idéal à gauche de R_j et à droite de R_i défini par :

$$M_{i,j} = I_j^{-1} I_i = \mathrm{Hom}(E_i, E_j).$$

Ce $\mathbb{Z}$-module libre de rang 4 est muni de la forme quadratique donnée par la norme réduite N (voir [18]). Pour $b \in M_{i,j}$, le degré de l'isogénie $\phi_b \in \mathrm{Hom}(E_i, E_j)$ correspondante est donné par

$$\deg \phi_b = N(b)/N(M_{i,j}).$$

La série Theta associée à l'idéal $M_{i,j}$ est définie par

$$\Theta(M_{i,j}) = \sum_{b \in M_{i,j}} q^{N(b)/N(M_{i,j})} = \sum_{m \geq 0} 2 w_j B_{i,j}(m) q^m \tag{8}$$

où

$$B_{i,j}(m) = \frac{1}{2w_j} \,\mathrm{Card}\{b \in M_{i,j},\ N(b)/N(M_{i,j}) = m\}. \tag{9}$$

Pour m entier positif, la matrice $B(m)$ de terme général $B_{i,j}(m)$, $0 \leq i, j \leq g$, est la *matrice d'Eichler-Brandt de degré m*.

L'entier $B_{i,j}(m)$ est aussi le nombre de sous-schémas en groupes C d'ordre m de E_i tels que $E_i/C \cong E_j$. On en déduit que sur la base $(x_i)_{0 \leq i \leq g}$ de $\mathcal{P}$, l'action de T_m ($m \geq 1$) est donnée par la matrice d'Eichler-Brandt $B(m) = (B_{i,j})_{0 \leq i,j \leq g}$:

$$T_m x_i = \sum_{j=0}^{g} B_{i,j}(m) x_j. \tag{10}$$

Nous renvoyons le lecteur à [4], notamment à la proposition 2.7, pour les propriétés de ces matrices. Signalons en particulier la relation de symétrie

$$w_j B_{i,j}(m) = w_i B_{j,i}(m), \ (\forall m \in \mathbb{N}), \tag{11}$$

et la relation

$$\sum_{j=0}^{g} B_{i,j}(m) = \sigma'(m). \tag{12}$$

4 Comparaisons

4.1 Espaces propres sous l'action de $\widetilde{\mathbb{T}}$

Les $\widetilde{\mathbb{T}}_{\mathbb{Q}}$-modules $\mathcal{M}_{\mathbb{Q}}$ et $\mathcal{P}_{\mathbb{Q}}$ et les $\mathbb{T}_{\mathbb{Q}}$-modules $\mathcal{M}^0_{\mathbb{Q}}$, $\mathcal{P}^0_{\mathbb{Q}}$, $\mathcal{H}^+_{\mathbb{Q}}$ et $\mathcal{H}^-_{\mathbb{Q}}$ sont libres de rang 1 (voir par exemple [4] pour le module supersingulier et [9] pour l'homologie).

On appellera *forme de Hecke* toute forme modulaire propre pour les opérateurs de Hecke et normalisée, et *forme primitive* toute forme de Hecke parabolique.

Les idempotents de $\widetilde{\mathbb{T}}_{\bar{\mathbb{Q}}}$ sont en correspondance bijective avec les formes de Hecke et engendrent les sous-$\widetilde{\mathbb{T}}_{\bar{\mathbb{Q}}}$-modules irréductibles de $\widetilde{\mathbb{T}}_{\bar{\mathbb{Q}}}$. On note $\mathbf{1}_f$ l'idempotent de $\widetilde{\mathbb{T}}_{\bar{\mathbb{Q}}}$ associé à une forme de Hecke f. Les opérateurs de Hecke étant autoadjoints pour les accouplements $(\, ,)$ sur $\mathcal{M} \times \mathcal{M}$, $\langle \, , \rangle$ sur $\mathcal{P} \times \mathcal{P}$ et $\bullet$ sur $\mathcal{H}^+ \times \mathcal{H}^-$, chacun de ces modules de Hecke se décomposent en somme directe de sous-espaces propres orthogonaux après extension des scalaires à $\bar{\mathbb{Q}}$.

4.1.1 Éléments d'Eisenstein

Soit $E \in \mathcal{N}$ la forme de Hecke définie par la série d'Eisenstein normalisée de poids 2 pour $\Gamma_0(p)$:

$$E = \frac{p-1}{24} + \sum_{m \geq 1} \sigma'(m) q^m. \tag{13}$$

Considérons l'élément

$$a_E = \sum_{i=0}^{g} \frac{x_i}{w_i} \in \check{\mathcal{P}} \subset \mathcal{P}_{\mathbb{Q}}. \tag{14}$$

Il vérifie

$$\deg a_E = \frac{p-1}{12} \qquad \text{et} \qquad \langle x, a_E \rangle = \deg x \quad (x \in \mathcal{P}).$$

Le sous-$\mathbb{Z}$-module $\mathcal{P}^E$ de $\check{\mathcal{P}}$ engendré par a_E est l'orthogonal de $\mathcal{P}^0$ pour $\langle\ ,\ \rangle : \mathcal{P} \times \check{\mathcal{P}} \longrightarrow \mathbb{Z}$. On a la décomposition (voir [2] démonstration du lemme 3.16)

$$\mathcal{P}\left[\tfrac{1}{n\delta}\right] = \mathcal{P}^E\left[\tfrac{1}{n\delta}\right] \oplus \mathcal{P}^0\left[\tfrac{1}{n\delta}\right]. \tag{15}$$

Soit π^0 la surjection de $\mathcal{P}\left[\tfrac{1}{n\delta}\right]$ sur $\mathcal{P}^0\left[\tfrac{1}{n\delta}\right]$ définie par

$$\pi^0(x) = x - \frac{12}{p-1} \deg(x)\ a_E \qquad \left(x \in \mathcal{P}\left[\tfrac{1}{n\delta}\right]\right). \tag{16}$$

On note encore π^0 tout homomorphisme qui étend π^0 par linéarité.

D'après (11), (12) et (10), l'élément a_E est un vecteur propre de T_m pour la valeur propre $\sigma'(m)$ pour tout $m \geq 1$. Il engendre donc l'espace $\widetilde{\mathbb{T}}_{\bar{\mathbb{Q}}}$-propre associé à E : $\mathbf{1}_E\left(\mathcal{P}_{\bar{\mathbb{Q}}}\right) = \mathcal{P}^E \otimes \bar{\mathbb{Q}}$; c'est pourquoi on l'appelle *élément d'Eisenstein de* $\mathcal{P}_{\bar{\mathbb{Q}}}$.

4.1.2 Espaces propres associés aux formes primitives

Pour f une forme primitive, notons $\mathcal{P}^f_{\bar{\mathbb{Q}}} = \mathbf{1}_f\left(\mathcal{P}_{\bar{\mathbb{Q}}}\right)$, $\mathcal{H}^{+f}_{\bar{\mathbb{Q}}} = \mathbf{1}_f\left(\mathcal{H}^+_{\bar{\mathbb{Q}}}\right)$, $\mathcal{H}^{-f}_{\bar{\mathbb{Q}}} = \mathbf{1}_f\left(\mathcal{H}^-_{\bar{\mathbb{Q}}}\right)$ et choisissons respectivement $a_f,\ c_f$, et d_f un vecteur directeur de chacune de ces $\bar{\mathbb{Q}}$-droites. On vérifie aisément que pour $x \in \mathcal{P}_{\bar{\mathbb{Q}}},\ c \in \mathcal{H}^+_{\bar{\mathbb{Q}}}$, et $d \in \mathcal{H}^-_{\bar{\mathbb{Q}}}$, on a

$$\mathbf{1}_f(x) = \frac{\langle x, a_f \rangle}{\langle a_f, a_f \rangle}\ a_f, \qquad \mathbf{1}_f(c) = \frac{c \bullet d_f}{c_f \bullet d_f}\ c_f \quad \text{et} \quad \mathbf{1}_f(d) = \frac{c_f \bullet d}{c_f \bullet d_f}\ d_f.$$

Pour x dans $\mathcal{P}_{\bar{\mathbb{Q}}}$, $\mathcal{H}^+_{\bar{\mathbb{Q}}}$ ou $\mathcal{H}^-_{\bar{\mathbb{Q}}}$, on notera parfois $x^f = \mathbf{1}_f(x)$.

Notons Prim l'ensemble des formes primitives de poids 2 pour $\Gamma_0(p)$. On a les décompositions en sous-espaces $\mathbb{T}_{\bar{\mathbb{Q}}}$-propres deux à deux orthogonaux pour $\langle\ ,\ \rangle$ et $\bullet$ respectivement

$$\mathcal{P}^0_{\bar{\mathbb{Q}}} = \bigoplus_{f \in \mathrm{Prim}} \mathcal{P}^f_{\bar{\mathbb{Q}}}, \quad \mathcal{H}^+_{\bar{\mathbb{Q}}} = \bigoplus_{f \in \mathrm{Prim}} \mathcal{H}^{+f}_{\bar{\mathbb{Q}}}, \quad \mathcal{H}^-_{\bar{\mathbb{Q}}} = \bigoplus_{f \in \mathrm{Prim}} \mathcal{H}^{-f}_{\bar{\mathbb{Q}}}. \tag{17}$$

4.1.3 Une base particulière de vecteurs propres de l'homologie

Lemme 1 *Pour toute forme différentielle holomorphe ω sur X, il existe $c_\omega \in \mathcal{H}_{\mathbb{C}}^{+}$ et $d_\omega \in \mathcal{H}_{\mathbb{C}}^{-}$ tels que*

$$\int_d \omega = d \bullet c_\omega \quad (d \in \mathcal{H}_{\mathbb{C}}^{-}) \quad \text{et} \quad \int_c \bar{\omega} = c \bullet d_\omega \quad (c \in \mathcal{H}_{\mathbb{C}}^{+}). \tag{18}$$

De plus, on a

$$c_\omega \bullet d_\eta = \iint_X \omega \wedge \bar{\eta} \quad (\omega, \eta \in H^0(X, \Omega^1)). \tag{19}$$

