UNIVERSITÉ PIERRE ET MARIE CURIE – PARIS VI
Institut de Mathématiques de Jussieu U. M. R. n° 7586

THÈSE

présentée pour obtenir le titre de

Docteur en Sciences

spécialité : MATHÉMATIQUES

par

Marusia REBOLLEDO

MODULE SUPERSINGULIER ET POINTS RATIONNELS DES COURBES MODULAIRES

Soutenue le 27 septembre 2004 devant le jury composé de :

M. Sebastiaan Edixhoven	(Leiden)	Rapporteur
M. Michael Harris	(Paris 7)	
M. Loïc Merel	(Paris 7)	Directeur
M. Jean-François Mestre	(Paris 7)	Président
M. Jan Nekovar	(Paris 6)	
M. Jacques Tilouine	(Paris 13)	Rapporteur

Remerciements

Je tiens en premier lieu à remercier plus que vivement Loïc Merel qui a su, au long de ces années de DEA puis de doctorat, non seulement diriger mes recherches et me faire part de ses nombreuses idées mais surtout me transmettre sa passion des mathématiques.

C'est pour moi un honneur que Sebastiaan Edixhoven et Jacques Tilouine aient rapporté cette thèse. Leurs remarques claires et encourageantes sont à l'origine de nombreuses améliorations de ce manuscrit.

J'ai rencontré Sebastiaan Edixhoven lors de la soutenance de thèse de Pierre Parent en novembre 1999. L'importance de ses travaux et de ceux de Pierre Parent dans l'élaboration de ma thèse montrent que celle-ci ne pouvait trouver rapporteur plus approprié.

J'ai pu apprécier la disponibilité de Jacques Tilouine qui a su m'accorder du temps pour discuter de ma thèse et me faire part des travaux de Hida généralisant ceux d'Emerton.

Toute ma gratitude revient également à Jean-François Mestre, Jan Nekovar et Michael Harris pour avoir accepté de faire partie du jury de soutenance. Déjà présent dans mon jury de DEA, Jean-François Mestre a toujours été à l'écoute de mes questions quelles qu'elles soient.

Je remercie chaleureusement Pierre Parent, car, comme en témoigne en partie cette thèse, ses travaux, sa disponibilité et son amitié ont été pour moi déterminants.

Ce sont les cours de maîtrise de Gilles Christol qui m'ont conduit vers la théorie des nombres et c'est sur ses conseils que j'ai demandé à Loïc Merel de diriger mes travaux de DEA. Je lui en suis très reconnaissante.

Mon intérêt pour les mathématiques doit également beaucoup aux cours de Terminale de Madame Sauvage, professeur au lycée M. Ravel. Je lui adresse donc ici des remerciements spéciaux.

Je souhaite aussi exprimer ma reconnaissance aux membres des différents laboratoires qui m'ont accueillie au long de ces années et ont contribué à la bonne marche de mon travail tant d'un point de vue scientifique, qu'informatique ou encore administratif.

Tout d'abord aux membres de l'Institut Mathématiques de Jussieu où j'effectue mes études depuis la licence. En particulier Dominique Bernardi, Daniel Bertrand, Gilles Christol, Pierre Colmez, Christophe Cornut, Sinnou David, Joseph Oesterlé, Vincent Maillot, et Michel Waldshmidt qui ont pris le temps d'écouter mes questions ; ainsi que Joël Marchand et Colette Orion qui ont assuré les questions d'ordre matériel ; et enfin aux autres membres de l'Institut dont la solidarité a été par moments essentielle et notamment Charles, Christophe, Esther, Gwendal, Gwenaëlle, Nicolas, Oliver, Samy, Sybille, Yann et de nouveau Vincent.

Ma reconnaissance va ensuite aux membres du laboratoire de mathématiques de l'université Clermont-Ferrand II qui m'ont accueillie dès ma troisième année de monitorat. Je dois notamment à Youssef Amirat, Bernard Brunet et Alain Escassut d'avoir pu être rattachée au laboratoire. L'ambiance chaleureuse qui y règne, propice au travail, doit en particulier beaucoup à Jérome Chabert, Claire Debord, Benjamin Delay, Guillaume Havard, Michaël Heusener, Jean-Marie Lescure, Dominique Manchon, Hervé Oyono, Sylvie Paycha, Claire Schenkel, sans oublier Thierry Lambre dont la passion est à l'origine de notre groupe de travail, mon compagnon de bureau François Gautero, les amis de longue date retrouvés à Clermont : Yanick Heurteaux et François Martin, et enfin François Dumas dont l'amitié m'a toujours été un grand soutien et déborde du contexte mathématique.

Je me dois également de remercier les membres du LLAIC de l'université Clermont-Ferrand I et en particulier Olivier Guinaldo, Marie-Alix Lapadu, Rémi Malgouyres et Malika More pour m'avoir intégrée dans l'équipe cette année. La cordialité dont ils font preuve fut encore une fois essentielle pour la bonne marche des enseignements que j'y ai dispensés.

François Martin et Emmanuelle Tosel ont pris le temps de relire en détail ce manuscrit et ont ainsi contribué à son amélioration ; je leur en suis très reconnaissante.

Enfin, cette thèse n'aurait probablement pas abouti sans le soutien constant de mes plus chers amis, de la famille Hochart, ainsi que de ma famille proche ou éloignée géographiquement. Je leur adresse donc ici d'immenses remerciements.

Des pensées dans le désordre pour Anne-Marie et Jean-Claude et leur générosité inépuisable, Luc, Nicolas et Emmanuelle, Gilles et Sara, Pierre et Angela, les musiciens du lundi soir, Marie et Nicolas, Caroline et Eric, Didier, Fred et Anh Thu, la famille Quinsat sans qui notre acclimatation à Clermont se serait faite plus lentement, ainsi qu'Alvaro et Viera pour leur appui fraternel.

Il va sans dire que mes pensées les plus chères vont à celui qui m'a accompagnée toutes ces années autant dans les moments de bonheur que dans les moments plus difficiles.

A la mémoire de Jorge Araya

A Max

Table des matières

Introduction

Soit $p > 3$ un nombre premier. Les classes d'isomorphisme de courbes elliptiques supersingulières en caractéristique p sont en nombre fini $g+1$ où

$$g = \begin{cases} (p-13)/12 & \text{si } p \equiv 1 \mod 12 \\ (p-5)/12 & \text{si } p \equiv 5 \mod 12 \\ (p-7)/12 & \text{si } p \equiv 7 \mod 12 \\ (p+1)/12 & \text{si } p \equiv 11 \mod 12. \end{cases}$$

Notons $\mathcal{S} = \{x_0, \ldots, x_g\}$ l'ensemble de ces classes. On appelle *module supersingulier* le $\mathbb{Z}$-module libre $\mathcal{P} = \mathbb{Z}[\mathcal{S}]$. On note $\mathcal{P}^0$ le sous-$\mathbb{Z}$-module de $\mathcal{P}$ formé des éléments de degré nul.

Le module supersingulier est muni *a priori* de deux structures algébriques :

1. un accouplement non dégénéré $\langle\ ,\ \rangle : \mathcal{P} \times \mathcal{P} \longrightarrow \mathbb{Z}$ défini par

$$\langle x_i, x_j \rangle = \begin{cases} w_i & \text{si } x_i = x_j \\ 0 & \text{sinon} \end{cases}$$

   où, pour $i \in \{0, \ldots, g\}$, on note w_i la moitié de l'ordre du groupe des automorphismes d'une courbe elliptique E_i dans la classe x_i ;

2. une suite d'opérateurs $(T_m)_{m \geq 1}$ définis sur une classe $x_i = [E_i]$ par

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

   où C parcourt l'ensemble des sous-schémas en groupes d'ordre m de E_i.

Les opérateurs $T_m,\ m \geq 1$, ainsi définis, dits *opérateurs de Hecke,* sont autoadjoints pour l'accouplement $\langle\ ,\ \rangle$. Ces opérateurs engendrent un anneau commutatif $\widetilde{\mathbb{T}}$, appelé *algèbre de Hecke*, qui laisse stable $\mathcal{P}^0$. On note $\mathbb{T}$ le quotient de $\widetilde{\mathbb{T}}$ qui agit fidèlement sur $\mathcal{P}^0$.

On fixe, pour la suite de cette introduction, une clôture algébrique $\bar{\mathbb{Q}}$ de $\mathbb{Q}$ et une clôture algébrique $\bar{\mathbb{F}}_p$ de $\mathbb{F}_p$.

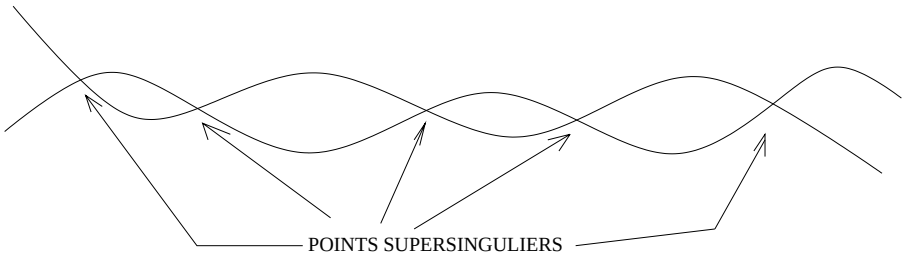
Aspect géométrique

L'ensemble $\mathcal{S}$ est muni d'une structure de schéma sur $\mathbb{F}_p$.

Soient $X_0(p) = X_0(p)_{\mathbb{Q}}$ la courbe modulaire sur $\mathbb{Q}$ classifiant grossièrement les courbes elliptiques généralisées munies d'un groupe cyclique d'ordre p et $J_0(p) = J_0(p)_{\mathbb{Q}}$ sa jacobienne. On note $X_0(p)_{\mathbb{Z}}$ la normalisation de $\mathbb{P}^1_{\mathbb{Z}}$ dans $X_0(p)$ via le morphisme $X_0(p) \longrightarrow X_0(1) \cong \mathbb{P}^1_{\mathbb{Z}}$ et $J_0(p)_{\mathbb{Z}}$ le modèle de Néron de $J_0(p)$ sur $\mathbb{Z}$.

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 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 $X_0(p)$.

Notons $J_0(p)^0_{\mathbb{F}_p}$ la composante neutre de la fibre en p de $J_0(p)_{\mathbb{Z}}$. La variété abélienne $J_0(p)$ est à réduction torique, autrement dit $J_0(p)^0_{\mathbb{F}_p}$ est un tore. Le groupe des caractères $\bar{\mathbb{F}}_p$-rationnels du tore $J_0(p)^0_{\mathbb{F}_p}$ est isomorphe à $\mathcal{P}^0$ (voir [41] ou le paragraphe 1.2.3).



Pour tout entier $m \geq 1$, le schéma $X_0(p)_{\mathbb{Z}}$ est doté de la correspondance de Hecke $\mathbf{T}_m$ dont la restriction au lieu supersingulier $\mathcal{S}$ de $X_0(p)_{\mathbb{F}_p}$ coïncide avec l'opérateur T_m. La correspondance $\mathbf{T}_m$ définit, par fonctorialité de Picard, un endomorphisme de $J_0(p)$. L'application qui associe cet endomorphisme à l'opérateur de Hecke T_m détermine un endomorphisme d'anneaux injectif $\mathbb{T} \hookrightarrow \mathrm{End}_{\mathbb{Q}} J_0(p)$. Pour $t \in \mathbb{T}$, on note encore t l'endomorphisme de $J_0(p)$ défini par t, ainsi que l'endomorphisme de $J_0(p)_{\mathbb{Z}}$ obtenu par propriété des modèles de Néron.

Pour $d > 0$ un entier, on désigne par $X_0(p)^{(d)}_{\mathbb{Z}}$ la puissance symétrique d-ième de $X_0(p)_{\mathbb{Z}}$. Soient $\pi_d : X_0(p)^d_{\mathbb{Z}} \longrightarrow X_0(p)^{(d)}_{\mathbb{Z}}$ le morphisme canonique, et $P = \pi_d(P_1, \ldots, P_d)$ un point $\bar{\mathbb{F}}_p$-rationnel du lieu lisse de $X_0(p)^{(d)}_{\mathbb{F}_p}$. On considère le morphisme

$$\begin{array}{rccc} \phi_P^{(d)} & : & X_0(p)^{(d)}_{\bar{\mathbb{F}}_p,\mathrm{lisse}} & \longrightarrow & J_0(p)_{\bar{\mathbb{F}}_p} \\ & & \pi_d(Q_1, \ldots, Q_d) & \longmapsto & [(Q_1) + \cdots + (Q_d) - (P_1) - \cdots - (P_d)]. \end{array}$$

Pour $t \in \mathbb{T}$, notons $t\phi_P^{(d)}$ le morphisme composé de $\phi_P^{(d)}$ avec l'endomorphisme de $J_0(p)_{\mathbb{F}_p}$ défini par t.

Nous nous proposons d'étudier la géométrie de $t\phi_P^{(d)}$. Les travaux de Mazur et Kamienny ont mis en évidence l'importance de la notion d'*immersion formelle*

dans l'étude des points globaux des courbes modulaires. Mazur [21] et Kamienny [13] ont travaillé en la pointe ∞ en toute caractéristique. Nous donnons au chapitre 1 de cette thèse un critère d'immersion formelle pour $t\phi_P^{(d)}$ en tout point de $X_0(p)_{\mathbb{F}_p}$ en terme d'éléments de $\mathcal{P}^0$. Ce critère généralise le critère de Merel pour le cas $d = 1$ (voir [25] proposition 4). Dans le cadre de cette introduction, au théorème 0.1 ci-dessous, nous énonçons ce critère pour $d = 2$. L'énoncé analogue pour $d > 2$, nécessitant plus de notations, se trouve dans le paragraphe 1.3.

Considérons un point $\bar{\mathbb{F}}_p$-rationnel $P = (y_1, y_2)$ de $X_0(p)^{(2)}_{\mathbb{F}_p}$ tel que ni y_1 ni y_2 ne soit un point double de $X_0(p)_{\mathbb{F}_p}$. Dans ce cas, le point P est dans la partie lisse de $X_0(p)^{(2)}_{\mathbb{F}_p}$. Les pointes 0 et ∞ de $X_0(p)$ s'étendent en deux sections de $X_0(p)_{\mathbb{Z}}$ notées respectivement $0_{\mathbb{Z}}$ et $\infty_{\mathbb{Z}}$. Les sections de $X_0(p)_{\mathbb{F}_p}$ obtenues par spécialisation de $0_{\mathbb{Z}}$ et $\infty_{\mathbb{Z}}$ seront notées $0_{\mathbb{F}_p}$ et $\infty_{\mathbb{F}_p}$. Chaque composante de $X_0(p)_{\mathbb{F}_p}$ ne contient qu'une seule des deux pointes $0_{\mathbb{F}_p}$ et $\infty_{\mathbb{F}_p}$. On note Γ_0 (resp. Γ_∞) la composante irréductible de $X_0(p)_{\mathbb{F}_p}$ contenant la pointe $0_{\mathbb{F}_p}$ (resp. $\infty_{\mathbb{F}_p}$).

Notons $j_i = j(x_i)$ pour $i \in \{0, \ldots, g\}$. Pour $k = 1, 2$, posons

$$J_k = \begin{cases} j(y_k) & \text{si } y_k \in \Gamma_\infty \\ j(w(y_k)) & \text{si } y_k \in \Gamma_0. \end{cases}$$

Soit $\delta = \sum_{i=0}^g \lambda_i x_i$ dans $\mathcal{P}^0$. Au couple (P, δ), on associe le vecteur $V_P(\delta)$ de $\bar{\mathbb{F}}_p^2$ défini par

$$V_P(\delta) = \begin{cases} \left(\sum_{i=0}^g \lambda_i\, j_i\,,\ \sum_{i=0}^g \lambda_i\, j_i^2\right) & \text{si } P = (\infty_{\mathbb{F}_p})^{(2)} \text{ ou } P = (0_{\mathbb{F}_p})^{(2)}, \\ \left(\sum_{i=0}^g \lambda_i\, j_i\,,\ \sum_{i=0}^g \dfrac{\lambda_i}{J_1 - j_i}\right) & \text{si } J_2 = \infty, \text{ et } J_1 \neq \infty, \\ \left(\sum_{i=0}^g \dfrac{\lambda_i}{J_1 - j_i}\,,\ \displaystyle\sum_{i=0}^g \dfrac{\lambda_i}{(J_1 - j_i)^2}\right) & \text{si } J_1 = J_2 \neq \infty, \\ \left(\sum_{i=0}^g \dfrac{\lambda_i}{J_1 - j_i}\,,\ \displaystyle\sum_{i=0}^g \dfrac{\lambda_i}{J_2 - j_i}\right) & \text{sinon.} \end{cases}$$

Théorème 0.1
S'il existe deux éléments δ et γ de $t\mathcal{P}^0$ tels que $V_P(\delta)$ et $V_P(\gamma)$ sont linéairement indépendants dans $\bar{\mathbb{F}}_p^2$, alors $t\phi_P^{(2)}$ est une immersion formelle en P.

On donne également des variantes de ce théorème dans le paragraphe 1.4.

Le théorème 0.1 et ses variantes se prêtent à des tests numériques et trouvent dans le chapitre 2 une application à l'étude du corps engendré par les points de p-division des courbes elliptiques.

Comparaison avec d'autres modules de Hecke

Soit $\mathcal{H} = H_1(X, \mathbb{Z})$ le premier groupe d'homologie singulière absolue de la surface de Riemann $X = X_0(p)(\mathbb{C})$. Les correspondances de Hecke fournissent,

par transport de structure, des endomorphismes de $\mathcal{H}$. Cela définit une action de $\mathbb{T}$ sur $\mathcal{H}$. La conjugaison complexe sur $X_0(p)$ détermine une involution $\mathbf{c}$ sur $\mathcal{H}$ qui commute avec l'action de $\mathbb{T}$. On note $\mathcal{H}^+$ (resp. $\mathcal{H}^-$) la partie invariante (resp. anti-invariante) de $\mathcal{H}$ sous l'action de $\mathbf{c}$. Le produit d'intersection sur $\mathcal{H}$ fournit un accouplement bilinéaire

$$\bullet : \mathcal{H}^+ \times \mathcal{H}^- \longrightarrow \mathbb{Z}.$$

Cet accouplement est parfait après extension des scalaires à $\mathbb{Z}\left[\frac{1}{2}\right]$. Les opérateurs de Hecke sont autoadjoints pour $\bullet$.

Pour tout $\mathbb{Z}$-module M, notons $M_{\mathbb{Q}} = M \otimes \mathbb{Q}$. Les $\mathbb{T}_{\mathbb{Q}}$-modules $\mathcal{P}^0_{\mathbb{Q}}$, $\mathcal{H}^+_{\mathbb{Q}}$, et $\mathcal{H}^-_{\mathbb{Q}}$ sont libres de rang 1. La théorie des symboles modulaires donne une description par générateurs et relations de $\mathcal{H}^+_{\mathbb{Q}}$ et $\mathcal{H}^-_{\mathbb{Q}}$ (voir [19]). En dépit de ces descriptions explicites, à notre connaissance, aucun isomorphisme général n'a pu être exhibé entre $\mathcal{P}^0_{\mathbb{Q}}$ d'une part, et $\mathcal{H}^+_{\mathbb{Q}}$ ou $\mathcal{H}^-_{\mathbb{Q}}$ d'autre part. Notons $\check{\mathcal{P}}^0 = \mathrm{Hom}(\mathcal{P}^0, \mathbb{Z})$. L'algèbre $\mathbb{T}$ agit par dualité sur $\check{\mathcal{P}}^0$. Nous allons donner une relation explicite entre $\mathcal{P}^0 \otimes_{\mathbb{T}} \check{\mathcal{P}}^0$ 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 $\check{\mathcal{P}}^0$. 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

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

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

Pour M et N deux $\mathbb{Z}$-modules et $f : M \longrightarrow N$ un homomorphisme de $\mathbb{Z}$-modules, notons $M\left[\frac{1}{2}\right] = M \otimes \mathbb{Z}\left[\frac{1}{2}\right]$, et $f\left[\frac{1}{2}\right] = f \otimes 1 : M\left[\frac{1}{2}\right] \longrightarrow N\left[\frac{1}{2}\right]$ le morphisme obtenu par extension des scalaires à $\mathbb{Z}\left[\frac{1}{2}\right]$.

Il résulte des travaux de Mazur [20] et d'Emerton [8] que l'on a un isomorphisme de $\mathbb{T}\left[\frac{1}{2}\right]$-modules :

$$\Phi = \psi\left[\tfrac{1}{2}\right]^{-1} \circ \theta^0\left[\tfrac{1}{2}\right] \ : \ \mathcal{P}^0\left[\tfrac{1}{2}\right] \otimes_{\mathbb{T}\left[\frac{1}{2}\right]} \check{\mathcal{P}}^0\left[\tfrac{1}{2}\right] \longrightarrow \mathcal{H}^+\left[\tfrac{1}{2}\right] \otimes_{\mathbb{T}\left[\frac{1}{2}\right]} \mathcal{H}^-\left[\tfrac{1}{2}\right].$$

Ce fait est démontré au paragraphe 4.4.2.

On définit l'*élément d'Eisenstein* a_E de $\mathcal{P}_{\mathbb{Q}}$ par

$$a_E = \sum_{i=0}^{g} \frac{x_i}{w_i}.$$

Dans le but de décrire l'isomorphisme $\Phi_{\mathbb{Q}}$ déduit de Φ par $\mathbb{Q}$-linéarité, nous déterminons l'image par $\Phi_{\mathbb{Q}}$ de l'élément $\bar{\Delta}^0_2$ défini par :

$$\bar{\Delta}^0_2 = \sum_{i=0}^{g} \frac{1}{w_i}(x_i \otimes_{\mathbb{T}_{\mathbb{Q}}} x_i) - \frac{12}{p-1} a_E \otimes_{\mathbb{T}_{\mathbb{Q}}} a_E.$$

La formule de masse d'Eichler montre que $\bar{\Delta}_2^0$ est un élément de $\mathcal{P}_{\mathbb{Q}}^0 \otimes_{\mathbb{T}_{\mathbb{Q}}} \mathcal{P}_{\mathbb{Q}}^0$.

Posons $\mathcal{H}^{\mathrm{ptes}} = H_1(X, \mathrm{ptes}; \mathbb{Z})$ où ptes est l'ensemble des pointes de $X_0(p)$. Notons $\mathfrak{H}$ le demi-plan de Poincaré. La surface de Riemann X s'identifie à $\Gamma_0(p)\backslash(\mathfrak{H} \cup \mathbb{P}^1(\mathbb{Q}))$. Pour u, v dans $\mathbb{P}^1(\mathbb{Q})$ notons $\{u, v\}$ la classe d'homologie dans $\mathcal{H}^{\mathrm{ptes}}$ de l'image dans X d'une géodésique de $\mathfrak{H}$ d'origine u et d'extrémité v. Pour $g \in \mathrm{SL}_2(\mathbb{Z})$ le symbole modulaire $\{g0, g\infty\}$ ne dépend que de la classe de g modulo $\Gamma_0(p)$ (voir [19]). On note $\xi^0(g)$ cet élément de $\mathcal{H}^{\mathrm{ptes}}$.

Notons

$$\tau = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}).$$

L'élément

$$\frac{1}{6} \sum_{g \in \Gamma_0(p)\backslash \mathrm{SL}_2(\mathbb{Z})} (\xi^0(g\tau) \otimes_{\mathbb{T}_{\mathbb{Q}}} \xi^0(g) - \xi^0(g) \otimes_{\mathbb{T}_{\mathbb{Q}}} \xi^0(g\tau))$$

est un élément de $\mathcal{H}_{\mathbb{Q}} \otimes_{\mathbb{T}_{\mathbb{Q}}} \mathcal{H}_{\mathbb{Q}}$. Notons $\bar{\Lambda}_2^0$ son image par le morphisme canonique

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

Théorème 0.2

1. *L'élément $\bar{\Delta}_2^0$ engendre le $\mathbb{T}_{\mathbb{Q}}$-module libre $\mathcal{P}_{\mathbb{Q}}^0 \otimes_{\mathbb{T}_{\mathbb{Q}}} \mathcal{P}_{\mathbb{Q}}^0$;*
2. *l'élément $\bar{\Lambda}_2^0$ engendre le $\mathbb{T}_{\mathbb{Q}}$-module libre $\mathcal{H}_{\mathbb{Q}}^+ \otimes_{\mathbb{T}_{\mathbb{Q}}} \mathcal{H}_{\mathbb{Q}}^-$;*
3. *on a $\Phi_{\mathbb{Q}}(\bar{\Delta}_2^0) = \bar{\Lambda}_2^0$.*

Lien avec les fonctions L

Soit I_e l'idéal de $\mathbb{T}$ annulateur de l'élément d'enroulement $e \in \mathcal{H}_{\mathbb{Q}}^+$ défini par Mazur (voir [20] p. 136 ou le paragraphe 5.2 ci-dessous). L'ensemble des éléments de $\mathcal{H}_{\mathbb{Q}}^+$ annulés par I_e est $\mathcal{H}_{\mathbb{Q}}^+[I_e] = \mathbb{T}_{\mathbb{Q}}\, e$.

Rappelons que l'algèbre $\mathbb{T}$ agit sur l'ensemble des formes modulaires paraboliques de poids 2 pour $\Gamma_0(p)$. On appelle *forme primitive* toute forme parabolique propre pour les opérateurs de Hecke et normalisée. L'idéal I_e est l'annulateur des formes primitives f pour lesquelles $L(f, 1) \neq 0$. D'après le théorème de Kolyvagin-Logachev, cela implique que le *quotient d'enroulement*, *i.e.* la variété abélienne quotient

$$J_e = J_0(p)/I_e J_0(p),$$

n'a qu'un nombre fini de points rationnels. La conjecture de Birch et Swinnerton-Dyer suggère que le quotient d'enroulement est maximal pour cette propriété de finitude.

On note $\mathcal{P}_{\mathbb{Q}}^0[I_e]$ l'ensemble des éléments de $\mathcal{P}_{\mathbb{Q}}^0$ annulés par I_e. Nous ne connaissons actuellement pas de générateur de ce $\mathbb{T}_{\mathbb{Q}}$-module analogue à l'élément d'enroulement pour $\mathcal{H}_{\mathbb{Q}}^+[I_e]$. Cependant, nous allons voir comment les formules de Gross-Zhang et Gross-Kudla mettent en évidence certains éléments de $\mathcal{P}_{\mathbb{Q}}^0[I_e]$.

Formule de Gross-Zhang

Rappelons l'interprétation algébrique des éléments de $\mathcal{S}$. Soit $\{E_0, \ldots, E_g\}$ un système de représentants de $\mathcal{S}$. La courbe elliptique E_0 étant supersingulière en caractéristique p, l'anneau R_0 de ses endomorphismes est un ordre de l'algèbre de quaternions $B = R_0 \otimes \mathbb{Q}$ ramifiée en p et l'infini. L'ensemble des classes d'idéaux à gauche de R_0 est un ensemble fini de cardinal g, indépendant de l'ordre R_0 et en correspondance bijective avec $\mathcal{S}$. Soit $i \in \{0, \ldots, g\}$. Tout représentant de la classe d'idéaux à gauche de R_0 correspondant à E_i a pour ordre à droite l'anneau d'endomorphismes R_i de E_i. On a $w_i = |R_i^*/\langle \pm 1 \rangle|$.

Fixons $-D < 0$ un discriminant quadratique imaginaire premier à p. Notons $\mathcal{O}_{-D}$ l'ordre de discriminant $-D$, $h(-D)$ son nombre de classes, $u(-D)$ l'ordre de $\mathcal{O}_{-D}^*/\langle \pm 1 \rangle$, et $h_i(-D)$ le nombre de plongements optimaux de $\mathcal{O}_{-D}$ dans R_i, modulo conjugaison par R_i^*. On a $u(-4) = 2,\ u(-3) = 3$ et $u(-D) = 1$ si $D \neq 3, 4$.

Le *D-ième élément de Gross* est l'élément

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

Les opérateurs de Hecke étant autoadjoints pour l'accouplement $\langle\ ,\ \rangle$, ils sont simultanément diagonalisables sur $\mathcal{P}_{\bar{\mathbb{Q}}} = \mathcal{P} \otimes \bar{\mathbb{Q}}$. Soit f une forme primitive de poids 2 pour $\Gamma_0(p)$. On note $\mathcal{P}_{\bar{\mathbb{Q}}}^f$ la composante f-isotypique de $\mathcal{P}_{\bar{\mathbb{Q}}}$ et x^f le projeté d'un élément x de $\mathcal{P}_{\bar{\mathbb{Q}}}$ sur $\mathcal{P}_{\bar{\mathbb{Q}}}^f$. Soit π^0 la surjection de $\mathcal{P}_{\bar{\mathbb{Q}}}$ sur $\mathcal{P}_{\bar{\mathbb{Q}}}^0$ définie par $\pi^0(x) = x - \frac{12}{p-1} \deg(x)\ a_E$.

Notons ε_D le caractère non trivial de $\mathrm{Gal}(\mathbb{Q}(\sqrt{-D})/\mathbb{Q})$, et $f \otimes \varepsilon_D$ la forme primitive de niveau pD^2 tordue de f par ε_D. La formule suivante est due à Gross [10] lorsque D est premier et à Zhang [50] dans le cas général.

Théorème 0.3 (Formule de Gross-Zhang)
On a

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

Posons $\gamma_D^0 = \pi^0(\gamma_D) \in \mathcal{P}_{\mathbb{Q}}^0$ et considérons la forme modulaire parabolique de poids 2 pour $\Gamma_0(p)$

$$\mathbf{g}_D = \theta_{\mathbb{Q}}^0(\gamma_D^0 \otimes_{\mathbb{Q}} \gamma_D^0) \in \mathcal{M}_{\mathbb{Q}}^0.$$

La forme parabolique $\mathbf{g}_D$ admet pour développement de Fourier à l'infini

$$\sum_{m \geq 1} \langle \gamma_D^0, T_m \gamma_D^0 \rangle q^m.$$

Soit

$$e_D = \sum_{b \mod D} \varepsilon_D(b) \left\{ -\frac{b}{D}, \infty \right\} \ \in\ \mathcal{H}_{\mathbb{Q}}^{\mathrm{ptes}}.$$

L'élément e_D est un élément de $\mathcal{H}_{\mathbb{Q}}^-$. C'est l'*élément d'enroulement tordu par* ε_D.

Comme corollaire de la formule de Gross-Zhang, on montre dans le chapitre 5 le théorème suivant.

Théorème 0.4
L'image de $\gamma_D^0 \otimes_{\mathbb{T}_{\mathbb{Q}}} \gamma_D^0$ *par l'isomorphisme*

$$\Phi_{\mathbb{Q}} : \mathcal{P}_{\mathbb{Q}}^0 \otimes_{\mathbb{T}_{\mathbb{Q}}} \mathcal{P}_{\mathbb{Q}}^0 \xrightarrow{\sim} \mathcal{H}_{\mathbb{Q}}^+ \otimes_{\mathbb{T}_{\mathbb{Q}}} \mathcal{H}_{\mathbb{Q}}^-$$

est donnée par :

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

En d'autres termes, on a l'égalité

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

La formule de Gross-Zhang entraîne que γ_D^0 est un élément de $\mathcal{P}_{\mathbb{Q}}^0[I_e]$. Notons A l'ensemble des discriminants quadratiques imaginaires premiers à p. Soit $\mathcal{G}$ le $\mathbb{Q}$-espace vectoriel engendré par $\{\gamma_D^0, -D \in A\}$. A l'aide d'un théorème de non-annulation de Waldspurger, Parent a montré que $\mathcal{G} = \mathcal{P}_{\mathbb{Q}}^0[I_e]$ (voir [37]).

Soit $\mathcal{X}'_D$ l'ensemble des matrices $M = \left(\begin{smallmatrix} u & v \\ w & t \end{smallmatrix}\right)$ à coefficients entiers, de déterminant D, et telles que $u > v \geq 0$, $0 \leq w < t$, et $(w,t) = 1$. Pour $M \in \mathcal{X}'_D$, on note b_M l'entier modulo D solution du système

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

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

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

où $\bar{B}_1$ est la fonction périodique de période 1 définie par $\bar{B}_1(x) = x - \frac{1}{2}$ si $x \in]0,1[$ et $\bar{B}_1(0) = 0$

En calculant le premier coefficient de la forme parabolique $\mathbf{g}_D$, on montre dans le paragraphe 5.3 la formule suivante :

Théorème 0.5
On a

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

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

Eléments de $\mathcal{P}^0[I_e]$ issus de la formule de Gross-Kudla

Soient f, g et h trois formes primitives. Considérons la fonction $L(f \otimes g \otimes h, s)$ définie suivant le procédé de Serre (voir [11] ou le paragraphe 6.2). Cette fonction admet un prolongement analytique à $\mathbb{C}$ et satisfait une équation fonctionnelle symétrique en $s = 2$. Dans les cas non triviaux, c'est-à-dire lorsque le signe de l'équation fonctionnelle est négatif, Gross et Kudla [11] donnent une formule pour la valeur en 2 de la fonction $L(f \otimes g \otimes h, s)$. L'élément

$$\Delta_3 = \sum_{i=0}^{g} \frac{1}{w_i} x_i^{\otimes 3} \in \mathcal{P}_{\mathbb{Q}}^{\otimes 3}$$

y joue un rôle central.