Démonstration. Notons momentanément $\Omega = H^0(X, \Omega^1)$. Rappelons que la dualité de Poincaré ainsi que les théorèmes de De Rham et Hodge (voir [3] ou [7]) permettent d'associer à tout $\eta \in \Omega \oplus \bar{\Omega}$ un unique cycle $u_\eta \in \mathcal{H}_{\mathbb{C}}$ caractérisé par l'une des propriétés équivalentes suivantes :

$$i) \quad \int_c \eta = c \bullet u_\eta \quad (c \in \mathcal{H}_{\mathbb{C}}); \qquad ii) \int_{u_\eta} \xi = \iint_X \eta \wedge \xi \quad (\eta \in \Omega \oplus \bar{\Omega}).$$

Pour $\omega \in \Omega$ notons α_ω (resp. β_ω) le cycle associé par ce procédé à $\omega + \bar{\omega}$ (resp. $i(\bar{\omega} - \omega)$). Remarquons que puisque $\omega + \bar{\omega}$ et $i(\bar{\omega} - \omega)$ sont réelles, les cycles α_ω et β_ω sont en fait dans $\mathcal{H}_{\mathbb{R}}$. On vérifie aisément que les cycles

$$c_\omega = \frac{1}{2}\pi^{+}(\alpha_\omega + i\beta_\omega) \in \mathcal{H}_{\mathbb{C}}^{+} \quad \text{et} \quad d_\omega = \frac{1}{2}\pi^{-}(\alpha_\omega - i\beta_\omega) \in \mathcal{H}_{\mathbb{C}}^{-}$$

satisfont (18) et (19). □

Pour f une forme primitive, on note $\tilde{c}_f = c_{\omega_f}$ et $\tilde{d}_f = d_{\omega_f}$. Puisque les opérateurs de Hecke sont autoadjoints pour $[\ ,\ ]$ et $\bullet$, les éléments $\tilde{c}_f$ et $\tilde{d}_f$ engendrent respectivement $\mathcal{H}_{\mathbb{C}}^{+f}$ et $\mathcal{H}_{\mathbb{C}}^{-f}$. De plus, d'après (19), on a

$$\tilde{c}_f \bullet \tilde{d}_f = -i(f, f). \tag{20}$$

4.2 Résultats locaux

Pour $\mathfrak{m}$ un idéal maximal de $\widetilde{\mathbb{T}}$ et U un $\widetilde{\mathbb{T}}$-module, notons $k_{\mathfrak{m}} = \widetilde{\mathbb{T}}/\mathfrak{m}$ et $U_{\mathfrak{m}} = \varprojlim \left(U/\mathfrak{m}^k U\right)$ le séparé complété de U pour la topologie $\mathfrak{m}$-adique.

Lorsque $\mathfrak{m}$ est un idéal maximal de $\widetilde{\mathbb{T}}$ de caractéristique $l \neq 2$, l'anneau $\widetilde{\mathbb{T}}_{\mathfrak{m}}$ est de Gorenstein (voir [9] corollaires 15.2 et 16.3). Les $\widetilde{\mathbb{T}}_{\mathfrak{m}}$-modules $\mathcal{N}_{\mathfrak{m}}$, $\mathcal{M}_{\mathfrak{m}}$, $\mathcal{P}_{\mathfrak{m}}$ et les $\mathbb{T}_{\mathfrak{m}}$-modules $\mathcal{M}_{\mathfrak{m}}^0$ et $\mathcal{P}_{\mathfrak{m}}^0$ sont alors libres de rang 1 (voir le théorème 0.5 de [2]). Le $\mathbb{T}_{\mathfrak{m}}$-module $\mathcal{H}_{\mathfrak{m}}$ est libre de rang 2 (voir [9] paragraphe 15). Comme $\mathcal{H}_{\mathfrak{m}} = \mathcal{H}_{\mathfrak{m}}^{+} \oplus \mathcal{H}_{\mathfrak{m}}^{-}$, il s'ensuit que les $\mathbb{T}_{\mathfrak{m}}$-modules $\mathcal{H}_{\mathfrak{m}}^{+}$ et $\mathcal{H}_{\mathfrak{m}}^{-}$ sont libres de rang 1.

4.3 Produits tensoriels sur l'algèbre de Hecke

Considérons le $\widetilde{\mathbb{T}}$-module $\mathcal{P}\otimes_{\widetilde{\mathbb{T}}}\mathcal{P}$ et les $\mathbb{T}$-modules $\mathcal{P}^0\otimes_{\mathbb{T}}\mathcal{P}^0$ et $\mathcal{H}^+\otimes_{\mathbb{T}}\mathcal{H}^-$.

Lemme 2 *Les sous-espaces $\widetilde{\mathbb{T}}_{\bar{\mathbb{Q}}}$-propres de $\mathcal{P}_{\bar{\mathbb{Q}}}\otimes_{\widetilde{\mathbb{T}}_{\bar{\mathbb{Q}}}}\mathcal{P}_{\bar{\mathbb{Q}}}$ sont les $\widetilde{\mathbb{T}}_{\bar{\mathbb{Q}}}$-modules $\mathcal{P}^g_{\bar{\mathbb{Q}}}\otimes_{\widetilde{\mathbb{T}}_{\bar{\mathbb{Q}}}}\mathcal{P}^g_{\bar{\mathbb{Q}}}$ pour g décrivant l'ensemble des formes de Hecke. Les sous-espaces $\mathbb{T}_{\bar{\mathbb{Q}}}$-propres de $\mathcal{H}^+_{\bar{\mathbb{Q}}}\otimes_{\mathbb{T}_{\bar{\mathbb{Q}}}}\mathcal{H}^-_{\bar{\mathbb{Q}}}$ sont les $\mathbb{T}_{\bar{\mathbb{Q}}}$-modules $\mathcal{H}^{+g}_{\bar{\mathbb{Q}}}\otimes_{\mathbb{T}_{\bar{\mathbb{Q}}}}\mathcal{H}^{-g}_{\bar{\mathbb{Q}}}$ pour $g\in$ Prim. Plus précisément, on a les décompositions en sous-espaces deux à deux orthogonaux*

$$\begin{aligned}
\mathcal{P}_{\mathbb{Q}}\otimes_{\widetilde{\mathbb{T}}_{\mathbb{Q}}}\mathcal{P}_{\mathbb{Q}} &= (\mathcal{P}^E_{\mathbb{Q}}\otimes_{\widetilde{\mathbb{T}}_{\mathbb{Q}}}\mathcal{P}^E_{\mathbb{Q}})\oplus(\mathcal{P}^0_{\mathbb{Q}}\otimes_{\mathbb{T}_{\mathbb{Q}}}\mathcal{P}^0_{\mathbb{Q}}) && (21)\\
\mathcal{P}^0_{\bar{\mathbb{Q}}}\otimes_{\mathbb{T}_{\bar{\mathbb{Q}}}}\mathcal{P}^0_{\bar{\mathbb{Q}}} &= \bigoplus_{g\in\mathrm{Prim}}\left(\mathcal{P}^g_{\bar{\mathbb{Q}}}\otimes_{\mathbb{T}_{\bar{\mathbb{Q}}}}\mathcal{P}^g_{\bar{\mathbb{Q}}}\right) && (22)\\
\mathcal{H}^+_{\bar{\mathbb{Q}}}\otimes_{\mathbb{T}_{\bar{\mathbb{Q}}}}\mathcal{H}^-_{\bar{\mathbb{Q}}} &= \bigoplus_{g\in\mathrm{Prim}}\left(\mathcal{H}^{+g}_{\bar{\mathbb{Q}}}\otimes_{\mathbb{T}_{\bar{\mathbb{Q}}}}\mathcal{H}^{-g}_{\bar{\mathbb{Q}}}\right). && (23)
\end{aligned}$$

Démonstration. D'après (15) et (17), il suffit de montrer que $\mathcal{P}^g_{\bar{\mathbb{Q}}}\otimes_{\widetilde{\mathbb{T}}_{\bar{\mathbb{Q}}}}\mathcal{P}^h_{\bar{\mathbb{Q}}}$ est nul pour tout couple (g,h) de formes de Hecke distinctes. Ceci résulte du théorème de multiplicité 1 sur les formes de Hecke. En effet si g (resp. h) a pour développement de Fourier à l'infini $g(z)=\sum_{m\geq 0}b_mq^m$ (resp. $h(z)=\sum_{m\geq 0}c_mq^m$,) alors l'image $a_g\otimes_{\widetilde{\mathbb{T}}_{\bar{\mathbb{Q}}}}a_h$ de $a_g\otimes a_h$ dans $\mathcal{P}_{\bar{\mathbb{Q}}}\otimes_{\widetilde{\mathbb{T}}_{\bar{\mathbb{Q}}}}\mathcal{P}_{\bar{\mathbb{Q}}}$ vérifie pour tout $m\geq 1$,

$$b_ma_g\otimes_{\widetilde{\mathbb{T}}_{\bar{\mathbb{Q}}}}a_h=T_ma_g\otimes_{\widetilde{\mathbb{T}}_{\bar{\mathbb{Q}}}}a_h=a_g\otimes_{\widetilde{\mathbb{T}}_{\bar{\mathbb{Q}}}}(T_ma_h)=c_ma_g\otimes_{\widetilde{\mathbb{T}}_{\bar{\mathbb{Q}}}}a_h.$$

On en déduit que si $g\neq h$, alors $a_g\otimes_{\widetilde{\mathbb{T}}_{\bar{\mathbb{Q}}}}a_h=0$.