Notons $s_{\widetilde{\mathbb{T}}} : \mathcal{P}_{\mathbb{Q}} \otimes_{\mathbb{Q}} \mathcal{P}_{\mathbb{Q}} \twoheadrightarrow \mathcal{P}_{\mathbb{Q}} \otimes_{\widetilde{\mathbb{T}}_{\mathbb{Q}}} \mathcal{P}_{\mathbb{Q}}$ la surjection canonique. On déduit de la formule de Gross-Kudla que l'élément $\bar{\Delta}_3^0 = (\pi^0 \otimes s_{\widetilde{\mathbb{T}}})(\Delta_3)$ de $\mathcal{P}_{\mathbb{Q}}^0 \otimes_{\mathbb{Q}} (\mathcal{P}_{\mathbb{Q}} \otimes_{\widetilde{\mathbb{T}}_{\mathbb{Q}}} \mathcal{P}_{\mathbb{Q}})$ est en fait dans $\mathcal{P}_{\mathbb{Q}}^0[I_e] \otimes_{\mathbb{Q}} (\mathcal{P}_{\mathbb{Q}}^0 \otimes_{\mathbb{T}_{\mathbb{Q}}} \mathcal{P}_{\mathbb{Q}}^0)$.

Pour $m \geq 1$, posons

$$y_m = \sum_{i=0}^{g} \langle T_m x_i, \frac{x_i}{w_i} \rangle \; x_i \; \in \; \mathcal{P} \qquad \text{et} \qquad y_m^0 = \pi^0(y_m) \; \in \; \mathcal{P}_{\mathbb{Q}}^0.$$

Observons que $\langle T_m x_i, \frac{x_i}{w_i} \rangle$ est le nombre de m-isogénies de E_i dans E_i à automorphisme près. L'élément y_m énumère donc les boucles du graphe des m-isogénies étudié par Mestre et Oesterlé [28].

Théorème 0.6

1. *Pour tout $m \geq 1$, $y_m^0 \in \mathcal{P}_{\mathbb{Q}}^0[I_e]$.*
2. *On a*

$$y_m = \epsilon(m)\, a_E \; + \sum_{\substack{(s,d) \in \mathbb{Z}^2 \\ 4m - s^2 = dr^2 > 0}} \gamma_d$$

où

$$\epsilon(m) = \begin{cases} 1 & \text{si } m \text{ est un carré} \\ 0 & \text{sinon.} \end{cases}$$

Remarque 0.1 L'assertion 1. peut se déduire de la formule de Gross-Kudla ou de la combinaison de la formule de Gross-Zhang et de l'assertion 2. La démonstration de l'assertion 2. s'inspire du calcul classique qui permet d'établir la formule des traces d'Eichler [7], [10].

On ne sait pas actuellement si $\{y_m^0 \, ; \, m \geq 1\}$ engendre $\mathcal{P}_{\mathbb{Q}}^0[I_e]$ comme $\mathbb{Q}$-espace vectoriel ou même comme $\mathbb{T}_{\mathbb{Q}}$-module. On a toutefois la

Proposition 0.7

Le $\mathbb{Q}$-espace vectoriel engendré par $(y_m^0)_{m \geq 1}$ est égal au $\mathbb{Q}$-espace vectoriel engendré par $(y_m^0)_{1 \leq m \leq g+1}$.

Notons $\mathcal{Y}$ le $\mathbb{T}_{\mathbb{Q}}$-module engendré par $(y_m^0)_{m\geq 1}$.

Proposition 0.8
Les conditions suivantes sont équivalentes :

i) les $\mathbb{T}_{\mathbb{Q}}$-modules $\mathcal{Y}$ et $\mathcal{P}_{\mathbb{Q}}^0[I_e]$ sont égaux,

ii) pour toute forme primitive f de poids 2 pour $\Gamma_0(p)$ telle que $L(f,1)\neq 0$, il existe une forme primitive h de poids 2 pour $\Gamma_0(p)$ telle que

$$L(f\otimes h\otimes h, 2)\neq 0.$$

Les conditions de la proposition 0.8 entraînent une version précise d'un théorème de non-annulation :

Corollaire 0.9
Si $\mathcal{Y}=\mathcal{P}_{\mathbb{Q}}^0[I_e]$ et si f est une forme modulaire primitive de poids 2 pour $\Gamma_0(p)$ telle que $L(f,1)\neq 0$, alors il existe $d\leq 4g+4$ tel que $L(f\otimes\varepsilon_d,1)\neq 0$.

Corps engendré par les points de p-division des courbes elliptiques

La motivation initiale de ma thèse est l'étude du problème suivant.

Soient d et n des entiers strictement positifs. Soit E une courbe elliptique sur un corps de nombres. Les propriétés des accouplements de Weil montrent que le corps de définition dans $\bar{\mathbb{Q}}$ des points de n-torsion de E contient le corps $\mathbb{Q}(\mu_n)$ engendré par les racines n-ièmes de l'unité dans $\bar{\mathbb{Q}}$. Soit $S(d)$ l'ensemble des nombres premiers p pour lesquels il existe une extension L de degré d de $\mathbb{Q}(\mu_p)$ et une courbe elliptique E définie sur L dont les points de p-torsion sont L-rationnels. Il est connu que l'ensemble $S(1)$ contient les nombres 2, 3, 5 et Halberstadt a prouvé que 7 n'est pas dans $S(1)$. Merel et Stein [25, 26] ont montré qu'aucun nombre premier p compris entre 8 et 1000 et distinct de 13 n'appartient à $S(1)$. Leur méthode s'appuie sur l'analogue du théorème 0.1 pour $d=1$, et un théorème de Kato [14] en direction de la conjecture de Birch et Swinnerton-Dyer.

Le cas $p=13$ se traite sans l'usage de $\mathcal{P}$. À l'aide de calculs explicites sur les symboles modulaires et du théorème de Kato (*loc. cit.*), nous montrons dans le chapitre 3 le

Théorème 0.10
Aucune courbe elliptique sur un corps de nombres n'a tous ses points $\bar{\mathbb{Q}}$-rationnels d'ordre 13 définis sur $\mathbb{Q}(\mu_{13})$ (autrement dit $13\notin S(1)$).

Nous donnons dans le chapitre 2 des résultats partiels sur $S(2)$ utilisant une variante du théorème 0.1 et le théorème de Kato (*loc. cit.*).

Propriétés galoisiennes des courbes elliptiques

Soit E une courbe elliptique sans multiplication complexe définie sur $\mathbb{Q}$. Soit

$$\rho_p(E) \ : \ \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{Aut}(E[p]) \cong \mathrm{GL}_2(\mathbb{F}_p)$$

la représentation induite par l'action de $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ sur E. Serre [45] a prouvé que $\rho_p(E)$ est surjective pour tout nombre premier p plus grand qu'une constante dépendant de E. Il demande, notamment dans [45] ou [46] p. 288, si on peut choisir cette constante indépendamment de E. Ce problème revient essentiellement à déterminer si l'image de $\rho_p(E)$ est contenue dans l'un des sous-groupes de $\mathrm{Aut}(E[p]) \cong \mathrm{GL}_2(\mathbb{F}_p)$ suivants :

- un sous-groupe de Borel ; (B)
- le normalisateur d'un sous-groupe de Cartan déployé ; (CD)
- le normalisateur d'un sous-groupe de Cartan non déployé. (CND)

Mazur a montré que la situation (B) ne se produit pas pour $p > 37$. Le cas (CND) est mal connu. Nous nous intéressons au cas (CD).

Nous faisons appel au résultat suivant de Parent [37] qui s'inspire d'une méthode de Momose [31, 32, 33].

Pour $j \in \mathbb{P}^1(\bar{\mathbb{F}}_p) - j(\mathcal{S})$, considérons l'application

$$\begin{array}{rccc} \iota_j \ : & \mathcal{P} & \longrightarrow & \bar{\mathbb{F}}_p \\ & \sum_{i=0}^g \lambda_i x_i & \longmapsto & \sum_{i=0}^g \frac{\lambda_i}{j-j_i}. \end{array}$$

Si, pour tout $j \in \mathbb{P}^1(\mathbb{F}_p) - j(\mathcal{S})$, il existe $x \in \mathcal{P}^0[I_e]$ tel que $\iota_j(x) \neq 0$ alors le cas (CD) n'intervient pas.

En appliquant le critère précédent à des combinaisons linéaires bien choisies des éléments $\gamma_D^0 \in \mathcal{P}_{\mathbb{Q}}^0[I_e]$, Parent [37] détermine un ensemble de nombres premiers $\mathcal{A}$ de densité analytique $7/2^9$ pour lequel on a le

Théorème 0.11 (Parent)
Si $p \geq 11$, $p \neq 13$ et $p \notin \mathcal{A}$, alors le cas (CD) n'intervient pas.

Comme alternative aux éléments γ_D, nous proposons de considérer les éléments

$$y_{k,m} = \mathrm{Tr}(T_m) y_k - \mathrm{Tr}(T_k) y_m \in \mathcal{P}_{\mathbb{Q}}^0[I_e],$$

pour $m > 0$ et $k > 0$ deux entiers.

Soit $\mathcal{C}$ l'ensemble des nombres premiers p qui sont simultanément un carré modulo $3, 4, 7$ et tels que l'une des conditions suivantes est vérifiée :

1. p carré modulo $11, 19, 23, 43, 67, 163$, non carré modulo 8 ;
2. p carré modulo $8, 11, 19$, et modulo au moins deux des nombres premiers $43, 67, 163$, et vérifiant l'une des conditions suivantes
   (a) p carré modulo 5 ;
   (b) p non carré modulo 5 et 23 ;
   (c) p non carré modulo 5 et carré modulo $23, 59, 71$;

   (d) p non carré modulo $5, 59, 71$ et carré modulo 23 ;

3. p carré modulo $5, 8, 11, 43, 67, 163$, non carré modulo 19 et l'une des conditions suivantes est vérifiée :
   (a) p carré modulo 23 ;
   (b) p non carré modulo 23 et $\left(\frac{p}{31}\right)\left(\frac{p}{36319}\right)\left(\frac{p}{l}\right) = 1$ où $l = 45321935159$;
4. p carré modulo $5, 8, 19, 43, 67, 163$, non carré modulo 11 et p carré modulo au moins un des nombres : $23, 797$.

L'ensemble $\mathcal{C}$ est de densité $5/2^9$.

Des calculs sur les fractions $\iota_j(y_{k,m})$ pour $(k, m) \in \{2, 3, 5, 6, 7\}$ effectués suivant la méthode du graphe de Mestre et Oesterlé [28], combinés aux résultats de Parent, montrent le théorème suivant.

Théorème 0.12
Si $p > 19$, $p \notin \mathcal{C}$, le cas (CD) n'intervient pas.

Chapitre 1

Géométrie en caractéristique p

Notations. — Soient $d > 0$ un entier et $p > 2$ un nombre premier.

On note $X_0(p) = X_0(p)_{\mathbb{Q}}$ la courbe modulaire sur $\mathbb{Q}$ classifiant grossièrement les courbes elliptiques généralisées munies d'un sous-groupe cyclique d'ordre p et $Y_0(p) = Y_0(p)_{\mathbb{Q}}$ le complémentaire des deux pointes 0 et ∞ de $X_0(p)$. On pose $J_0(p) = J_0(p)_{\mathbb{Q}}$ la jacobienne de $X_0(p)$. On note $\mathfrak{H}$ le demi-plan de Poincaré, $Y = Y_0(p)(\mathbb{C}) = \Gamma_0(p)\backslash\mathfrak{H}$ et $X = X_0(p)(\mathbb{C}) = \Gamma_0(p)\backslash\left(\mathfrak{H} \cup \mathbb{P}^1(\mathbb{Q})\right)$ les surfaces de Riemann associées, et $J = J_0(p)(\mathbb{C})$ la jacobienne de X.

Soit $X_0(p)_{\mathbb{Z}}$ la normalisation de $\mathbb{P}^1_{\mathbb{Z}}$ dans $X_0(p)$ via la composée du revêtement canonique $X_0(p) \longrightarrow X_0(1)$ et de l'isomorphisme $j : X_0(1) \cong \mathbb{P}^1_{\mathbb{Q}}$. Le schéma $X_0(p)_{\mathbb{Z}}$ est projectif sur $\mathbb{Z}$. On note $X_0(p)_{\mathbb{Z},\text{lisse}}$ le lieu lisse de $X_0(p)_{\mathbb{Z}}$. Les pointes 0 et ∞ de $X_0(p)$ s'étendent en deux sections de $X_0(p)_{\mathbb{Z},\text{lisse}}$ sur $\operatorname{Spec}\mathbb{Z}$ que l'on note $0_{\mathbb{Z}}$ et $\infty_{\mathbb{Z}}$ respectivement.

Soient $\mathcal{O}$ un anneau de Dedekind et K son corps des fractions. Pour A une variété abélienne sur K, on note $A_{\mathcal{O}}$ son modèle de Néron sur $\mathcal{O}$. On pose $X_0(p)_{\mathcal{O}} = X_0(p)_{\mathbb{Z}} \times_{\mathbb{Z}} \mathcal{O}$. Pour un schéma X sur $\mathcal{O}$, on notera X_K la fibre générique de X et $X_{k_{\mathfrak{p}}}$ sa fibre spéciale en un idéal premier $\mathfrak{p}$ de $\mathcal{O}$.

On note $X_0(p)^{(d)}_{\mathbb{Z}}$ le schéma quotient de $X_0(p)^d_{\mathbb{Z}}$ par l'action du groupe symétrique $\mathfrak{S}_d$, et $\pi_d : X_0(p)^d_{\mathbb{Z}} \longrightarrow X_0(p)^{(d)}_{\mathbb{Z}}$ le morphisme canonique (voir par exemple [29]). On a

$$\pi_d(X_0(p)_{\mathbb{Z},\text{lisse}})^d \subset X_0(p)^{(d)}_{\mathbb{Z},\text{lisse}}.$$

Soit $P = \pi_d(P_1, \ldots, P_d)$ un point $\bar{\mathbb{F}}_p$-rationnel du lieu lisse $X_0(p)^{(d)}_{\mathbb{F}_p,\text{lisse}}$ de $X_0(p)^{(d)}_{\mathbb{F}_p}$. On considère le morphisme

$$\begin{array}{rccc} \phi_P^{(d)} & : & X_0(p)^{(d)}_{\bar{\mathbb{F}}_p,\text{lisse}} & \longrightarrow & J_0(p)_{\bar{\mathbb{F}}_p} \\ & & \pi_d(Q_1, \ldots, Q_d) & \mapsto & [(Q_1) + \cdots + (Q_d) - (P_1) - \cdots - (P_d)]. \end{array}$$

Dans ce chapitre, nous nous proposons d'étudier la géométrie de $\phi_P^{(d)}$.

1.1 Rappels, définitions, et notations préliminaires

1.1.1 Immersions formelles

Soient X et Y deux schémas nœthériens. Soit $f : X \longrightarrow Y$ un morphisme de schémas, x un point de X et $y = f(x)$. Notons $\mathcal{O}_{X,x}$ (resp. $\mathcal{O}_{Y,y}$) l'anneau local de X en x (resp. de Y en y) et $\widehat{\mathcal{O}}_{X,x}$ (resp. $\widehat{\mathcal{O}}_{Y,y}$) son complété.

Définition 1.1 (immersion formelle)
On dit que f est une immersion formelle *en x si le morphisme d'anneaux $\widehat{f_x}$: $\widehat{\mathcal{O}}_{Y,y} \longrightarrow \widehat{\mathcal{O}}_{X,x}$ qui se déduit de f sur les complétés des anneaux locaux est surjectif.*

Remarque 1.1 Notons $f^\sharp : \mathcal{O}_Y \longrightarrow f_*\mathcal{O}_X$ le morphisme de faisceaux sous-jacent à f et $f_x^\sharp : \mathcal{O}_{Y,y} \longrightarrow \mathcal{O}_{X,x}$ le morphisme qui s'en déduit sur les anneaux locaux. Le morphisme d'anneaux $\widehat{f_x}$ est surjectif si et seulement si les deux conditions suivantes sont satisfaites :

1. le morphisme $f_x^\sharp$ induit un isomorphisme sur les corps résiduels ;
2. l'application f^* déduite de f par passage aux espaces cotangents est surjective.

La définition 1.1 est motivée par la

Proposition 1.2
Soit $f : X \longrightarrow Y$ un morphisme de schémas nœthériens, X séparé de type fini, et soit $x \in X$ tel que f soit une immersion formelle en x. Si T est un schéma intègre nœthérien, $t \in T$ et g_1, g_2 deux morphismes de T dans X tels que $g_1(t) = g_2(t) = x$ et $f \circ g_1 = f \circ g_2$, alors $g_1 = g_2$.

Démonstration. — Rappelons et détaillons ici la démonstration donnée par Oesterlé dans [34]. Comme $\widehat{g_{1t}} \circ \widehat{f_x} = \widehat{g_{2t}} \circ \widehat{f_x}$ et $\widehat{f_x}$ surjectif, on a $\widehat{g_{1t}} = \widehat{g_{2t}} : \widehat{\mathcal{O}}_{X,x} \longrightarrow \widehat{\mathcal{O}}_{T,t}$. Les schémas X et T étant nœthériens, les anneaux locaux $\mathcal{O}_{X,x}$, $\mathcal{O}_{T,t}$ s'identifient à des sous-anneaux de leur complété respectif $\widehat{\mathcal{O}}_{X,x}$, $\widehat{\mathcal{O}}_{T,t}$. Par conséquent, on a $g_{1,t}^\sharp = g_{2,t}^\sharp$. Le schéma X étant de type fini, [12] 6.5.1 montre que g_1 coïncide avec g_2 dans un voisinage ouvert de t donc au point générique de T. De plus X est séparé et T intègre, donc la proposition [12] 5.4.7 permet de conclure. □

1.1.2 Algèbre de Hecke

On note $\mathbb{T}$ le sous-anneau de $\mathrm{End}_{\mathbb{Q}}(J_0(p))$ engendré par les endomorphismes T_n, $n \geq 1$, déduits des correspondances de Hecke sur $X_0(p)$ par passage à la jacobienne. [1] L'*algèbre de Hecke* $\mathbb{T}$ agit sur le $\mathbb{C}$-espace vectoriel $\mathcal{M}_{\mathbb{C}}^0 = S_2(\Gamma_0(p))$ des formes modulaires paraboliques de poids 2 via l'isomorphisme $\mathbb{C}$-linéaire

[1] D'après un théorème de Ribet (voir [43] corollaire 3.3), on a en fait $\mathbb{T} = \mathrm{End}(J)$; on ne se servira pas de ce fait ici.

$\mathcal{M}_{\mathbb{C}}^0 \xrightarrow{\sim} H^0(X, \Omega_X^1)$ qui à une forme modulaire parabolique f associe la forme différentielle holomorphe ω_f sur X déduite de la forme différentielle

$$2i\pi f(z)dz = f\frac{dq}{q}$$

sur le demi-plan de Poincaré $\mathfrak{H}$.

Par propriété des modèles de Néron, tout élément t de $\mathbb{T}$ s'étend en un endomorphisme de $J_0(p)_{\mathbb{Z}}$ sur $\mathbb{Z}$ encore noté t et on note également $\mathbb{T}$ l'image de l'algèbre $\mathbb{T}$ dans $\mathrm{End}(J_0(p)_{\mathbb{Z}})$.

La correspondance d'Atkin-Lehner sur $X_0(p)$, déduite de l'involution $z \mapsto -1/pz$ sur $\mathfrak{H} \cup \mathbb{P}^1(\mathbb{Q})$, s'étend en une involution w sur $X_0(p)_{\mathbb{Z}}$ qui échange les deux pointes , et induit sur $J_0(p)_{\mathbb{Z}}$ une involution qui coïncide[2] avec $-T_p$.

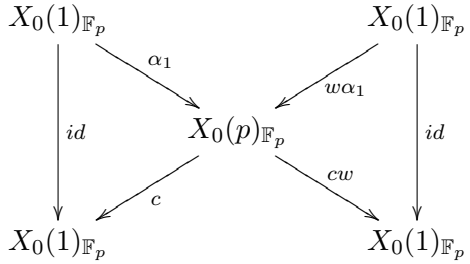
1.2 Fibres en p (rappels)

1.2.1 Fibre en p de $X_0(p)_{\mathbb{Z}}$

Soit S un schéma de caractéristique p et E une courbe elliptique généralisée sur S. Notons $F : E \longrightarrow E^{(p)}$ le morphisme de Frobenius et $V : E^{(p)} \longrightarrow E$ le morphisme de Verschiebung. Afin de simplifier les notations notons encore $w = w_{\mathbb{F}_p}$. Considérons les morphismes de schémas α_1 et α_2 de $X_0(1)_{\mathbb{F}_p}$ vers $X_0(p)_{\mathbb{F}_p}$ définis par

$$\alpha_1(E) = (E, \mathrm{Ker}F) \quad \text{et} \quad \alpha_2(E) = w\alpha_1(E) = (E^{(p)}, \mathrm{Ker}V)$$

dans $X_0(p)_{\mathbb{F}_p}(S)$. Notons enfin $c : (E, C) \mapsto E$ le revêtement de $X_0(p)_{\mathbb{Z}}$ sur $X_0(1)_{\mathbb{Z}}$.

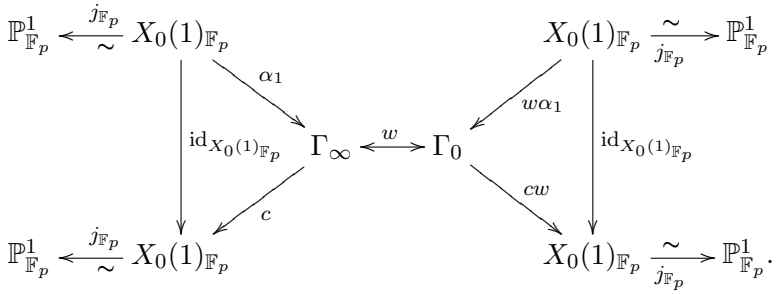


On a $c\alpha_1 = cww\alpha_1 = \mathrm{id}_{X_0(1)_{\mathbb{F}_p}}$ et les diagonales $cw\alpha_1$ sont égales à F.

Les morphismes α_1 et $\alpha_2 = w\alpha_1$ sont des immersions fermées d'images les deux composantes irréductibles de $X_0(p)_{\mathbb{F}_p}$ (voir [5] V 1.15 et V 1.16). Etant échangées par w, chacune d'elles ne contient qu'une seule des deux pointes : on note $\Gamma_0 = \mathrm{Im}(\alpha_2)$ celle contenant la pointe $0_{\mathbb{F}_p}$ et $\Gamma_\infty = \mathrm{Im}(\alpha_1)$ celle contenant la pointe $\infty_{\mathbb{F}_p}$.

Soit $j_{\mathbb{Z}} : X_0(1)_{\mathbb{Z}} \longrightarrow \mathbb{P}^1_{\mathbb{Z}}$ l'isomorphisme prolongeant j. Le morphisme $j_{\mathbb{F}_p}c : X_0(p)_{\mathbb{F}_p} \longrightarrow \mathbb{P}^1_{\mathbb{F}_p}$ définit un isomorphisme de Γ_∞ sur $\mathbb{P}^1_{\mathbb{F}_p}$, et donc $j_{\mathbb{F}_p}cw$ définit un isomorphisme de Γ_0 sur $\mathbb{P}^1_{\mathbb{F}_p}$.

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



Notons g le genre de $X_0(p)$. Les deux composantes irréductibles Γ_0 et Γ_∞ de $X_0(p)_{\mathbb{F}_p}$ se coupent transversalement en $g+1$ points. L'ensemble des points doubles de $X_0(p)_{\mathbb{F}_p}$ est en correspondance bijective avec l'ensemble fini $\mathcal{S}$ des classes d'isomorphisme des courbes elliptiques supersingulières en caractéristique p. La fibre de $X_0(p)_{\mathbb{Z}}$ en p est donc obtenue en recollant deux copies de $\mathbb{P}^1_{\mathbb{F}_p}$ en les points supersinguliers, un point supersingulier x d'une copie de $\mathbb{P}^1_{\mathbb{F}_p}$ étant identifié à son image x^p par w sur l'autre copie, car $j_{\mathbb{F}_p} c_{|\Gamma_0} = j^p_{\mathbb{F}_p} cw$. On note $\{x_0, \ldots, x_g\}$ l'ensemble des points doubles de $X_0(p)_{\mathbb{F}_p}$. On identifie dorénavant $\mathcal{S}$ à $\{x_0, \ldots, x_g\}$. On pose $\Gamma'_0 = \Gamma_0 \backslash \mathcal{S}$ et $\Gamma'_\infty = \Gamma_\infty \backslash \mathcal{S}$.

Dans toute la suite de cette thèse, afin de simplifier les notations, nous noterons

$$j = j_{\mathbb{F}_p} c : X_0(p)_{\mathbb{F}_p} \longrightarrow \mathbb{P}^1_{\mathbb{F}_p} \quad \text{et} \quad j_i = j(x_i) \quad (i \in \{0, \ldots, g\}).$$

Le lieu lisse $X_0(p)_{\mathbb{Z},\text{lisse}}$ de $X_0(p)_{\mathbb{Z}}$ est obtenu en ôtant à $X_0(p)_{\mathbb{Z}}$ les sections supersingulières dans la fibre en p.

1.2.2 Fibre en p de $X_0(p)^{(d)}_{\mathbb{Z}}$

Pour a et b deux entiers, notons

$$C_{a,b} = \Gamma_\infty^{(a)} \times \Gamma_0^{(b)}. \tag{1.1}$$

L'application $(j^{(a)}, (jw)^{(b)})$ définit un isomorphisme

$$C_{a,b} \xrightarrow{\sim} (\mathbb{P}^1_{\mathbb{F}_p})^{(a)} \times (\mathbb{P}^1_{\mathbb{F}_p})^{(b)}.$$

La description de $X_0(p)_{\mathbb{F}_p}$ montre que la fibre en p de $X_0(p)^{(d)}$ est recouverte par les $d+1$ composantes $C_{a,b}$ où (a,b) parcourt l'ensemble des couples d'entiers positifs de somme égale à d.

Par la suite on identifiera $\Gamma_\infty^{(a)}$ (resp. $\Gamma_0^{(b)}$) avec l'ensemble des diviseurs effectifs de degré a sur Γ_∞ (resp. de degré b sur Γ_0). Un point

$$\pi_d(\underbrace{\infty_{\mathbb{F}_p}, \ldots, \infty_{\mathbb{F}_p}}_{r_0}, \underbrace{y_1, \ldots, y_1}_{r_1}, \ldots, \underbrace{y_l, \ldots, y_l}_{r_l}, \underbrace{0_{\mathbb{F}_p}, \ldots, 0_{\mathbb{F}_p}}_{r_{l+1}}) \in C_{a,b},$$

où

$$a = \sum_{u=0}^{k} r_u, \quad b = \sum_{v=k+1}^{l+1} r_v,$$

et

$$y_u \in \Gamma_\infty \quad (1 \leq u \leq k), \quad y_u \in \Gamma_0 \quad (k+1 \leq u \leq l),$$

sera donc noté

$$\left(r_0.\infty_{\mathbb{F}_p} + \sum_{u=1}^{k} r_u.y_u, \ \sum_{v=k+1}^{l} r_v.y_v + r_{l+1}.0_{\mathbb{F}_p} \right).$$

Lorsque b (resp. a) est nul, on omet la deuxième coordonnée (resp. la première coordonnée).

Définition 1.3
Un point

$$P = \left(r_0.\infty_{\mathbb{F}_p} + \sum_{u=1}^{k} r_u.y_u, \ \sum_{v=k+1}^{l} r_v.y_v + r_{l+1}.0_{\mathbb{F}_p} \right) \in C_{a,b}$$

est p-supersingulier *s'il existe* $i \in \{1, \ldots, l\}$ *tel que* y_i *est un point double de* $X_0(p)_{\mathbb{F}_p}$. *Dans le cas contraire, on dit que* P *est* non p-supersingulier.

Soient a et b deux entiers positifs de somme égale à d. On note

$$C'_{a,b} = {\Gamma'_\infty}^{(a)} \times {\Gamma'_0}^{(b)}. \tag{1.2}$$

Tout point de $C_{a,b}$ non p-supersingulier est un point de $C'_{a,b}$. Comme

$$\pi_d(X_0(p)^d_{\mathbb{Z},\text{lisse}}) \subset X_0(p)^{(d)}_{\mathbb{Z},\text{lisse}},$$

les points non p-supersinguliers de $X_0(p)_{\mathbb{F}_p}$ sont dans l'ouvert de lissité $X_0(p)^{(d)}_{\mathbb{F}_p,\text{lisse}}$ de $X_0(p)^{(d)}_{\mathbb{F}_p}$.

Exemple 1.1 Soient $y_1, y_2 \in X_0(p)_{\mathbb{F}_p}$. Les différentes configurations possibles pour un point de $X_0(p)^{(2)}_{\mathbb{F}_p}$ sont :

$$\left.\begin{array}{c} (2.\infty_{\mathbb{F}_p}) \in \Gamma_\infty^{(2)} \\ (\infty_{\mathbb{F}_p} + y_1) \in \Gamma_\infty^{(2)} \\ (2.y_1) \in \Gamma_\infty^{(2)} \\ (y_1 + y_2) \in \Gamma_\infty^{(2)} \\ (y_1, 0_{\mathbb{F}_p}) \in C_{1,1} \end{array}\right\} \xrightarrow{w} \left\{\begin{array}{c} (2.0_{\mathbb{F}_p}) \in \Gamma_0^{(2)} \\ (y_1 + 0_{\mathbb{F}_p}) \in \Gamma_0^{(2)} \\ (2.y_1) \in \Gamma_0^{(2)} \\ (y_1 + y_2) \in \Gamma_0^{(2)} \\ (\infty_{\mathbb{F}_p}, y_1) \in C_{1,1} \end{array}\right.$$

$$(\infty_{\mathbb{F}_p}, 0_{\mathbb{F}_p}) \in C_{1,1}, \qquad (y_1, y_2) \in C_{1,1}.$$

1.2.3 Fibre en p de $J_0(p)_{\mathbb{Z}}$

Soit $P = \mathrm{Pic}_{X_0(p)_{\mathbb{Z}}/\mathbb{Z}}$ le schéma de Picard relatif à $X_0(p)_{\mathbb{Z}}$ sur $\mathbb{Z}$. C'est le schéma en groupes représentant le foncteur de Picard relatif à $X_0(p)_{\mathbb{Z}}$. Sa formation commute au passage aux fibres (voir par exemple [41]). Soient $\widetilde{P}$ le noyau du morphisme *degré total* de P dans $\mathbb{Z}$ et P^0 la composante neutre de $P \times \mathbb{F}_p = \mathrm{Pic}_{X_0(p)_{\mathbb{F}_p}/\mathbb{F}_p}$. Soit $J_0(p)^0_{\mathbb{F}_p}$ la composante neutre du schéma en groupe $J_0(p)_{\mathbb{F}_p}$ de type fini sur $\mathbb{F}_p$. Le morphisme naturel $\widetilde{P} \longrightarrow J_0(p)_{\mathbb{Z}}$ prolongeant l'isomorphisme sur les fibres génériques par propriété des modèles de Néron, induit un isomorphisme entre P^0 et $J_0(p)^0_{\mathbb{F}_p}$ (voir [41] théorème 2). La géométrie de $X_0(p)_{\mathbb{F}_p}$ montre que $J_0(p)$ est une *variété abélienne à réduction torique*, en d'autres termes la composante neutre $J_0(p)^0_{\mathbb{F}_p}$ admet une structure de tore (*loc. cit.*). Soit n le numérateur de $(p-1)/12$. Le groupe des composantes de $J_0(p)_{\mathbb{F}_p}$ est le groupe cyclique C_0 d'ordre n engendré par la réduction modulo p de la classe du diviseur $(0) - (\infty)$ (voir [20]). On a $J_0(p)_{\mathbb{F}_p} = J_0(p)^0_{\mathbb{F}_p} \times C_0$.

La structure de $\mathbb{T}$-module de $J_0(p)_{\mathbb{Z}}$ induit par spécialisation une action de $\mathbb{T}$ sur $J_0(p)_{\mathbb{F}_p}$ qui laisse stable $J_0(p)^0_{\mathbb{F}_p}$. Nous noterons encore t l'endomorphisme de $J_0(p)^0_{\mathbb{F}_p}$ induit par $t \in \mathbb{T}$.

Groupe des caractères de $J_0(p)^0_{\mathbb{F}_p}$

Considérons le $\mathbb{Z}$-module libre de rang $g+1$

$$\mathcal{P} = \mathbb{Z}[\mathcal{S}] = \bigoplus_{i=0}^{g} \mathbb{Z}\, x_i \tag{1.3}$$

appelé *module supersingulier*. On désigne par $\mathcal{P}^0$ le sous-groupe de $\mathcal{P}$ formé des éléments de degré nul.

Le choix d'une composante de $X_0(p)_{\mathbb{F}_p}$ fournit un isomorphisme canonique entre le groupe $\mathcal{P}^0$ et le groupe $\widehat{J_0(p)^0_{\mathbb{F}_p}}$ des caractères du tore $J_0(p)^0_{\mathbb{F}_p}$ (voir [41], p. 14).

L'isomorphisme canonique

$$\psi : \mathcal{P}^0 \xrightarrow{\sim} \widehat{J_0(p)^0_{\mathbb{F}_p}}$$

obtenu en privilégiant la composante Γ_0 est décrit de la manière suivante. Soit $\sum_{i=0}^{g} \lambda_i x_i \in \mathcal{P}^0$. Soit $\mathcal{F}$ un faisceau inversible sur $X_0(p)_{\mathbb{F}_p}$ dont la classe $[\mathcal{F}]$ est dans $\mathrm{Pic}^0_{X_0(p)_{\mathbb{Z}}/\mathbb{Z}} \times \mathbb{F}_p = \mathrm{Pic}^0_{X_0(p)_{\mathbb{F}_p}/\mathbb{F}_p}$, c'est-à-dire tel que $\mathcal{F}|_{\Gamma_0}$ et $\mathcal{F}|_{\Gamma_\infty}$ sont de degré 0. Les deux composantes irréductibles Γ_0 et Γ_∞ étant de genre nul, $\mathcal{F}|_{\Gamma_0}$ et $\mathcal{F}|_{\Gamma_\infty}$ sont trivialisables et on peut en choisir respectivement deux sections s_0 et s_∞ partout non nulles. Le caractère $\chi = \psi(\sum_{i=0}^{g} \lambda_i x_i)$ est alors défini par

$$\chi([\mathcal{F}]) = \prod_{i=0}^{g} \left(\frac{s_0(\alpha_2(x_i))}{s_\infty(\alpha_1(x_i))} \right)^{\lambda_i}. \tag{1.4}$$

On note

$$\psi' : \mathcal{P}^0 \xrightarrow{\sim} \widehat{J_0(p)^0_{\mathbb{F}_p}}$$

l'isomorphisme canonique obtenu en privilégiant Γ_∞. L'isomorphisme composé

$$\mathcal{P}^0 \xrightarrow{\psi'} \widehat{J_0(p)^0_{\mathbb{F}_p}} \xrightarrow{\psi^{-1}} \mathcal{P}^0$$

est simplement le changement de signe (*loc. cit.*) : $\sum_{i=0}^{g} \lambda_i x_i \mapsto -\sum_{i=0}^{g} \lambda_i x_i$. On choisit pour la suite de privilégier la composante Γ_0. L'isomorphisme ψ est compatible avec l'action de $\mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)$ sur $\mathcal{P}^0$ et $\widehat{J_0(p)^0_{\mathbb{F}_p}}$.

L'action de $\mathbb{T}$ sur $J_0(p)^0_{\mathbb{F}_p}$ induit, via ψ, une action de $\mathbb{T}$ sur $\mathcal{P}^0$. Cette définition de l'action de $\mathbb{T}$ sur $\mathcal{P}^0$ coïncide avec la définition élémentaire présentée dans l'introduction et dans le paragraphe 4.3.2.

Espace cotangent à $J_0(p)_{\bar{\mathbb{F}}_p}$

Puisque $J_0(p)$ est une variété abélienne à réduction torique, l'application

$$\begin{array}{ccc} \bar{\mathbb{F}}_p \otimes \widehat{J_0(p)^0_{\mathbb{F}_p}} & \longrightarrow & \mathrm{Cot}(J_0(p)_{\bar{\mathbb{F}}_p}) \\ a \otimes \chi & \longmapsto & a \left.\frac{d\chi}{\chi}\right|_0 \end{array}$$

est un isomorphisme de $\bar{\mathbb{F}}_p$-espaces vectoriels. En composant avec ψ, on en déduit un isomorphisme de $\bar{\mathbb{F}}_p$-espaces vectoriels entre $\bar{\mathbb{F}}_p \otimes \mathcal{P}^0$ et $\mathrm{Cot}(J_0(p)_{\bar{\mathbb{F}}_p})$. Soit $t \in \mathbb{T}$. Par définition de l'action de $\mathbb{T}$ sur $\mathcal{P}^0$, le diagramme suivant commute

$$\begin{array}{ccc} \bar{\mathbb{F}}_p \otimes \mathcal{P}^0 & \xrightarrow{\sim} & \mathrm{Cot}(J_0(p)_{\bar{\mathbb{F}}_p}) \\ {\scriptstyle t}\uparrow & & \uparrow{\scriptstyle t^*} \\ \bar{\mathbb{F}}_p \otimes \mathcal{P}^0 & \xrightarrow{\sim} & \mathrm{Cot}(J_0(p)_{\bar{\mathbb{F}}_p}). \end{array} \tag{1.5}$$

1.3 Critère d'immersion formelle en caractéristique p

Remarquons tout d'abord que, pour tous points P et Q du lieu lisse $X_0(p)^{(d)}_{\mathbb{F}_p,\mathrm{lisse}}$ de $X_0(p)^{(d)}_{\mathbb{F}_p}$, on a :

$$\phi_P^{(d)} = \tau_{\phi_Q^{(d)}(P)} \circ \phi_Q^{(d)},$$

où $\tau_{\phi_Q^{(d)}(P)}$ est la translation par $\phi_Q^{(d)}(P)$. Il suffit donc d'étudier la géométrie du morphisme $\phi_P^{(d)}$ au point P lui-même.

Soit

$$P = \left(r_0.\infty_{\mathbb{F}_p} + \sum_{u=1}^{k} r_u.y_u,\ \sum_{v=k+1}^{l} r_v.y_v + r_{l+1}.0_{\mathbb{F}_p} \right)$$

un point non p-supersingulier de $X_0(p)^{(d)}_{\mathbb{F}_p}$ et $t \in \mathbb{T}$. On considère dans ce paragraphe le morphisme composé

$$t\phi_P^{(d)} : X_0(p)^{(d)}_{\bar{\mathbb{F}}_p,\mathrm{lisse}} \xrightarrow{\phi_P^{(d)}} J_0(p)_{\bar{\mathbb{F}}_p} \xrightarrow{t} J_0(p)_{\bar{\mathbb{F}}_p}.$$

Posons

$$J_i = \begin{cases} j(y_i) & \text{si } 1 \leq i \leq k \\ jw(y_i) & \text{si } k+1 \leq i \leq l. \end{cases}$$

Pour $\delta = \sum_{i=0}^{g} \lambda_i x_i \in \mathcal{P}^0$, on note

$$V_P(\delta) = (\eta_1, \ldots, \eta_{r_0}, \eta_1, \ldots, \eta_{r_{l+1}}, \iota_1(J_1), \ldots, \iota_{r_1}(J_1), \ldots, \iota_1(J_l), \ldots, \iota_{r_l}(J_l)),$$

où, pour tout entier $v > 0$,

$$\eta_v = \sum_{i=0}^{g} \lambda_i j_i^v \quad \text{et} \quad \iota_v(j) = \sum_{i=0}^{g} \frac{\lambda_i}{(j - j_i)^v}$$

et où l'on omet le terme correspondant à r_k si $r_k = 0$.

Théorème 1.4
S'il existe $\delta_1, \ldots, \delta_d$ dans $t\mathcal{P}^0$, tels que les vecteurs $V_P(\delta_1), \ldots, V_P(\delta_d)$ sont linéairement indépendants dans $\bar{\mathbb{F}}_{\mathrm{p}}^d$, alors $t\phi_P^{(d)}$ est une immersion formelle en P.

Remarque 1.2 Lorsque r_0 et r_{l+1} sont non nuls, ou lorsque $J_h = J_i$ pour deux entiers h et i de $\{1, \ldots, l\}$ distincts, le théorème 1.4 n'a aucun intérêt car les vecteurs $V_P(\delta_1), \ldots V_P(\delta_d)$ sont liés quels que soient $\delta_1, \ldots, \delta_d$ dans $\mathcal{P}^0$.

Table 1.1 (d=2) Soit $P = (y_1, y_2) \in X_0(p)^{(2)}_{\mathbb{F}_p}$ non p-supersingulier. Soit $\delta = \sum_{i=0}^{g} \lambda_i x_i \in \mathcal{P}^0$. Le tableau 1.1 donne $V_P(\delta)$ suivant les différentes possibilités pour le point P. Le critère du théorème 1.4 ne s'applique pas lorsque P est de la forme $(y_1, wy_1) \in C_{1,1}$.

Remarque 1.3 (Restriction des hypothèses) 1) Le groupe des composantes de $J_0(p)_{\mathbb{F}_p}$ étant cyclique d'ordre n, $(p-1)\phi_P^{(d)}$ est à image dans $J_0(p)^0_{\mathbb{F}_p}$;
2) le morphisme de schémas $t\phi_P^{(d)}$ est une immersion formelle en P si et seulement si $(p-1)t\phi_P^{(d)}$ est une immersion formelle en P.

On suppose désormais que $\phi_P^{(d)}$ est à image dans $J_0(p)^0_{\mathbb{F}_p}$, quitte à multiplier par $p-1$, comme le permet la remarque 1.3.

1.3.1 Préliminaires à la démonstration du théorème 1.4

Soient a et b tels que $P \in C'_{a,b}$. Posons

$$P_{a,b} = (\mathbb{P}^1_{\mathbb{F}_p})^{(a)} \times (\mathbb{P}^1_{\mathbb{F}_p})^{(b)}$$

et

$$\underline{J} = (j^{(a)}, (jw)^{(b)})(P) = (\underbrace{\infty, \ldots, \infty}_{r_0}, \underbrace{J_1, \ldots, J_1}_{r_1}, \ldots, \underbrace{J_l, \ldots, J_l}_{r_l}, \underbrace{\infty, \ldots, \infty}_{r_{l+1}}) \in P_{a,b}.$$

TAB. 1.1 – Vecteur $V_P(\delta)$ dans le cas $d = 2,\ P \neq (\infty_{\mathbb{F}_p}, 0_{\mathbb{F}_p})$.

P	$V_P(\delta)$
$(2.\infty_{\mathbb{F}_p}) \in \Gamma_\infty'^{(2)}$ $(2.0_{\mathbb{F}_p}) \in \Gamma_0'^{(2)}$	$\left(\sum_{i=0}^g \lambda_i\, j_i\,,\ \sum_{i=0}^g \lambda_i\, j_i^2\right)$
$(\infty_{\mathbb{F}_p} + y_1) \in \Gamma_\infty'^{(2)}$ $(y_1 + 0_{\mathbb{F}_p}) \in \Gamma_0'^{(2)}$ $(\infty_{\mathbb{F}_p}, y_1) \in C'_{1,1}$ $(y_1, 0_{\mathbb{F}_p}) \in C'_{1,1}$	$\left(\sum_{i=0}^g \lambda_i\, j_i\,,\ \sum_{i=0}^g \dfrac{\lambda_i}{J_1 - j_i}\right)$
$(2y_1) \in \Gamma_\infty'^{(2)}$ $(2y_1) \in \Gamma_0'^{(2)}$	$\left(\sum_{i=0}^g \dfrac{\lambda_i}{J_1 - j_i}\,,\ \sum_{i=0}^g \dfrac{\lambda_i}{(J_1 - j_i)^2}\right)$
$(y_1 + y_2) \in \Gamma_\infty'^{(2)}$ $(y_1 + y_2) \in \Gamma_0'^{(2)}$ $(y_1, y_2) \in C'_{1,1}$	$\left(\sum_{i=0}^g \dfrac{\lambda_i}{J_1 - j_i}\,,\ \sum_{i=0}^g \dfrac{\lambda_i}{J_2 - j_i}\right)$

L'application $\alpha_{a,b} = ((\alpha_1 j^{-1})^{(a)}, (\alpha_2 j^{-1})^{(b)})$ détermine un isomorphisme de $P_{a,b}$ dans $\Gamma_\infty^{(a)} \times \Gamma_0^{(b)}$. On a $\alpha_{a,b}(\underline{J}) = P$.

On se propose de déterminer l'application composée

$$\Phi_P : \bar{\mathbb{F}}_p \otimes \mathcal{P}^0 \xrightarrow{\sim} \mathrm{Cot}(J_0(p)_{\bar{\mathbb{F}}_p}) \xrightarrow{\phi_P^{(d)*}} \mathrm{Cot}_P(X_0(p)^{(d)}_{\bar{\mathbb{F}}_p}) \xrightarrow{\alpha_{a,b}^*} \mathrm{Cot}_{\underline{J}}(P_{a,b}).$$

Soient $\delta = \sum_{i=0}^g \lambda_i x_i \in \mathcal{P}^0$ et $\chi = \psi(\delta)$. On a

$$\Phi_P(\delta) = \left.\frac{d(\chi \circ \phi_P^{(d)} \circ \alpha_{a,b})}{\chi \circ \phi_P^{(d)} \circ \alpha_{a,b}}\right|_{\underline{J}}.$$

Détermination de $\chi \circ \phi_P^{(d)}$

PROPOSITION 1.5 (CAS $d = 1$)
Si $P \in \Gamma'_\infty$, on a l'égalité de morphismes de Γ'_∞ dans $\mathbb{G}_{m\mathbb{F}_p}$ suivante

$$\chi \circ \phi_P|_{\Gamma'_\infty} = \prod_{i=0}^g \left(\frac{j - j_i}{j(P) - j_i}\right)^{\lambda_i}.$$

Si $P \in \Gamma'_0$, on a l'égalité de morphismes de Γ'_0 dans $\mathbb{G}_{m\mathbb{F}_p}$:

$$\chi \circ \phi_P|_{\Gamma'_0} = \prod_{i=0}^g \left(\frac{jw - j_i}{jw(P) - j_i}\right)^{-\lambda_i}.$$

Remarque 1.4 Pour $P = \infty_{\mathbb{F}_p}$, on obtient

$$\chi \circ \phi_\infty|_{\Gamma'_\infty} = \prod_{i=0}^{g} (j - j_i)^{\lambda_i}.$$

En effet, $\prod_{i=0}^{g}(j-j_i)^{\lambda_i} = \prod_{i=0}^{g}(1-\frac{j_i}{j})^{\lambda_i}$ car $\sum_{i=0}^{g}\lambda_i = 0$. Pour $P = 0_{\mathbb{F}_p}$, on obtient de façon analogue

$$\chi \circ \phi_0|_{\Gamma'_0} = \prod_{i=0}^{g} (jw - j_i)^{-\lambda_i}.$$

La formule de la proposition 1.5 dans le cas où $P \in \Gamma'_\infty$ est due à Mestre et Oesterlé (voir [28] proposition 16). La démonstration dans le cas général est *mutatis mutandis* celle de *loc. cit.*, mais cet article restant à ce jour non publié, nous la rappelons.

Démonstration. — Soit Q un point de $X_0(p)_{\bar{\mathbb{F}}_p}$. Notons $\mathcal{L}_Q$ le faisceau inversible sur $X_0(p)_{\bar{\mathbb{F}}_p}$ formé des germes de fonctions rationnelles de diviseur supérieur à $-\phi_P(Q)$. La classe de $\mathcal{L}_Q$ est l'image de $\phi_P(Q) \in J_0(p)^0_{\bar{\mathbb{F}}_p}$ par l'isomorphisme $J_0(p)^0_{\bar{\mathbb{F}}_p} \xrightarrow{\sim} P^0_{\bar{\mathbb{F}}_p}$ (voir [29] paragraphe 4). Chacune des composantes irréductibles de $X_0(p)_{\bar{\mathbb{F}}_p}$ étant de genre nul, la restriction de $\mathcal{L}_Q$ à une composante est trivialisable. Une section globale de $\mathcal{L}_Q|_{\Gamma_\infty}$ (resp. $\mathcal{L}_Q|_{\Gamma_0}$) est une fonction rationnelle sur Γ_∞ (resp. Γ_0) s'annulant en P si $P \in \Gamma'_\infty$ (resp. $P \in \Gamma'_0$) et ayant un pôle en Q si $Q \in \Gamma'_\infty$ (resp. $Q \in \Gamma'_0$). Si $P, Q \in \Gamma'_\infty$, distincts de $\infty_{\mathbb{F}_p}$, alors $s_\infty = \frac{j(P)-j}{j(Q)-j}$ est une section globale non nulle de $\mathcal{L}_Q|_{\Gamma_\infty}$, et $s_0 = 1$ une section globale de $\mathcal{L}_Q|_{\Gamma_0}$. D'après (1.4), on a alors

$$\chi \circ \phi_P(Q) = \prod_{i=0}^{g} \left(\frac{j(Q) - j_i}{j(P) - j_i} \right)^{\lambda_i}.$$

Lorsque P et Q sont dans Γ'_0 et distincts de $0_{\mathbb{F}_p}$, le choix $s_\infty = 1,\ s_0 = \frac{jw(P)-jw}{jw(Q)-jw}$ donne la formule attendue pour ce cas. Lorsque $P = \infty_{\mathbb{F}_p}$, on conclut en posant $s_\infty = 1 - \frac{j}{j(Q)}$ et $s_0 = 1$. Lorsque $P = 0_{\mathbb{F}_p}$, on pose $s_\infty = 1$ et $s_0 = 1 - \frac{jw}{jw(Q)}$. □

Corollaire 1.6 (cas $d \geq 1$)
On a l'égalité de morphismes de $C'_{a,b} = {\Gamma'_\infty}^{(a)} \times {\Gamma'_0}^{(b)}$ dans $\mathbb{G}_{m\bar{\mathbb{F}}_p}$:

$$\chi \circ \phi_P^{(d)}|_{C'_{a,b}} = \frac{F_\chi}{F_\chi(P)},$$

où, pour tout $(Q_1, \ldots, Q_d) \in {\Gamma'_0}^a \times {\Gamma'_\infty}^b$,

$$F_\chi \circ \pi_{a,b}(Q_1, \ldots, Q_d) = \prod_{i=0}^{g} \left[\frac{\prod_{t=1}^{a}(j(Q_t) - j_i)}{\prod_{t=1}^{b}(jw(Q_t) - j_i)} \right]^{\lambda_i}.$$

DÉMONSTRATION. — Ce corollaire se déduit immédiatement de la proposition 1.5. En effet si $P = \pi_d(P_1, \ldots, P_d)$, alors $\phi_P^{(d)} \circ \pi_d(Q_1, \ldots, Q_d) = \phi_{P_1}(Q_1) + \cdots + \phi_{P_d}(Q_d)$. □

Détermination de Φ_P

Soit

$$(\frac{1}{j_{0,1}}, \ldots, \frac{1}{j_{0,r_0}}, j_{1,1}, \ldots, j_{1,r_1}, \ldots, j_{l,1}, \ldots, j_{l,r_l}, \frac{1}{j_{l+1,1}}, \ldots, \frac{1}{j_{l+1,r_{l+1}}})$$

un paramètre formel en $\underline{J}$. L'espace cotangent à $P_{a,b}$ en $\underline{J}$ admet pour base

$$(\mathcal{B}) \qquad d\sigma_{0,1}, \ldots, d\sigma_{0,r_0}, \ldots, d\sigma_{l+1,1}, \ldots, d\sigma_{l+1,r_{l+1}},$$

où $\sigma_{t,u}$ est la u-ème fonction symétrique élémentaire en

$$\begin{cases} \dfrac{1}{j_{t,1}}, \ldots, \dfrac{1}{j_{t,r_t}} & \text{si } t = 0 \text{ ou } l+1, \\ j_{t,1}, \ldots, j_{t,r_t} & \text{si } 1 \leq t \leq l. \end{cases}$$

Posons

$$\epsilon_t = \begin{cases} 1 & \text{si } 0 \leq t \leq k \\ -1 & \text{si } k+1 \leq t \leq l+1. \end{cases}$$

On rappelle que $\delta = \sum_{i=0}^{g} \lambda_i x_i \in \mathcal{P}^0$ et $\chi = \psi(\delta)$.

PROPOSITION 1.7
Dans la base $\mathcal{B}$ de $\mathrm{Cot}_{\underline{J}}(P_{a,b})$, on a

$$\Phi_P(\delta) = \sum_{t=0}^{l+1} \sum_{u=1}^{r_t} A_{t,u}(\delta)\ d\sigma_{t,u}$$

où

$$A_{t,u}(\delta) = \begin{cases} \epsilon_t (-1)^u \sum_{i=0}^{g} \lambda_i j_i^u & \text{si } t = 0 \text{ ou } l+1 \\ \epsilon_t (-1)^{r_t - u} \sum_{i=0}^{g} \dfrac{\lambda_i j_i^{r_t - u}}{(J_t - j_i)^{r_t}} & \text{si } 1 \leq t \leq l. \end{cases}$$

DÉMONSTRATION. — Notons

$$\underline{j} = (j_{0,1} + \cdots + j_{0,r_0} + \cdots + j_{k,r_k},\ j_{k+1,1} + \cdots + j_{l+1,r_{l+1}}) \in P_{a,b}.$$

D'après le corollaire 1.6, on a

$$\Phi_P(\delta) = \left. \frac{dF_\chi}{F_\chi} \right|_{\underline{J}}.$$

Or, on a

$$F_\chi(\underline{j}) = \prod_{i=0}^{g}\left[\prod_{s=1}^{r_0}\left(1-\frac{j_i}{j_{0,s}}\right)\prod_{t=1}^{l}\prod_{u=1}^{r_t}(j_{t,u}-j_i)^{\epsilon_t}\prod_{v=1}^{r_{l+1}}\left(1-\frac{j_i}{j_{l+1,v}}\right)^{-1}\right]^{\lambda_i}$$

C'est-à-dire

$$\begin{aligned} F_\chi(\underline{j}) &= \prod_{i=0}^{g}\left[\sum_{s=0}^{r_0}(-1)^s j_i^s\sigma_{0,s}\prod_{t=1}^{l}\left(\sum_{u=0}^{r_t}(-1)^{r_t-u}j_i^{r_t-u}\sigma_{t,u}\right)^{\varepsilon_t}\right]^{\lambda_i} \\ &\quad\times\prod_{i=0}^{g}\left(\sum_{v=0}^{r_{l+1}}(-1)^v j_i^v\sigma_{l+1,v}\right)^{-\lambda_i}, \end{aligned}$$

où, par convention, on pose $\sigma_{t,0}=1$ pour tout entier t.

On en déduit l'écriture de la différentielle logarithmique de F_χ en $\underline{j}$ dans la base $(\mathcal{B})$:

$$\begin{aligned} \left.\frac{dF_\chi}{F_\chi}\right|_{\underline{j}} &= \sum_{i=0}^{g}\lambda_i\left[\frac{\sum_{s=1}^{r_0}(-1)^s j_i^s d\sigma_{0,s}}{\sum_{s=0}^{r_0}(-1)^s j_i^s\sigma_{0,s}}+\sum_{t=1}^{l}\epsilon_t\frac{\sum_{u=1}^{r_t}(-1)^{r_t-u}j_i^{r_t-u}d\sigma_{t,u}}{\sum_{u=0}^{r_t}(-1)^{r_t-u}j_i^{r_t-u}\sigma_{t,u}}\right. \\ &\quad\left.-\frac{\sum_{v=1}^{r_{l+1}}(-1)^v j_i^v d\sigma_{l+1,v}}{\sum_{v=0}^{r_{l+1}}(-1)^v j_i^v\sigma_{l+1,v}}\right]. \end{aligned}$$

D'où la proposition. □

1.3.2 Démonstration du théorème 1.4

Puisque le diagramme (1.5) commute, il suffit de montrer que le morphisme composé

$$\Phi_P\circ t : \bar{\mathbb{F}}_p\otimes\mathcal{P}^0 \xrightarrow{t} \bar{\mathbb{F}}_p\otimes\mathcal{P}^0 \xrightarrow{\sim} \mathrm{Cot}(J_0(p)_{\bar{\mathbb{F}}_p}) \xrightarrow{\phi_P^{(d)*}} \mathrm{Cot}_P(X_0(p)^{(d)}_{\bar{\mathbb{F}}_p}) \xrightarrow{\alpha_{a,b}^*} \mathrm{Cot}_{\underline{J}}(P_{a,b})$$

est surjectif.

Pour $i\in\{1,\dots,d\}$, on note δ_i' l'antécédent de δ_i par t. Un calcul élémentaire montre que la matrice de vecteurs colonnes $\Phi_P(\delta_1),\dots,\Phi_P(\delta_d)$ a au signe près même déterminant que la matrice de vecteurs colonnes $V_P(\delta_1),\dots,V_P(\delta_d)$. Cela montre que les vecteurs $\Phi_P\circ t(\delta_1'),\dots,\Phi_P\circ t(\delta_d')$ sont linéairement indépendants dans le $\bar{\mathbb{F}}_p$-espace vectoriel $\mathrm{Cot}_{\underline{J}}(P_{a,b})$ de dimension d. On en déduit que $\Phi_P\circ t$ est surjectif, ce qui termine la démonstration du théorème 1.4.

1.4 Variantes

1.4.1 Schémas $\check{M}\otimes J_0(p)_{\mathbb{Z}}$

Définitions

Soient S un schéma et G un schéma en groupes commutatifs sur S. Considérons un anneau R agissant sur G par S-endomorphismes et un R-module M de présentation finie.

Le foncteur en R-modules

$$T \mapsto \mathrm{Hom}_R(M, G(T))$$

de la catégorie des schémas sur S dans la catégorie des R-modules est représentable par un schéma en groupes commutatifs sur S que nous noterons $\mathrm{Hom}_R(M, G)$ (voir par exemple l'appendice de [3] ou [28] 1.7). La formation de ce schéma commute aux changements de base $S' \longrightarrow S$. Le foncteur $M \mapsto \mathrm{Hom}_R(M, G)$ est contravariant et exact à droite. Le foncteur $G \mapsto \mathrm{Hom}_R(M, G)$ est covariant et exact à gauche.

Supposons de plus que M est projectif. Le dual $\check{M} = \mathrm{Hom}_R(M, R)$ de M dans R est également projectif et on a, pour tout S-schéma T, un isomorphisme de R-modules

$$\mathrm{Hom}_R(M, G(T)) \cong \check{M} \otimes_R G(T).$$

On note alors $\check{M} \otimes_R G = \mathrm{Hom}_R(M, G)$. Lorsque $R = \mathbb{Z}$, on note $\check{M} \otimes_{\mathbb{Z}} G = \check{M} \otimes G$.

Lemme 1.8
Soit G un schéma en groupes sur un schéma affine $S = \mathrm{Spec}\ A$ et M un $\mathbb{Z}$-module projectif de type fini. On a alors

$$\mathrm{Cot}(\check{M} \otimes G) = (M \otimes A) \otimes_A \mathrm{Cot}(G).$$

Démonstration du lemme. — Remarquons que $M \otimes A$ est projectif de type fini sur A. D'après [3] proposition 10.5.1, on a

$$\begin{aligned} \mathrm{Tan}(\check{M} \otimes G) &= \mathrm{Lie}(\mathrm{Hom}_R(M, G)) \\ &= \mathrm{Hom}_A(M \otimes A,\ \mathrm{Tan}(G)) \\ &= \mathrm{Hom}_A(M \otimes A, A) \otimes_A \mathrm{Tan}(G). \end{aligned}$$

On a alors

$$\begin{aligned} \mathrm{Cot}(\check{M} \otimes G) &= \mathrm{Hom}_A(\mathrm{Tan}(\check{M} \otimes G), A) \\ &= (M \otimes A) \otimes_A \mathrm{Cot}(G) \end{aligned}$$

◇

Immersions formelles dans $\check{M} \otimes J_0(p)$

Soient M un $\mathbb{Z}$-module projectif de type fini et $t \in \check{M} \otimes \mathbb{T}$. Un tel élément t définit un morphisme de schémas de $J_0(p)_{\mathbb{Z}}$ dans $\check{M} \otimes J_0(p)_{\mathbb{Z}}$. Reprenons les notations introduites au début de ce chapitre et considérons le morphisme de schémas

$$t \circ \phi_P^{(d)} : X_0(p)_{\bar{\mathbb{F}}_p, \mathrm{lisse}} \longrightarrow J_0(p)_{\bar{\mathbb{F}}_p} \longrightarrow \check{M} \otimes J_0(p)_{\bar{\mathbb{F}}_p}$$

obtenu en composant $\phi_P^{(d)}$ avec le morphisme de schémas sur $\bar{\mathbb{F}}_p$ défini à partir de t par passage à la fibre en p.

Par ailleurs, t définit un morphisme de $\mathbb{Z}$-modules de $M \otimes \mathcal{P}^0$ dans $\mathcal{P}^0$.

Théorème 1.9
S'il existe $\delta_1, \ldots, \delta_d$ dans $t\,(M \otimes \mathcal{P}^0)$ tels que les vecteurs $V_P(\delta_1), \ldots, V_P(\delta_d)$ sont linéairement indépendants dans $\bar{\mathbb{F}}_p^d$, alors $t \circ \phi_P^{(d)}$ est une immersion formelle en P.

Démonstration. — D'après le lemme 1.8, on a

$$\mathrm{Cot}(\check{M} \otimes J_0(p)_{\bar{\mathbb{F}}_p}) = (M \otimes \bar{\mathbb{F}}_p) \otimes_{\bar{\mathbb{F}}_p} \mathrm{Cot}(J_0(p)_{\bar{\mathbb{F}}_p}).$$

D'après (1.5), par platitude de M, on a

$$(M \otimes \bar{\mathbb{F}}_p) \otimes_{\bar{\mathbb{F}}_p} \mathrm{Cot}(J_0(p)_{\bar{\mathbb{F}}_p}) \cong (M \otimes \bar{\mathbb{F}}_p) \otimes_{\bar{\mathbb{F}}_p} (\bar{\mathbb{F}}_p \otimes \mathcal{P}^0) \cong \bar{\mathbb{F}}_p \otimes M \otimes \mathcal{P}^0$$

et le diagramme suivant commute :

$$\begin{array}{ccc} \bar{\mathbb{F}}_p \otimes \mathcal{P}^0 & \xrightarrow{\sim} & \mathrm{Cot}(J_0(p)_{\bar{\mathbb{F}}_p}) \\ {\scriptstyle t}\uparrow & & \uparrow{\scriptstyle t^*} \\ \bar{\mathbb{F}}_p \otimes M \otimes \mathcal{P}^0 & \xrightarrow{\sim} & M \otimes \mathrm{Cot}(J_0(p)_{\bar{\mathbb{F}}_p}). \end{array} \tag{1.6}$$

La démonstration est ensuite *mutatis mutandis* celle du théorème 1.4. □

Ce théorème trouve une application dans le chapitre 2.

1.4.2 Quotients de $J_0(p)$

Supposons que $p > 2$.

Soient $\mathfrak{a}$ un idéal saturé de $\mathbb{T}$ *i.e.* tel que $\mathbb{T}/\mathfrak{a}$ est un $\mathbb{Z}$-module sans torsion et $J^{\mathfrak{a}}$ la variété abélienne quotient

$$J^{\mathfrak{a}} = J_0(p)/\mathfrak{a}J_0(p). \tag{1.7}$$

On note $\mathcal{P}^0[\mathfrak{a}]$ l'ensemble des éléments de $\mathcal{P}^0$ annulés par $\mathfrak{a}$.

On considère le morphisme composé

$$\varpi^{\mathfrak{a}} \circ \phi_P^{(d)} : X_0(p)_{\mathbb{F}_p,\mathrm{lisse}} \xrightarrow{\phi_P^{(d)}} J_0(p)_{\mathbb{F}_p} \xrightarrow{\varpi^{\mathfrak{a}}} J^{\mathfrak{a}}_{\mathbb{F}_p},$$

où $\varpi^{\mathfrak{a}}$ est le morphisme canonique.

Théorème 1.10
S'il existe $\delta_1, \ldots, \delta_d$ dans $\mathcal{P}^0[\mathfrak{a}]$ tels que les vecteurs $V_P(\delta_1), \ldots, V_P(\delta_d)$ sont linéairement indépendants dans $\bar{\mathbb{F}}_p^d$, alors $\varpi^{\mathfrak{a}} \circ \phi_P^{(d)}$ est une immersion formelle en P.

Démonstration. — D'après le corollaire 1.1 de [21], comme $p > 2$, la suite exacte

$$0 \longrightarrow \mathfrak{a}J_0(p) \longrightarrow J_0(p) \longrightarrow J^{\mathfrak{a}} \longrightarrow 0$$

donne lieu à la suite exacte de $\mathbb{Z}_p$-modules

$$0 \longrightarrow \mathrm{Cot}(J^{\mathfrak{a}}_{\mathbb{Z}_p}) \longrightarrow \mathrm{Cot}(J_0(p)_{\mathbb{Z}_p}) \longrightarrow \mathrm{Cot}(\mathfrak{a}J_0(p)_{\mathbb{Z}_p}) \longrightarrow 0.$$

On en déduit que $\mathrm{Cot}(J^{\mathfrak{a}}_{\bar{\mathbb{F}}_p}) \cong \mathrm{Cot}(J_0(p)_{\bar{\mathbb{F}}_p})[\mathfrak{a}] \cong \bar{\mathbb{F}}_p \otimes \mathcal{P}^0[\mathfrak{a}]$. On procède ensuite comme dans la démonstration du théorème 1.4. □

Chapitre 2

Points de torsion des courbes elliptiques

On fixe désormais $\bar{\mathbb{Q}}$ une clôture algébrique de $\mathbb{Q}$.

Soit $d > 0$ un entier. Soit E une courbe elliptique sur un corps de nombres. Les propriétés des accouplements de Weil montrent que le corps de définition dans $\bar{\mathbb{Q}}$ des points de p-torsion de E est une extension du corps $\mathbb{Q}(\mu_p)$ engendré par les racines p-ièmes de l'unité dans $\bar{\mathbb{Q}}$. On étudie dans ce chapitre l'occurence du degré relatif d pour cette extension. Plus précisément, on étudie l'ensemble $S(d)$ des nombres premiers p pour lesquels il existe une extension L de degré d de $\mathbb{Q}(\mu_p)$ et une courbe elliptique E définie sur L dont les points $\bar{\mathbb{Q}}$-rationnels d'ordre p sont L-rationnels. On dit qu'une telle paire (E, L) est *associée à* $p \in S(d)$.

Supposons que $p \in S(d)$. Soit (E, L) une paire associée à p. Le choix d'une base de $E[p]$ détermine un plongement L-rationnel $\pi : (\mathbb{Z}/p\mathbb{Z})^2 \hookrightarrow E[p]$. Rappelons que la courbe modulaire $X(p)$ classifie les courbes elliptiques généralisées munies d'un tel plongement. Le couple (E, π) définit donc un point L-rationnel x de l'ouvert affine $Y(p)$ de $X(p)$. Soient $\sigma_1, \ldots, \sigma_d$ les plongements de L dans $\bar{\mathbb{Q}}$ au-dessus de $\mathbb{Q}(\mu_p)$. Le d-uplet $(\sigma_1(x), \ldots, \sigma_d(x))$ détermine un point de $Y(p)^{(d)}(\mathbb{Q}(\mu_p))$. Merel et Stein [25, 26] ont montré qu'aucun nombre premier p distinct de 13 compris entre 7 et 1000 n'appartient à $S(1)$.