On procède de même pour $\mathcal{H}^+\otimes_{\mathbb{T}}\mathcal{H}^-$. □

Notons $\langle\ ,\ \rangle^{\otimes 2}:\mathcal{P}^{\otimes 2}\times\mathcal{P}^{\otimes 2}\longrightarrow\mathbb{Z}$ l'accouplement défini composante par composante autrement dit défini par

$$\langle a_1\otimes a_2,b_1\otimes b_2\rangle^{\otimes 2}=\langle a_1,b_1\rangle\langle a_2,b_2\rangle\quad(a_i,b_i\in\mathcal{P},\ i=1,2).$$

De même notons $\bullet^{\otimes 2}:\mathcal{H}^{\otimes 2}\times\mathcal{H}^{\otimes 2}\longrightarrow\mathbb{Z}$ l'accouplement défini par $\bullet$. Soient $s:\mathcal{P}\otimes\mathcal{P}\twoheadrightarrow\mathcal{P}\otimes_{\widetilde{\mathbb{T}}}\mathcal{P}$, et $s':\mathcal{H}^+\otimes\mathcal{H}^-\twoheadrightarrow\mathcal{H}^+\otimes_{\mathbb{T}}\mathcal{H}^-$ les surjections canoniques. Un calcul élémentaire montre que pour $f\in$ Prim, $x\in\mathcal{P}^{\otimes 2}_{\bar{\mathbb{Q}}}$ et $c\in\mathcal{H}^+_{\bar{\mathbb{Q}}}\otimes_{\bar{\mathbb{Q}}}\mathcal{H}^-_{\bar{\mathbb{Q}}}$, on a

$$\mathbf{1}_f(s(x))=\frac{\langle x,a_f\otimes_{\bar{\mathbb{Q}}}a_f\rangle^{\otimes 2}}{\langle a_f\otimes_{\bar{\mathbb{Q}}}a_f,a_f\otimes_{\bar{\mathbb{Q}}}a_f\rangle^{\otimes 2}}\,a_f\otimes_{\mathbb{T}_{\bar{\mathbb{Q}}}}a_f \tag{24}$$

et

$$\mathbf{1}_f(s(c))=\frac{c\bullet^{\otimes 2}(d_f\otimes_{\bar{\mathbb{Q}}}c_f)}{(c_f\otimes_{\bar{\mathbb{Q}}}d_f)\bullet^{\otimes 2}(d_f\otimes_{\bar{\mathbb{Q}}}c_f)}\,c_f\otimes_{\mathbb{T}_{\bar{\mathbb{Q}}}}d_f. \tag{25}$$

Considérons l'homomorphisme de $\widetilde{\mathbb{T}}$-modules déduit de l'accouplement sur $\mathcal{P} \times \check{\mathcal{P}}$:

$$\begin{array}{rcl} \theta \ : \ \mathcal{P} \otimes_{\widetilde{\mathbb{T}}} \check{\mathcal{P}} & \longrightarrow & \mathrm{Hom}(\widetilde{\mathbb{T}}, \mathbb{Z}) \cong \mathcal{N} \\ x \otimes_{\widetilde{\mathbb{T}}} y & \longmapsto & \dfrac{\deg x . \deg y}{2} + \displaystyle\sum_{m \geq 1} \langle T_m x, y \rangle \, q^m. \end{array}$$

On a en particulier

$$\theta(x_i \otimes_{\widetilde{\mathbb{T}}} \frac{x_j}{w_j}) = \frac{1}{2w_j} \Theta(M_{i,j}), \ 0 \leq i, j \leq g.$$

Rappelons que $\theta^0 : \mathcal{P}^0 \times \check{\mathcal{P}}^0 \longrightarrow \mathcal{M}^0$ et $\psi : \mathcal{H}^+ \times \mathcal{H}^- \longrightarrow \mathcal{M}^0$ désignent de même les homomorphismes de $\mathbb{T}$-modules déduits des accouplements sur $\mathcal{P}^0 \times \check{\mathcal{P}}^0$ et $\mathcal{H}^+ \times \mathcal{H}^-$ respectivement.

Théorème 6 (Emerton) *Les homomorphismes θ et θ^0 sont surjectifs. De plus, on a*

$$\theta(\mathcal{P} \otimes_{\widetilde{\mathbb{T}}} \mathcal{P}) = \mathcal{M} \quad \textit{et} \quad \theta^0(\mathcal{P}^0 \otimes_{\mathbb{T}} \mathcal{P}^0) = \mathcal{I}\mathcal{M}^0,$$

où $\mathcal{I}$ est l'idéal d'Eisenstein.

Démonstration. Voir [2] théorèmes 0.3, 0.6, et 0.10. □

Pour $\mathfrak{m}$ un idéal maximal de $\widetilde{\mathbb{T}}$ et $u : U \longrightarrow V$ un homomorphisme de $\widetilde{\mathbb{T}}$-modules, on note $u_{\mathfrak{m}} : U_{\mathfrak{m}} \longrightarrow V_{\mathfrak{m}}$ l'homomorphisme qui s'en déduit sur les séparés complétés.

Corollaire 2 (Emerton) *Pour $\mathfrak{m}$ un idéal maximal de $\widetilde{\mathbb{T}}$ de caractéristique résiduelle $l \neq 2$, l'homomorphisme de $\widetilde{\mathbb{T}}_{\mathfrak{m}}$-modules $\theta_{\mathfrak{m}}$ et l'homomorphisme de $\mathbb{T}_{\mathfrak{m}}$-modules $\theta^0_{\mathfrak{m}}$ sont des isomorphismes.*

Proposition 1 *Pour tout idéal maximal $\mathfrak{m}$ de $\mathbb{T}$ de caractéristique résiduelle $l \neq 2$, le morphisme de $\mathbb{T}_{\mathfrak{m}}$-modules $\psi_{\mathfrak{m}} : \mathcal{H}^+_{\mathfrak{m}} \otimes_{\mathbb{T}_{\mathfrak{m}}} \mathcal{H}^-_{\mathfrak{m}} \longrightarrow \mathcal{M}^0_{\mathfrak{m}}$ est un isomorphisme.*

Démonstration. On a

$$\mathbb{T} \otimes \mathbb{Z}_l = \bigoplus_{\mathfrak{m}} \mathbb{T}_{\mathfrak{m}},$$

où $\mathfrak{m}$ décrit l'ensemble des idéaux maximaux de $\mathbb{T}$ de caractéristique résiduelle l. On a donc $\mathcal{H}^{\pm} \otimes \mathbb{Z}_l = \bigoplus_{\mathfrak{m}} \mathcal{H}^{\pm}_{\mathfrak{m}}$ pour $\mathfrak{m}$ parcourant l'ensemble des idéaux maximaux de $\mathbb{T}$ de caractéristique résiduelle l. Les opérateurs de Hecke étant autoadjoints pour $\bullet$, l'accouplement sur les séparés complétés

$$(\mathcal{H}^+ \otimes \mathbb{Z}_l) \times (\mathcal{H}^- \otimes \mathbb{Z}_l) \longrightarrow \mathbb{Z}_l \tag{26}$$

est trivial sur $\mathcal{H}^+_{\mathfrak{m}} \times \mathcal{H}^-_{\mathfrak{m}'}$ pour tout couple $(\mathfrak{m}, \mathfrak{m}')$ d'idéaux maximaux de $\mathbb{T}$ distincts. Par conséquent, l'accouplement (26) est la somme directe de ses restrictions

$$\mathcal{H}^+_{\mathfrak{m}} \times \mathcal{H}^-_{\mathfrak{m}} \longrightarrow \mathbb{Z}_l.$$

De plus, puisque $l \neq 2$, l'accouplement (26) est parfait.

On en déduit que pour tout idéal maximal $\mathfrak{m}$ de $\mathbb{T}$ de caractéristique résiduelle $l \neq 2$, l'accouplement

$$\mathcal{H}^+_{\mathfrak{m}} \times \mathcal{H}^-_{\mathfrak{m}} \longrightarrow \mathbb{Z}_l$$

est parfait. Par ailleurs, $\mathcal{H}^+_{\mathfrak{m}}, \mathcal{H}^-_{\mathfrak{m}}$ et $\mathcal{M}^0_{\mathfrak{m}}$ sont des $\mathbb{T}_{\mathfrak{m}}$-modules libres de rang 1. Le lemme 2.4 de [2] permet alors de conclure. $\square$

On déduit immédiatement du corollaire 2 et de la proposition 1 la proposition suivante :

Proposition 2 *Les applications $\theta\left[\frac{1}{2}\right]$, $\theta^0\left[\frac{1}{2}\right]$ et $\psi\left[\frac{1}{2}\right]$ obtenues par extension des scalaires à $\mathbb{Z}\left[\frac{1}{2}\right]$, sont respectivement des isomorphismes de $\widetilde{\mathbb{T}}\left[\frac{1}{2}\right]$-modules et $\mathbb{T}\left[\frac{1}{2}\right]$-modules localement libres de rang* 1.

Remarque 1 L'homomorphisme de $\mathbb{T}$-modules

$$\Upsilon : \mathcal{H}^+ \otimes_{\mathbb{T}} \mathcal{H}^- \longrightarrow \mathcal{H} \wedge_{\mathbb{T}} \mathcal{H}$$

composé de l'homomorphisme injectif de $\mathbb{T}$-modules $\mathcal{H}^+ \otimes_{\mathbb{T}} \mathcal{H}^- \hookrightarrow \mathcal{H} \otimes_{\mathbb{T}} \mathcal{H}$ et de la surjection canonique $\mathcal{H} \otimes_{\mathbb{T}} \mathcal{H} \twoheadrightarrow \mathcal{H} \wedge_{\mathbb{T}} \mathcal{H}$ est surjectif. Il s'ensuit que $\Upsilon\left[\frac{1}{2}\right]$ est un isomorphisme de $\mathbb{T}\left[\frac{1}{2}\right]$-modules. Nous aurions donc pu faire usage du $\mathbb{T}$-module $\mathcal{H} \wedge_{\mathbb{T}} \mathcal{H}$ plutôt que de $\mathcal{H}^+ \otimes_{\mathbb{T}} \mathcal{H}^-$ sur lequel l'antisymétrie de $\bullet$ est cachée.

4.4 Générateurs explicites sur $\mathbb{Q}$

Nous montrons dans ce paragraphe le théorème 1 énoncé dans l'introduction.