Les méthodes inventées par Mazur pour étudier $X_1(p)(\mathbb{Q})$ ont pu être généralisées pour étudier $X_1(p)^{(d)}(\mathbb{Q})$. Nous allons voir que les méthodes de [25, 26] pour l'étude de $X(p)(\mathbb{Q}(\mu_p))$ semblent actuellement loin de se prêter à une généralisation aisée à l'étude de $X(p)^{(d)}(\mathbb{Q}(\mu_p))$.

Notons $S(d)_{\text{sps}}$ le sous-ensemble des nombres premiers $p \in S(d)$ tels qu'il existe une paire (E, L) associée à p où E a potentiellement bonne réduction supersingulière en un idéal $\mathfrak{p}$ de L au-dessus de p. Le paragraphe 2.1 est consacré à l'étude plus élémentaire du sous-ensemble $S(d)_{\text{sps}}$ de $S(d)$.

Dans le paragraphe 2.2, nous exposons les techniques permettant de descendre le corps de définition d'un point de $X_0(p)^{(d)}(\mathbb{Q}(\mu_p))$ à un sous-corps de $\mathbb{Q}(\mu_p)$.

L'application de ces techniques dans le cas $d = 2$ nous permet d'énoncer dans le paragraphe 2.3 des résultats partiels concernant $S(2)$.

Dans tout ce chapitre, nous utiliserons librement les notions introduites ou rappelées dans le chapitre 1.

Notations. — Pour L un corps de nombres et $\mathfrak{P}$ un idéal premier de L, on note $\mathcal{O}_L$ l'anneau des entiers de L et $k_\mathfrak{P}$ le corps résiduel de L en $\mathfrak{P}$. Pour E une courbe elliptique sur L, on note $\mathcal{E}$ le modèle de Néron de E sur $\mathcal{O}_L$, $\mathcal{E}_{k_\mathfrak{P}}$ sa fibre en $\mathfrak{P}$ et $\mathcal{E}^0_{k_\mathfrak{P}}$ la composante neutre de $\mathcal{E}_{k_\mathfrak{P}}$.

2.1 Cas supersingulier

Théorème 2.1
Soient $p \in S(d)$ et (E, L) une paire associée à p. Soit $\mathfrak{P}$ un idéal de L au-dessus de p. Si $p \geq \mathrm{Max}(5, d)$, alors ou bien E a réduction potentiellement multiplicative au-dessus de $\mathfrak{P}$, ou bien E a potentiellement bonne réduction ordinaire au-dessus de $\mathfrak{P}$ et $\mathcal{E}^0_{k_\mathfrak{P}}$ possède une section d'ordre p. En particulier, tout nombre premier de $S(d)_{\mathrm{sps}}$ est strictement inférieur à $\mathrm{Max}(5, d)$.

Démonstration. — Supposons au contraire que E a potentiellement bonne réduction supersingulière en un idéal premier $\mathfrak{P}$ de L. Soit e l'indice de ramification de $\mathfrak{P}$ au-dessus de p. Par hypothèse, $e \leq d(p-1) \leq p(p-1)$. Le théorème se déduit alors de la proposition 2.2 suivante appliquée à $K = L_\mathfrak{P}$. □

Soit K une extension finie de $\mathbb{Q}_p$ de corps résiduel k et d'indice de ramification e. Soit E une courbe elliptique définie sur K ayant potentiellement bonne réduction.

Proposition 2.2
Supposons que les points $\bar{\mathbb{Q}}_p$-rationnels d'ordre p de E sont définis sur K et que $e < p^2 - 1$. Alors E a potentiellement bonne réduction ordinaire et la fibre spéciale de son modèle de Néron possède une section d'ordre p sur k.

Démonstration. — Dans cette démonstration, notons $\mathcal{O}$ l'anneau d'entiers de K et $\mathcal{E}$ le modèle de Néron de E sur $\mathcal{O}$. Posons $E_0(K)$ (resp. $E_1(K)$) le sous-groupe de $E(K)$ formé des points qui donnent lieu à une section de $\mathcal{E}$ non singulière (resp. qui coïncide avec l'élément neutre) dans la fibre en l'idéal premier de K au-dessus de p.

Lemme 2.3
Le nombre d'éléments d'ordre p de $E_1(K)$ est inférieur ou égal à e.

Démonstration du lemme. — Ce lemme est bien connu. On peut en trouver une démonstration dans [25] proposition 15. ◇

Par hypothèse, le groupe $C = E[p]$ des points de p-torsion, isomorphe à $(\mathbb{Z}/p\mathbb{Z})^2$, est un sous-groupe de $E(K)$. D'après le lemme 2.3, on a

$$|(C \setminus \{0\}) \cap E_1(K)| \leq e.$$

Si E a potentiellement bonne réduction supersingulière, on a $C \subset E_1(K)$, et l'inégalité précédente devient $p^2 - 1 \leq e$, ce qui est, par hypothèse, exclu.

Par ailleurs, comme E a potentiellement bonne réduction, l'indice de $E_0(K)$ dans $E(K)$ est inférieur à 4 et donc $C \subset E_0(K)$ car $p > 3$. De plus, ce qui précède assurant que E a potentiellement bonne réduction ordinaire, on a $|C \cap E_1(K)| = p$. Par conséquent $\mathcal{E}_k^0(k) = E_0(K)/E_1(K)$ possède un point d'ordre p. □

2.2 Etude du cas non supersingulier

Soit $L \subset \mathbb{Q}_p(\mu_p)$ une extension finie de $\mathbb{Q}_p$. On note $\mathcal{O}_L$ l'anneau des entiers de L, $\mathfrak{P}$ l'idéal premier de L au-dessus de p, et $k_{\mathfrak{P}}$ le corps résiduel de L en $\mathfrak{P}$.

Soit $P = \pi_d(P_1, \ldots, P_d) \in X_0(p)^{(d)}(L)$, on note $P_{k_{\mathfrak{P}}}$ le point de $X_0(p)^{(d)}_{\bar{\mathbb{F}}_p}(k_{\mathfrak{P}})$ obtenu par spécialisation en $\mathfrak{P}$ de la section

$$s : \operatorname{Spec} \mathcal{O}_L \longrightarrow X_0(p)^{(d)}_{\mathcal{O}_L}$$

définie par P. On dira que P est non $\mathfrak{P}$-supersingulier si $P_{k_{\mathfrak{P}}}$ est non p-supersingulier au sens de la définition 1.3. Dans ce cas, s est à image dans le lieu lisse de $X_0(p)_{\mathcal{O}_L}$ et le morphisme

$$\pi_d(Q_1, \ldots, Q_d) \mapsto [(Q_1) + \cdots + (Q_d) - (P_1) - \cdots - (P_d)]$$

de $X_0(p)^{(d)}$ dans $J_0(p)$ s'étend en un morphisme noté $\phi_P^{(d)}$ de $X_0(p)^{(d)}_{\mathcal{O}_L,\text{lisse}}$ dans $J_0(p)_{\mathcal{O}_L}$. Le morphisme obtenu par passage à la fibre en $\mathfrak{P}$ n'est autre que le morphisme $\phi^{(d)}_{P_{k_{\mathfrak{P}}}}$ défini au chapitre précédent.

On notera désormais $\phi_P^{(d)}$ tout morphisme obtenu à partir de $\phi_P^{(d)}$ par passage aux fibres.

On rappelle que si M est un $\mathbb{Z}$-module de présentation finie, $M \otimes J_0(p)_{\mathcal{O}_L}$ désigne le schéma en groupes représentant le foncteur $T \mapsto M \otimes_{\mathbb{Z}} J_0(p)_{\mathcal{O}_L}(T)$ de la catégorie des schémas sur $\mathcal{O}_L$ dans la catégories des $\mathbb{Z}$-modules (voir le paragraphe 1.4.1). On a donc en particulier $M \otimes J_0(p)_{\mathcal{O}_L}(\mathcal{O}_L) \cong M \otimes J_0(p)(L)$. De plus, lorsque M est libre de type fini, $M \otimes J_0(p)\mathcal{O}_L$ est lisse ; c'est alors le modèle de Néron de $M \otimes J_0(p)$ sur $\mathcal{O}_L$ (voir l'appendice de [3] 10.5.4 et proposition 11.1.2).

On considère ici le $\mathrm{Gal}(L/\mathbb{Q}_p)$-module $J_0(p)(L) \cong J_0(p)_{\mathcal{O}_L}(\mathcal{O}_L)$. Après extension des scalaires à $\mathbb{Q}(\mu_{p-1})$, ce module est semi-simple, les composantes isotypiques étant données par les caractères de $\mathrm{Gal}(L/\mathbb{Q}_p)$. Pour un tel caractère χ, on note $\mathbb{Z}[\chi]$ le sous-$\mathbb{Z}$-module de $\mathbb{Z}[\mu_{p-1}]$ engendré par les valeurs de χ.

Proposition 2.4
Soient P_1 et P_2 deux points de $X_0(p)^{(d)}(L)$ non $\mathfrak{P}-$supersinguliers tels que $P_{1,k_{\mathfrak{P}}} = P_{2,k_{\mathfrak{P}}} = P_{k_{\mathfrak{P}}}$. Supposons que pour tout caractère χ de $\mathrm{Gal}(L/\mathbb{Q}_p)$, il existe $t_\chi = \sum r_i t_i \in \mathbb{Z}[\chi] \otimes \mathbb{T}$ tels que

1. *$t_\chi \circ \phi_P^{(d)} : X_0(p)^{(d)}_{\bar{\mathbb{F}}_p,\text{lisse}} \longrightarrow \mathbb{Z}[\chi] \otimes J_0(p)_{\bar{\mathbb{F}}_p}$ est une immersion formelle en $P_{k_{\mathfrak{P}}}$;*

2. $t_\chi \circ \phi_P^{(d)}(P_1)$ *et* $t_\chi \circ \phi_P^{(d)}(P_2)$ *ont même image dans la composante* χ*-isotypique de* $\mathbb{Q}(\mu_{p-1}) \otimes J_0(p)(L)$.

Les sections s_1 *et* s_2 *sont alors égales.*

DÉMONSTRATION. — Il suffit d'appliquer la proposition 1 de [25] à $\mathcal{X} = X_0(p)^{(d)}_{\mathcal{O}_L}$, $\mathcal{A} = J_0(p)_{\mathcal{O}_L}$ et $\phi_\chi = \phi_P^{(d)}$. On remarque en effet que le couple (t_χ, ϕ_χ) de [25] est une *pseudo-immersion formelle* au point $\bar{s}$ si et seulement si $t_\chi \circ \phi_\chi$ est une immersion formelle de $\mathcal{X}$ dans $\mathbb{Z}[\chi] \otimes \mathcal{A}$ au point $\bar{s}$.

□

On fixe désormais K un sous-corps strict de $\mathbb{Q}(\mu_p)$ et $P \in X_0(p)^{(d)}(\mathbb{Q}(\mu_p))$ non $\mathfrak{P}$-supersingulier. On note $\mathfrak{P}$ l'unique idéal premier de $\mathbb{Q}(\mu_p)$ au dessus de p.

COROLLAIRE 2.5
Si pour tout caractère χ *de* $G = \mathrm{Gal}(\mathbb{Q}(\mu_p)/K)$, *il existe* $t_\chi \in \mathbb{Z}[\chi] \otimes \mathbb{T}$ *tel que*

1. $t_\chi \circ \phi_P^{(d)}$ *est une immersion formelle en* $P_{k_\mathfrak{P}}$,
2. *la composante* χ*-isotypique de* $t_\chi(J_0(p)(\mathbb{Q}(\mu_p)))$ *est finie,*

alors P *est un point* K*-rationnel de* $X_0(p)^{(d)}$.

DÉMONSTRATION. — La démonstration est *mutatis mutandis* celle du corollaire 1 de [25]. Soit g un générateur de $\mathrm{Gal}(\mathbb{Q}(\mu_p)/K)$. Il suffit de montrer que $P = P^g$. Notons s_1 et s_2 les sections de $X_0(p)^{(d)}_{\mathbb{Z}[\mu_p]}$ étendant P et P^g respectivement. L'extension $\mathbb{Q}(\mu_p)/K$ étant totalement ramifiée en $\mathfrak{P}$, les sections s_1 et s_2 coïncident dans la fibre en $\mathfrak{P}$: $P_{k_\mathfrak{P}} = s_1(\mathfrak{P}) = s_2(\mathfrak{P})$.

Soit χ un caractère de $\mathrm{Gal}(\mathbb{Q}(\mu_p)/K)$. Notons

$$D_\chi = t_\chi \circ \phi_P^{(d)} \circ s_1 - t_\chi \circ \phi_P^{(d)} \circ s_2 \in \mathbb{Z}[\chi] \otimes J_0(p)_{\mathbb{Z}[\mu_p]}(\mathbb{Z}[\mu_p])$$

et $D_\chi(0)$ la section correspondante dans la fibre générique. Soit n l'ordre du projeté de $D_\chi(0)$ sur la composante χ-isotypique de $t_\chi(J_0(p)(\mathbb{Q}(\mu_p)))$. Puisque $J_0(p)$ ne possède pas de point $\mathbb{Q}(\mu_p)$-rationnel d'ordre p (voir [25] proposition 2) et que $\mathbb{Z}[\chi]$ est un anneau plat, l'entier n est premier à p. Dans ce cas, $D_\chi \in \mathbb{Z}[\chi] \otimes J_0(p)_{\mathbb{Z}[\mu_p]}(\mathbb{Z}[\mu_p]) \cong \mathbb{Z}[\chi] \otimes J_0(p)(\mathbb{Q}(\mu_p))$ est encore d'ordre n dans la fibre en p. Puisque $s_1(\mathfrak{P}) = s_2(\mathfrak{P})$, on a alors $n = 0$ et donc $D_\chi = 0$. On applique alors la proposition 2.4 avec $P_1 = P$ et $P_2 = P^g$. □

On reprend ici les notations du chapitre 1.

COROLLAIRE 2.6
Si pour tout caractère χ *de* $G = \mathrm{Gal}(\mathbb{Q}(\mu_p)/K)$, *il existe* $t_\chi \in \mathbb{Z}[\chi] \otimes \mathbb{T}$ *et* $\delta_1, \ldots, \delta_d$ *dans* $t_\chi(\mathbb{Z}[\chi] \otimes \mathcal{P}^0)$ *tels que*

1. *les vecteurs* $V_P(\delta_1), \ldots, V_P(\delta_d)$ *sont linéairement indépendants dans* $\bar{\mathbb{F}}_p^d$,
2. *pour toute forme primitive* f *dans* $t_\chi \mathrm{S}_2(\Gamma_0(p))$, *on a* $L(f, \chi, 1) \neq 0$,

alors P est alors un point K-rationnel de $X_0(p)^{(d)}$.

DÉMONSTRATION. — D'après le théorème 1.9, la condition 1. du corollaire 2.6 entraîne la condition 1. du corollaire 2.5. Par ailleurs, un résultat récent de Kato [14] en direction de la conjecture de Birch et Swinnerton-Dyer montre que la condition 2. du corollaire 2.6 entraîne la finitude de la composante χ-isotypique de $t_\chi\left(\mathbb{Z}[\chi] \otimes J_0(p)(\mathbb{Q}(\mu_p))\right)$ c'est-à-dire la condition 2. du corollaire 2.5. Il suffit à présent d'appliquer le corollaire 2.5 pour conclure. □

2.3 Application au cas $d = 2$

2.3.1 Contraintes de congruences sur p pour $d = 2$

PROPOSITION 2.7
Soient $p > 3$ dans $S(2)$ et (E, L) une paire associée à p. Soit K un sous-corps strict de $\mathbb{Q}(\mu_p)$. On suppose que pour tout sous-groupe C d'ordre p de E, il existe une courbe elliptique E_C et un sous-groupe D_C d'ordre p de E_C définis sur une extension quadratique K_C de K, tels que (E_C, D_C) est isomorphe sur $\bar{\mathbb{Q}}$ à (E, C).

Dans ce cas, l'une des trois conditions suivantes est vérifiée :

1. *$j(E) \neq 0, 1728$ et $p \not\equiv 1 \pmod{4[K : \mathbb{Q}]}$;*
2. *$j(E) = 1728$ et $p \leq 1 + 32[K : \mathbb{Q}]$;*
3. *$j(E) = 0$ et $p \leq 1 + 108[K : \mathbb{Q}]$.*

DÉMONSTRATION. — Soit C un sous-groupe d'ordre p de E. Considérons la paire (E_C, D_C) et l'isomorphisme

$$\phi_C : E_C \xrightarrow{\sim} E$$

tel que $\phi_C(D_C) = C$, associés à C.

Soient D' et D'' deux sous-groupes (distincts) d'ordre p de E_C distincts de D_C. Notons

$$C' = \phi_C(D') \quad \text{et} \quad C'' = \phi_C(D'').$$

Considérons les paires $(E_{C'}, D_{C'})$ et $(E_{C''}, D_{C''})$ associées respectivement à C' et C''. L'image de $D_{C'}$ par l'isomorphisme $\phi_{C'C} = \phi_C^{-1} \circ \phi_{C'} : E_{C'} \longrightarrow E_C$ est le groupe D' :

$$\begin{array}{ccccc} E_{C'} & \xrightarrow{\phi_{C'}} & E & \xrightarrow{\phi_C^{-1}} & E_C \\ & & C & \longrightarrow & D_C \\ D_{C'} & \longrightarrow & C' & \longrightarrow & D'. \end{array}$$

Posons

$$n = \begin{cases} 1 & \text{si } j(E_C) = j(E) \neq 0, 1728 \\ 2 & \text{si } j(E) = 1728 \\ 3 & \text{si } j(E) = 0. \end{cases}$$

L'isomorphisme $\phi_{C'C}$ peut être défini sur une extension de degré divisant $2n$ de $K_C K_{C'}$ et $D_{C'}$ est défini sur $K_{C'}$. On en déduit que D' est L'-rationnel où L' est une extension de $K_C K_{C'}$ de degré divisant n.

Le même raisonnement pour D'' montre qu'il existe une extension L'' de degré divisant n de $K_C K_{C''}$ telle que D'' est L''-rationnel.

Notons K_0 le compositum de $K_C, K_{C'}$ et $K_{C''}$, et L_0 celui de L' et L''. L'extension L_0/K_0 est de degré divisant n^2. Les extensions $K_C, K_{C'}, K_{C''}$ sont de degré 2 sur K. Leur compositum K_0 est donc une extension d'exposant 2 de K de degré divisant 8.

Notons

$$\rho_C : \mathrm{Gal}(\bar{\mathbb{Q}}/K_0) \longrightarrow \mathrm{Aut}(E_C[p]) \cong \mathrm{GL}_2(\mathbb{F}_p)$$

la représentation associée à E_C. Ce qui précède montre que le sous-groupe $\mathrm{Gal}(\bar{\mathbb{Q}}/L_0)$ de $\mathrm{Gal}(\bar{\mathbb{Q}}/K_0)$ laisse stables trois sous-groupes d'ordre p de E_C. Par conséquent l'action de $\mathrm{Gal}(\bar{\mathbb{Q}}/L_0)$ sur $E_C[p]$ est scalaire. Autrement dit, il existe un caractère

$$\alpha : \mathrm{Gal}(\bar{\mathbb{Q}}/L_0) \longrightarrow \mathbb{F}_p^*$$

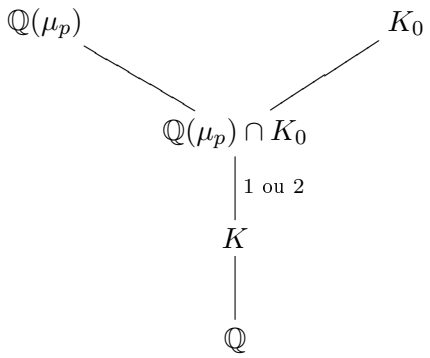
tel que

$$\rho_C(\sigma)(P) = P^\sigma = \alpha(\sigma) \qquad (P \in E_C[p], \sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/L_0)).$$

Supposons tout d'abord, que $j \neq 0, 1728$. Dans ce cas, on a $n = 1$ et donc $L_0 = K_0$. La théorie des accouplements de Weil montre que $\det(\rho_C) = \kappa$, où κ est le caractère cyclotomique modulo p. Le caractère κ se factorise par $\mathrm{Gal}(K_0(\mu_p)/K_0)$. Par conséquent,

$$\alpha^2 = \det(\rho_C) = \kappa : \mathrm{Gal}(K_0(\mu_p)/K_0) \longrightarrow \mathbb{F}_p^*.$$

Le caractère cyclotomique modulo p engendre le groupe des caractères modulo p de $\mathrm{Gal}(K_0(\mu_p)/K_0)$. Ce groupe ne peut donc pas être d'ordre pair.



On a

$$\mathrm{Gal}(K_0(\mu_p)/K_0) \cong \mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q}(\mu_p) \cap K_0).$$

L'extension $\mathbb{Q}(\mu_p)/\mathbb{Q}(\mu_p) \cap K_0$ est galoisienne d'ordre

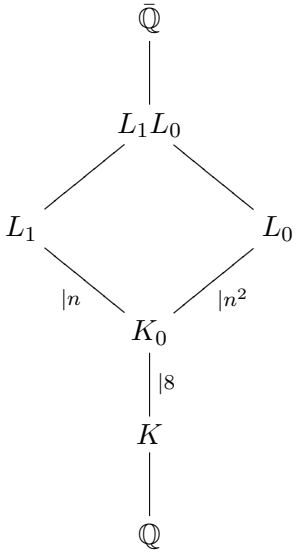
$$\frac{(p-1)}{[\mathbb{Q}(\mu_p) \cap K_0 : K][K : \mathbb{Q}]}.$$

De plus l'extension $\mathbb{Q}(\mu_p) \cap K_0/K$ est cyclique et d'exposant 2 donc de degré 1 ou 2. Si $p \equiv 1 \pmod{4[K : \mathbb{Q}]}$, alors $\mathrm{Gal}(K_0(\mu_p)/K_0)$ est d'ordre pair, ce qui est impossible.

Supposons à présent que $j(E) = 0$ ou 1728. Il existe alors un modèle E' de E défini sur $\mathbb{Q}$. Notons $\bar{\rho}'$ (resp. $\bar{\rho}_C$) la composée de la représentation

$$\rho' : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{Aut}(E'[p])$$

(resp. ρ_C) avec la surjection canonique $\mathrm{GL}_2(\mathbb{F}_p) \twoheadrightarrow \mathrm{PGL}_2(\mathbb{F}_p)$. Les tordues de E_C étant de degré $2n$, il existe une extension L_1 de degré divisant n de K_0 telle que $\bar{\rho}'$ et $\bar{\rho}_C$ coïncident sur $\mathrm{Gal}(\bar{\mathbb{Q}}/L_1)$.



L'action de $\mathrm{Gal}(\bar{\mathbb{Q}}/L_0)$ sur $E_C[p]$ est scalaire, donc l'action de $\mathrm{Gal}(\bar{\mathbb{Q}}/L_1L_0)$ sur $E'[p]$, qui coïncide avec celle sur $E_C[p]$, l'est également. Par conséquent, $\bar{\rho}'$ se factorise par $\mathrm{Gal}(L_1L_0/\mathbb{Q})$.

De plus E' est, comme E, à multiplication complexe par

$$M = \begin{cases} \mathbb{Q}(\sqrt{-1}) & \text{si } j(E) = 1728, \\ \mathbb{Q}(\sqrt{-3}) & \text{si } j(E) = 0, \end{cases}$$

et $p > 3$ est non ramifié dans M, donc l'image de ρ' est le normalisateur d'un Cartan, et en particulier est d'ordre $2(p^2 - 1)$ ou $2(p - 1)^2$. On en déduit que $2(p+1)$ ou $2(p-1)$ divise l'ordre de $\mathrm{Gal}(L_1L_0/\mathbb{Q})$ donc divise $n^3 8[K : \mathbb{Q}]$, d'où le résultat annoncé. □

2.3.2 Conséquences pour $d = 2$

On suppose que $p > 3$.

Soit R un anneau plat sur $\mathbb{Z}$. Soient J_1, J_2 deux éléments de $\mathbb{P}^1(\bar{\mathbb{F}}_p) - j(\mathcal{S})$ et $\delta = \sum_{i=0}^{g} \lambda_i x_i \in R \otimes \mathcal{P}^0$. A un tel triplet (J_1, J_2, δ), on associe le vecteur $V_{J_1,J_2}(\delta)$ de $(R \otimes \bar{\mathbb{F}}_p)^2$ défini par

$$V_{J_1,J_2}(\delta) = \begin{cases} \left(\sum_{i=0}^{g} \lambda_i\, j_i\,,\ \sum_{i=0}^{g} \lambda_i\, j_i^2\right) & \text{si } J_1 = J_2 = \infty \\ \left(\sum_{i=0}^{g} \lambda_i\, j_i\,,\ \sum_{i=0}^{g} \dfrac{\lambda_i}{J_1 - j_i}\right) & \text{si } J_2 = \infty, \text{ et } J_1 \neq \infty \\ \left(\sum_{i=0}^{g} \dfrac{\lambda_i}{J_1 - j_i}\,,\ \sum_{i=0}^{g} \dfrac{\lambda_i}{(J_1 - j_i)^2}\right) & \text{si } J_1 = J_2 \neq \infty \\ \left(\sum_{i=0}^{g} \dfrac{\lambda_i}{J_1 - j_i}\,,\ \sum_{i=0}^{g} \dfrac{\lambda_i}{J_2 - j_i}\right) & \text{sinon} \end{cases}$$

Supposons que $p \in S(2)$ et soit (E, L) une paire associée à p. On note σ l'automorphisme non trivial de L au-dessus de $\mathbb{Q}(\mu_p)$ et $\mathfrak{p}$ un idéal premier de L au-dessus de p. Le modèle de Néron de E^σ est $\mathcal{E}^\sigma$.

Théorème 2.8
Soit K un sous-corps strict de $\mathbb{Q}(\mu_p)$. On suppose que pour tous J_1 et J_2 dans $\mathbb{F}_{p^2}$ et tout caractère χ non trivial de $\mathrm{Gal}(\mathbb{Q}(\mu_p)/K)$, il existe $t_\chi \in \mathbb{Z}[\chi] \otimes \mathbb{T}$ et δ_1, δ_2 dans $t_\chi(\check{\mathbb{Z}}[\chi] \otimes \mathcal{P}^0)$ tels que

a. *les vecteurs $V_{J_1,J_2}(\delta_1)$ et $V_{J_1,J_2}(\delta_2)$ sont linéairement indépendants dans $\mathbb{F}_{p^2}^2$;*
b. *pour toute forme primitive f dans $t_\chi \mathrm{S}_2(\Gamma_0(p))$, on a $L(f, \chi, 1) \neq 0$.*

Dans ce cas, l'une des conditions suivantes est vérifiée :

1. *$j(E) \neq 0$, 1728 et $p \not\equiv 1 \pmod{4[K:\mathbb{Q}]}$;*
2. *$j(E) = 1728$ et $p \leq 1 + 32[K:\mathbb{Q}]$;*
3. *$j(E) = 0$ et $p \leq 1 + 108[K:\mathbb{Q}]$;*
4. *les courbes elliptiques E et E^σ ont réduction potentiellement multiplicative en $\mathfrak{p}$ et il existe un sous-groupe C d'ordre p de E se réduisant dans $\mathcal{E}^0_{k_\mathfrak{p}}$ si et seulement si C^σ se réduit hors de $\mathcal{E}^{\sigma\,0}_{k_\mathfrak{p}}$;*
5. *les courbes elliptiques E et E^σ ont potentiellement bonne réduction ordinaire en $\mathfrak{p}$ et il existe un sous-groupe C d'ordre p de $\mathcal{E}_{k_\mathfrak{p}}$ et un isomorphisme $\bar{\mathbb{F}}_p$-rationnel de $\mathcal{E}_{k_\mathfrak{P}}/C$ dans $\mathcal{E}^\sigma_{k_\mathfrak{P}}$ qui envoie $\mathcal{E}_{k_\mathfrak{P}}[p]$ sur C^σ.*

Démonstration. — Soit C un sous-groupe d'ordre p de E. Notons x_C le point de $X_0(p)(L)$ défini par (E, C). Le couple (x_C, x_C^σ) détermine un point $\widetilde{P}_C$ de $X_0(p)^{(2)}(\mathbb{Q}(\mu_p))$. Notons s_C : Spec $\mathbb{Z}[\mu_p] \longrightarrow X_0(p)^{(2)}_{\mathbb{Z}}$ la section qui s'en déduit. D'après le théorème 2.1, $d = 2$ n'est pas p-supersingulier lorsque $p > 3$, autrement dit s_C est à image dans $X_0(p)^{(2)}_{\mathbb{Z},\mathrm{lisse}}$. Notons P_C le point non p-supersingulier de $X_0(p)^{(2)}_{\mathbb{F}_p}(\mathbb{F}_p)$ obtenu par spécialisation de s_C.

L'assertion 4. est équivalente à

$$P_C = (\infty_{\mathbb{F}_p}, 0_{\mathbb{F}_p}),$$

et l'assertion 5. est équivalente à

$$P_C = (y, wy) \quad (y \in \Gamma'_\infty(\bar{\mathbb{F}}_p)).$$

Supposons que les assertions 4. et 5. ne sont pas vérifiées. Il existe alors J_1 et J_2 dans $\mathbb{F}_p^2$ tels que

$$V_{J_1,J_2}(\delta) = V_{P_C}(\delta) \qquad (\delta \in \mathcal{P}^0).$$

D'après le corollaire 2.6, on a alors $\tilde{P}_C \in X_0(p)^{(d)}(K)$, et ce pour tout sous-groupe C d'ordre p de E. Cela montre que les hypothèses de la proposition 2.7 sont vérifiées. Par conséquent l'une des assertions 1., 2. ou 3. du théorème 2.8 est vérifiée. □

Chapitre 3

Treize torsion des courbes elliptiques

Ce chapitre a fait l'objet d'une publication [42]. Nous le reproduisons tel qu'il est paru. Cela explique les notations différentes de celles adoptées dans d'autres chapitres, ainsi que quelques redondances.

Soit E une courbe elliptique sur un corps de nombres. Les propriétés des accouplements de Weil montrent que le corps $K_n(E)$ engendré par les points de n-torsion de E est une extension du corps $\mathbb{Q}(\mu_n)$ engendré par les racines n-ièmes de l'unité dans une clôture algébrique $\bar{\mathbb{Q}}$ de $\mathbb{Q}$.

Soit S l'ensemble des nombres premiers p pour lesquels il existe une courbe elliptique E telle que $K_p(E) = \mathbb{Q}(\mu_p)$. Il est connu que l'ensemble S contient les nombres 2, 3, 5 et Halberstadt a prouvé que 7 n'est pas dans S. Merel a étudié plus avant cet ensemble. En particulier, il a montré avec Stein ([25], [26]) qu'aucun nombre premier $p \neq 13$, $7 < p < 1000$, n'appartient à S. L'objet de ce papier est de traiter le cas $p = 13$, pour lequel les techniques de Merel ne s'appliquent pas.

Nous démontrons le théorème suivant :

Théorème 3.1
Aucune courbe elliptique sur un corps de nombres n'a tous ses points d'ordre 13 *définis sur* $\mathbb{Q}(\mu_{13})$ *(autrement dit* $13 \notin S$*).*

Notons $Y(13)$ (resp. $Y_1(13)$) la courbe affine sur $\mathbb{Q}$ classifiant les classes d'isomorphismes de paires (E, π) (resp. (E, P)) où E est une courbe elliptique et $\pi : (\mathbb{Z}/13\mathbb{Z})^2 \hookrightarrow E[13]$ un plongement (resp. P un point d'ordre 13 de E). Soit $X(13)$ (resp. $X_1(13)$) la courbe complète obtenue en adjoignant les pointes à $Y(13)$ (resp. $Y_1(13)$).

Montrer le théorème revient à montrer que $Y(13)$ n'a pas de point $\mathbb{Q}(\mu_{13})$-rationnel. Pour ce faire, nous étudions la courbe $Y_1(13)$: l'examen détaillé d'un plongement de $X_1(13)$ dans sa jacobienne $J_1(13)$, et la description complète du groupe $J_1(13)(\mathbb{Q}(\mu_{13}))$, permettent de borner le cardinal de $Y_1(13)(\mathbb{Q}(\mu_{13}))$. On raisonne alors par l'absurde : l'image d'un point de $Y(13)(\mathbb{Q}(\mu_{13}))$ par le revêtement $X(13) \longrightarrow X_1(13)$ fournirait "trop" de points de $Y_1(13)(\mathbb{Q}(\mu_{13}))$.

Nous noterons par la suite $\bar{n}$ l'image dans $\mathbb{Z}/13\mathbb{Z}$ d'un entier n, et $\widetilde{a}$ un relevé dans $\mathbb{Z}$ d'un entier a modulo 13. Soient $\Gamma_0(13)$, $\Gamma = \Gamma_1(13)$ les sous-groupes de $\mathrm{SL}_2(\mathbb{Z})$ formés des éléments congrus respectivement à $\left(\begin{smallmatrix}\star & \star\\ 0 & \star\end{smallmatrix}\right)$ et $\left(\begin{smallmatrix}1 & \star\\ 0 & 1\end{smallmatrix}\right)$ modulo 13. Nous noterons $S = S_2(\Gamma_1(13))$ l'espace des formes modulaires paraboliques de poids 2 pour $\Gamma_1(13)$. Pour $\phi : (\mathbb{Z}/13\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times$ un caractère, $S_2(13,\phi)$ désignera l'ensemble des formes f de S telles que, pour tout $\left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right)$ dans $\Gamma_0(13)$, $f|\left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right) = \phi(\bar{d}).f$. Nous noterons enfin W_{13} l'opérateur d'Atkin-Lehner, c'est-à-dire l'involution de $X_1(13)$ déduite de l'involution $z \mapsto -\frac{1}{13z}$ sur $\bar{\mathfrak{H}}$, où $\bar{\mathfrak{H}} = \mathfrak{H} \cup \mathbb{P}^1(\mathbb{Q})$, $\mathfrak{H}$ étant le demi-plan de Poincaré.

3.1 Etude du groupe $J_1(13)(\mathbb{Q}(\mu_{13}))$

Rappelons que deux pointes

$$\alpha_i = \frac{p_i}{q_i},\ i = 1,2,\ \mathrm{pgcd}(p_i, q_i) = 1,$$

sont équivalentes modulo $\Gamma = \Gamma_1(13)$ si et seulement si

$$q_2 = \lambda q_1 \pmod{13},\ p_2 = \lambda p_1 \pmod{\mathrm{pgcd}(q_1, 13)} \quad \lambda = \pm 1$$

(voir [4]). De plus les pointes sont toutes $\mathbb{Q}(\mu_{13})$-rationnelles et $\sigma \in (\mathbb{Z}/13\mathbb{Z})^\times \cong \mathrm{Gal}(\mathbb{Q}(\mu_{13})/\mathbb{Q})$ opère sur une pointe par $\left(\begin{smallmatrix}\sigma & 0\\ 0 & 1\end{smallmatrix}\right)$. Ainsi la courbe $X_1(13)$ possède six pointes $\mathbb{Q}$-rationnelles : $P_i = \Gamma.\frac{13}{i}$, $1 \le i \le 6$, et six autres pointes : $Q_j = \Gamma.\frac{j}{13}$, $1 \le j \le 6$. L'opérateur d'Atkin-Lehner W_{13} échange P_i et Q_i pour $1 \le i \le 6$.

Choisissons le plongement de $X_1(13)$ dans $J_1(13)$ donné par la pointe P_6 :

$$\begin{array}{rccc} \iota\ : & X_1(13) & \longrightarrow & J_1(13) \\ & P & \longmapsto & [(P) - (P_6)] \end{array}$$

Ogg [35] montre que le sous-groupe de $J_1(13)(\mathbb{Q}(\mu_{13}))$ engendré par les images sous ι des pointes $\mathbb{Q}$-rationnelles :

$$C_1 = \langle u_1, ..u_6\rangle\ u_i = \iota(P_i),\ 1 \le i \le 6,$$

est cyclique d'ordre 19. Par conséquent, le sous-groupe

$$C_2 = W_{13}.C_1 = \langle v_1, ..v_6\rangle,\ v_j = [(Q_j) - (Q_6)],\ 1 \le j \le 6,$$

l'est également. Ces deux groupes d'ordre 19, distincts pour des raisons de rationnalité, sont donc en somme directe et on a

$$(\mathbb{Z}/19\mathbb{Z})^2 \cong C_1 \oplus C_2 \subset J_1(13)(\mathbb{Q}(\mu_{13})).$$

On va en fait montrer l'égalité :

Proposition 3.2
On a $J_1(13)(\mathbb{Q}(\mu_{13})) = C_1 \oplus C_2$.

L'essentiel de la démonstration repose sur le lemme suivant :

Lemme 3.3
Le groupe $J_1(13)(\mathbb{Q}(\mu_{13}))$ est fini.

D'après ce qui précède, le lemme suivant suffira alors à prouver la proposition :

Lemme 3.4
Pour tout premier l distinct de 19, on a $J_1(13)(\mathbb{Q}(\mu_{13}))[l] = \{0\}$,
et pour tout $n \in \mathbb{N}$,

$$J_1(13)(\mathbb{Q}(\mu_{13}))[19^n] = J_1(13)(\mathbb{Q}(\mu_{13}))[19] \cong (\mathbb{Z}/19\mathbb{Z})^2.$$

3.1.1 Finitude de $J_1(13)(\mathbb{Q}(\mu_{13}))$

Rappelons que la courbe $X_1(13)$ est de genre $g = 2$. Le groupe $\Gamma_0(13)/\Gamma_1(13) \cong (\mathbb{Z}/13\mathbb{Z})^\times$ agissant sur S, on a : $S = \bigoplus_\phi S_2(13, \phi)$, où ϕ décrit l'ensemble des caractères pairs de $(\mathbb{Z}/13\mathbb{Z})^\times$ (voir [6]).

La formule de Riemann-Hurwitz montre que $S_2(13, \phi) = 0$ pour ϕ d'ordre distinct de l'ordre maximal 6. En effet si $\Gamma_1(13) \subset \mathrm{Ker}\phi \subset \Gamma_0(13)$ sont des inclusions strictes, la courbe modulaire associée à $\mathrm{Ker}\phi$ est de genre nul. Notons $\varepsilon, \bar{\varepsilon}$ les deux caractères d'ordre 6 de $(\mathbb{Z}/13\mathbb{Z})^\times$, et ζ une racine primitive douzième de l'unité. Ces deux caractères sont définis par $\varepsilon(2) = \zeta^2$, $\bar{\varepsilon}(2) = \zeta^{-2}$. On a $S = S_2(13, \epsilon) \oplus S_2(13, \bar{\epsilon})$, et les $\mathbb{C}$-espaces vectoriels $S_2(13, \epsilon)$ et $S_2(13, \bar{\epsilon})$ sont de dimension 1 engendrés chacun par une forme primitive f_ε et $f_{\bar{\varepsilon}}$ respectivement.

Les résultats de Kato ([14], corollaire 14.3) en direction de la conjecture de Birch et Swinnerton-Dyer montrent que si $L(J_1(13), \mathbb{Q}(\mu_{13}), 1) \neq 0$ alors $J_1(13)(\mathbb{Q}(\mu_{13}))$ est fini. De plus, d'après un théorème de Shimura complété par Carayol,

$$L(J_1(13), \mathbb{Q}(\mu_{13}), s) = \prod_{\chi,\ f} L(f, \chi, s),$$

où χ décrit l'ensemble des caractères de Dirichlet modulo 13 et f l'ensemble des formes primitives de poids 2 de niveau 13. D'après ce qui précède, on a donc :

$$L(J_1(13), \mathbb{Q}(\mu_{13}), 1) = \prod_{\chi:(\mathbb{Z}/13\mathbb{Z})^\times \to \mathbb{C}^\times} L(f_\varepsilon, \chi, 1).L(f_{\bar{\varepsilon}}, \chi, 1).$$

Pour prouver la finitude du groupe $J_1(13)(\mathbb{Q}(\mu_{13}))$, il suffit alors de prouver que la condition (C_1) suivante est satisfaite :

$$(C_1) \qquad \forall \chi : (\mathbb{Z}/13\mathbb{Z})^\times \to \mathbb{C}^\times,\ L(f_\varepsilon, \chi, 1) \neq 0,\ L(f_{\bar{\varepsilon}}, \chi, 1) \neq 0.$$

Pour $\chi : (\mathbb{Z}/13\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times$, notons $\tau(\chi) = \sum_{b \bmod 13} \chi(b) e^{-\frac{2i\pi\tilde{b}}{13}}$ la somme de Gauss. La formule ([19] théorèmes 3.9 et 4.2)

$$L(f, \chi, 1) = -\tau(\chi) \sum_{a \bmod 13} \bar{\chi}(a) \int_{\tilde{a}/13}^{\infty} f(u)du,\ (f \in S),$$

nous conduit à utiliser les symboles modulaires. Nous allons énoncer une condition (C_2) sur certains symboles modulaires qui entraîne (C_1) et donc la finitude de $J_1(13)(\mathbb{Q}(\mu_{13}))$.

Symboles modulaires et condition suffisante à la finitude de $J_1(13)(\mathbb{Q}(\mu_{13}))$

Dans cette section, nous verrons $X = X_1(13)(\mathbb{C})$ comme la surface de Riemann compacte connexe $\Gamma\backslash\bar{\mathfrak{H}}$, où $\bar{\mathfrak{H}} = \mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})$, $\mathfrak{H}$ étant le demi-plan de Poincaré. Pour ce qui concerne la théorie des symboles modulaires nous renvoyons à [4], [19], [22].

Soient $H_1(X;\mathbb{Z})$ (resp. $H_1(X, \text{ptes};\mathbb{Z})$) l'homologie singulière absolue (resp. relative à l'ensemble {ptes} des pointes) de X. Pour $\alpha,\ \beta \in \mathbb{P}^1(\mathbb{Q})$, on note $\{\alpha,\beta\}$, appelé *symbole modulaire*, la classe d'homologie dans $H_1(X, \text{ptes};\mathbb{Z})$ de l'image d'une géodésique reliant α à β.

Notons $H = H_1(X;\mathbb{C})$ et $H' = H_1(X, \text{ptes};\mathbb{C})$. Le $\mathbb{C}$-espace vectoriel H est de dimension $2g = 4$ et vérifie la suite exacte longue d'homologie :

$$(*) \qquad 0 \to H \to H' \xrightarrow{\delta} \mathbb{C}[\text{ptes}] \xrightarrow{\deg} \mathbb{C} \to 0,$$

où δ est l'application "bord" : $\{\alpha,\beta\} \mapsto (\Gamma\beta) - (\Gamma\alpha)$, et deg l'application "degré" usuelle sur les diviseurs. L'espace vectoriel H' est donc de dimension 15 sur $\mathbb{C}$.

On dispose également de l'homomorphisme de groupes de Manin :

$$\begin{array}{rccl} \xi\ : & \mathbb{C}[\Gamma\backslash SL_2(\mathbb{Z})] & \longrightarrow & H' \\ & [\Gamma.g] & \longmapsto & \{g0, g\infty\} = \{b/d, a/c\} \end{array}, \text{ avec } g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z}).$$

Rappelons que ξ est surjectif, de noyau engendré par les *relations de Manin*, c'est-à-dire par les éléments de la forme $[x] + [x\sigma]$, $[x] + [x\tau] + [x\tau^2]$, où $x \in \Gamma\backslash SL_2(\mathbb{Z})$, et $\sigma,\ \tau$ des éléments de $SL_2(\mathbb{Z})$ d'ordre respectif 4 et 3 :

$$\sigma = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right),\ \tau = \left(\begin{smallmatrix} 0 & -1 \\ 1 & -1 \end{smallmatrix}\right).$$

Notons $\mathcal{A} = [(\mathbb{Z}/13\mathbb{Z})^2 - (0,0)]$. Remarquons que l'application

$$\Gamma.\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mapsto (\bar{c}, \bar{d})$$

est une bijection de $\Gamma\backslash SL_2(\mathbb{Z})$ sur $\mathcal{A}$. Le morphisme de Manin fournit donc une application encore notée ξ sur $\mathbb{C}[\mathcal{A}]$. On note $[c,d]$, appelé *symbole de Manin*, l'image par ξ dans H' de l'élément (c,d) de $\mathcal{A}$. Le groupe $SL_2(\mathbb{Z})$ agit sur les symboles de Manin par multiplication à droite.

Les correspondances de Hecke $T_n,\ n \in \mathbb{N}$, et les opérateurs diamants $\langle m\rangle$, $(m,13) = 1$, sur $X_1(13)$, induisent des endomorphismes de H' que nous noterons respectivement T'_n et $\langle m\rangle'$: $t'.\{\alpha,\beta\} = \{t.\alpha, t.\beta\}$, où $\alpha,\beta \in \mathbb{P}^1(\mathbb{Q})$, $t = T_n$ ou $\langle m\rangle$. Soit $\mathbb{T}'$ la sous-algèbre de End (H') engendrée par les endomorphismes T'_p, et $\langle q\rangle'$ pour $p,\ q$ premiers, $q \neq 13$. L'espace H vu comme sous-espace de H' est stable sous l'action de $\mathbb{T}'$. L'action des opérateurs diamants est donnée par :

$$\langle m\rangle'[c,d] = [\bar{m}c, \bar{m}d].$$

Pour χ caractère de Dirichlet modulo 13 et x dans H', notons H'^{χ} (resp. H^{χ}) la composante χ-isotypique de H' (resp. H), et x^{χ} la projection de x sur H'^{χ}. Posons également :

$$e_\chi = t_\chi . \sum_{a \bmod 13} \chi(a).[1,a] \qquad \text{avec } t_\chi = \begin{cases} 1 & \text{si } \chi \text{ est impair,} \\ (T'_2 - 2\langle 2\rangle' - 1) & \text{si } \chi \text{ est pair.} \end{cases}$$

Lemme 3.5
La condition (C_2) suivante entraîne la condition (C_1) et donc la finitude du groupe $J_1(13)(\mathbb{Q}(\mu_{13}))$:

$$(C_2) \qquad \forall \chi : (\mathbb{Z}/13\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times,\ \theta_\chi^\epsilon \neq 0,\ \theta_\chi^{\bar\epsilon} \neq 0.$$

Démonstration du lemme. — Montrons tout d'abord que l'élément e_χ de H' est en réalité dans H.

On a

$$\delta(e_\chi) = \delta\left(t_\chi . \sum_{a \bmod 13} \chi(a).\left\{\frac{-1}{\widetilde{a}}, 0\right\}\right) = -\sum_{a \bmod 13} \chi(a)\left(t_\chi\left(\Gamma.\frac{-1}{\widetilde{a}}\right)\right).$$

Or

$$\Gamma.\left(\frac{-1}{\widetilde{a}}\right) = \Gamma.\frac{1}{\widetilde{a}} = \Gamma.\left(\frac{-1}{-\widetilde{a}}\right),$$

donc pour χ impair,

$$\delta(e_\chi) = -\sum_{k=1}^{6}(\chi(\bar k) + \chi(-\bar k))\left(\Gamma.\frac{1}{k}\right) = 0.$$

Pour χ pair, un calcul montre que $t_\chi(\Gamma.\frac{1}{\widetilde{a}}) = 0$ (voir [38], 2.4).

La conjugaison complexe sur X, déduite de l'involution $z \mapsto -\bar z$ sur $\mathfrak{H}$, induit sur H' l'involution $i : [c, d] \mapsto [-c, d]$. Le sous-espace H est stable sous i. Notons H^+ (resp. H^-) la partie invariante (resp.anti-invariante) de H sous i. On a $H = H^+ \oplus H^-$, et $H^+,\ H^-$ sont des $\mathbb{C}$-espaces vectoriels de dimension 2. On vérifie que $e_\chi \in H^+$ pour χ pair, et $e_\chi \in H^-$ pour χ impair.

On dispose d'autre part de l'application $\mathbb{C}$-linéaire : :

$$H \longrightarrow \mathrm{Hom}_{\mathbb{C}}(H^0(X, \Omega^1_X), \mathbb{C}), \qquad c \longmapsto \left(\omega \mapsto \int_c \omega\right).$$

Pour $f \in S = S_2(\Gamma_1(13))$, notons ω_f la différentielle holomorphe sur $X_1(13)$ induite par $2i\pi f(z)dz$. L'application $(f \mapsto \omega_f)$ est un isomorphisme de S sur $H^0(X, \Omega^1_X)$. Le morphisme qui s'en déduit :

$$F : \begin{cases} H \longrightarrow \mathrm{Hom}_{\mathbb{C}}(S, \mathbb{C}) \\ c \mapsto (f \mapsto \int_c \omega_f) \end{cases}$$

induit un isomorphisme F^+ sur H^+, resp. F^- sur H^-.

Soit $\mathbb{T}$ l'algèbre engendrée par les correspondances de Hecke T_p et les diamants $\langle q\rangle$ sur $X_1(13)$, pour $p,\ q$ premiers, $q \neq 13$. L'algèbre $\mathbb{T}$ agit à droite sur les formes modulaires et donc sur $\mathrm{Hom}_{\mathbb{C}}(S, \mathbb{C})$. Cette action munit l'espace vectoriel H^+, resp. H^-, d'une structure de $\mathbb{T}$-module : pour $t \in \mathbb{T},\ c \in H^\pm$, $t.c$ est défini par $\int_{t.c}\omega_f = \int_c \omega_{t.f}$. Les actions de $\mathbb{T}$ et $\mathbb{T}'$ sur H coïncident. En particulier l'action des opérateurs diamants fournit des isomorphismes sur chaque composante : $F^{\pm,\phi} : H^{\pm,\phi} \xrightarrow{\sim} \mathrm{Hom}_{\mathbb{C}}(S_2(13, \phi), \mathbb{C})$, pour ϕ caractère modulo 13. On en déduit $H^\phi = 0$ pour $\phi \neq \varepsilon,\ \bar\varepsilon$, et $H = H^\varepsilon \oplus H^{\bar\varepsilon}$.

Soient

$$c_\chi = \sum_{a \bmod 13} \bar{\chi}(a) \left\{ \frac{\widetilde{a}}{13}, \infty \right\} \in H', \quad f \in S, \quad \chi : (\mathbb{Z}/13\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times.$$

On a :

$$L(f, \chi, 1) = -\frac{\tau(\chi)}{13} \int_{c_\chi} \omega_f.$$

On remarque que $e_\chi = t_\chi W_{13} c_{\bar{\chi}}$. Notons t_χ^* l'élément de $\mathbb{T}$ tel que l'on a $t_\chi W_{13} = W_{13} t_\chi^*$.

Supposons à présent que la condition (C_2) est vérifiée. En particulier $\theta_\chi^\epsilon \neq 0$. Les isomorphismes $F^{\pm,\varepsilon}$ montrent qu'il existe $f \in S_2(13, \epsilon)$ telle que $\int_{\theta_\chi^\epsilon} \omega_f \neq 0$. L'espace $S_2(13, \epsilon)$ étant engendré par f_ε, il s'ensuit que $\int_{e_\chi} \omega_{f_\varepsilon} = \int_{\theta_\chi^\epsilon} \omega_{f_\varepsilon} \neq 0$.

Or

$$\int_{e_\chi} \omega_{f_\varepsilon} = \int_{t_\chi . W_{13} c_{\bar{\chi}}} \omega_{f_\varepsilon} = \int_{t_\chi^* . c_{\bar{\chi}}} \omega_{f_{\bar{\varepsilon}}} = \lambda_\chi . \int_{c_{\bar{\chi}}} \omega_{f_{\bar{\varepsilon}}} = -\frac{13 \lambda_\chi}{\tau(\bar{\chi})} L(f_{\bar{\varepsilon}}, \bar{\chi}, 1),$$

où $t_\chi^* . f_{\bar{\varepsilon}} = \lambda_\chi . f_{\bar{\varepsilon}}$, $\lambda_\chi \in \mathbb{C}$. Ceci prouve que si $\theta_\chi^\epsilon \neq 0$ alors $L(f_{\bar{\varepsilon}}, \bar{\chi}, 1) \neq 0$. De même, si $\theta_\chi^{\bar{\epsilon}} \neq 0$ alors $L(f_\varepsilon, \bar{\chi}, 1) \neq 0$. ◇

Vérification de la condition (C_2)

Nous allons faire les calculs dans les composantes H'^{ε}, $H'^{\bar{\varepsilon}}$ de H', espace pour lequel nous disposons de la présentation de Manin. Pour cela nous allons déterminer une base de H'^{ε} (resp. $H'^{\bar{\varepsilon}}$) et exprimer θ_χ^ϵ (resp. $\theta_\chi^{\bar{\epsilon}}$) dans cette base. La dimension de ces composantes se déduit de la suite exacte $(*)$ de la section 1.1.1 :

Lemme 3.6
On a $\dim H' = 15$, *et* $\dim H'^{\phi}$ *vaut* 0 *si* ϕ *est impair,* 1 *si* ϕ *est trivial,* 4 *si* $\phi = \varepsilon$ *ou* $\bar{\varepsilon}$, *et* 2 *sinon.*

Soit ϕ désignant indifféremment ε ou $\bar{\varepsilon}$. On peut voir H'^{ϕ} comme le quotient de H' par les relations :

$$[nu, nv] = \phi(n).[u, v], \ (n \in (\mathbb{Z}/13\mathbb{Z})^\times, \ (u, v) \in \mathcal{A}).$$

Notons $[u, v]^\phi$ l'image de $[u, v]$ dans H'^{ϕ}. Pour $u \neq 0$ dans $\mathbb{Z}/13\mathbb{Z}$, on a

$$[u, v]^\phi = \phi(u).[1, vu^{-1}]^\phi \quad \text{et} \quad [0, v]^\phi = \phi(v).[0, 1]^\phi.$$

On en déduit que $\{[0, 1]^\phi, \ [1, w]^\phi \, ; \, w \in \mathbb{Z}/13\mathbb{Z}\}$ forme un système de générateurs de H'^{ϕ}. En écrivant les relations de Manin pour ces générateurs, on obtient la proposition suivante :

Lemme 3.7
Les éléments $[1,0]^\phi,\ [1,2]^\phi,\ [1,3]^\phi,\ [1,-3]^\phi$ *forment une base de* H'^ϕ, *où* $\phi = \varepsilon$ *ou* $\bar{\varepsilon}$. *Dans cette base, les générateurs* $[0,1]^\phi,\ [1,w]^\phi,\ w \in \mathbb{Z}/13\mathbb{Z}$ *s'écrivent respectivement :*

$$\begin{array}{ll} [0,1]^\phi = -[1,0]^\phi & [1,1]^\phi = [1,-1]^\phi = 0 \\ [1,-2]^\phi = [1,2]^\phi & [1,6]^\phi = [1,-6]^\phi = -\phi(6).[1,2]^\phi \\ [1,4]^\phi = -\phi(4).[1,3]^\phi & [1,-4]^\phi = -\phi(4).[1,-3]^\phi \\ [1,5]^\phi = \phi(6).[1,3]^\phi - \phi(6).[1,2]^\phi & [1,-5]^\phi = \phi(4).[1,2]^\phi - \phi(4).[1,-3]^\phi \end{array}$$

Pour χ impair, on a alors :

$$\begin{aligned} e_\chi^\phi &= (\chi(3) - \chi(4)\phi(4) + \chi(5)\phi(6)).[1,3]^\phi \\ &\quad + (-\chi(3) + \chi(4)\phi(4) + \chi(5)\phi(4)).[1,-3]^\phi. \end{aligned}$$

Or χ est défini par $\chi(2) = \zeta^k$, ζ une racine primitive douzième de l'unité, $k = 1,3,5,7,9,11$. Donc $\chi(3) - \chi(4)\varepsilon(4) + \chi(5)\varepsilon(6) = \zeta^{4k} - \zeta^{2k+4} + \zeta^{9k+10}$. Ce terme est non nul pour $k = 1,3,5,7,9,11$, donc θ_χ^ϵ est non nul pour χ impair. De même, on montre que $\theta_\chi^{\bar{\epsilon}} \neq 0$ pour χ impair.

D'après [22], on a : $T_2'.[c,d] = [2c,d] + [2c,c+d] + [c+d,2d] + [c,2d]$. Donc, pour χ pair, on a :

$$\begin{aligned} e_\chi^\phi &= \sum_{a=1}^{12} \chi(a).([2,a]^\phi + [2,1+a]^\phi + [1+a,2a]^\phi + [1,2a]^\phi \\ &\quad - 2[2,2a]^\phi - [1,a]^\phi) \\ &= A_\phi.[1,2]^\phi + B_\phi.[1,3]^\phi + C_\phi.[1,-3]^\phi \end{aligned}$$

où

$$\begin{aligned} C_\phi &= [\chi(2)(1 - \phi(4) - \phi(2)) - \chi(3)\phi(2) + \chi(4)\phi(5) \\ &\quad + \chi(5)(\phi(2) + \phi(4)) + 2\chi(6)\phi(2)] \end{aligned}$$

Si χ est défini par $\chi(2) = \zeta^k$, on a

$$C_\varepsilon = \zeta^k(1 - \zeta^4 - \zeta^2) - \zeta^{4k+2} - \zeta^{2k+3} + \zeta^{9k}(\zeta^4 + \zeta^2) + 2\zeta^{5k+2}.$$

Ce terme étant non nul pour $k = 2,4,6,8,12$, $\theta_\chi^\epsilon \neq 0$ pour χ pair. De même $C_{\bar{\varepsilon}} \neq 0$ montre que $\theta_\chi^{\bar{\epsilon}} \neq 0$ pour χ pair.

Ceci termine la preuve de la finitude de $J_1(13)(\mathbb{Q}(\mu_{13}))$ (c'est-à-dire du lemme 3.3).

□

3.1.2 Fin de la preuve de la proposition 3.2

Comme nous l'avons signalé au début de la section 3.1, le groupe $J_1(13)(\mathbb{Q}(\mu_{13}))$ étant fini et contenant $C_1 \oplus C_2$, il suffit maintenant de montrer le lemme 3.4 pour achever la preuve de la proposition 3.2.

Preuve du lemme 3.4 : Soient p un nombre premier distinct de 13 et $\mathfrak{p}$ un idéal de $\mathbb{Z}[\mu_{13}]$ au dessus de p. Notons k_p (resp. $f_p = [k_p : \mathbb{F}_p]$) le corps (resp. le degré)

résiduel en $\mathfrak{p}$ de $\mathbb{Z}[\mu_{13}]$, $\overline{k_p}$ une clôture algébrique de k_p, et $\phi_p \in \mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)$ un endomorphisme de Frobenius en p. Le modèle de Néron $\mathcal{J}_1(13)$ sur $\mathbb{Z}$ de $J_1(13)$ a bonne réduction modulo p. Par conséquent, pour tout nombre premier l distinct de p, on a :

$$J_1(13)(\mathbb{Q}(\mu_{13}))[l] \hookrightarrow J_1(13)(k_p)[l].$$

Or $J_1(13)(k_p)[l]$ est l'ensemble des invariants sous $\phi_p^{f_p}$ de $J_1(13)(\overline{k_p})[l]$ muni de sa stucture de module galoisien. Montrons que pour $l \neq 19$ cet ensemble se réduit à $\{0\}$.

Pour $l \neq 2$, le $\mathbb{T}/l\mathbb{T}$-module $J_1(13)(\overline{k_p})[l]$ est libre de rang 2 (se reporter à [47], théorème 3.4 corollaire 2), et la relation d'Eichler-Shimura dans $\mathrm{End}_{\mathbb{T}}(J_1(13)(\overline{k_p})[l])$ (voir par exemple [44], théorème 2) :

$$\phi_p^2 - T_p\phi_p + p\langle p\rangle = 0$$

permet de trouver un polynôme $P_p \in \mathbb{T}/l\mathbb{T}[X]$ annulant $\phi_p^{f_p}$. Si le $\mathbb{T}/l\mathbb{T}$-module $J_1(13)(\overline{k_p})[l]$ admettait des invariants sous $\phi_p^{f_p}$ alors 1 serait racine de P_p. Un choix judicieux de p permet de conclure. Nous utiliserons également le fait que $\mathbb{T} \cong \mathbb{Z}[Y]/\Phi_6(Y)$ en niveau 13 (voir [17]).

Choisissons d'abord $p = 3$. Soit l premier $l \neq 2, 3$. On a $f_3 = 3$, et un calcul montre que le polynôme suivant annule ϕ_3^3 :

$$P_3 = X^2 + (9\langle 3\rangle T_3 - T_3^3)X + 27\langle 3\rangle^3.$$

Dans $\mathbb{T}/l\mathbb{T} \cong \mathbb{F}_l[Y]/\overline{\Phi_6}(Y)$, T_3 s'écrit $2Y - 2$ et $\langle 3\rangle = Y$ (voir [17]), donc

$$P_3(1) = 1 + 9Y(2Y - 2) + 27Y^3 = 2 \times 19.$$

On en déduit que pour $l \neq 2, 3, 19$, on a $J_1(13)(\mathbb{Q}(\mu_{13}))[l] = \{0\}$.

Soit maintenant $p = 5$ et $l \neq 2,\ 5$. On a $f_5 = 4$ et ϕ_5^4 est annulé par :

$$P_5 = X^2 + (20\langle 5\rangle T_5^2 - T_5^4 - 50\langle 5\rangle^2)X + 625\langle 5\rangle^4.$$

Dans $\mathbb{T}/l\mathbb{T} \cong \mathbb{F}_l[Y]/\overline{\Phi_6}(Y)$, $T_5 = -2Y + 1$ et $\langle 5\rangle = -1$, donc

$$P_5(1) = 627 = 3 \times 11 \times 19,$$

et pour $l \neq 2, 3, 5, 11, 19$, $J_1(13)(\mathbb{Q}(\mu_{13}))[l] = \{0\}$.

Les choix de p qui précèdent montrent que pour l distinct de $2, 3$ et 19, on a $J_1(13)(\mathbb{Q}(\mu_{13}))[l] = \{0\}$. Pour le cas $l = 3$, choisissons $p = 79$. On a $f_{79} = 1$ car $79 \equiv 1 \pmod{13}$. Le polynôme $P_{79} = X^2 - T_{79}X + 79\langle 79\rangle$ annule ϕ_{79}. Dans $\mathbb{T}/3\mathbb{T} \cong \mathbb{F}_3[Y]/\overline{\Phi_6}(Y)$, on a $T_{79} = 4$, $\langle 79\rangle = 1$, donc $P_{79}(1) = 76$. Or $76 \not\equiv 0 \mod 3$, donc $J_1(13)(\mathbb{Q}(\mu_{13}))[3] = \{0\}$.

Examinons le cas de la 2-torsion. Considérons ϕ_5^4 sur le $\mathbb{F}_2$-espace vectoriel $J_1(13)(\overline{\mathbb{F}_5})[2]$ de dimension 4. Le polynôme

$$P_5 = X^2 + X + 1 \in \mathbb{F}_2[X] \subset \mathbb{T}/2\mathbb{T}[X] \cong \mathbb{F}_4[X]$$

annule ϕ_5^4 et n'admet pas 1 pour racine. Donc $J_1(13)(\mathbb{Q}(\mu_{13}))[2] = \{0\}$.

Terminons par le cas de la 19-torsion. On a

$$(\mathbb{Z}/19\mathbb{Z})^2 \cong C_1 \oplus C_2 \subset J_1(13)(\mathbb{Q}(\mu_{13}))[19].$$

D'autre part, le calcul de la borne de Weil pour $J_1(13)(\mathbb{F}_{3^3})$ donne

$$|J_1(13)(\mathbb{F}_{3^3})| \leq 1587.$$

Or $19^3 > 1587$, donc $|J_1(13)(\mathbb{F}_{3^3})[19^\infty]| = 19^k$ avec $k \leq 2$. On en déduit que $|J_1(13)(\mathbb{Q}(\mu_{13}))[19]| = |J_1(13)(\mathbb{Q}(\mu_{13}))[19^\infty]| = 19^2$.

□

3.2 Borne pour le cardinal de $Y_1(13)(\mathbb{Q}(\mu_{13}))$

3.2.1 Quotient de $X_1(13)$ par une involution et conséquences

Lemme 3.8
Soit $(i,j) \in \{1,\ldots,6\}^2$. Aucune fonction rationnelle sur $X_1(13)$ n'a pour diviseur des pôles $P_i + Q_j$.

Démonstration. — Considérons la courbe modulaire $X_2(13)$ associée au sous-groupe d'indice 3 de $\Gamma_0(13)$ suivant :

$$\Gamma_2(13) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(13),\ a^2 \equiv \pm 1 \pmod{13}\}.$$

Cette courbe est de genre nul et induit les revêtements :

$$X_1(13) \xrightarrow{2} X_2(13) \xrightarrow{3} X_0(13).$$

Notons $f : X_1(13) \longrightarrow X_2(13)$, et σ_5 l'élément de $\Gamma_0(13)$ congru à $\left(\begin{smallmatrix} \bar{5}^{-1} & 0 \\ 0 & \bar{5} \end{smallmatrix}\right)$ modulo 13. Comme $\bar{5}^2 \equiv -1 \pmod{13}$, on a $\sigma_5 \in \Gamma_2(13)$. D'autre part, σ_5 agit sur les pointes de $X_1(13)$ par

$$\sigma_5.P_i = \Gamma.\frac{13}{5i},\ \sigma_5.Q_j = \Gamma.\frac{5j}{13}.$$

Donc $f(P_1) = f(P_5),\ f(P_2) = f(P_3),\ f(P_4) = f(P_6),\ f(Q_1) = f(Q_5),\ f(Q_2) = f(Q_3),\ f(Q_4) = f(Q_6)$ sont des pointes de $X_2(13)$.

Soit ψ un isomorphisme de $X_2(13)$ sur $\mathbb{P}^1$ qui envoie la pointe $f(P_1)$ sur $\infty \in \mathbb{P}^1$. La fonction $\widetilde{f} = \psi \circ f$ est un revêtement de degré 2 de $X_1(13)$ sur $\mathbb{P}^1$. Ce qui précède montre que la fonction rationnelle sur $X_1(13)$ induite par $\widetilde{f}$ admet pour diviseur des pôles

$$P_1 + P_5 \sim P_2 + P_3 \sim P_4 + P_6 \sim Q_1 + Q_5 \sim Q_2 + Q_3 \sim Q_4 + Q_6.$$

Une fonction rationnelle de diviseur des pôles $P_i + Q_j,\ (i,j) \in \{1,..6\}^2$, induirait un revêtement de degré 2 de $X_1(13)$ sur $\mathbb{P}^1$ distinct de $\widetilde{f}$, ses fibres au dessus de ∞ étant distinctes. L'unicité d'un revêtement de degré 2 de $\mathbb{P}^1$ par une courbe de genre 2 interdit cette éventualité. □

3.2.2 Borne

Proposition 3.9
Le cardinal de $Y_1(13)(\mathbb{Q}(\mu_{13}))$ est inférieur ou égal à 12^2.