Considérons l'élément de $\mathcal{P}_{\mathbb{Q}} \otimes_{\mathbb{Q}} \mathcal{P}_{\mathbb{Q}}$ suivant

$$\Delta_2 = \sum_{i=0}^{g} \frac{1}{w_i} x_i \otimes_{\mathbb{Q}} x_i. \tag{27}$$

L'élément Δ_2^0 défini dans l'introduction n'est autre que

$$\Delta_2^0 = (\pi^0 \otimes_{\mathbb{Q}} 1)(\Delta_2) = (\pi^0 \otimes_{\mathbb{Q}} \pi^0)(\Delta_2) \in \mathcal{P}^0_{\mathbb{Q}} \otimes_{\mathbb{Q}} \mathcal{P}^0_{\mathbb{Q}}.$$

Notons $s^0 : \mathcal{P}^0 \otimes \mathcal{P}^0 \twoheadrightarrow \mathcal{P}^0 \otimes_{\mathbb{T}} \mathcal{P}^0$ la surjection canonique. Soit $\bar{\Delta}_2 = s(\Delta_2)$. Puisque $s^0 \circ (\pi^0 \otimes \pi^0) = (\pi^0 \otimes_{\widetilde{\mathbb{T}}} \pi^0) \circ s$, l'élément $\bar{\Delta}_2^0$ de l'introduction est $\bar{\Delta}_2^0 = (\pi^0 \otimes_{\widetilde{\mathbb{T}}} \pi^0)(\bar{\Delta}_2)$.

Soit

$$\Lambda_2 = \frac{1}{6} \sum_{x \in \mathbb{F}_p^* \setminus \{1\}} \left(\xi^0 \left(\frac{1}{1-x} \right) \otimes_{\mathbb{Q}} \xi^0(x) - \xi^0(x) \otimes_{\mathbb{Q}} \xi^0 \left(\frac{1}{1-x} \right) \right) \tag{28}$$

un relèvement dans $\mathcal{H}_{\mathbb{Q}} \otimes_{\mathbb{Q}} \mathcal{H}_{\mathbb{Q}}$ de l'élément $\bar{\Lambda}_2$ défini dans l'introduction.

Lemme 3 *On a*

$$\Lambda_2 = \frac{1}{6} \sum_{g \in \Gamma_0(p) \backslash \mathrm{SL}_2(\mathbb{Z})} \left(\xi^0(g\tau) \otimes_{\mathbb{Q}} \xi^0(g) - \xi^0(g) \otimes_{\mathbb{Q}} \xi^0(g\tau) \right).$$

Démonstration. On a en effet

$$\begin{aligned} 6\Lambda_2 \quad = \quad & \frac{1}{6} \sum_{g \in \Gamma_0(p) \backslash \mathrm{SL}_2(\mathbb{Z})} \left(\xi^0(g\tau) \otimes_{\mathbb{Q}} \xi^0(g) - \xi^0(g) \otimes_{\mathbb{Q}} \xi^0(g\tau) \right) \\ & -\xi^0(1) \otimes_{\mathbb{Q}} \xi^0(0) + \xi^0(0) \otimes_{\mathbb{Q}} \xi^0(1) - \xi^0(0) \otimes_{\mathbb{Q}} \xi^0(\infty) + \xi^0(\infty) \otimes_{\mathbb{Q}} \xi^0(0). \end{aligned}$$

Or $\xi^0(0) = -\xi^0(\infty)$ et $\xi^0(1) = 0$ (voir le paragraphe 2.1). D'où le lemme. □

Proposition 3 *Pour $u, v \in \mathcal{P}_{\mathbb{Q}}$ et $c, d \in \mathcal{H}_{\mathbb{Q}}$, on a*

$$\langle \Delta_2, u \otimes_{\mathbb{Q}} v \rangle^{\otimes 2} = \langle u, v \rangle \qquad \textit{et} \qquad \Lambda_2 \bullet^{\otimes 2} (c \otimes_{\mathbb{Q}} d) = c \bullet d.$$

Démonstration. Soient $u = \sum_{i=0}^g \lambda_i x_i$ et $v = \sum_{i=0}^g \mu_i x_i$ dans $\mathcal{P}_{\mathbb{Q}}^0$, on a

$$\langle \Delta_2, u \otimes_{\mathbb{Q}} v \rangle^{\otimes 2} = \sum_{i=0}^{g} \langle x_i, u \rangle . \langle \frac{x_i}{w_i}, v \rangle = \sum_{i=0}^{g} \lambda_i \mu_i w_i = \langle u, v \rangle.$$

Dans les calculs qui suivent, les sommes portent sur $\Gamma_0(p) \backslash \mathrm{SL}_2(\mathbb{Z})$. D'après le lemme 3, on a

$$6\, \Lambda_2 \bullet^{\otimes 2} (c \otimes_{\mathbb{Q}} d) = \sum_g \left[(\xi^0(g\tau) \bullet c)(\xi^0(g) \bullet d) - (\xi^0(g) \bullet c)(\xi^0(g\tau) \bullet d) \right].$$

Par bilinéarité de $\bullet$, on peut supposer que c et d sont dans $\mathcal{H}$. Il existe $x = \sum_g \lambda_g g$ et $y = \sum_h \mu_h h$ dans $\mathcal{E}_{\Gamma_0(p)}$ tels que $c = \alpha_{\mathrm{ptes}}(\xi_0(x))$ et $d =$

$\alpha_{\mathrm{ptes}}(\xi_0(y))$. En utilisant le théorème 4 et le corollaire 1, on obtient

$$\begin{aligned}
6\,\Lambda_2 \bullet^{\otimes 2} (c \otimes d) &= \sum_g \big[(\xi^0(g\tau) \bullet \xi_0(x))(\xi^0(g) \bullet \xi_0(y)) \\
&\qquad -(\xi^0(g) \bullet \xi_0(x))(\xi^0(g\tau) \bullet \xi_0(y))\big] \\
&= \sum_g \lambda_{g\tau}\mu_g - \lambda_g \mu_{g\tau} \\
&= 6\, c \bullet d.
\end{aligned}$$

□

Montrons à présent le théorème 1. Comme $\theta^0_{\mathbb{Q}}$ et $\psi_{\mathbb{Q}}$ sont des isomorphismes de $\mathbb{T}_{\mathbb{Q}}$-modules, si $\theta^0_{\mathbb{Q}}(\bar{\Delta}^0_2) = \psi_{\mathbb{Q}}(\bar{\Lambda}^0_2)$ alors $\bar{\Delta}^0_2$ engendre $\mathcal{P}^0_{\mathbb{Q}} \otimes_{\mathbb{T}_{\mathbb{Q}}} \mathcal{P}^0_{\mathbb{Q}}$ si et seulement si $\bar{\Lambda}^0_2$ engendre $\mathcal{H}^+_{\mathbb{Q}} \otimes_{\mathbb{T}_{\mathbb{Q}}} \mathcal{H}^-_{\mathbb{Q}}$. Cependant nous démontrons ces faits de façon indépendante.

Soit f une forme primitive de poids 2 pour $\Gamma_0(p)$. La proposition précédente et (24) montrent que

$$\begin{aligned}
\mathbf{1}_f(\bar{\Delta}^0_2) &= \mathbf{1}_f(\bar{\Delta}_2) \\
&= \frac{\langle \Delta_2, a_f \otimes_{\mathbb{Q}} a_f\rangle^{\otimes 2}}{\langle a_f \otimes_{\mathbb{Q}} a_f, a_f \otimes_{\mathbb{Q}} a_f\rangle^{\otimes 2}}\, a_f \otimes_{\mathbb{T}_{\mathbb{Q}}} a_f \\
&= \frac{1}{\langle a_f, a_f\rangle}\, a_f \otimes_{\mathbb{T}_{\bar{\mathbb{Q}}}} a_f.
\end{aligned}$$

En particulier $\mathbf{1}_f\bar{\Delta}^0_2$ est non nul pour toute forme primitive f. Par conséquent, $\bar{\Delta}^0_2$ engendre le $T_{\mathbb{Q}}$-module libre $\mathcal{P}^0_{\mathbb{Q}} \otimes_{\mathbb{T}_{\mathbb{Q}}} \mathcal{P}^0_{\mathbb{Q}}$.

De même, on a

$$\begin{aligned}
\mathbf{1}_f(\bar{\Lambda}^0_2) &= \mathbf{1}_f(\bar{\Lambda}_2) \\
&= \frac{\Lambda_2 \bullet^{\otimes 2} (d_f \otimes_{\mathbb{Q}} c_f)}{(c_f \otimes_{\mathbb{Q}} d_f) \bullet^{\otimes 2} (d_f \otimes_{\mathbb{Q}} c_f)}\, c_f \otimes_{\mathbb{T}_{\mathbb{Q}}} d_f \\
&= \frac{1}{c_f \bullet d_f}\, c_f \otimes_{\mathbb{T}_{\bar{\mathbb{Q}}}} d_f.
\end{aligned}$$

Cela montre que $\bar{\Lambda}^0_2$ engendre $\mathcal{H}^+_{\mathbb{Q}} \otimes_{\mathbb{T}_{\mathbb{Q}}} \mathcal{H}^-_{\mathbb{Q}}$.

De plus, la forme modulaire $\mathbf{1}_f\ \theta^0_{\bar{\mathbb{Q}}}(\bar{\Delta}^0_2) = \theta^0_{\bar{\mathbb{Q}}}(\mathbf{1}_f\bar{\Delta}^0_2)$ admet pour q-développement

$$\sum_{m\geq 1} \frac{\langle T_m a_f, a_f\rangle}{\langle a_f, a_f\rangle} q^m = \sum_{m\geq 1} a_m(f) q^m.$$

On en déduit que $\mathbf{1}_f\ \theta^0_{\bar{\mathbb{Q}}}(\bar{\Delta}^0_2) = f$.

De façon analogue, la forme modulaire $\mathbf{1}_f\ \psi_{\bar{\mathbb{Q}}}(\bar{\Lambda}^0_2)$ a pour q-développement $\sum_{m\geq 1} \frac{T_m c_f \bullet d_f}{c_f \bullet d_f} q^m$. Par conséquent $\mathbf{1}_f\ \psi_{\bar{\mathbb{Q}}}(\bar{\Lambda}^0_2) = f$.

Cela termine la démonstration du théorème 1.

5 Valeurs spéciales de fonctions L de formes modulaires

5.1 Formule de Gross

Soit $D > 0$ un entier. Rappelons que γ_D désigne le D-ième élément de Gross (voir (1)). On suppose désormais que $-D$ est un discriminant quadratique imaginaire (c'est-à-dire le discriminant d'un ordre d'un corps quadratique imaginaire). Dans le cas contraire on a en effet $\gamma_D = 0$.

Soient R un ordre maximal de $\mathcal{B}$ et $\mathcal{O}$ un ordre quadratique. On rappelle qu'un *plongement optimal de* $\mathcal{O}$ *dans* R est un morphisme d'algèbres $\sigma : \mathcal{O} \otimes \mathbb{Q} \hookrightarrow \mathcal{B}$ tel que $\sigma(\mathcal{O} \otimes \mathbb{Q}) \cap R = \sigma(\mathcal{O})$. Un corps quadratique L se plonge dans l'algèbre de quaternions $\mathcal{B}$ ramifié en p et à l'infini si et seulement si p est inerte ou ramifié dans L (voir par exemple [18]). On en déduit que $\gamma_D = 0$ si p est décomposé dans $\mathbb{Q}(\sqrt{-D})$.

Soit $f \in \mathrm{S}_2(\Gamma_0(p))$ une forme primitive de développement de Fourier à l'infini $f = \sum_{m \geq 1} a_m(f) q^m$. Pour χ caractère primitif de conducteur r, la série $\sum_{m \geq 1} a_m(f)\chi(m) q^m$ définit une forme modulaire de poids 2 que l'on note $f \otimes \chi$. Lorsque r est premier à p, cette forme modulaire est primitive de niveau pr^2 (voir [14] 4.3).

On suppose désormais que $-D$ est un discriminant quadratique imaginaire premier à p. Rappelons que l'on note $\varepsilon_D = \left(\frac{-D}{\cdot}\right)$ le caractère quadratique non trivial de $\mathrm{Gal}(\mathbb{Q}(\sqrt{-D})/\mathbb{Q})$.

La formule suivante a été démontrée par Gross [4] dans le cas des discriminants premiers et généralisée par Zhang [20].

Théorème 7 (Gross-Zhang) *On a*

$$L(f, 1) L(f \otimes \varepsilon_D, 1) = \frac{(f, f)}{\sqrt{D}} \langle \gamma_D^f, \gamma_D^f \rangle.$$

Lorsque p est décomposé dans $\mathbb{Q}(\sqrt{-D})$, chacun des membres de l'égalité du théorème 7 est nul. On suppose donc désormais que p est inerte dans $\mathbb{Q}(\sqrt{-D})$.

5.2 Interprétation : carré tensoriel des éléments de Gross

Dans ce paragraphe, nous démontrons le théorème 2 énoncé dans l'introduction.

L'homomorphisme injectif de $\mathbb{T}$-modules F (voir (7)) induit un isomorphisme $\mathbb{T}$-linéaire de $\mathbb{R}$-espaces vectoriels :

$$F_{\mathbb{R}} : \mathcal{H}_{\mathbb{R}} \xrightarrow{\sim} \mathrm{Hom}_{\mathbb{C}}(H^0(X, \Omega^1), \mathbb{C}).$$

L'élément d'enroulement e de Mazur est l'antécédent de $\omega \mapsto -\int_{\{0,\infty\}} \omega$ par $F_{\mathbb{R}}$ (voir [9] (18.5)). Cette définition coïncide avec celle donnée dans l'introduction car pour toute forme primitive f, on a (voir [8] théorème 4.1)

$$L(f, 1) = [e, \omega_f]. \tag{29}$$

L'élément d'enroulement e est en fait un élément de $\mathcal{H}_{\mathbb{Q}}^{+}$ (voir [9] lemme 18.6).

Soient $r > 0$ un entier premier à p et χ un caractère primitif modulo r. Notons $g(\chi) = \sum_{b \mod r} \chi(b) e^{2i\pi b/r}$ la somme de Gauss associée à χ. Considérons le symbole modulaire suivant :

$$e_\chi = \sum_{b \mod r} \bar{\chi}(b) \left\{ -\frac{b}{r}, \infty \right\} \in \mathcal{H}_{\mathbb{C}}^{\mathrm{ptes}}. \tag{30}$$

Un calcul classique (se reporter[4] à [8] théorème 4.2) montre que

$$L(f \otimes \chi, 1) = \frac{-g(\chi)}{r} [e_\chi, \omega_f]. \tag{31}$$

C'est pourquoi on appelle e_χ l'*élément d'enroulement tordu par le caractère* χ.

Le caractère ε_D est impair, primitif de conducteur D et vérifie $g(\varepsilon_D) = i\sqrt{D}$. L'élément e_D défini dans l'introduction n'est autre que $e_{\varepsilon_D} = \sum_{b \mod D} \varepsilon_D(b) \left\{ -\frac{b}{D}, \infty \right\}$.

Lemme 4 *On a $e_\chi \in \mathcal{H}_{\mathbb{Z}[\chi]}$. Plus précisément, $e_\chi \in \mathcal{H}_{\mathbb{Z}[\chi]}^{-}$ si χ est impair et $e_\chi \in \mathcal{H}_{\mathbb{Z}[\chi]}^{+}$ si χ est pair.*

Démonstration. Notons $[\frac{r}{s}]$ la classe d'un élément $\frac{r}{s} \in \mathbb{P}^1(\mathbb{Q})$ modulo $\Gamma_0(p)$. D'après [8] proposition 2.2, on peut choisir un système $\{[1; 1], [p; 1]\}$ de représentants de $\Gamma_0(p)\backslash\mathbb{P}^1(\mathbb{Q})$ tel que, pour r et s entiers

$$[\infty] = [p\,;\,1], \qquad \left[\frac{r}{s}\right] = \begin{cases} [p\,;\,1] & \text{si } p \mid s, \\ [1\,;\,1] & \text{sinon.} \end{cases}$$

Pour tout caractère χ, le bord de e_χ est

$$\beta(e_\chi) = \sum_{b \mod r} \bar{\chi}(b)([\infty]) - \sum_{b \mod r} \bar{\chi}(b) \left(\left[\frac{-b}{r} \right] \right) = 0.$$

[4] Avec les notations adoptées par Manin on a $L(f \otimes \chi, s) = -L_{\omega_f, \chi}(s)$.

Donc $e_\chi \in \mathcal{H}_{\mathbb{Z}[\chi]}$ (car $\mathcal{H}$ est le noyau de l'application bord et $\mathbb{Z}[\chi]$ est plat).

De plus, l'image de e_χ sous l'action de la conjugaison complexe est

$$\overline{e_\chi} = \sum_{b \mod r} \bar{\chi}(b) \left\{ \frac{b}{r}, \infty \right\} = \begin{cases} -\displaystyle\sum_{a \mod r} \bar{\chi}(a) \left\{ -\frac{a}{r}, \infty \right\} & \text{si } \chi \text{ est impair} \\ \displaystyle\sum_{a \mod r} \bar{\chi}(a) \left\{ -\frac{a}{r}, \infty \right\} & \text{si } \chi \text{ est pair.} \end{cases}$$

Ceci termine la démonstration du lemme. $\square$

Démontrons à présent le théorème 2.

Soit f une forme primitive de poids 2 pour $\Gamma_0(p)$.

La forme modulaire $\mathbf{1}_f\ \theta^0_{\bar{\mathbb{Q}}}(\gamma^0_D \otimes_{\mathbb{T}_{\bar{\mathbb{Q}}}} \gamma^0_D) = \theta_{\bar{\mathbb{Q}}}(\gamma^f_D \otimes_{\mathbb{T}_{\bar{\mathbb{Q}}}} \gamma^f_D)$ a pour q-développement

$$\begin{aligned} \sum_{m \geq 1} \langle \gamma^f_D, T_m \gamma^f_D \rangle q^m &= \sum_{m \geq 1} \langle \gamma^f_D, \gamma^f_D \rangle a_m(f) q^m \\ &= \langle \gamma^f_D, \gamma^f_D \rangle f. \end{aligned}$$

D'après la formule de Gross-Zhang (théorème 7), on a donc

$$\mathbf{1}_f\ \theta^0_{\bar{\mathbb{Q}}}(\gamma^0_D \otimes_{\mathbb{T}_{\bar{\mathbb{Q}}}} \gamma^0_D) = \frac{\sqrt{D}\ L(f,1)L(f \otimes \varepsilon_D, 1)}{(f,f)}\ f.$$

De façon analogue, $\mathbf{1}_f \psi_{\bar{\mathbb{Q}}}(e \otimes_{\mathbb{T}_{\bar{\mathbb{Q}}}} e_D) = \psi_{\bar{\mathbb{Q}}}(e^f \otimes_{\mathbb{T}_{\bar{\mathbb{Q}}}} e^f_D)$ admet pour q-développement

$$\begin{aligned} \sum_{m \geq 1} (T_m e^f \bullet e^f_D) q^m &= \sum_{m \geq 1} (e^f \bullet e^f_D) a_m(f) q^m \\ &= (e^f \bullet e^f_D)\ f. \end{aligned}$$

Choisissons ici les générateurs $\tilde{c}_f$ de $\mathcal{H}^{+f}_{\mathbb{C}}$ et $\tilde{d}_f$ de $\mathcal{H}^{-f}_{\mathbb{C}}$ associés à la forme différentielle holomorphe ω_f (voir le paragraphe 4.1.3). On a

$$e^f \bullet e^f_D = \frac{(e \bullet \tilde{d}_f)(e_D \bullet \tilde{c}_f)}{\tilde{d}_f \bullet \tilde{c}_f}.$$

Or d'après (29), $e \bullet \tilde{d}_f = [e, \bar{\omega}_f] = \overline{L(f,1)} = L(f,1)$ car $L(f,1) \in \mathbb{R}$, et d'après (31), $e_D \bullet \tilde{c}_f = [e_D, \omega_f] = i\sqrt{D}\ L(f \otimes \varepsilon_D, 1)$. Enfin on rappelle que $\tilde{d}_f \bullet \tilde{c}_f = i(f,f)$ (voir (20)). On obtient finalement l'égalité

$$e^f \bullet e^f_D = \frac{\sqrt{D}\ L(f,1)L(f \otimes \varepsilon_D, 1)}{(f,f)}.$$

Ceci achève la démonstration du théorème 2.