Démonstration. — Rappelons que l'on a $J_1(13)(\mathbb{Q}(\mu_{13})) = C_1 \oplus C_2$, avec $C_1 = \langle u_1, ..u_6\rangle \subset J_1(13)(\mathbb{Q})$, $C_2 = W_{13}.C_1 = \langle v_1, ..v_6\rangle$, $u_i = \iota(P_i)$, et $v_j = [(Q_j) - (Q_6)]$, pour $1 \leq i,\ j \leq 6$ (proposition 3.2). Les résultats de Ogg [35] montrent que C_1 et C_2 sont des groupes cycliques d'ordre 19, et que l'on a $u_i = a_i u_4,\ v_i = a_i v_4,\ a_i \in \mathbb{Z}/19\mathbb{Z}$, avec $a_1 = 4,\ a_2 = -5,\ a_3 = 6,\ a_4 = 1,\ a_5 = -3,\ a_6 = 0$, où on note encore n la classe d'un entier n dans $\mathbb{Z}/19\mathbb{Z}$.

En particulier, il existe $(a, b) \in (\mathbb{Z}/19\mathbb{Z})^2$ tels que

$$\iota(Q_6) = [(Q_6) - (P_6)] = au_4 + bv_4.$$

Or $W_{13}.\iota(Q_6) = -\iota(Q_6) = bu_4 + av_4$ donc $b = -a$ dans $\mathbb{Z}/19\mathbb{Z}$. De plus d'après 2.1, on a $P_4 + P_6 \sim Q_4 + Q_6$ donc $2\iota(Q_6) = u_4 - v_4 = 2au_4 - 2av_4$. On en déduit que $a = -9$ et $\iota(Q_6) = -9u_4 + 9v_4$.

Considérons à présent P dans $Y_1(13)(\mathbb{Q}(\mu_{13}))$. Notons $u = \iota(P)$ et soient $(\mu, \nu) \in (\mathbb{Z}/19\mathbb{Z})^2$ tels que $u = \mu u_4 + \nu v_4$. Ogg montre que $C_1 \cap \iota(Y_1(13)) = \emptyset$. On en déduit que $\nu \neq 0$. D'autre part, si $\mu = -9$, on a $u = \iota(Q_6) + (\nu - 9)v_4$, donc $[(P) - (Q_6)] \in C_2$, c'est-à-dire $\iota(W_{13}.P) \in C_1 \cap \iota(Y_1(13))$. Ceci étant impossible, $\mu \neq -9$. Supposons maintenant qu'il existe i, j et k dans $\{1, ..6\}$ tels que $u = u_i + v_j - v_k$. On aurait alors $P + Q_k \sim P_i + Q_j$, ce qui est impossible d'après 2.1. La différence $a_j - a_k$ décrivant $\mathbb{Z}/19\mathbb{Z}$ lorsque j, k décrivent $\{1, ..6\}$, ceci impose $\mu \neq 0, 1, 4, 6, -3, -5$. De même, on montre que $u \neq u_i - u_k + v_j + \iota(Q_6)$, ce qui impose $\nu \neq 9, -9, 6, -6, 4, -4$.

Les contraintes précédentes sur les valeurs de (μ, ν) montrent la proposition. □

3.3 Preuve du théorème 3.1

Il s'agit de montrer que $Y(13)(\mathbb{Q}(\mu_{13}))$ est vide. Procédons par l'absurde : soit (E, π) un point de $Y(13)(\mathbb{Q}(\mu_{13}))$, où E est une courbe elliptique définie sur $\mathbb{Q}(\mu_{13})$ et π est un plongement : $\pi : (\mathbb{Z}/13\mathbb{Z})^2 \longrightarrow E[13]$. Un tel point donne lieu à $(13^2 - 1)/2 = 84$ points[1] de $Y_1(13)(\mathbb{Q}(\mu_{13}))$. Notons $\mathcal{P}_{(E,\pi)}$ cet ensemble de points. Supposons que pour tout x de $\mathcal{P}_{(E,\pi)}$, $W_{13}.x$ n'est pas dans $\mathcal{P}_{(E,\pi)}$. Alors le sous-ensemble $\mathcal{P}_{(E,\pi)} \cup W_{13}.\mathcal{P}_{(E,\pi)}$ de $Y_1(13)(\mathbb{Q}(\mu_{13}))$ est de cardinal $2 \times 84 = 168 > 12^2$, ce qui est impossible d'après la proposition 3.9.

Par conséquent, il existe $x \in \mathcal{P}_{(E,\pi)}$ tel que $y = W_{13}.x \in \mathcal{P}_{(E,\pi)}$. Autrement dit, il existe $P,\ Q$ deux points d'ordre 13 de E définis sur $\mathbb{Q}(\mu_{13})$ et un isomorphisme défini sur $\mathbb{Q}(\mu_{13})$ envoyant (E, Q) sur

$$W_{13}.(E, P) = (E/\langle P\rangle, P' + \langle P\rangle),$$

[1] En effet, $\mathrm{Aut}(E)$ est d'ordre 2, *i.e.* $j(E) \neq 0, 1728$, car $\mathbb{Q}(\mu_{13})$ ne contient ni $\mathbb{Q}(\sqrt{-1})$ ni $\mathbb{Q}(\sqrt{-3})$.

où P' est le point d'ordre 13 de E tel que $e_{13}(P', P) = e^{2i\pi/13}$, l'application $e_{13} : E[13] \times E[13] \longrightarrow \mu_{13}$ l'accouplement de Weil.

En particulier, on dispose d'une isogénie ψ de E dans E de degré 13 définie sur $\mathbb{Q}(\mu_{13})$. La courbe elliptique E est donc à multiplication complexe. L'ensemble des endomorphismes End E de E sur $\mathbb{C}$ est isomorphe à un ordre R d'un corps quadratique imaginaire. Soit $[.] : R \longrightarrow$ End E l'isomorphisme normalisé, et $\alpha \in R$ tel que $\psi = [\alpha]$. L'isogénie $[\alpha]$ étant définie sur $\mathbb{Q}(\mu_{13})$ ainsi que la courbe elliptique E, on a $\alpha \in \mathbb{Q}(\mu_{13})$. Or $13 \equiv 1 \pmod 4$, donc $\mathbb{Q}(\mu_{13})$ ne contient aucun corps quadratique imaginaire, et donc $\alpha \in \mathbb{Q}$. C'est impossible car sinon, $13 = \deg[\alpha] = | N_{\mathbb{Q}}^{K}(\alpha) |$ serait un carré. Ceci achève la preuve.

□

3.4 Remarque

Lorsque j'ai exposé cette démonstration pendant les vingt-deuxièmes Journées Arithmétiques (juin 2001), B. Poonen m'a signalé un résultat de R. F. Coleman qui, en utilisant la finitude du groupe $J_1(13)(\mathbb{Q}(\mu_{13}))$, fournit une borne plus petite du cardinal de $Y_1(13)(\mathbb{Q}(\mu_{13}))$, et simplifie alors la démonstration du théorème.

Rappelons le résultat de Coleman [2] :

Théorème 3.10 (Coleman)
Soient C une courbe de genre g définie sur un corps de nombres K, et J sa jacobienne. Supposons que le rang de $J(K)$ soit au plus $g-1$. Soit $\mathfrak{p}$ un idéal non ramifié de K en lequel C a bonne réduction et de caractéristique résiduelle supérieure à $2g$. Notons $f_{\mathfrak{p}}$ le degré résiduel en $\mathfrak{p}$. Alors

$$|C(K)| \leq f_{\mathfrak{p}} + 2g(\sqrt{f_{\mathfrak{p}}} + 1) - 1.$$

Appliquons ce théorème à $C = X_1(13)$, $K = \mathbb{Q}(\mu_{13})$, $\mathfrak{p}|53$, pour lesquels les hypothèses sont vérifiées, en particulier grâce au lemme 3.3 qui assure que le rang de $J_1(13)(\mathbb{Q}(\mu_{13}))$ est inférieur à $g - 1 = 1$. On obtient : $|X_1(13)(\mathbb{Q}(\mu_{13}))| \leq 85$ donc $|Y_1(13)(\mathbb{Q}(\mu_{13}))| \leq 73$. On raisonne alors par l'absurde comme dans la section 3 : un point de $Y(13)(\mathbb{Q}(\mu_{13}))$ donnerait lieu à 84 points de $Y_1(13)(\mathbb{Q}(\mu_{13}))$, ce qui est impossible d'après ce qui précède.

Chapitre 4

Homologie des courbes modulaires et module supersingulier

Notations. — Dans ce chapitre et ceux qui suivent nous adopterons les notations suivantes. Soit p un nombre premier. On note $\bar{\mathbb{F}}_p$ une clôture algébrique de $\mathbb{F}_p$. On désigne par n le numérateur et par δ le dénominateur de $(p-1)/12$.

Soit A un anneau (dans ce qui suit $A = \mathbb{Q}, \bar{\mathbb{Q}}, \mathbb{C}$, ou $\mathbb{Z}\big[\frac{1}{a}\big]$). Pour M et N des $\mathbb{Z}$-modules, et $u : M \longrightarrow N$ un morphisme de $\mathbb{Z}$-modules, on pose $M_A = M \otimes A$ et $u_A : M_A \longrightarrow N_A$ le morphisme de A-modules obtenu par extension des scalaires. Lorsque le contexte est suffisamment clair, nous nous permettons d'omettre l'indice pour u_A. Si $A = \mathbb{Z}\big[\frac{1}{a}\big]$, a entier non nul, on note plus simplement $M\big[\frac{1}{a}\big] = M \otimes A$ et $u\big[\frac{1}{a}\big] = u_A$.

On rappelle que $Y = \Gamma\backslash\mathfrak{H} = Y_0(p)(\mathbb{C})$ est la surface de Riemann associée à $\Gamma_0(p)$, $X = \Gamma_0(p)\backslash\big(\mathfrak{H} \cup \mathbb{P}^1(\mathbb{Q})\big) = X_0(p)(\mathbb{C})$ sa compactifiée, et $J = J_0(p)(\mathbb{C})$ la jacobienne de X. On note ptes l'ensemble des pointes de X et

$$\varpi : \mathfrak{H} \cup \mathbb{P}^1(\mathbb{Q}) \twoheadrightarrow X$$

la surjection canonique.

Soit $\widetilde{\mathbb{T}}$ l'algèbre engendrée par l'action des opérateurs de Hecke $T_m,\ m \geq 1$ sur le $\mathbb{C}$-espace vectoriel $\mathrm{M}_2(\Gamma_0(p))$ des formes modulaires de poids 2 et de niveau p. L'algèbre $\mathbb{T}$ introduite au paragraphe 1.1.2 n'est autre que l'image de $\widetilde{\mathbb{T}}$ dans l'anneau des endomorphismes du sous-espace vectoriel $\mathrm{S}_2(\Gamma_0(p))$ de $\mathrm{M}_2(\Gamma_0(p))$ constitué des formes paraboliques. Ce sont les notations adoptées par Mazur [20].

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

Soient $\mathfrak{m}$ un idéal maximal de $\widetilde{\mathbb{T}}$, U et V des $\widetilde{\mathbb{T}}$-modules, et $u : U \longrightarrow V$ un morphisme de $\widetilde{\mathbb{T}}$-modules. On note $k_\mathfrak{m} = \widetilde{\mathbb{T}}/\mathfrak{m}$, $U_\mathfrak{m} = \varprojlim \big(U/\mathfrak{m}^k U\big)$ le séparé complété de U pour la topologie $\mathfrak{m}$-adique, et $u_\mathfrak{m} : U_\mathfrak{m} \longrightarrow V_\mathfrak{m}$ le morphisme de $\widetilde{\mathbb{T}}_\mathfrak{m}$-modules induit par u sur les séparés complétés.

4.1 Formes modulaires (rappels)

Soit $\mathcal{M}$ le $\mathbb{Z}$-module des formes modulaires de développement de Fourier à l'infini $\sum_{m\geq 0} a_m q^m$ avec $a_0 \in \frac{1}{2}\mathbb{Z}$ et $a_m \in \mathbb{Z}$ pour $m \geq 1$. L'algèbre $\widetilde{\mathbb{T}}$ agit fidèlement sur $\mathcal{M}$. Il est connu que le $\widetilde{\mathbb{T}}_{\mathbb{Q}}$-module $\mathcal{M}_{\mathbb{Q}}$ est libre de rang 1. Soit $\mathcal{N}$ le sous-$\widetilde{\mathbb{T}}$-module de $\mathcal{M}_{\mathbb{Q}}$ constitué des formes modulaires de développement de Fourier à l'infini $\sum_{m\geq 0} a_m q^m$ avec $a_m \in \mathbb{Z}$ pour $m \geq 1$. Enfin, notons $\mathcal{M}^0$ le sous-$\mathbb{Z}$-module des formes paraboliques dans $\mathcal{M}$ ou $\mathcal{N}$ indifféremment. L'action de $\widetilde{\mathbb{T}}$ sur $\mathcal{M}^0$ se factorise par $\mathbb{T}$. Le $\mathbb{T}_{\mathbb{Q}}$-module $\mathcal{M}^0_{\mathbb{Q}}$ est libre de rang 1. L'accouplement défini par $\langle f, T\rangle = a_1(f \mid T)$ induit un isomorphisme naturel de $\widetilde{\mathbb{T}}$-modules

$$\mathcal{N} \xrightarrow{\sim} \mathrm{Hom}(\widetilde{\mathbb{T}}, \mathbb{Z})$$

et un isomorphisme de $\mathbb{T}$-modules

$$\mathcal{M}^0 \xrightarrow{\sim} \mathrm{Hom}(\mathbb{T}, \mathbb{Z})$$

(voir par exemple [8] proposition 1.3). Le conoyau de l'injection de $\mathcal{M}$ dans $\mathcal{N}$ est isomorphe à $\mathbb{Z}/\delta\mathbb{Z}$ (*loc. cit.* proposition 1.1).

Considérons l'application injective

$$\mathcal{M}_{\mathbb{C}} = \mathrm{M}_2(\Gamma_0(p)) \longrightarrow \mathbb{C}[[q]] \tag{4.1}$$

qui à une forme modulaire associe son développement de Fourier à l'infini. Le $\mathbb{Z}$-module $\mathcal{M}^0$ n'est autre que l'intersection entre $\mathrm{S}_2(\Gamma_0(p))$ et la préimage de $\mathbb{Z}[[q]]$ par cette application. Pour A un anneau, un élément de $\mathcal{M}^0_A$ sera appelé *forme parabolique à coefficients dans* A (voir par exemple [6] 12.3). Le morphisme

$$\mathcal{M}^0_A \longrightarrow A[[q]]$$

déduit de (4.1) par extension des scalaires à A est encore injectif.

Lorsque $\mathfrak{m}$ est un idéal maximal de $\widetilde{\mathbb{T}}$ de caractéristique $l \neq 2$, l'anneau $\mathbb{T}_{\mathfrak{m}}$ est de Gorenstein (voir [20] corollaires 15.2 et 16.3). Il s'ensuit (voir par exemple [8]) que $\mathcal{N}_{\mathfrak{m}}$ et $\mathcal{M}_{\mathfrak{m}}$ sont des $\widetilde{\mathbb{T}}_{\mathfrak{m}}$-modules libres de rang 1, et que $\mathcal{M}^0_{\mathfrak{m}}$ est un $\mathbb{T}_{\mathfrak{m}}$-module libre de rang 1.

Soit

$$E = \frac{p-1}{24} + \sum_{m\geq 1} \sigma'(m) q^m, \quad \text{où} \quad \sigma'(m) = \sum_{d|m,(p,d)=1} d, \tag{4.2}$$

la série d'Eisenstein normalisée de poids 2 sur $\Gamma_0(p)$. La série $E \in \mathcal{N}$ est une forme propre pour l'action de $\widetilde{\mathbb{T}}$ et définit donc un morphisme de groupes surjectif

$$\begin{array}{rccc} \pi : & \widetilde{\mathbb{T}} & \longrightarrow & \mathbb{Z} \\ & T_m & \longmapsto & \sigma'(m) \end{array}.$$

Soit I l'idéal de $\widetilde{\mathbb{T}}$ noyau de π. L'idéal I est engendré par $1+w$ et $1+l-T_l$ pour l parcourant l'ensemble des nombres premiers distincts de p. Son image $\mathcal{I} = I\mathbb{T}$ dans $\mathbb{T}$ est l'*idéal d'Eisenstein* de [20]. Un idéal premier dans le support

de $\mathcal{I}$ est appelé *idéal premier d'Eisenstein*. Il en existe dès lors que $g > 0$. L'idéal $\mathcal{I}$ est d'indice fini n dans $\mathbb{T}$ (voir [20] proposition 9.7).

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 [10], on normalise le produit scalaire de Petersson d'une forme parabolique f et d'une forme modulaire g de la façon suivante

$$(f,g) = \iint_X \omega_f \wedge i\,\overline{\omega}_g = 8\pi^2 \iint_{\Gamma_0(p)\backslash\mathfrak{H}} f(z)\overline{g(z)}dxdy. \tag{4.3}$$

4.2 Homologie des courbes modulaires (rappels)

4.2.1 La théorie de Manin

Reprenons les notations de [23]. Notons

$$\mathcal{H}^{\mathrm{ptes}} = H_1(X, \mathrm{ptes}\,;\mathbb{Z}), \quad \mathcal{H}_{\mathrm{ptes}} = H_1(Y\,;\mathbb{Z}), \quad \text{et} \quad \mathcal{H} = H_1(X\,;\mathbb{Z}).$$

On a une injection canonique

$$\alpha^{\mathrm{ptes}} : \mathcal{H} \hookrightarrow \mathcal{H}^{\mathrm{ptes}}, \tag{4.4}$$

et une surjection canonique

$$\alpha_{\mathrm{ptes}} : \mathcal{H}_{\mathrm{ptes}} \twoheadrightarrow \mathcal{H}. \tag{4.5}$$

Les produits d'intersection définissent des accouplements parfaits notés $\bullet$:

$$\mathcal{H}^{\mathrm{ptes}} \times \mathcal{H}_{\mathrm{ptes}} \longrightarrow \mathbb{Z} \quad \text{et} \quad \mathcal{H} \times \mathcal{H} \longrightarrow \mathbb{Z}. \tag{4.6}$$

Ces accouplements sont compatibles à α_{ptes} et α^{ptes}, *i.e.* on a

$$\alpha^{\mathrm{ptes}}(x) \bullet y = x \bullet \alpha_{\mathrm{ptes}}(y) \quad (y \in \mathcal{H}_{\mathrm{ptes}},\ x \in \mathcal{H}). \tag{4.7}$$

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 $\mathfrak{H}$.

Le groupe $\mathcal{H}$, identifié à un sous-groupe de $\mathcal{H}^{\mathrm{ptes}}$, est le noyau de l'application *bord* β définie par

$$\begin{array}{rccc} \beta\ : & \mathcal{H}^{\mathrm{ptes}} & \longrightarrow & \mathbb{Z}[\mathrm{ptes}] \\ & \{x,y\} & \longmapsto & (\Gamma_0(p).y) - (\Gamma_0(p).x). \end{array} \tag{4.8}$$

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

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

Dorénavant, 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 $\Gamma_0(p)$.

Posons $\rho = e^{2i\pi/3}$, $R = \varpi(\mathrm{SL}_2(\mathbb{Z})\rho)$ et $I = \varpi(\mathrm{SL}_2(\mathbb{Z})i)$. 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

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

avec, pour tout $g \in \Gamma_0(p)\backslash\mathrm{SL}_2(\mathbb{Z})$,

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

Pour $g \in \Gamma_0(p)\backslash\mathrm{SL}_2(\mathbb{Z})$, 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 $x = \sum_{g\in\Gamma_0(p)\backslash\mathrm{SL}_2(\mathbb{Z})} \lambda_g\, g \in \mathcal{E}_{\Gamma_0(p)}$. 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 [23]). Cela définit une application :

$$\begin{array}{rccc} \xi_0\ : & \mathcal{E}_{\Gamma_0(p)} & \longrightarrow & \mathcal{H}_{\mathrm{ptes}} \\ & \sum_{g\in\Gamma_0(p)\backslash\mathrm{SL}_2(\mathbb{Z})} \lambda_g g & \longmapsto & \sum_{g\in\Gamma_0(p)\backslash\mathrm{SL}_2(\mathbb{Z})} \lambda_g[gi, g\rho]. \end{array}$$

Théorème 4.1 (Manin, Merel)

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

$$\xi^0(g) \bullet \xi_0\left(\sum \mu_{h\in\Gamma_0(p)\backslash\mathrm{SL}_2(\mathbb{Z})} h\right) = \mu_g.$$

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 *:*

$$\xi^0(g) + \xi^0(g\sigma) = 0 \quad \textit{et} \quad \xi^0(g) + \xi^0(g\tau) + \xi^0(g\tau^2) = 0. \tag{4.9}$$

Démonstration. — Voir [19] et [24]. □

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 à l'action à droite de $\mathrm{SL}_2(\mathbb{Z})$ sur $\Gamma_0(p)\backslash\mathrm{SL}_2(\mathbb{Z})$ et $\mathbb{P}^1(\mathbb{F}_p)$. On rappelle que $\mathrm{SL}_2(\mathbb{Z})$ agit à droite sur $\mathbb{P}^1(\mathbb{F}_p)$ par

$$[c:d]\begin{pmatrix} u & v \\ w & t \end{pmatrix} = [uc+wd : vc+td] \quad \left([c:d]\in\mathbb{P}^1_{\mathbb{F}_p},\ \begin{pmatrix} u & v \\ w & t \end{pmatrix}\in \mathrm{SL}_2(\mathbb{Z})\right).$$

Notons encore ξ^0 l'application de $\mathbb{Z}[\mathbb{P}^1(\mathbb{F}_p)]$ vers $\mathcal{H}^{\mathrm{ptes}}$ obtenue 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

$$\xi^0([\bar{c}:\bar{d}]) = \left\{\frac{b}{d}, \frac{a}{c}\right\}$$

où $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. Remarquons que

$$[\bar{c}:\bar{d}] = \begin{cases} [\bar{c}\bar{d}^{-1}:1] & \text{si } d\not\equiv 0 \pmod p \\ [\bar{c}:0]=[1:0] & \text{sinon.} \end{cases}$$

Passons à un système non homogène de coordonnées : on note $\infty = [1:0] \in \mathbb{P}^1_{\mathbb{F}_p}$ et $c/d = [c:d]$. pour c et d deux entiers tels que p ne divise pas d.

Pour c et d deux entiers premiers entre eux, on a donc

$$\xi^0\left(\frac{c}{d}\right) = \begin{cases} \xi^0(0) & \text{si } c\equiv 0 \pmod p \\ \xi^0(\infty) & \text{si } d\equiv 0 \pmod p \\ \xi^0(k) & \text{sinon, avec } k\in\mathbb{Z},\ (k,p)=1,\ kd\equiv c \pmod p. \end{cases} \tag{4.10}$$

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 $\xi^0(0) = \{0,\infty\} = -\xi^0(\infty)$.

Pour $[\bar{c}:\bar{d}] \in \mathbb{P}^1(\mathbb{F}_p)$, on a $[\bar{c}:\bar{d}]\sigma = [\bar{d}:-\bar{c}]$, et $[\bar{c}:\bar{d}]\tau = [\bar{d}:\bar{d}-\bar{c}]$. Les relations de Manin peuvent s'écrire :

$$\xi^0\left(\frac{c}{d}\right) + \xi^0\left(-\frac{d}{c}\right) = 0 \quad \text{et} \quad \xi^0\left(\frac{c}{d}\right) + \xi^0\left(\frac{d}{d-c}\right) + \xi^0\left(\frac{c-d}{c}\right) = 0. \tag{4.11}$$

Considérons le morphisme de groupes

$$\alpha^{\mathrm{ptes}} \circ \alpha_{\mathrm{ptes}} : \mathcal{H}_{\mathrm{ptes}} \longrightarrow \mathcal{H}^{\mathrm{ptes}}.$$

Théorème 4.2
Pour tout $u = \sum_{g\in\Gamma_0(p)\backslash\mathrm{SL}_2(\mathbb{Z})} \lambda_g g \in \mathcal{E}_{\Gamma_0(p)}$, on a

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

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 4.2 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). Dans les calculs qui suivent les sommes portent sur $\Gamma_0(p)\backslash\mathrm{SL}_2(\mathbb{Z})$. On a

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

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

$$\begin{aligned}\sum_g\lambda_g\{gi,g\rho\} &= \frac{1}{2}\sum_g(\lambda_g\{gi,g\infty\}-\lambda_g\{gi,g0\})\\ &\quad-\frac{1}{3}\sum_h(\lambda_{h\tau}+\lambda_{h\tau^2})\{h\infty,h\rho\}\\ &\quad-\frac{1}{3}\sum_h(\lambda_{h\tau}\{h\rho,h0\}+\lambda_{h\tau^2}\{h\rho,h\tau0\})\\ &= \frac{1}{2}\sum_g\lambda_g\{g0,g\infty\}-\frac{1}{3}\sum_g\lambda_{g\tau}\{g\infty,g0\}\\ &\quad-\frac{1}{3}\sum_g\lambda_{g\tau^2}\{g\infty,g\tau0\}.\end{aligned}$$

Donc on a

$$\begin{aligned}\sum_g \lambda_g\{gi, g\rho\} &= -\frac{1}{2}\sum_{g\in A(\Gamma_0(p))} \lambda_{g\tau}\{g0, g\infty\} - \frac{1}{2}\sum_{g\in A(\Gamma_0(p))} \lambda_{g\tau^2}\{g0, g\infty\} \\ &\quad + \frac{1}{3}\sum_g \lambda_{g\tau}\{g0, g\infty\} + \frac{1}{3}\sum_g \lambda_{g\tau^2}\{g0, g\infty\} \\ &\quad + \frac{1}{3}\sum_g \lambda_{g\tau^2}\{g\tau 0, g\tau\infty\}.\end{aligned}$$

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

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

On en déduit l'égalité annoncée. □

Corollaire 4.3
Pour tous $x = \sum_{g\in\Gamma_0(p)\backslash \mathrm{SL}_2(\mathbb{Z})} \lambda_g g$ *et* $y = \sum_{h\in\Gamma_0(p)\backslash \mathrm{SL}_2(\mathbb{Z})} \mu_h h$ *dans* $\mathcal{E}_{\Gamma_0(p)}$, *on a dans* $\mathcal{H}$:

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

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

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

□

4.2.2 Algèbre de Hecke et conjugaison complexe

Action de l'algèbre de Hecke

Les correspondances de Hecke sur $X_0(p)$ définissent 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

$$\bullet : \mathcal{H}^{\mathrm{ptes}} \times \mathcal{H}_{\mathrm{ptes}} \longrightarrow \mathbb{Z}.$$

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 :

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

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 n'est autre que la conjugaison complexe. La conjugaison complexe laisse stable l'ensemble ptes et définit par conséquent des involutions de $\mathcal{H}^{\text{ptes}}$ et $\mathcal{H}_{\text{ptes}}$. On note $\bar{c}$ l'image d'un cycle c sous l'action de la conjugaison complexe.

Un petit calcul (voir [19]) montre que l'action de la conjugaison complexe sur $\mathcal{H}^{\text{ptes}}$ est donnée par :

$$\overline{\xi^0\left(\frac{c}{d}\right)} = \xi^0\left(\frac{-c}{d}\right) \ (c, d \in \mathbb{Z}, (c,d) = 1).$$

Le sous-groupe $\mathcal{H}$ de $\mathcal{H}^{\text{ptes}}$ est stable sous l'action de la conjugaison complexe, et on a $\alpha_{\text{ptes}}(\bar{c}) = \overline{\alpha_{\text{ptes}}(c)}$ pour tout $c \in \mathcal{H}_{\text{ptes}}$.

Pour c, d dans $\mathcal{H}$, on a

$$\bar{c} \bullet \bar{d} = -c \bullet d. \tag{4.12}$$

On notera $\mathcal{H}^+$ (resp. $\mathcal{H}^-$) la partie invariante (resp. anti-invariante) de $\mathcal{H}$ sous l'action de la conjugaison complexe. On a $\mathcal{H}\left[\frac{1}{2}\right] = \mathcal{H}^+\left[\frac{1}{2}\right] \oplus \mathcal{H}^-\left[\frac{1}{2}\right]$ et 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 extension des scalaires à $\mathbb{Z}\left[\frac{1}{2}\right]$, est parfait. En fait, on a

$$\mathcal{H}^+ = (1 + \mathbf{c})\mathcal{H} \quad \text{et} \quad \mathcal{H}^- = (1 - \mathbf{c})\mathcal{H}$$

où $\mathbf{c}$ est la conjugaison complexe (voir [27] proposition 5).

On note

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

les surjections canoniques.

Le $\mathbb{T}$-module $\mathcal{H}$

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

$$\begin{array}{rccc} [\,,\,] \ : & \mathcal{H} \times H^0(X, \Omega^1) & \longrightarrow & \mathbb{C} \\ & (c, \omega) & \longmapsto & [c, \omega] = \int_c \omega. \end{array} \tag{4.13}$$

L'image du morphisme injectif qui s'en déduit

$$\begin{array}{rccc} F \ : & \mathcal{H} & \longrightarrow & \mathrm{Hom}_{\mathbb{C}}(H^0(X, \Omega^1), \mathbb{C}) \\ & c & \longmapsto & (\omega \mapsto \int_c \omega) \end{array} \tag{4.14}$$

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 $\mathcal{H}^{\text{ptes}}$.

Le morphisme F s'étend en un isomorphisme $\mathbb{T}$-linéaire de $\mathbb{R}$-espaces vectoriels :

$$\mathcal{H}_{\mathbb{R}} \xrightarrow{\sim} \mathrm{Hom}_{\mathbb{C}}(H^0(X, \Omega^1), \mathbb{C}). \tag{4.15}$$

La restriction de F à la partie invariante $\mathcal{H}^+$ (resp. la partie anti-invariante $\mathcal{H}^-$) de $\mathcal{H}$ sous l'action de la conjugaison complexe s'étend en un isomorphisme $\mathbb{T}$-linéaire de $\mathbb{C}$-espaces vectoriels :

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

$$(\text{resp. } F^- : \mathcal{H}^-_{\mathbb{C}} \xrightarrow{\sim} \mathrm{Hom}_{\mathbb{C}}(H^0(X, \Omega^1), \mathbb{C})).$$

Cela est dû au théorème de De Rham, au théorème de décomposition de Hodge ainsi qu'à la dualité de Poincaré (voir par exemple [9]). Pour tout $\omega \in H^0(X, \Omega^1)$, il existe donc $c \in \mathcal{H}^+_{\mathbb{C}}$ et $d \in \mathcal{H}^-_{\mathbb{C}}$ caractérisés par l'une des propriétés suivantes :

$$\int_{c'} \omega = c' \bullet c \quad \text{et} \quad \int_{c'} \bar{\omega} = c' \bullet d \quad (c' \in \mathcal{H}_{\mathbb{C}}) \; ; \tag{4.16}$$

ou, de façon équivalente,

$$\iint_X \omega \wedge \bar{\eta} = \int_c \bar{\eta} \quad \text{et} \quad \iint_X \bar{\omega} \wedge \eta = \int_d \eta \quad (\eta \in H^0(X, \Omega^1)). \tag{4.17}$$

Le $\mathbb{T}_{\mathbb{C}}$-module $\mathrm{Hom}_{\mathbb{C}}(H^0(X, \Omega^1), \mathbb{C})$ étant libre de rang 1, il en est de même pour $\mathcal{H}^+_{\mathbb{C}}$ et $\mathcal{H}^-_{\mathbb{C}}$. Cela implique que $\mathcal{H}^+_{\mathbb{Q}}$ et $\mathcal{H}^-_{\mathbb{Q}}$ sont des $\mathbb{T}_{\mathbb{Q}}$-modules libres de rang 1.

Soit $\mathfrak{m}$ un idéal maximal de $\mathbb{T}$ de caractéristique résiduelle $l \neq 2$. Le $\mathbb{T}_{\mathfrak{m}}$-module $\mathcal{H}_{\mathfrak{m}}$ est libre de rang 2 (voir [20] 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 Le module supersingulier (rappels)

Pour les rappels qui suivent, nous nous inspirons des textes [10], [11], [8], [15], et [48]. Nous attirons l'attention sur le fait que les notations diffèrent quelque peu de celles adoptées par Emerton [8], notamment celles concernant l'algèbre de Hecke.

4.3.1 Courbes elliptiques supersingulières et algèbres de quaternions

Soit E_0 une courbe elliptique supersingulière sur $\bar{\mathbb{F}}_p$. L'anneau $R_0 = \mathrm{End}E_0$ des endomorphismes de E_0 est un ordre maximal de l'algèbre de quaternions $\mathcal{B} = R_0 \otimes \mathbb{Q}$ sur $\mathbb{Q}$ définie ramifiée en p et ∞. 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 [48]). De même l'ensemble $\mathcal{S}$ des classes d'isomorphismes de courbes elliptiques supersingulières sur $\bar{\mathbb{F}}_p$ est fini de cardinal $g+1$ où g est le genre de $X_0(p)$. L'application $\mathrm{Hom}(., E_0)$ fournit une bijection de $\mathcal{S}$ vers $\mathcal{C}_g(R_0)$. On notera $E_0, \ldots, E_g$ des représentants de $\mathcal{S}$ et $I_0 = R_0, \ldots, I_g = \mathrm{Hom}(E_g, E_0)$ les idéaux à gauche de R_0 correspondants. Pour $0 \leq i \leq g$, l'ordre à droite de I_i est alors $R_i = \mathrm{End}(E_i)$, et toute classe de conjugaison des ordres maximaux de $\mathcal{B}$ est représentée par un élément de $\{R_0, \ldots, R_g\}$.

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

$$\prod_{i=0}^{g} w_i = \delta\ , \tag{4.18}$$

$$\sum_{i=0}^{g} \frac{1}{w_i} = \frac{p-1}{12} = \frac{n}{\delta}, \quad \text{où } (n,\delta) = 1. \tag{4.19}$$

L'égalité (4.19) 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 [48]). 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

$$\Theta(M_{i,j}) = \sum_{b \in M_{i,j}} q^{N(b)/N(M_{i,j})} = \sum_{m \geq 0} 2 w_j B_{i,j}(m) q^m \tag{4.20}$$

où

$$B_{i,j}(m) = \frac{1}{2w_j}\ \mathrm{Card}\{b \in M_{i,j},\ N(b)/N(M_{i,j}) = m\}. \tag{4.21}$$

L'entier $B_{i,j}(m)$ est aussi le nombre de sous-schémas en groupes C d'ordre m de E_i tels que $E_i/C \cong E_j$.