5.3 Application : analogue quadratique de la formule d'Eichler

D'après le théorème 2, on a

$$\langle \gamma_D^0, T_m \gamma_D^0 \rangle = e \bullet T_m e_D \quad (m \geq 1).$$

Nous nous proposons de calculer chacun des membres de l'égalité précédente pour $m = 1$. Ceci permet d'établir la formule pour $\sum_{i=0}^{g} h_i(-D)^2 w_i$ énoncée dans le théorème 3.

5.3.1 Calcul de $\langle \gamma_D^0, \gamma_D^0 \rangle$

Lemme 5 *On a*

$$\langle \gamma_D^0, \gamma_D^0 \rangle = \frac{1}{4u(-D)^2} \left[\sum_{i=0}^{g} h_i(-D)^2 w_i - \frac{48}{(p-1)} h(-D)^2 \right].$$

Démonstration. On a

$$\begin{aligned} \langle \gamma_D^0, \gamma_D^0 \rangle &= \langle \gamma_D, \gamma_D \rangle - \frac{12(\deg \gamma_D)^2}{p-1} \\ &= \frac{1}{4u(-D)^2} \sum_{i=0}^{g} h_i(-D)^2 w_i - \frac{12(\deg \gamma_D)^2}{p-1}. \end{aligned}$$

De plus, puisque p est inerte dans $\mathbb{Q}(\sqrt{-D})$, la formule d'Eichler (se reporter à l'introduction ou à [4] (1.12)) donne :

$$2u(-D) \deg \ \gamma_D = \sum_{i=0}^{g} h_i(-D) = 2h(-D).$$

On en déduit le lemme. □

5.3.2 Produit d'intersection des éléments d'enroulement

Soit $r > 0$ un entier. L'ensemble $\mathcal{X}'_r$ et les entiers b_M modulo r ($M \in \mathcal{X}'_r$) de la proposition ci-dessous ont été définis dans l'introduction (voir (2) et (3)).

Proposition 4 *Pour tout caractère primitif χ modulo r, on a*

$$e_\chi = \sum_{M = \left(\begin{smallmatrix} u & v \\ w & t \end{smallmatrix}\right) \in \mathcal{X}'_r} \bar{\chi}(b_M) \, \xi^0\left(\frac{w}{t}\right).$$

Démonstration. Pour $0 \le b < d$, d divisant r, notons

$$m_{d,b} = \begin{pmatrix} d & b \\ 0 & \frac{r}{d} \end{pmatrix}, \quad w_{d,b} = m_{d,b}^{-1} = \begin{pmatrix} \frac{1}{d} & -\frac{b}{r} \\ 0 & \frac{d}{r} \end{pmatrix} \quad \text{et} \quad n_{d,b} = \begin{pmatrix} \frac{r}{d} & 0 \\ b & d \end{pmatrix}.$$

L'ensemble $\{m_{d,b},\ 0 \le b < d,\ d \mid r\}$ (resp. $\{n_{d,b},\ 0 \le b < d,\ d \mid r\}$) est un système de représentants de $\mathrm{M}_2(\mathbb{Z})_r/\mathrm{SL}_2(\mathbb{Z})$ dont les éléments sont les seules matrices $M = \left(\begin{smallmatrix} u & v \\ w & t \end{smallmatrix}\right)$ de $\mathcal{X}'_r$ telles que $w = 0$ *i.e.* $M\infty = \infty$ (resp. telles que $v = 0$ *i.e.* $M0 = 0$). Notons $C(d,b) = m_{d,b}\mathrm{SL}_2(\mathbb{Z})$ la classe d'équivalence de $m_{d,b}$. La classe $C(d,b)$ est l'ensemble des matrices $M = \left(\begin{smallmatrix} u & v \\ w & t \end{smallmatrix}\right)$ telles que

$$w_{d,b}M = \begin{pmatrix} \frac{u}{d} - \frac{bw}{r} & \frac{v}{d} - \frac{bt}{r} \\ \frac{dw}{r} & \frac{dt}{r} \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}). \tag{32}$$

Pour tout $M \in C(d,b)$, on a donc

$$\xi^0\left(\frac{w}{t}\right) = \xi^0\left(\Gamma_0(p).w_{d,b}M\right) = \{w_{d,b}M.0, w_{d,b}M.\infty\}.$$

Notons

$$S_\chi = \sum_{M=\left(\begin{smallmatrix} u & v \\ w & t \end{smallmatrix}\right) \in \mathcal{X}'_r} \bar{\chi}(b_M)\xi^0(\frac{w}{t}).$$

Nous allons montrer que S_χ est égal à e_χ. Notons $\mathrm{Div}^0(\mathbb{P}^1(\mathbb{Q}))$ le groupe des diviseurs de degré nul à support dans $\mathbb{P}^1(\mathbb{Q})$. On dispose d'une application

$$\begin{array}{cccc} \iota : & \mathrm{Div}^0(\mathbb{P}^1(\mathbb{Q})) & \longrightarrow & \mathcal{H}^{\mathrm{ptes}} \\ & (\alpha) - (\beta) & \longmapsto & \{\alpha, \beta\} \end{array}.$$

Il suffit d'établir que S_χ et e_χ ont un antécédent commun par ι.

Soit $M \in \mathrm{M}_2(\mathbb{Z})_r$. Il existe b et d avec $0 \le b < d$, $d \mid r$, tels que $M \in C(d,b)$. D'après (32), l'entier r/d divise alors t et w. Si $M \in \mathcal{X}'_r$, on obtient $d = r$, car $(w,t) = 1$. Par conséquent

$$\mathcal{X}'_r = \bigcup_{0 \le b < r} (\mathcal{X}'_r \cap C(r,b)).$$

De plus $M = \left(\begin{smallmatrix} u & v \\ w & t \end{smallmatrix}\right) \in C(r,b)$ si et seulement si $u \equiv bw \pmod r$ et $v \equiv bt \pmod r$. En particulier, si $M \in C(r,b)$ alors $b_M \equiv b \pmod r$.

On pose $D(r,b) = \mathcal{X}'_r \cap C(r,b)$.

Ce qui précède montre que

$$S_\chi = \sum_{0 \le b < r} \sum_{M \in D(r,b)} \bar{\chi}(b)\{w_{r,b}M.0, w_{r,b}M.\infty\}.$$

Donc

$$S_\chi = \iota\left(\sum_{0\leq b<r}\bar{\chi}(b)\left[\sum_{M\in D(r,b)}(w_{r,b}M.0) - \sum_{M\in D(r,b)}(w_{r,b}M.\infty)\right]\right).$$

Soit

$$M = \begin{pmatrix} u & v \\ w & t \end{pmatrix} \in \mathcal{X}_r'.$$

Si $M\infty \neq \infty$, il existe une unique matrice $A(M) \in \mathcal{X}_r' \cap M\mathrm{SL}_2(\mathbb{Z})$ telle que $M\infty = A(M)0$: c'est la matrice

$$A(M) = M\begin{pmatrix} m(M) & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} um(M) - v & u \\ wm(M) - t & w \end{pmatrix}$$

où $m(M)$ est le plus petit entier supérieur à t/w. Remarquons que $u \neq 0$ car $M \in \mathcal{X}_r'$, par conséquent $A(M)0 \neq 0$.

Si

$$M' = \begin{pmatrix} u' & v' \\ w' & t' \end{pmatrix} \in \mathcal{X}_r'$$

est telle que $M'0 \neq 0$, il existe une unique matrice $B(M') \in \mathcal{X}_r' \cap M'\mathrm{SL}_2(\mathbb{Z})$, telle que $M'0 = B(M')\infty$: c'est la matrice

$$B(M') = M'\begin{pmatrix} 0 & -1 \\ 1 & n(M') \end{pmatrix} = \begin{pmatrix} v' & -u' + v'n(M') \\ t' & -w' + t'n(M') \end{pmatrix}$$

où $n(M')$ est le plus petit entier supérieur à u'/v'. On a $B(M')\infty \neq \infty$.

Lemme 6 *Soit $0 \leq b < r$. L'application A définit une bijection de*

$$D(r,b)\backslash\{M\,;\, M\infty = \infty\} = D(r,b)\backslash\{m_{r,b}\}$$

vers

$$D(r,b)\backslash\{M\,;\, M0 = 0\} = D(r,b)\backslash\{n_{r,b}\}$$

de bijection réciproque l'application B.

Démonstration. Soient $M = \left(\begin{smallmatrix} u & v \\ w & t \end{smallmatrix}\right), \in \mathcal{X}_r'$ telles que $M\infty \neq \infty$. On a

$$B(A(M)) = \begin{pmatrix} u & -um + v + un \\ w & -wm + t + wn \end{pmatrix}$$

où $m = m(M)$ et $n = n(A(M))$. L'entier n est le plus petit entier supérieur à $m - \frac{v}{u}$. Or $0 \leq \frac{v}{u} < 1$, donc $n = m$, et on en déduit que $B(A(M)) = M$.

Considérons à présent $M' = \begin{pmatrix} u' & v' \\ w' & t' \end{pmatrix} \in \mathcal{X}'_r$ telle que $M'0 \neq 0$. De façon analogue, on a

$$A(B(M')) = \begin{pmatrix} v'm' + u' - v'n' & v' \\ t'm' + w' - t'n' & t' \end{pmatrix}$$

où $n' = n(M')$ et $m' = m(B(M'))$. L'entier m' est le plus petit entier supérieur à $n' - \frac{w'}{t'}$. Or $0 \leq \frac{w'}{t'} < 1$ donc $n' = m'$ et $A(B(M')) = M'$.

Supposons que $M \in D(r,b)\backslash\{m_{r,b}\}$, autrement dit $u \equiv bw \pmod r$ et $v \equiv bt \pmod r$. On a alors $um(M) - v \equiv b(wm(M) - t) \pmod r$, ce qui prouve que $A(M)$ est dans $D(r,b)\backslash\{n_{r,b}\}$. $\square$

Le lemme précédent montre que

$$\begin{aligned}
S_\chi &= \iota\left(\sum_{0\leq b<r} \bar{\chi}(b)\left[\sum_{M'\in D(r,b)} (w_{r,b}M'.0) - \sum_{M\in D(r,b)} (w_{r,b}M.\infty)\right]\right) \\
&= \iota\left(\sum_{0\leq b<r} \bar{\chi}(b)\left[\sum_{\substack{M'\in D(r,b)\\ M'0=0}} (w_{r,b}M'.0) - \sum_{\substack{M'\in D(r,b)\\ M'\infty=\infty}} (w_{r,b}M.\infty)\right]\right. \\
&\quad \left. + \sum_{0\leq b<r} \bar{\chi}(b)\left[\sum_{\substack{M'\in D(r,b)\\ M'0\neq 0}} (w_{r,b}M'.0) - \sum_{\substack{M'\in D(r,b)\\ M'\infty\neq\infty}} (w_{r,b}M.\infty)\right]\right) \\
&= \iota\left(\sum_{0\leq b<r} \bar{\chi}(b) \sum_{\substack{M'\in D(r,b)\\ M'0=0}} (w_{r,b}.0) - \sum_{0\leq b<r} \bar{\chi}(b) \sum_{\substack{M'\in D(r,b)\\ M'\infty=\infty}} (w_{r,b}M.\infty)\right).
\end{aligned}$$

On rappelle que les seuls éléments $M \in \mathcal{X}'_r$ tels que $M0 = 0$ (resp. $M\infty = \infty$) sont les matrices $n_{d,a}$ (resp. $m(d,a)$) avec $0 \leq a < d$ et $d \mid r$, et que ces matrices forment un système de représentants pour $\mathrm{M}_2(\mathbb{Z})_r/\mathrm{SL}_2(\mathbb{Z})$. Par conséquent,

$$S_\chi = \iota\left(\sum_{0\leq b<r} \bar{\chi}(b)\left(-\frac{b}{r}\right) - \sum_{0\leq b<r} \bar{\chi}(b)(\infty)\right). \tag{33}$$

Comme $\sum_{0\leq b<r} \bar{\chi}(b) = 0$, on a finalement

$$S_\chi = e_\chi,$$

d'où le résultat annoncé dans la proposition 4. $\square$

Remarque 2 Puisque $e_\chi \in \mathcal{H}_\mathbb{Q}$, les contributions de $\xi^0(0)$ et $\xi^0(\infty)$ dans S_χ s'annulent.

Pour u, v deux entiers premiers entre eux, $v > 0$, la *somme de Dedekind* $S(u, v)$ est donnée par

$$S(u,v) = \sum_{h=0}^{v-1} \bar{B}_1\left(\frac{h}{v}\right) \bar{B}_1\left(\frac{uh}{v}\right) \tag{34}$$

où $\bar{B}_1$ est la fonction périodique de période 1 définie par $\bar{B}_1(x) = x - 1/2$ si $x \in]0, 1[$ et $\bar{B}_1(0) = 0$ (voir par exemple [16]). Rappelons que pour $k \in \{1, \ldots, p-1\}$, on note k_* l'unique élément de $\{1, \ldots, p-1\}$ tel que $kk_* \equiv -1 \pmod p$.

Corollaire 3 *On a*

$$e \bullet e_\chi = \sum_{k=1}^{p-1} \sum_{\substack{M=\left(\begin{smallmatrix} u & v \\ w & t \end{smallmatrix}\right) \in \mathcal{X}'_r \\ w \equiv tk \mod p}} \bar{\chi}(b_M) \left(\frac{k_* - k}{p} - 12\frac{S(k,p)}{p-1} \right).$$

Démonstration. Ce corollaire se déduit de la proposition 4 et de la formule suivante due à Merel [11] :

$$(p-1)e \bullet \xi^0(k) = \frac{k - k_*}{p}(1-p) - 12S(k,p) \qquad (k \in \{1, \ldots, p-1\}).$$

$\square$

5.3.3 Application : preuve du théorème 3

D'après le lemme 5, on a

$$\sum_{i=0}^{g} h_i(-D)^2 w_i = 4u(-D)^2 \langle \gamma_D^0, \gamma_D^0 \rangle + \frac{48}{p-1} h(-D)^2.$$

Or, le théorème 2 donne l'égalité :

$$\langle \gamma_D^0, \gamma_D^0 \rangle = e \bullet e_D.$$

Le corollaire 3 appliqué à $\chi = \varepsilon_D$ montre alors le théorème 3.

5.3.4 Remarque : une autre approche pour le calcul de $e \bullet e_D$

Soit $z \in \mathfrak{H}$. Pour $g \in \Gamma_0(p)$, notons c_g la classe dans $\mathcal{H}_{\text{ptes}}$ de l'image dans Y d'une géodésique de $\mathfrak{H}$ reliant z à gz. La classe c_g est indépendante du choix de z. L'application $g \mapsto c_g$ définit un homomorphisme surjectif de groupes de $\Gamma_0(p)$ dans $\mathcal{H}_{\text{ptes}}$.

Pour tout entier b tel que $0 \leq b < D$ et $(b, D) = 1$, on note

$$g_b = \left(\begin{smallmatrix} u_b & b \\ w_b & D \end{smallmatrix}\right)$$

l'unique matrice de $\Gamma_0(p)$ telle que $0 \leq \frac{w_b}{p} < D$. Lorsque $b \in [0, D[$ n'est pas premier à D, on note $g_b = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$.

Posons dans $\mathcal{H}_{\text{ptes}}$

$$\widetilde{e_D} = \sum_{b=0}^{D-1} \varepsilon_D(b) c_{g_b}.$$

L'image de $\widetilde{e_D}$ par la surjection canonique $\alpha_{\text{ptes}} : \mathcal{H}_{\text{ptes}} \twoheadrightarrow \mathcal{H}$ est égale à e_D. En effet, pour b premier à D, l'image de c_{g_b} par α_{ptes} est égale à la classe de $\{0, g_b 0\} = \{0, \frac{b}{D}\}$ dans $\mathcal{H}$ et ε_D est impair ; cela entraîne

$$\alpha_{\text{ptes}}(\widetilde{e_D}) = \sum_{b \in \mathbb{Z}, (b,D)=1} \varepsilon_D(b) \left\{0, \frac{b}{D}\right\} = e_D.$$

Rappelons que l'*élément d'Eisenstein* $\mathcal{E}$ est l'unique élément de $\mathcal{H}_{\mathbb{Q}}^{\text{ptes}}$ de bord $(p-1)\left((\Gamma_0(p)\infty) - (\Gamma_0(p)0)\right)$ dans $\mathbb{Z}[\text{ptes}]$ et tel que

$$T_m \mathcal{E} = \sigma'(m) \mathcal{E}$$

(voir [11]). On a l'égalité suivante (voir *loc. cit.* lemme 1)

$$(p-1)e = \mathcal{E} - (p-1)\{0, \infty\}.$$

Par conséquent, on a

$$(p-1)e \bullet e_D = \mathcal{E} \bullet \widetilde{e_D} - (p-1)\{0, \infty\} \bullet \widetilde{e_D}.$$

Soit B_{1,ε_D} le premier nombre de Bernoulli généralisé associé au caractère ε_D.

Proposition 5 *On a*

$$\mathcal{E} \bullet \widetilde{e_D} = 2(p-1)\frac{h(-D)}{u(-D)} - 24\frac{h(-D)^2}{u(-D)^2}.$$

Démonstration. Notons R l'application à valeurs dans $\mathbb{Z}$ qui à une matrice $\left(\begin{smallmatrix} u & v \\ w & t \end{smallmatrix}\right) \in \Gamma_0(p)$ associe $(p-1)\frac{v}{t}$ si $w = 0$ et

$$(p-1)\frac{u+t}{w} + 12\frac{w}{|w|}\left(S(t,|w|) - S\left(t, \left|\frac{w}{p}\right|\right)\right)$$

sinon. Cette application est un homomorphisme de groupes appelé *homomorphisme de Rademacher* (voir [15] et [11]). On a (*loc. cit*)

$$R(g) = -\mathcal{E} \bullet c_g \quad (g \in \Gamma_0(p)).$$

On en déduit

$$\begin{aligned} \mathcal{E} \bullet \widetilde{e_D} &= \sum_{b=0}^{D-1} \varepsilon_D(b)\ \mathcal{E} \bullet c_{g_b} \\ &= -\sum_{b=0}^{D-1} \varepsilon_D(b)\ R(g_b). \end{aligned}$$

Or, puisque $D \neq 1$, on a $w_b \neq 0$ pour tout $b \in \{0, \ldots, D-1\}$. Par conséquent

$$\begin{aligned} R(g_b) &= (p-1)\frac{u_b + D}{w_b} + 12\left(S(D, w_b) - S\left(D, \frac{w_b}{p}\right)\right) \\ &= (p-1)\left(\frac{b}{D} + \frac{1}{Dw_b} + \frac{D}{w_b}\right) + 12\left(S(D, w_b) - S\left(D, \frac{w_b}{p}\right)\right) \end{aligned}$$

car $u_b D - w_b b = 1$ et $w_b > 0$.

Rappelons la loi de réciprocité de Dedekind (voir par exemple [16] théorème 1) : pour $u > 0$ et $v > 0$ deux entiers premiers entre eux, on a

$$12\,(S(u,v) + S(v,u)) = -3 + \frac{u}{v} + \frac{v}{u} + \frac{1}{uv}. \tag{35}$$

On a également les propriétés élémentaires suivantes :

$$S(-u,v) = -S(u,v) \quad \text{et} \quad S(u',v) = S(u,v), \tag{36}$$

où $u' > 0$ est un entier tel que $uu' \equiv 1 \pmod{v}$.