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*. Nous renvoyons le lecteur à [10], notamment à la proposition 2.7, pour les propriétés de ces matrices. Signalons en particulier la relation de symétrie

$$w_j B_{i,j}(m) = w_i B_{j,i}(m),\ (\forall m \in \mathbb{N}), \tag{4.22}$$

et la relation

$$\sum_{j=0}^{g} B_{i,j}(m) = \sigma'(m). \tag{4.23}$$

4.3.2 Le module supersingulier

Définition

Rappelons que les classes d'isomorphisme de courbes elliptiques supersingulières sur $\bar{\mathbb{F}}_p$ sont également en correspondance bijective avec les points doubles de la fibre $X_0(p)_{\mathbb{F}_p}$ en p de $X_0(p)_{\mathbb{Z}}$ (voir chapitre 1). Pour $i \in \{0,\ldots,g\}$ on note x_i le point double de $X_0(p)_{\mathbb{F}_p}$ correspondant à la classe d'isomorphisme $[E_i]$.

On rappelle que le *module supersingulier* est le $\mathbb{Z}$-module libre $\mathcal{P}$ de rang $g+1$ engendré par $x_0, \ldots, x_g$:

$$\mathcal{P} = \bigoplus_{i=0}^{g} \mathbb{Z} x_i. \tag{4.24}$$

Soit

$$\begin{array}{rccc} \deg : & \mathcal{P} & \longrightarrow & \mathbb{Z} \\ & \sum_{i=0}^{g} \lambda_i x_i & \longmapsto & \sum_{i=0}^{g} \lambda_i \end{array}$$

l'homorphisme de groupes *degré*. Le sous-groupe de $\mathcal{P}$ formé des éléments de degré nul est noté $\mathcal{P}^0$.

On munit le module supersingulier de l'accouplement $\mathbb{Z}$-bilinéaire défini positif

$$\begin{array}{rccc} \langle\ ,\ \rangle : & \mathcal{P} \times \mathcal{P} & \longrightarrow & \mathbb{Z} \\ & (x_i, x_j) & \longmapsto & \langle x_i, x_j \rangle = w_j \delta_{i,j}. \end{array} \tag{4.25}$$

Opérateurs de Hecke

Les correspondances de Hecke sur $X_0(p)$ induisent une action de $\widetilde{\mathbb{T}}$ sur $\mathcal{P}$. Plus précisément, pour toute courbe elliptique supersingulière E et tout schéma en groupes finis d'ordre m de E, la courbe elliptique E/C est encore supersingulière. Cela permet de définir l'action de l'opérateur de Hecke T_m sur une classe d'isomorphisme $[E]$ de la façon suivante :

$$T_m[E] = \sum_C [E/C]$$

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

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

Les opérateurs de Hecke vérifient les relations suivantes (voir [28] 1.2.1) :

$$T_{nm} = T_n T_m \qquad (n \geq 1,\ m \geq 1,\ (m,n) = 1)$$

$$T_{l^{r+2}} = T_{l^{r+1}} T_l - l T_{l^r} \qquad (l \text{ premier},\ l \neq p,\ r \geq 0)$$

$$T_{p^r} = (T_p)^r = \begin{cases} T_p & \text{si } r \text{ est impair,} \\ \mathrm{Id}_{\mathcal{P}} & \text{si } r \text{ est pair.} \end{cases}$$

Sur la base $(x_i)_{0 \leq i \leq g}$ de $\mathcal{P}$, l'action de T_m est donnée par la matrice d'Eichler-Brandt $B(m) = (B_{i,j})_{0 \leq i,j \leq g}$:

$$T_m x_i = \sum_{j=0}^{g} B_{i,j}(m) x_j. \tag{4.26}$$

Modules de Hecke

L'action de $\widetilde{\mathbb{T}}$ sur $\mathcal{P}$ est fidèle. L'homomorphisme canonique $\widetilde{\mathbb{T}} \longrightarrow \mathrm{End}_{\widetilde{\mathbb{T}}}\mathcal{P}$ est même un isomorphisme (voir [8] théorème 0.4).

On rappelle que $\sigma'(m)$ est la somme des diviseurs de m premiers à p. Toute courbe elliptique supersingulière en caractéristique p a $\sigma'(m)$ sous-schémas en groupes finis d'ordre m. Par conséquent, le sous-groupe $\mathcal{P}^0$ de $\mathcal{P}$ est stable sous l'action de $\widetilde{\mathbb{T}}$. Le quotient $\mathbb{T}$ de $\widetilde{\mathbb{T}}$ agit fidèlement sur $\mathcal{P}^0$. L'homomorphisme canonique $\mathbb{T} \longrightarrow \mathrm{End}_{\mathbb{T}}\mathcal{P}^0$ est un isomorphisme (voir [8] théorème 0.6).

Notons $\check{\mathcal{P}} = \mathrm{Hom}(\mathcal{P}, \mathbb{Z})$ et $\check{\mathcal{P}}^0 = \mathrm{Hom}(\mathcal{P}^0, \mathbb{Z})$. L'algèbre $\widetilde{\mathbb{T}}$ (resp. $\mathbb{T}$) agit sur $\check{\mathcal{P}}$ (resp. $\check{\mathcal{P}}^0$) par dualité. Les opérateurs de Hecke sont autoadjoints pour $\langle\ ,\ \rangle$. L'accouplement $\langle\ ,\ \rangle$ induit un morphisme injectif de $\widetilde{\mathbb{T}}$-modules de $\mathcal{P}$ dans $\check{\mathcal{P}}$ de conoyau isomorphe à $\mathbb{Z}/\delta\mathbb{Z}$ (voir [8] lemme 3.16). L'accouplement canonique

$$\mathcal{P} \times \check{\mathcal{P}} \longrightarrow \mathbb{Z}$$

étend donc l'accouplement $\langle\ ,\ \rangle$ et sera encore noté $\langle\ ,\ \rangle$. Le $\widetilde{\mathbb{T}}$-module $\check{\mathcal{P}}$ s'identifie au sous-$\widetilde{\mathbb{T}}$-module $\bigoplus_{i=0}^{g} \mathbb{Z}\frac{x_i}{w_i}$ de $\mathcal{P}_{\mathbb{Q}}$. On fera désormais l'identification

$$\check{\mathcal{P}} \cong \bigoplus_{i=0}^{g} \mathbb{Z}\frac{x_i}{w_i}. \tag{4.27}$$

On étend deg à $\mathcal{P}_{\mathbb{Q}}$ par linéarité.

L'accouplement bilinéaire $\langle\ ,\ \rangle$ restreint à $\mathcal{P}^0 \times \mathcal{P}^0$ induit un morphisme injectif de $\mathbb{T}$-modules de $\mathcal{P}^0$ dans $\check{\mathcal{P}}^0$ de conoyau isomorphe à $\mathbb{Z}/n\mathbb{Z}$ (*loc. cit.*). L'accouplement canonique $\mathcal{P}^0 \times \check{\mathcal{P}}^0 \longrightarrow \mathbb{Z}$ étend $\langle\ ,\ \rangle|_{\mathcal{P}^0 \times \mathcal{P}^0}$.

Le $\widetilde{\mathbb{T}}_{\mathbb{Q}}$-module $\mathcal{P}_{\mathbb{Q}}$ et le $\mathbb{T}_{\mathbb{Q}}$-module $\mathcal{P}^0_{\mathbb{Q}}$ sont libres de rang 1 (voir [10]).

Proposition 4.4 (Emerton)
Soit $\mathfrak{m}$ un idéal maximal de $\widetilde{\mathbb{T}}$ de caractéristique résiduelle $l \neq 2$. Le $\widetilde{\mathbb{T}}_{\mathfrak{m}}$-module $\mathcal{P}_{\mathfrak{m}}$ et le $\mathbb{T}_{\mathfrak{m}}$-module $\mathcal{P}^0_{\mathfrak{m}}$ sont libres de rang 1.

Démonstration. — C'est un cas particulier du théorème 0.5 de [8]. □

4.4 Comparaison des différents modules de Hecke

4.4.1 Rappels : espaces propres sous l'action de $\widetilde{\mathbb{T}}$

Les $\widetilde{\mathbb{T}}_{\mathbb{Q}}$-modules $\mathcal{M}_{\mathbb{Q}}$ et $\mathcal{P}_{\mathbb{Q}}$ sont libres de rang 1. 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. Les opérateurs de Hecke sont autoadjoints pour les accouplements $(\ ,\ )$ sur $\mathcal{M} \times \mathcal{M}$, $\langle\ ,\ \rangle$ sur $\mathcal{P} \times \mathcal{P}$ et $\bullet$ sur $\mathcal{H}^+ \times \mathcal{H}^-$. Les idempotents de $\widetilde{\mathbb{T}}_{\bar{\mathbb{Q}}}$ sont en correspondance bijective avec les formes de Hecke (voir par exemple [30]), 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.

L'élément d'Eisenstein

Considérons l'*élément d'Eisenstein*

$$a_E = \sum_{i=0}^{g} \frac{x_i}{w_i} \in \check{\mathcal{P}}. \tag{4.28}$$

D'après la formule de masse d'Eichler (4.19), le degré de a_E est

$$\deg a_E = \frac{p-1}{12}. \tag{4.29}$$

On a

$$\langle x, a_E \rangle = \deg x \quad (x \in \mathcal{P}). \tag{4.30}$$

Notons $\mathcal{P}^E$ le sous-$\mathbb{Z}$-module de $\check{\mathcal{P}}$ engendré par a_E. Le $\mathbb{Z}$-module $\mathcal{P}^E$ est orthogonal à $\mathcal{P}^0$ pour $\langle\ ,\ \rangle : \mathcal{P} \times \check{\mathcal{P}} \longrightarrow \mathbb{Z}$. On a la décomposition (voir [8] démonstration du lemme 3.16)

$$\mathcal{P}\left[\tfrac{1}{n\delta}\right] = \mathcal{P}^E\left[\tfrac{1}{n\delta}\right] \oplus \mathcal{P}^0\left[\tfrac{1}{n\delta}\right]. \tag{4.31}$$

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

$$\pi^0(x) = x - \frac{12}{p-1} \deg(x)\ a_E \qquad (x \in \mathcal{P}\left[\tfrac{1}{n\delta}\right]). \tag{4.32}$$

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

D'après (4.23) et (4.26), a_E est un vecteur propre de T_m pour la valeur propre $\sigma'(m)$ pour tout $m \geq 1$. L'espace $\widetilde{\mathbb{T}}_{\bar{\mathbb{Q}}}$-propre $\mathbf{1}_E\left(\mathcal{P}_{\bar{\mathbb{Q}}}\right)$ est la $\bar{\mathbb{Q}}$-droite engendrée par a_E. On a donc $\mathbf{1}_E\left(\mathcal{P}_{\bar{\mathbb{Q}}}\right) = \mathcal{P}^E \otimes \bar{\mathbb{Q}}$. On note $\mathcal{P}^E \otimes \bar{\mathbb{Q}} = \mathcal{P}^E_{\bar{\mathbb{Q}}}$.

Espaces propres associés aux formes primitives

Pour f une forme primitive, posons

$$\mathcal{P}^f_{\bar{\mathbb{Q}}} = \mathbf{1}_f\left(\mathcal{P}_{\bar{\mathbb{Q}}}\right), \quad \mathcal{H}^{+f}_{\bar{\mathbb{Q}}} = \mathbf{1}_f\left(\mathcal{H}^+_{\bar{\mathbb{Q}}}\right), \quad \mathcal{H}^{-f}_{\bar{\mathbb{Q}}} = \mathbf{1}_f\left(\mathcal{H}^-_{\bar{\mathbb{Q}}}\right). \tag{4.33}$$

Les espaces propres $\mathcal{P}^f_{\bar{\mathbb{Q}}}$, $\mathcal{H}^{+f}_{\bar{\mathbb{Q}}}$ et $\mathcal{H}^{-f}_{\bar{\mathbb{Q}}}$ sont des $\bar{\mathbb{Q}}$-droites. Choisissons a_f (resp. c_f, resp. d_f) une base de $\mathcal{P}^f_{\bar{\mathbb{Q}}}$ (resp. $\mathcal{H}^{+f}_{\bar{\mathbb{Q}}}$, resp. $\mathcal{H}^{-f}_{\bar{\mathbb{Q}}}$) comme $\bar{\mathbb{Q}}$-droite.

On a

$$\begin{aligned}
\mathbf{1}_f(x) &= \frac{\langle x, a_f \rangle}{\langle a_f, a_f \rangle}\, a_f \quad (x \in \mathcal{P}_{\bar{\mathbb{Q}}})\ ; \\
\mathbf{1}_f(c) &= \frac{c \bullet d_f}{c_f \bullet d_f}\, c_f \quad (c \in \mathcal{H}^+_{\bar{\mathbb{Q}}})\ ; \\
\mathbf{1}_f(c) &= \frac{c_f \bullet c}{c_f \bullet d_f}\, d_f \quad (c \in \mathcal{H}^-_{\bar{\mathbb{Q}}}).
\end{aligned}$$

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

Notons $\mathrm{Prim}(p)$ 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

$$\mathcal{P}^0_{\bar{\mathbb{Q}}} = \bigoplus_{f\in\mathrm{Prim}(p)} \mathcal{P}^f_{\bar{\mathbb{Q}}}, \tag{4.34}$$

$$\mathcal{H}^+_{\bar{\mathbb{Q}}} = \bigoplus_{f\in\mathrm{Prim}(p)} \mathcal{H}^{+f}_{\bar{\mathbb{Q}}}, \tag{4.35}$$

$$\mathcal{H}^-_{\bar{\mathbb{Q}}} = \bigoplus_{f\in\mathrm{Prim}(p)} \mathcal{H}^{-f}_{\bar{\mathbb{Q}}}. \tag{4.36}$$

De plus, puisque les opérateurs de Hecke sont auto-adjoints pour l'accouplement $[\ ,\ ]$ (voir (4.13)), après extension des scalaires à $\mathbb{C}$, on peut choisir comme générateurs de $\mathcal{H}^{+f}_{\mathbb{C}}$ et $\mathcal{H}^{-f}_{\mathbb{C}}$ les cycles $\tilde{c}_f$ et $\tilde{d}_f$ associés à la forme différentielle ω_f au sens de (4.16). Ils sont caractérisés par la propriété :

$$\int_c \omega_f = c\bullet\tilde{c}_f \quad \text{et} \quad \int_c \bar{\omega}_f = c\bullet\tilde{d}_f \quad (c\in\mathcal{H}^+_{\mathbb{C}}). \tag{4.37}$$

La caractérisation équivalente (4.17) montre qu'on a alors

$$\tilde{c}_f\bullet\tilde{d}_f = -i(f,f). \tag{4.38}$$

4.4.2 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 $\mathcal{H}^+\otimes_{\mathbb{T}}\mathcal{H}^-$. On note

$$s_{\widetilde{\mathbb{T}}} : \mathcal{P}\otimes\mathcal{P} \twoheadrightarrow \mathcal{P}\otimes_{\widetilde{\mathbb{T}}}\mathcal{P}, \quad s^0_{\mathbb{T}} : \mathcal{P}^0\otimes\mathcal{P}^0 \twoheadrightarrow \mathcal{P}^0\otimes_{\mathbb{T}}\mathcal{P}^0$$

et

$$s'_{\mathbb{T}} : \mathcal{H}^+\otimes\mathcal{H}^- \twoheadrightarrow \mathcal{H}^+\otimes_{\mathbb{T}}\mathcal{H}^-$$

les surjections canoniques.

Lemme 4.5
Les sous-espaces propres de $\mathcal{P}_{\bar{\mathbb{Q}}}\otimes_{\widetilde{\mathbb{T}}_{\bar{\mathbb{Q}}}}\mathcal{P}_{\bar{\mathbb{Q}}}$ sous l'action de $\widetilde{\mathbb{T}}_{\bar{\mathbb{Q}}}$ 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 $g\in\mathrm{Prim}(p)$.
Plus précisément, on a les décompositions en sous-espaces deux à deux orthogonaux

$$\mathcal{P}_{\mathbb{Q}}\otimes_{\widetilde{\mathbb{T}}_{\mathbb{Q}}}\mathcal{P}_{\mathbb{Q}} = (\mathcal{P}^E_{\mathbb{Q}}\otimes_{\widetilde{\mathbb{T}}_{\mathbb{Q}}}\mathcal{P}^E_{\mathbb{Q}})\oplus(\mathcal{P}^0_{\mathbb{Q}}\otimes_{\mathbb{T}_{\mathbb{Q}}}\mathcal{P}^0_{\mathbb{Q}}) \tag{4.39}$$

$$\mathcal{P}^0_{\bar{\mathbb{Q}}}\otimes_{\mathbb{T}_{\bar{\mathbb{Q}}}}\mathcal{P}^0_{\bar{\mathbb{Q}}} = \bigoplus_{g\in\mathrm{Prim}(p)} \left(\mathcal{P}^g_{\bar{\mathbb{Q}}}\otimes_{\mathbb{T}_{\bar{\mathbb{Q}}}}\mathcal{P}^g_{\bar{\mathbb{Q}}}\right) \tag{4.40}$$

$$\mathcal{H}^+_{\bar{\mathbb{Q}}}\otimes_{\mathbb{T}_{\bar{\mathbb{Q}}}}\mathcal{H}^-_{\bar{\mathbb{Q}}} = \bigoplus_{g\in\mathrm{Prim}(p)} \left(\mathcal{H}^{+g}_{\bar{\mathbb{Q}}}\otimes_{\mathbb{T}_{\bar{\mathbb{Q}}}}\mathcal{H}^{-g}_{\bar{\mathbb{Q}}}\right). \tag{4.41}$$

Démonstration du lemme. — D'après (4.31) et (4.35), 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

$$g(z) = \sum_{m\geq 0} b_m q^m \quad \left(\text{resp. } h(z) = \sum_{m\geq 0} c_m q^m \right),$$

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 $m \geq 1$,

$$b_m a_g \otimes_{\widetilde{\mathbb{T}}_{\bar{\mathbb{Q}}}} a_h = T_m a_g \otimes_{\widetilde{\mathbb{T}}_{\bar{\mathbb{Q}}}} a_h = a_g \otimes_{\widetilde{\mathbb{T}}_{\bar{\mathbb{Q}}}} (T_m a_h) = c_m a_g \otimes_{\widetilde{\mathbb{T}}_{\bar{\mathbb{Q}}}} a_h.$$

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

$$\theta : \mathcal{P} \otimes_{\widetilde{\mathbb{T}}} \check{\mathcal{P}} \longrightarrow \mathrm{Hom}(\widetilde{\mathbb{T}}, \mathbb{Z}) \cong \mathcal{N},$$

$$(\text{resp. } \theta^0 : \mathcal{P}^0 \otimes_{\mathbb{T}} \check{\mathcal{P}}^0 \longrightarrow \mathrm{Hom}(\mathbb{T}, \mathbb{Z}) \cong \mathcal{M}^0),$$

le morphisme canonique de $\widetilde{\mathbb{T}}$-modules (resp. de $\mathbb{T}$-modules) déduit de l'accouplement canonique sur $\mathcal{P} \times \check{\mathcal{P}}$ (resp. $\mathcal{P}^0 \times \check{\mathcal{P}}^0$).

Avec l'identification (4.27), θ s'écrit

$$\begin{array}{rccl} \theta & : & \mathcal{P} \otimes_{\widetilde{\mathbb{T}}} \check{\mathcal{P}} & \longrightarrow \quad \mathrm{Hom}(\widetilde{\mathbb{T}}, \mathbb{Z}) \cong \mathcal{N} \\ & & x \otimes_{\widetilde{\mathbb{T}}} y & \longmapsto \quad \dfrac{\deg x . \deg y}{2} + \displaystyle\sum_{m\geq 1} \langle T_m x, y \rangle \, q^m. \end{array} \tag{4.42}$$

En particulier, on a

$$\theta(x_i \otimes_{\widetilde{\mathbb{T}}} \frac{x_j}{w_j}) = \frac{1}{2w_j} \Theta(M_{i,j}), \ 0 \leq i,j \leq g. \tag{4.43}$$

Théorème 4.6 (Emerton)

1. *Le morphisme de $\widetilde{\mathbb{T}}$-modules θ est surjectif. De plus, on a*

$$\theta(\mathcal{P} \otimes_{\widetilde{\mathbb{T}}} \mathcal{P}) = \mathcal{M}.$$

2. *Le morphisme de $\mathbb{T}$-modules θ^0 est surjectif. De plus, on a*

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

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

Démonstration. — Voir [8] théorèmes 0.3, 0.6, et 0.10. □

Soit $\mathfrak{m}$ un idéal maximal de $\widetilde{\mathbb{T}}$ de caractéristique résiduelle $l \neq 2$. Les $\widetilde{\mathbb{T}}_{\mathfrak{m}}$-modules $\mathcal{N}_{\mathfrak{m}}, \mathcal{M}_{\mathfrak{m}}$ et $\mathcal{P}_{\mathfrak{m}}$ et les $\mathbb{T}_{\mathfrak{m}}$-modules $\mathcal{M}^0_{\mathfrak{m}}$ et $\mathcal{P}^0_{\mathfrak{m}}$ sont libres de rang 1 (voir [8] théorème 0.5). Le théorème 4.6 entraîne donc le

Corollaire 4.7 (Emerton)
Les morphismes de $\widetilde{\mathbb{T}}_{\mathfrak{m}}$-modules

$$\theta_{\mathfrak{m}} : \mathcal{P}_{\mathfrak{m}} \otimes_{\widetilde{\mathbb{T}}_{\mathfrak{m}}} \check{\mathcal{P}}_{\mathfrak{m}} \longrightarrow \mathcal{N}_{\mathfrak{m}} \quad et \quad \mathcal{P}_{\mathfrak{m}} \otimes_{\widetilde{\mathbb{T}}_{\mathfrak{m}}} \mathcal{P}_{\mathfrak{m}} \longrightarrow \mathcal{M}_{\mathfrak{m}}$$

sont des isomorphismes. Le morphisme de $\mathbb{T}_{\mathfrak{m}}$-modules

$$\theta^0_{\mathfrak{m}} : \mathcal{P}^0_{\mathfrak{m}} \otimes_{\mathbb{T}_{\mathfrak{m}}} \check{\mathcal{P}}^0_{\mathfrak{m}} \longrightarrow \mathcal{M}^0_{\mathfrak{m}}$$

est un isomorphisme.

Notons

$$\begin{array}{rccc} \psi \ : & \mathcal{H}^+ \otimes_{\mathbb{T}} \mathcal{H}^- & \longrightarrow & \mathrm{Hom}(\mathbb{T},\mathbb{Z}) \cong \mathcal{M}^0 \\ & c \otimes_{\mathbb{T}} c' & \longmapsto & \sum_{m\geq 1} (T_m c \bullet c')\, q^m \end{array} \tag{4.44}$$

le morphisme canonique de $\mathbb{T}$-modules déduit de l'accouplement $\bullet$.

Proposition 4.8
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

$$(\mathcal{H}^+ \otimes \mathbb{Z}_l) \times (\mathcal{H}^- \otimes \mathbb{Z}_l) \longrightarrow \mathbb{Z}_l \tag{4.45}$$

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 (4.45) 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 (4.45) 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 [8] permet alors de conclure. □

On déduit immédiatement du corollaire 4.7 et de la proposition 4.8 la proposition suivante :

Proposition 4.9
Le morphisme de $\widetilde{\mathbb{T}}\left[\frac{1}{2}\right]$-modules

$$\theta\left[\tfrac{1}{2}\right] : \mathcal{P}\left[\tfrac{1}{2}\right] \otimes_{\widetilde{\mathbb{T}}\left[\frac{1}{2}\right]} \check{\mathcal{P}}\left[\tfrac{1}{2}\right] \longrightarrow \mathcal{N}\left[\tfrac{1}{2}\right]$$

obtenu après extension des scalaires de θ à $\mathbb{Z}\left[\frac{1}{2}\right]$, est un isomorphisme.

Les morphismes de $\mathbb{T}\left[\frac{1}{2}\right]$-modules

$$\theta^0\left[\tfrac{1}{2}\right] : \mathcal{P}^0\left[\tfrac{1}{2}\right] \otimes_{\mathbb{T}\left[\frac{1}{2}\right]} \check{\mathcal{P}}^0\left[\tfrac{1}{2}\right] \longrightarrow \mathcal{M}^0\left[\tfrac{1}{2}\right]$$

et

$$\psi\left[\tfrac{1}{2}\right] : \mathcal{H}^+\left[\tfrac{1}{2}\right] \otimes_{\mathbb{T}\left[\frac{1}{2}\right]} \mathcal{H}^-\left[\tfrac{1}{2}\right] \longrightarrow \mathcal{M}^0\left[\tfrac{1}{2}\right],$$

obtenus par extension des scalaires de θ^0 et ψ à $\mathbb{Z}\left[\frac{1}{2}\right]$, sont des isomorphismes.

On note désormais

$$\Phi = \psi\left[\tfrac{1}{2}\right]^{-1} \circ \theta^0\left[\tfrac{1}{2}\right] : \mathcal{P}^0\left[\tfrac{1}{2}\right] \otimes_{\mathbb{T}\left[\frac{1}{2}\right]} \check{\mathcal{P}}^0\left[\tfrac{1}{2}\right] \xrightarrow{\sim} \mathcal{H}^+\left[\tfrac{1}{2}\right] \otimes_{\mathbb{T}\left[\frac{1}{2}\right]} \mathcal{H}^-\left[\tfrac{1}{2}\right] \tag{4.46}$$

l'isomorphisme de $\mathbb{T}\left[\frac{1}{2}\right]$-modules composé.

Remarque 4.1 Considérons le morphisme canonique de $\mathbb{T}$-modules

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

composé du morphisme 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 $\mathcal{H} \otimes_{\mathbb{T}} \mathcal{H} \twoheadrightarrow \mathcal{H} \wedge_{\mathbb{T}} \mathcal{H}$.

Le morphisme $\Upsilon\left[\frac{1}{2}\right]$, obtenu après extension des scalaires de Υ à $\mathbb{Z}\left[\frac{1}{2}\right]$, est un isomorphisme de $\mathbb{T}\left[\frac{1}{2}\right]$-modules ; en effet, $\Upsilon\left[\frac{1}{2}\right]$ est surjectif. Le morphisme $\Upsilon_{\mathfrak{m}}$ sur les séparés complétés en un idéal maximal $\mathfrak{m}$ de caractéristique résiduelle $l \neq 2$ est donc un isomorphisme puisque $\mathcal{H}^+_{\mathfrak{m}} \otimes_{\mathbb{T}_{\mathfrak{m}}} \mathcal{H}^-_{\mathfrak{m}}$ et $\mathcal{H}_{\mathfrak{m}} \wedge_{\mathbb{T}_{\mathfrak{m}}} \mathcal{H}_{\mathfrak{m}}$ sont des $\mathbb{T}_{\mathfrak{m}}$-modules libres de rang 1.

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. Cependant, du fait des isomorphismes $\mathbb{T}$-linéaires $F^{\pm} : \mathcal{H}^{\pm}_{\mathbb{C}} \xrightarrow{\sim} \mathrm{Hom}_{\mathbb{C}}(H^0(X, \Omega^1), \mathbb{C})$ de $\mathbb{C}$-espaces vectoriels décrits plus haut, nous préférons travailler avec $\mathcal{H}^+ \otimes_{\mathbb{T}} \mathcal{H}^-$.

4.4.3 Une première description de $\Phi_{\mathbb{Q}}$

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

$$\Delta_2 = \sum_{i=0}^{g} \frac{1}{w_i} x_i \otimes_{\mathbb{Q}} x_i. \tag{4.47}$$

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

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

Par conséquent, on a $\Delta_2^0 = (\pi^0 \otimes \pi^0)(\Delta_2)$ et donc Δ_2^0 est un élément de $\mathcal{P}_{\mathbb{Q}}^0 \otimes_{\mathbb{Q}} \mathcal{P}_{\mathbb{Q}}^0$.

On note $\bar{\Delta}_2^0$ l'image de Δ_2^0 par la surjection canonique $s_{\mathbb{T}}^0$. Comme le diagramme

$$\begin{array}{ccc} \mathcal{P}_{\mathbb{Q}} \otimes_{\mathbb{Q}} \mathcal{P}_{\mathbb{Q}} & \xrightarrow{s_{\widetilde{\mathbb{T}}}} & \mathcal{P}_{\mathbb{Q}} \otimes_{\widetilde{\mathbb{T}}_{\mathbb{Q}}} \mathcal{P}_{\mathbb{Q}} \\ \downarrow{\scriptstyle \pi^0 \otimes_{\mathbb{Q}} \pi^0} & & \downarrow{\scriptstyle \pi^0 \otimes_{\mathbb{T}_{\mathbb{Q}}} \pi^0} \\ \mathcal{P}_{\mathbb{Q}}^0 \otimes_{\mathbb{Q}} \mathcal{P}_{\mathbb{Q}}^0 & \xrightarrow{s_{\mathbb{T}}^0} & \mathcal{P}_{\mathbb{Q}}^0 \otimes_{\mathbb{T}_{\mathbb{Q}}} \mathcal{P}_{\mathbb{Q}}^0 \end{array}$$

commute, on a

$$\bar{\Delta}_2^0 = \sum_{i=0}^{g} \frac{1}{w_i} x_i \otimes_{\widetilde{\mathbb{T}}_{\mathbb{Q}}} x_i - \frac{12}{p-1} a_E \otimes_{\widetilde{\mathbb{T}}_{\mathbb{Q}}} a_E. \tag{4.48}$$

Considérons à présent l'élément de $\mathcal{H}_{\mathbb{Q}}^{\mathrm{ptes}} \otimes_{\mathbb{Q}} \mathcal{H}_{\mathbb{Q}}^{\mathrm{ptes}}$ suivant :

$$\Lambda_2 = \frac{1}{6} \sum_{g \in \Gamma_0(p) \backslash \mathrm{SL}_2(\mathbb{Z})} \left(\xi^0(g\tau) \otimes_{\mathbb{Q}} \xi^0(g) - \xi^0(g) \otimes_{\mathbb{Q}} \xi^0(g\tau) \right). \tag{4.49}$$

Lemme 4.10
L'élément Λ_2 est dans $\mathcal{H}_{\mathbb{Q}} \otimes_{\mathbb{Q}} \mathcal{H}_{\mathbb{Q}}$.

Démonstration du lemme. — On a (voir le paragraphe 4.2.1)

$$\Lambda_2 = \frac{1}{6} \sum_{[c:d] \in \mathbb{P}^1_{\mathbb{F}_p}} \left(\xi^0 \left(\frac{d}{d-c} \right) \otimes_{\mathbb{Q}} \xi^0 \left(\frac{c}{d} \right) - \xi^0 \left(\frac{c}{d} \right) \otimes_{\mathbb{Q}} \xi^0 \left(\frac{d}{d-c} \right) \right).$$

Lorsque $c/d \neq 0, 1$, ou ∞, les éléments $\xi^0(\frac{c}{d})$ et $\xi^0(\frac{c}{d-c})$ sont dans $\mathcal{H}$. Il suffit donc de montrer que l'élément

$$\xi^0(1) \otimes_{\mathbb{Q}} \xi^0(0) - \xi^0(0) \otimes_{\mathbb{Q}} \xi^0(1) + \xi^0(0) \otimes_{\mathbb{Q}} \xi^0(\infty) - \xi^0(\infty) \otimes_{\mathbb{Q}} \xi^0(0)$$

est dans $\mathcal{H}_{\mathbb{Q}} \otimes_{\mathbb{Q}} \mathcal{H}_{\mathbb{Q}}$. Or $\xi^0(0) = -\xi^0(\infty)$ et $\xi^0(1) = 0$. D'où le lemme. ◇

On pose $\Lambda_2^0 = (\pi^+ \otimes_{\mathbb{Q}} \pi^-)(\Lambda_2) \in \mathcal{H}_{\mathbb{Q}}^+ \otimes_{\mathbb{Q}} \mathcal{H}_{\mathbb{Q}}^-$ et $\bar{\Lambda}_2^0 = s'_{\mathbb{T}}(\Lambda_2^0) \in \mathcal{H}_{\mathbb{Q}}^+ \otimes_{\mathbb{T}_{\mathbb{Q}}} \mathcal{H}_{\mathbb{Q}}^-$.

Théorème 4.11
1. *L'élément $\bar{\Delta}_2^0$ engendre le $\mathbb{T}_{\mathbb{Q}}$-module libre $\mathcal{P}_{\mathbb{Q}}^0 \otimes_{\mathbb{T}_{\mathbb{Q}}} \mathcal{P}_{\mathbb{Q}}^0$;*
2. *l'élément $\bar{\Lambda}_2^0$ engendre le $\mathbb{T}_{\mathbb{Q}}$-module libre $\mathcal{H}_{\mathbb{Q}}^+ \otimes_{\mathbb{T}_{\mathbb{Q}}} \mathcal{H}_{\mathbb{Q}}^-$;*
3. *on a $\Phi_{\mathbb{Q}}(\bar{\Delta}_2^0) = \bar{\Lambda}_2^0$.*

Remarque 4.2 Puisque $\Phi_{\mathbb{Q}}$ est un isomorphisme de $\mathbb{T}_{\mathbb{Q}}$-modules, si 3. est vraie, les assertions 1. et 2. sont équivalentes. On démontre cependant ces dernières de façon indépendante.