On a $bw_b \equiv -1 \pmod{D}$. D'après (35) et (36), on a alors

$$\begin{aligned} 12\ S(D, w_b) &= -12\ S(w_b, D) - 3 + \frac{D}{w_b} + \frac{w_b}{D} + \frac{1}{Dw_b} \\ &= 12\ S(b, D) - 3 + \frac{D}{w_b} + \frac{w_b}{D} + \frac{1}{Dw_b} \end{aligned}$$

et

$$\begin{aligned}12\,S\left(D,\frac{w_b}{p}\right) &= -12\,S\left(\frac{w_b}{p},D\right)-3+\frac{w_b}{Dp}+\frac{Dp}{w_b}+\frac{p}{Dw_b}\\ &= 12\,S(bp,D)-3+\frac{w_b}{Dp}+\frac{Dp}{w_b}+\frac{p}{Dw_b}.\end{aligned}$$

Cela donne

$$\begin{aligned}R(g_b) &= (p-1)\left(\frac{b}{D}+\frac{1}{Dw_b}+\frac{D}{w_b}\right)+\frac{D}{w_b}+\frac{w_b}{D}+\frac{1}{Dw_b}-\frac{w_b}{Dp}-\frac{Dp}{w_b}-\frac{p}{Dw_b}\\ &\quad +12\left(S(b,D)-S(bp,D)\right)\\ &= (p-1)\frac{b}{D}+\frac{w_b}{D}-\frac{w_b}{Dp}+12\left(S(b,D)-S(bp,D)\right)\\ &= \frac{p-1}{D}\left(b+\frac{w_b}{p}\right)+12\left(S(b,D)-S(bp,D)\right)\end{aligned}$$

D'où

$$\mathcal{E}\bullet\widetilde{e_D}=\frac{1-p}{D}\sum_{b=0}^{D-1}\varepsilon_D(b)b+\frac{1-p}{D}\sum_{b=0}^{D-1}\varepsilon_D(b)\frac{w_b}{p}+12\sum_{b=0}^{D-1}\varepsilon_D(b)\left(S(bp,D)-S(b,D)\right).$$

On rappelle l'égalité (voir par exemple [19] proposition 4.1) :

$$\sum_{b=0}^{D-1}\varepsilon_D(b)\bar{B}_1\left(\frac{b}{D}\right)=\sum_{b=0}^{D-1}\varepsilon_D(b)b=DB_{1,\varepsilon_D}.$$

Pour $b\in\{0,\dots,D-1\}$, posons $a=\frac{w_b}{p}$. L'entier $a\in\{0,\dots,D-1\}$ est tel que $w_a=bp$. En effet $\left(\begin{smallmatrix}u_b & \frac{w_b}{p}\\ bp & D\end{smallmatrix}\right)\in\Gamma_0(p)$ et $bp\in\{0,p,\dots,(D-1)p\}$. L'application $b\mapsto\frac{w_b}{p}$ définit donc une permutation de $\{0,\dots,p-1\}$. On a alors

$$\begin{aligned}\sum_{b=0}^{D-1}\varepsilon_D(b)\frac{w_b}{p} &= \sum_{b=0}^{D-1}\varepsilon_D(\frac{w_b}{p})b\\ &= -\sum_{b=0}^{D-1}\varepsilon_D(bp)b\\ &= -\left(\frac{-D}{p}\right)\sum_{b=0}^{D-1}\varepsilon_D(b)b\\ &= DB_{1,\varepsilon_D}.\end{aligned}$$

Par ailleurs, on a

$$\begin{aligned}
\sum_{b=0}^{D-1} \varepsilon_D(b) S(b,D) &= \sum_{b=0}^{D-1}\sum_{a=0}^{D-1} \varepsilon_D(b) \bar{B}_1\left(\frac{a}{D}\right) \bar{B}_1\left(\frac{ab}{D}\right) \\
&= \sum_{a=0}^{D-1} \varepsilon_D(a) \bar{B}_1\left(\frac{a}{D}\right) \sum_{b=0}^{D-1} \varepsilon_D(ab) \bar{B}_1\left(\frac{ab}{D}\right) \\
&= B_{1,\varepsilon_D}^2.
\end{aligned}$$

De façon analogue, on a

$$\begin{aligned}
\sum_{b=0}^{D-1} \varepsilon_D(b) S(bp,D) &= \sum_{b=0}^{D-1}\sum_{a=0}^{D-1} \varepsilon_D(b) \bar{B}_1\left(\frac{a}{D}\right) \bar{B}_1\left(\frac{abp}{D}\right) \\
&= \varepsilon_D(p) \sum_{a=0}^{D-1} \varepsilon_D(a) \bar{B}_1\left(\frac{a}{D}\right) \sum_{b=0}^{D-1} \varepsilon_D(abp) \bar{B}_1\left(\frac{abp}{D}\right) \\
&= -B_{1,\varepsilon_D}^2.
\end{aligned}$$

On a finalement

$$\mathcal{E} \bullet \widetilde{e_D} \quad = \quad 2(1-p)B_{1,\varepsilon_D} - 24B_{1,\varepsilon_D}^2.$$

Or, en combinant la formule du nombre de classe et les relations entre nombres de Bernoulli et fonctions L de Dirichlet (voir par exemple [19] théorème 4.9) on obtient

$$B_{1,\varepsilon_D} = -\frac{h(-D)}{u(-D)}.$$

On en déduit l'égalité annoncée dans la proposition 5. $\square$

Malheureusement, nous ne savons actuellement pas donner une expression simple pour $\{0,\infty\} \bullet \widetilde{e_D}$. Les observations suivantes fournissent peut-être une piste pour effectuer ce calcul.

Pour $k \in \{1,\dots,p-1\}$, posons

$$W_k = \begin{pmatrix} k_* & -1 \\ 1+kk_* & -k \end{pmatrix} \in \Gamma_0(p). \tag{37}$$

On rappelle que l'ensemble

$$\{\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ p & 1 \end{smallmatrix}\right), W_k, 1 \le k \le p-1\},$$

dit *système de générateurs de Rademacher*, est un système de générateurs de $\Gamma_0(p)$.

On a

$$\{0,\infty\} \bullet c_{W_k} = 0 \quad (k \in \{1,\ldots,p-1\})$$

(voir [11] démonstration du lemme 3). Par ailleurs, on a

$$\{0,\infty\} \bullet c_{\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)} = -1 \quad \text{et} \quad \{0,\infty\} \bullet c_{\left(\begin{smallmatrix}1&0\\p&1\end{smallmatrix}\right)} = 1.$$

Pour $b \in \{0,\ldots,D-1\}$, notons $n_0(b)$ (resp. $n_\infty(b)$) le nombre de $\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$ (resp. $\left(\begin{smallmatrix}1&0\\p&1\end{smallmatrix}\right)$) dans une décomposition de g_b dans le système de générateurs de Rademacher. La différence $n_\infty(b) - n_0(b)$ ne dépend pas de la décomposition choisie et on a

$$\{0,\infty\} \bullet \widetilde{e_D} = \sum_{b=0}^{D-1} \varepsilon_D(b)(n_\infty(b) - n_0(b)).$$

Références

[1] P. Deligne and M. Rapoport. Les schémas de modules de courbes elliptiques. In *Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pages 143–316. Lecture Notes in Math., Vol. 349. Springer, Berlin, 1973.

[2] M. Emerton. Supersingular elliptic curves, theta series and weight two modular forms. *J. Amer. Math. Soc.*, 15(3) :671–714 (electronic), 2002.

[3] P. Griffiths and J. Harris. *Principles of algebraic geometry.* Wiley Classics Library. John Wiley & Sons Inc., New York, 1994. Reprint of the 1978 original.

[4] B. H. Gross. Heights and the special values of L-series. In *Number theory (Montreal, Que., 1985)*, volume 7 of *CMS Conf. Proc.*, pages 115–187. Amer. Math. Soc., Providence, RI, 1987.

[5] B. H. Gross and S. S. Kudla. Heights and the central critical values of triple product L-functions. *Compositio Math.*, 81(2) :143–209, 1992.

[6] D. R. Kohel. Hecke module structure of quaternions. In *Class field theory—its centenary and prospect (Tokyo, 1998)*, volume 30 of *Adv. Stud. Pure Math.*, pages 177–195. Math. Soc. Japan, Tokyo, 2001.

[7] Stephen S. Kudla and John J. Millson. Harmonic differentials and closed geodesics on a Riemann surface. *Invent. Math.*, 54(3) :193–211, 1979.

[8] J. I. Manin. Parabolic points and zeta functions of modular curves. *Izv. Akad. Nauk SSSR Ser. Mat.*, 36 :19–66, 1972.

[9] B. Mazur. Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, (47) :33–186 (1978), 1977.

[10] L. Merel. Homologie des courbes modulaires affines et paramétrisations modulaires. In *Elliptic curves, modular forms, & Fermat's last theorem (Hong Kong, 1993)*, Ser. Number Theory, I, pages 110–130. Internat. Press, Cambridge, MA, 1995.

[11] L. Merel. Bornes pour la torsion des courbes elliptiques sur les corps de nombres. *Invent. Math.*, 124(1-3) :437–449, 1996.

[12] L. Merel. L'accouplement de Weil entre le sous-groupe de Shimura et le sous-groupe cuspidal de $J_0(p)$. *J. Reine Angew. Math.*, 477 :71–115, 1996.

[13] J.-F. Mestre and J. Oesterlé. Courbes elliptiques de conducteur premier, manuscript.

[14] T. Miyake. *Modular forms*. Springer-Verlag, Berlin, 1989. Translated from the Japanese by Yoshitaka Maeda.

[15] H. Rademacher. Zur theorie der modulfunktionen. *J. Reine Angew. Math.*, (167) :312–336, 1931.

[16] H. Rademacher and E. Grosswald. *Dedekind sums*. The Mathematical Association of America, Washington, D.C., 1972. The Carus Mathematical Monographs, No. 16.

[17] M. Raynaud. Jacobienne des courbes modulaires et opérateurs de Hecke. *Astérisque*, (196-197) :9–25 (1992), 1991. Courbes modulaires et courbes de Shimura (Orsay, 1987/1988).

[18] M.-F. Vignéras. *Arithmétique des algèbres de quaternions*, volume 800 of *Lecture Notes in Mathematics*. Springer, Berlin, 1980.

[19] L. C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1997.

[20] S.-W. Zhang. Gross-Zagier formula for GL_2. *Asian J. Math.*, 5(2) :183–290, 2001.