Démonstration. — Pour u et v dans $\mathcal{H}_{\mathbb{Q}}$, notons

$$A_g(u,v) = (\xi^0(g\tau) \bullet v)(u \bullet \xi^0(g)) - (\xi^0(g) \bullet v)(u \bullet \xi^0(g\tau)).$$

Nous ferons usage du lemme suivant.

Lemme 4.12

a. Pour tous u et v dans $\mathcal{P}^0_{\mathbb{Q}}$, on a

$$\sum_{i=0}^{g} \langle x_i, v\rangle.\langle u, \frac{x_i}{w_i}\rangle - \frac{12}{p-1}\langle a_E, v\rangle.\langle u, a_E\rangle = \langle u, v\rangle \ ;$$

b. Pour tous u et v dans $\mathcal{H}_{\mathbb{Q}}$, on a

$$\frac{1}{6} \sum_{g \in \Gamma_0(p)\backslash \mathrm{SL}_2(\mathbb{Z})} A_g(u,v) = u \bullet v.$$

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

$$\sum_{i=0}^{g} \langle x_i, v\rangle.\langle u, \frac{x_i}{w_i}\rangle - \frac{12}{p-1}\langle a_E, v\rangle.\langle u, a_E\rangle = \sum_{i=0}^{g} \lambda_i \mu_i w_i = \langle u, v\rangle.$$

Cela montre a.

Soient u et v dans $\mathcal{H}_{\mathbb{Q}}$. Il existe

$$x = \sum_{g \in \Gamma_0(p)\backslash \mathrm{SL}_2(\mathbb{Z})} \lambda_g g \ \in \ \mathcal{E}_{\Gamma_0(p)} \otimes \mathbb{Q}$$

et

$$y = \sum_{g \in \Gamma_0(p)\backslash \mathrm{SL}_2(\mathbb{Z})} \mu_g g \ \in \ \mathcal{E}_{\Gamma_0(p)} \otimes \mathbb{Q}$$

tels que $u = \alpha_{\mathrm{ptes}}(\xi_0(x))$ et $v = \alpha_{\mathrm{ptes}}(\xi_0(y))$ (voir le paragraphe 4.2.1, notamment le théorème 4.1). On a alors

$$\begin{aligned} A_g(u,v) &= -(\xi^0(g\tau) \bullet \xi_0(y))(\xi^0(g) \bullet \xi_0(x)) + (\xi^0(g) \bullet \xi_0(y))(\xi^0(g\tau) \bullet \xi_0(x)) \\ &= -\mu_{g\tau}\lambda_g + \mu_g \lambda_{g\tau}. \end{aligned}$$

En appliquant le corollaire 4.3, on obtient alors

$$\begin{aligned} \frac{1}{6} \sum_{g \in \Gamma_0(p)\backslash \mathrm{SL}_2(\mathbb{Z})} A_g(u,v) &= \frac{1}{6} \sum_{g \in \Gamma_0(p)\backslash \mathrm{SL}_2(\mathbb{Z})} \lambda_{g\tau}\mu_g - \lambda_g \mu_{g\tau} \\ &= \alpha_{\mathrm{ptes}}(\xi_0(x)) \bullet \alpha_{\mathrm{ptes}}(\xi_0(y)) \\ &= u \bullet v. \end{aligned}$$

◇

Soit f une forme primitive de poids 2 pour $\Gamma_0(p)$. On a dans $\mathcal{P}^f_{\bar{\mathbb{Q}}} \otimes_{\mathbb{T}_{\bar{\mathbb{Q}}}} \mathcal{P}^f_{\bar{\mathbb{Q}}}$

$$\mathbf{1}_f \bar{\Delta}_2^0 = \sum_{i=0}^{g} \frac{\langle x_i, a_f\rangle^2}{w_i \langle a_f, a_f\rangle^2}\ a_f \otimes_{\mathbb{T}_{\bar{\mathbb{Q}}}} a_f.$$

D'après l'assertion a. du lemme 4.12 cela donne

$$\mathbf{1}_f \bar{\Delta}_2^0 = \frac{1}{\langle a_f, a_f\rangle}\ a_f \otimes_{\mathbb{T}_{\bar{\mathbb{Q}}}} a_f. \tag{4.50}$$

En particulier $\mathbf{1}_f \bar{\Delta}_2^0$ est non nul pour toute forme primitive f. Ceci prouve l'assertion 1. du théorème 4.11.

On a dans $\mathcal{H}^{+f}_{\bar{\mathbb{Q}}} \otimes_{\mathbb{T}_{\bar{\mathbb{Q}}}} \mathcal{H}^{-f}_{\bar{\mathbb{Q}}}$

$$\mathbf{1}_f \bar{\Lambda}_2^0 = \frac{1}{6} \sum_{g \in \Gamma_0(p)\backslash \mathrm{SL}_2(\mathbb{Z})} \frac{A_g(c_f, d_f)}{(c_f \bullet d_f)^2}\ c_f \otimes_{\mathbb{T}_{\bar{\mathbb{Q}}}} d_f.$$

Donc, d'après l'assertion b. du lemme 4.12, on a

$$\mathbf{1}_f \bar{\Lambda}_2^0 = \frac{1}{c_f \bullet d_f} c_f \otimes_{\mathbb{T}_{\bar{\mathbb{Q}}}} d_f. \tag{4.51}$$

En particulier, $\mathbf{1}_f \bar{\Lambda}_2^0 \neq 0$ et ce pour toute forme primitive f. Cela prouve l'assertion 2. du théorème.

D'après (4.50), on a $\mathbf{1}_f \theta^0_{\bar{\mathbb{Q}}}(\bar{\Delta}_2^0) = f$. En effet, on a

$$\begin{aligned}
\mathbf{1}_f\ \theta^0_{\bar{\mathbb{Q}}}(\bar{\Delta}_2^0) &= \theta^0_{\bar{\mathbb{Q}}}(\mathbf{1}_f \bar{\Delta}_2^0) \\
&= \sum_{m \geq 1} \frac{\langle T_m a_f, a_f\rangle}{\langle a_f, a_f\rangle} q^m \\
&= \sum_{m \geq 1} a_m(f) q^m \\
&= f.
\end{aligned}$$

De même (4.51) entraîne l'égalité

$$\mathbf{1}_f\ \psi_{\bar{\mathbb{Q}}}(\bar{\Lambda}_2^0) = f.$$

Cela termine la démonstration du théorème 4.11. □

Chapitre 5

Formule de Gross et applications

Nous reprenons ici les notations du chapitre précédent. Rappelons notamment que p est un nombre premier, $\mathcal{B}$ est l'algèbre de quaternions définie ramifiée en p et à l'infini, et $R_0, \ldots, R_g$ les ordres à droite de représentants $I_0 = R_0, \ldots, I_g$ des classes d'idéaux à gauche d'un ordre maximal R_0 donné.

5.1 Formule de Gross

Puisque $\mathcal{B}$ est ramifié en p et à l'infini, un corps quadratique L se plonge dans $\mathcal{B}$ si et seulement si p est inerte ou ramifié dans L (voir par exemple [48]). 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 $\sigma(\mathcal{O} \otimes \mathbb{Q}) \cap R = \sigma(\mathcal{O})$.

Soit $D > 0$ un entier. Notons $\mathcal{O}_{-D}$ l'ordre de discriminant $-D$ s'il existe, $h(-D)$ son nombre de classes, $u(-D)$ l'ordre de $\mathcal{O}^*_{-D}/\langle \pm 1 \rangle$, et $h_i(-D)$ le nombre de plongements optimaux de $\mathcal{O}_{-D}$ dans R_i, modulo conjugaison par R_i^*. On a

$$u(-D) = \begin{cases} 2 & \text{si } D = 4 \\ 3 & \text{si } D = 3 \\ 1 & \text{sinon.} \end{cases}$$

Définition 5.1
On définit le D-ième élément de Gross[1]

$$\gamma_D = \frac{1}{2u(-D)} \sum_{i=0}^{g} h_i(-D) x_i \ \in \ \mathcal{P}[1/6].$$

Remarque 5.1 Par définition, γ_D est nul si $-D$ n'est pas un discriminant quadratique imaginaire, c'est-à-dire le discriminant d'un ordre d'un corps qua-

[1] Cet élément, introduit par Gross, est noté e_D dans [10]. Nous choisissons la notation γ_D dans le souci de ne pas confondre cet élément avec l'élément d'enroulement tordu introduit au paragraphe 5.2.

dratique imaginaire.[2] Si $-D$ est un discriminant quadratique imaginaire, γ_D est nul si p est décomposé dans $\mathcal{O}_{-D} \otimes \mathbb{Q} = \mathbb{Q}(\sqrt{-D})$ (car dans ce cas $\mathcal{O}_{-D} \otimes \mathbb{Q}$ ne se plonge pas dans $\mathcal{B}$).

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, on note

$$f \otimes \chi = \sum_{m \geq 1} a_m(f)\chi(m) q^m$$

la forme modulaire de poids 2 tordue de f par χ. Lorsque r est premier à p, cette forme modulaire est primitive de niveau pr^2 (voir [30]).

On suppose désormais que $-D$ est un discriminant quadratique imaginaire premier à p. 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 [10] dans le cas des discriminants premiers et généralisée par Zhang [50].

Théorème 5.2 (Formule de Gross-Zhang)
On a

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

Remarque 5.2 Lorsque p est décomposé dans $\mathbb{Q}(\sqrt{-D})$, chacun des membres de l'égalité du théorème 5.2 est nul. On suppose donc désormais que p est inerte dans $\mathbb{Q}(\sqrt{-D})$.

5.2 Carré tensoriel des éléments de Gross

Dans le chapitre précédent, nous avons étudié les isomorphismes de $\mathbb{T}_{\mathbb{Q}}$-modules suivants :

$$\theta^0_{\mathbb{Q}} : \mathcal{P}^0_{\mathbb{Q}} \otimes_{\mathbb{T}_{\mathbb{Q}}} \mathcal{P}^0_{\mathbb{Q}} \xrightarrow{\sim} \mathcal{M}^0_{\mathbb{Q}} \tag{5.1}$$

et

$$\psi_{\mathbb{Q}} : \mathcal{H}^+_{\mathbb{Q}} \otimes_{\mathbb{T}_{\mathbb{Q}}} \mathcal{H}^-_{\mathbb{Q}} \xrightarrow{\sim} \mathcal{M}^0_{\mathbb{Q}}. \tag{5.2}$$

Notons

$$\gamma^0_D = \pi^0(\gamma_D) \in \mathcal{P}^0_{\mathbb{Q}}.$$

[2] Rappelons que $-D$ est un discriminant quadratique imaginaire si et seulement s'il existe $f \in \mathbb{N}$ tel que $d = D'f^2$ avec $-D' < 0$ un discriminant fondamental, autrement dit tel que $D' \equiv 3 \mod 4$ et D' sans facteur carré, ou $D' \equiv 0 \mod 4$, $\frac{D'}{4}$ sans facteur carré, et $\frac{D'}{4} \equiv 1, 2 \mod 4$.

Comme corollaire de la formule de Gross, nous déterminons ici l'image de $\gamma_D^0 \otimes_{\mathbb{T}_\mathbb{Q}} \gamma_D^0 \in \mathcal{P}_\mathbb{Q}^0 \otimes_{\mathbb{T}_\mathbb{Q}} \mathcal{P}_\mathbb{Q}^0$ par $\Phi_\mathbb{Q} = \psi_\mathbb{Q}^{-1} \circ \theta_\mathbb{Q}^0$.

On rappelle qu'on a un isomorphisme $\mathbb{T}$-linéaire de $\mathbb{R}$-espaces vectoriels :

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

déduit de l'accouplement non dégénéré $[\ ,\ ] : \mathcal{H} \times H^0(X, \Omega^1) \longrightarrow \mathbb{C}$ défini par

$$[c, \omega] = \int_c \omega$$

(voir paragraphe (4.15)).

On appelle *élément d'enroulement* l'antécédent $e \in \mathcal{H}_\mathbb{R}$ par $F_\mathbb{R}$ de

$$\omega \mapsto -\int_{\{0,\infty\}} \omega$$

(voir [20] (18.5)). L'élément d'enroulement e est un élément de $\mathcal{H}_\mathbb{Q}^+$ (*loc. cit.* 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 appelé *élément d'enroulement tordu par le caractère* χ :

$$e_\chi = \sum_{b \mod r} \bar{\chi}(b) \left\{ -\frac{b}{r}, \infty \right\} \in H_1(X, \mathrm{ptes}; \mathbb{C}). \tag{5.3}$$

Lemme 5.3
Le symbole modulaire e_χ est un élément de $\mathcal{H} \otimes \mathbb{Z}[\chi]$, et lorsque χ est impair (resp. pair), $e_\chi \in \mathcal{H}^- \otimes \mathbb{Z}[\chi]$ (resp. $e_\chi \in \mathcal{H}^+ \otimes \mathbb{Z}[\chi]$.)

Démonstration du lemme. — Notons $[\frac{r}{s}]$ la classe d'un élément $\frac{r}{s} \in \mathbb{P}^1(\mathbb{Q})$ modulo $\Gamma_0(p)$. D'après [19] 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

$$\beta(e_\chi) = \sum_{b \mod r} \bar{\chi}(b)([\infty]) - \sum_{b \mod r} \bar{\chi}(b) \left(\left[\frac{-b}{r} \right] \right) = 0 - \sum_{b \mod r} \bar{\chi}(b)([1;1]) = 0.$$

Donc e_χ est un élément de $\mathcal{H} \otimes \mathbb{Z}[\chi]$ (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

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

Ceci prouve que, si χ est impair, e_χ est un élément de $\mathcal{H}^- \otimes \mathbb{Z}[\chi]$, et si χ est pair, e_χ est un élément de $\mathcal{H}^+ \otimes \mathbb{Z}[\chi]$. ◇

Le caractère ε_D est primitif de conducteur D, et impair. On note

$$e_D = e_{\varepsilon_D} = \sum_{b \mod D} \varepsilon_D(b) \left\{-\frac{b}{D}, \infty\right\} \in \mathcal{H}^-. \tag{5.4}$$

Définition 5.4
On appelle D-ième forme parabolique de Gross *la forme parabolique*

$$\mathbf{g}_D = \theta^0_{\mathbb{Q}}(\gamma^0_D \otimes_{\mathbb{T}_\mathbb{Q}} \gamma^0_D) \in \mathcal{M}^0_\mathbb{Q}. \tag{5.5}$$

Théorème 5.5
L'image de $\gamma^0_D \otimes_{\mathbb{T}_\mathbb{Q}} \gamma^0_D$ *par l'isomorphisme*

$$\Phi_\mathbb{Q} : \mathcal{P}^0_\mathbb{Q} \otimes_{\mathbb{T}_\mathbb{Q}} \mathcal{P}^0_\mathbb{Q} \xrightarrow{\sim} \mathcal{H}^+_\mathbb{Q} \otimes_{\mathbb{T}_\mathbb{Q}} \mathcal{H}^-_\mathbb{Q}$$

est donnée par :

$$\Phi_\mathbb{Q}(\gamma^0_D \otimes_{\mathbb{T}_\mathbb{Q}} \gamma^0_D) = e \otimes_{\mathbb{T}_\mathbb{Q}} e_D.$$

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

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

ou encore

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

Démonstration. — Soit f une forme primitive de poids 2 pour $\Gamma_0(p)$. On se propose de montrer que

$$\mathbf{1}_f \sum_{m \geq 1} \langle \gamma^0_D, T_m \gamma^0_D \rangle \, q^m = \mathbf{1}_f \sum_{m \geq 1} e \bullet T_m e_D \, q^m \ .$$

On a

$$\begin{aligned} \mathbf{1}_f \, \mathbf{g}_D &= \theta_{\bar{\mathbb{Q}}}(\gamma^f_D \otimes_{\mathbb{T}_{\bar{\mathbb{Q}}}} \gamma^f_D) \\ &= \sum_{m \geq 1} \langle \gamma^f_D, T_m \gamma^f_D \rangle q^m \\ &= \sum_{m \geq 1} \langle \gamma^f_D, \gamma^f_D \rangle a_m(f) q^m \\ &= \langle \gamma^f_D, \gamma^f_D \rangle f. \end{aligned}$$

D'après la formule de Gross-Zhang (théorème 5.2), on a donc

$$\mathbf{1}_f \, \mathbf{g}_D = \frac{L(f,1)L(f\otimes\varepsilon_D,1)\sqrt{D}}{(f,f)} \; f. \tag{5.6}$$

Lemme 5.6
Soit f une forme primitive de poids 2 pour $\Gamma_0(p)$. On a

$$\mathbf{1}_f \left(\psi(e\otimes_{\mathbb{T}_{\mathbb{Q}}} e_D)\right) = \frac{L(f,1)L(f\otimes\varepsilon_D,1)\sqrt{D}}{(f,f)} \; f.$$

Démonstration du lemme. — Soit $f=\sum_{m\geq 1} a_m(f)q^m$ une forme primitive de poids 2 pour $\Gamma_0(p)$. Un calcul classique montre que

$$L(f,1)=[e,\omega_f] \quad \text{et} \quad L(f\otimes\chi,1)=-\frac{g(\chi)}{r}[e_\chi,\omega_f]. \tag{5.7}$$

Nous renvoyons à [19] théorème 4.1 pour la première égalité de (5.7). Pour la deuxième égalité il suffit d'appliquer le théorème 4.2 (*loc. cit.*) en remarquant qu'avec les notations adoptées par Manin on a $L(f\otimes\chi,s)=-L_{\omega_f,\chi}(s)$ et en utilisant le fait que $\sum_{b \mod r}\bar{\chi}(b)=0$.

On a

$$\begin{aligned}
\mathbf{1}_f\psi_{\bar{\mathbb{Q}}}(e\otimes_{\mathbb{T}_{\bar{\mathbb{Q}}}} e_D) &= \psi_{\bar{\mathbb{Q}}}(e^f\otimes_{\mathbb{T}_{\bar{\mathbb{Q}}}} e_D^f)\\
&= \sum_{m\geq 1}(T_m e^f\bullet e_D^f)q^m\\
&= \sum_{m\geq 1}(e^f\bullet e_D^f)a_m(f)q^m\\
&= (e^f\bullet e_D^f)\; f.
\end{aligned}$$

Or on a

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

On choisit ici les générateurs $\tilde{c}_f$ de $\mathcal{H}_{\mathbb{C}}^{+f}$ et $\tilde{d}_f$ de $\mathcal{H}_{\mathbb{C}}^{-f}$ associés à la forme différentielle holomorphe ω_f caractérisés par (4.37). D'après la première égalité de (5.7), on a

$$e\bullet\tilde{d}_f=[e,\bar{\omega}_f]=\overline{L(f,1)}=L(f,1)$$

car $L(f,1)\in\mathbb{R}$. La deuxième égalité de (5.7), montre que l'on a dans $\mathbb{C}$

$$\tilde{c}_f\bullet e_D=-[e_D,\omega_f]=-i\sqrt{D}\;L(f\otimes\varepsilon_D,1)$$

car $g(\varepsilon_D)=i\sqrt{D}$. Enfin on rappelle que $\tilde{c}_f\bullet\tilde{d}_f=-i(f,f)$ (voir (4.38)). On obtient finalement l'égalité

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

Ceci achève la démonstration du lemme 5.6, et donc du théorème 5.5. ◇ □

5.3 Formule pour $\sum_{i=0}^{g} h_i(-D)^2 w_i$

D'après le théorème 5.5, on a, pour tout $m \geq 1$,

$$\langle \gamma_D^0, T_m \gamma_D^0 \rangle \, q^m = e \bullet T_m e_D \, q^m. \tag{5.8}$$

Nous nous proposons de calculer chacun des membres de l'égalité (5.8) dans le cas où $m = 1$. Ceci permet d'établir une formule pour $\sum_{i=0}^{g} h_i(-D)^2 w_i$.

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

Proposition 5.7
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

$$\gamma_D^0 = \gamma_D - \gamma_D^E = \gamma_D - \frac{\langle \gamma_D, a_E \rangle}{\langle a_E, a_E \rangle} \, a_E.$$

Par conséquent

$$\langle \gamma_D^0, \gamma_D^0 \rangle = \langle \gamma_D, \gamma_D \rangle - \frac{12(\deg \gamma_D)^2}{p-1}.$$

Rappelons que

$$\gamma_D = \frac{1}{2u(-D)} \sum_{i=0}^{g} h_i(-D) x_i.$$

De plus, puisque $(D, p) = 1$, la formule d'Eichler (voir [10] (1.12)) donne :

$$\sum_{i=0}^{g} h_i(-D) = \left(1 - \left(\frac{-D}{p}\right)\right) h(-D) = 2h(-D), \tag{5.9}$$

car p est inerte dans $\mathbb{Q}(\sqrt{-D})$. On en déduit la proposition. □

5.3.2 Calcul de $e \bullet e_D$

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

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

Proposition 5.8
Pour tout caractère primitif χ modulo r, on a

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

où, pour $M \in \mathcal{X}'_r$, b_M est l'entier modulo r solution du système

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

Remarque 5.3 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

$$\frac{u}{(w,r)}\left(\frac{w}{(w,r)}\right)^{-1} \equiv \frac{v}{(t,r)}\left(\frac{t}{(t,r)}\right)^{-1} \pmod{\delta}. \tag{5.10}$$

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.

Démonstration. — Pour $0 \leq b < d,\ d$ 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 $\{m_{d,b},\ 0 \leq b < d,\ d \mid r\}$ (resp. $\{n_{d,b},\ 0 \leq b < d,\ d \mid r\}$) 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

$$w_{d,b}M = \begin{pmatrix} \frac{u}{d} - \frac{bw}{r} & \frac{v}{d} - \frac{bt}{r} \\ \frac{dw}{r} & \frac{dt}{r} \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}). \tag{5.11}$$

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

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

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 $0 \leq b < d,\ d \mid r$, tels que $M \in C(d,b)$. D'après (5.11), 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

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

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

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

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 5.9
Soit $0 \le b < r$. 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 du lemme. — 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 $D(r,b)\backslash\{n_{r,b}\}$. ◇

Le lemme précédent montre que

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

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,

$$S_\chi = \iota\left(\sum_{0\leq b<r} \bar\chi(b)\left(-\frac{b}{r}\right) - \sum_{0\leq b<r} \bar\chi(b)(\infty)\right). \tag{5.12}$$

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 5.8. □

Remarque 5.4 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

$$S(u,v) = \sum_{h=0}^{v-1} \bar{B}_1\left(\frac{h}{v}\right) \bar{B}_1\left(\frac{uh}{v}\right) \tag{5.13}$$

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 [40]). Pour $k \in \{1, \ldots, p-1\}$, notons k_* l'unique élément de $\{1, \ldots, p-1\}$ tel que $kk_* \equiv -1 \pmod{p}$.

Corollaire 5.10
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 5.8 et de la formule suivante due à Merel [24] :

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

□

5.3.3 Application au calcul de $\sum_{i=0}^{g} h_i(-D)^2 w_i$

Théorème 5.11
On a

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

Démonstration. — D'après la proposition 5.7, 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 5.5 donne l'égalité :

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

Le corollaire 5.10 appliqué à $\chi = \varepsilon_D$ montre alors le théorème 5.11. □

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

$$g_b = \begin{pmatrix} u_b & b \\ w_b & D \end{pmatrix}$$

l'unique matrice de $\Gamma_0(p)$ telle que $0 \leq \frac{w_b}{p} < D$. Par commodité, on note

$$g_b = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

lorsque b n'est pas premier à D.

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

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

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

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

Par conséquent,

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

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

Proposition 5.12
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. — On rappelle que, pour u, v deux entiers premiers entre eux, $S(u,v)$ est la somme de Dedekind (voir 5.13). 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 [39] et [24]). On a (*loc. cit*)

$$R(g) = -\mathcal{E} \bullet c_g \quad (g \in \Gamma_0(p)). \tag{5.14}$$

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 [40] théorème 1). Pour $u > 0$ et $v > 0$ deux entiers premiers entre eux, on a

$$12\,(S(u,v) + S(v,u)) = -3 + \frac{u}{v} + \frac{v}{u} + \frac{1}{uv}. \tag{5.15}$$

On a également les propriétés élémentaires suivantes.

$$S(-u,v) = -S(u,v) \quad \text{et} \quad S(u',v) = S(u,v), \tag{5.16}$$

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

On a $bw_b \equiv -1 \pmod{D}$. D'après (5.15) et (5.16), 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 que

$$\sum_{b=0}^{D-1}\varepsilon_D(b)\bar{B}_1\left(\frac{b}{D}\right)=\sum_{b=0}^{D-1}\varepsilon_D(b)b=DB_{1,\varepsilon_D} \tag{5.17}$$

(voir par exemple [49] proposition 4.1).

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 $\begin{pmatrix} u_b & \frac{w_b}{p} \\ bp & D\end{pmatrix}\in\Gamma_0(p)$ 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

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

Or, en combinant la formule du nombre de classe et les relations entre nombres de Bernoulli et fonctions L de Dirichlet (voir par exemple [49] théorème 4.9) on obtient

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

On en déduit l'égalité annoncée dans la proposition 5.12. □

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

$$W_k=\begin{pmatrix}k_* & -1\\ 1+kk_* & -k\end{pmatrix}\in\Gamma_0(p), \tag{5.18}$$

où k_* est l'unique élément de $\{1,\dots,p-1\}$ tel que $kk_*\equiv -1 \pmod p$. On rappelle que l'ensemble

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

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

On a

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

(voir [24] 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 $b\in\{0,\dots,D-1\}$, 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

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

Chapitre 6

Interprétation de la formule de Gross-Kudla

6.1 Préliminaires

On considère dans ce chapitre les $\widetilde{\mathbb{T}}^{\otimes 3}$-modules $\mathcal{P}^{\otimes 3}$, $\mathcal{N}^{\otimes 3}$ et $\mathcal{M}^{\otimes 3}$, et les $\mathbb{T}^{\otimes 3}$-modules $\mathcal{P}^{0\otimes 3}$ et $\mathcal{M}^{0\otimes 3}$.

Pour f_1, f_2 et f_3 trois formes modulaires de poids 2 pour $\Gamma_0(p)$, la forme modulaire triple $F = f_1 \otimes f_2 \otimes f_3 \in \mathcal{N}_{\bar{\mathbb{Q}}}^{\otimes 3}$ est définie[1] par

$$F(z_1, z_2, z_3) = f_1(z_1) f_2(z_2) f_3(z_3) \qquad ((z_1, z_2, z_3) \in \mathfrak{H}^3).$$

On dit que $F = f_1 \otimes f_2 \otimes f_3 \in \mathcal{N}_{\bar{\mathbb{Q}}}^{\otimes 3}$ est une *forme de Hecke triple* (resp. *forme primitive triple*) si $f_1,\ f_2$ et f_3 sont des formes de Hecke (resp. des formes primitives). Pour $F = f_1 \otimes f_2 \otimes f_3 \in \mathcal{M}_{\bar{\mathbb{Q}}}^{0\ \otimes 3}$ et $G = g_1 \otimes g_2 \otimes g_3 \in \mathcal{N}_{\bar{\mathbb{Q}}}^{\otimes 3}$, le produit scalaire de Petersson de F et G est normalisé par (voir [11] (11.3)) :

$$(F, G)^{\otimes 3} = \prod_{i=1}^{3} (f_i, g_i) = 2^9 \pi^6 \iint_{\Gamma_0(p)^3 \backslash \mathfrak{H}^3} F(z) \overline{G(z)} dx dy, \tag{6.1}$$

où $z = (z_1, z_2, z_3)$, $z_k = x_k + i y_k,\ k = 1, 2, 3$, $dx = dx_1 dx_2 dx_3$ et $dy = dy_1 dy_2 dy_3$.

Par fonctorialité des algèbres tensorielles, on déduit de l'accouplement $\langle\ ,\ \rangle$ l'accouplement suivant

$$\begin{array}{rccc} \langle\ ,\ \rangle^{\otimes 3}\ : & \mathcal{P}^{\otimes 3} \times \check{\mathcal{P}}^{\otimes 3} & \longrightarrow & \mathbb{Z} \\ & (a_1 \otimes a_2 \otimes a_3\ ,\ b_1 \otimes b_2 \otimes b_3) & \longmapsto & \prod_{i=1}^{3} \langle a_i, b_i \rangle. \end{array}$$

Le morphisme de $\widetilde{\mathbb{T}}$-modules

$$\theta : \mathcal{P} \otimes_{\widetilde{\mathbb{T}}} \check{\mathcal{P}} \longrightarrow \mathcal{N}$$

produit le morphisme de $\widetilde{\mathbb{T}}^{\otimes 3}$-modules

$$\begin{array}{rccc} \theta^{\otimes 3}\ : & \mathcal{P}^{\otimes 3} \otimes_{\widetilde{\mathbb{T}}^{\otimes 3}} \check{\mathcal{P}}^{\otimes 3} & \longrightarrow & \mathcal{N}^{\otimes 3} \\ & (a_1 \otimes a_2 \otimes a_3) \otimes_{\widetilde{\mathbb{T}}^{\otimes 3}} (b_1 \otimes b_2 \otimes b_3) & \longmapsto & \prod_{i=1}^{3} \theta(a_i \otimes_{\widetilde{\mathbb{T}}} b_i). \end{array}$$

[1] L'application de $\mathcal{N}_{\bar{\mathbb{Q}}}^{\otimes 3}$ dans l'ensemble des fonctions holomorphes en trois variables sur $\mathfrak{H}^3$ définie par $f_1 \otimes f_2 \otimes f_3 \mapsto ((z_1, z_2, z_3) \mapsto f_1(z_1) f_2(z_2) f_3(z_3))$ est bien injective.

Les $\widetilde{\mathbb{T}}_{\mathbb{Q}}^{\otimes 3}$-modules $\mathcal{N}_{\mathbb{Q}}^{\otimes 3} = \mathcal{M}_{\mathbb{Q}}^{\otimes 3}$ et $\mathcal{P}_{\mathbb{Q}}^{\otimes 3}$ sont libres de rang 1 ; les $\mathbb{T}_{\mathbb{Q}}^{\otimes 3}$-modules ${\mathcal{M}_{\mathbb{Q}}^{0}}^{\otimes 3}$ et ${\mathcal{P}_{\mathbb{Q}}^{0}}^{\otimes 3}$ sont libres de rang 1. Les opérateurs de Hecke triples de $\widetilde{\mathbb{T}}^{\otimes 3}$ sont autoadjoints pour $(\ ,\ )^{\otimes 3}$ et $\langle\ ,\ \rangle^{\otimes 3}$.

Les idempotents de $\widetilde{\mathbb{T}}_{\bar{\mathbb{Q}}}^{\otimes 3}$ sont de la forme $\mathbf{1}_{f_1} \otimes \mathbf{1}_{f_2} \otimes \mathbf{1}_{f_3}$ pour f_1, f_2 et f_3 parcourant l'ensemble des formes de Hecke (voir le paragraphe 4.4.1 de cette thèse). On note

$$\mathcal{P}_{\bar{\mathbb{Q}}}^{F} \ = \ \mathbf{1}_F \left(\mathcal{P}_{\bar{\mathbb{Q}}}^{\otimes 3}\right) = \mathcal{P}_{\bar{\mathbb{Q}}}^{f_1} \otimes_{\bar{\mathbb{Q}}} \mathcal{P}_{\bar{\mathbb{Q}}}^{f_2} \otimes_{\bar{\mathbb{Q}}} \mathcal{P}_{\bar{\mathbb{Q}}}^{f_3}$$

le sous-espace propre de $\mathcal{P}_{\bar{\mathbb{Q}}}^{\otimes 3}$ correspondant à la forme de Hecke triple $F = f_1 \otimes f_2 \otimes f_3$. Le $\bar{\mathbb{Q}}$-espace vectoriel $\mathcal{P}_{\bar{\mathbb{Q}}}^{F}$ est une $\bar{\mathbb{Q}}$-droite de vecteur directeur $A_F = a_{f_1} \otimes_{\bar{\mathbb{Q}}} a_{f_2} \otimes_{\bar{\mathbb{Q}}} a_{f_3}$, où a_f est un vecteur directeur du $\bar{\mathbb{Q}}$-espace vectoriel $\mathcal{P}_{\bar{\mathbb{Q}}}^{f}$ de dimension 1 (voir la section 4.4.1). On a la décomposition en sous-espaces $\widetilde{\mathbb{T}}^{\otimes 3}$-propres deux à deux orthogonaux pour $\langle\ ,\ \rangle^{\otimes 3}$

$$\mathcal{P}_{\bar{\mathbb{Q}}}^{\otimes 3} = \bigoplus_{F} \mathcal{P}_{\bar{\mathbb{Q}}}^{F},$$

la somme directe portant sur l'ensemble des formes de Hecke triples. Le sous-$\bar{\mathbb{Q}}$-espace vectoriel $\left(\mathcal{P}_{\bar{\mathbb{Q}}}^{0}\right)^{\otimes 3}$ de $\mathcal{P}_{\bar{\mathbb{Q}}}^{\otimes 3}$ est donné par

$$\left(\mathcal{P}_{\bar{\mathbb{Q}}}^{0}\right)^{\otimes 3} = \bigoplus_{F} \mathcal{P}_{\bar{\mathbb{Q}}}^{F},$$

la somme directe portant cette fois sur l'ensemble des formes primitives triples.

Pour $B \in \mathcal{P}_{\bar{\mathbb{Q}}}^{\otimes 3}$, on note $B^F = \mathbf{1}_F B$. On vérifie aisément qu'on a dans $\mathcal{P}_{\bar{\mathbb{Q}}}^{F}$:

$$B^F = \frac{\langle A_F, B\rangle^{\otimes 3}}{\langle A_F, A_F\rangle^{\otimes 3}}\ A_F.$$

Considérons à présent le $\widetilde{\mathbb{T}} \otimes \widetilde{\mathbb{T}}$-module $\mathcal{P} \otimes \left(\mathcal{P} \otimes_{\widetilde{\mathbb{T}}} \mathcal{P}\right)$. D'après le lemme 4.5, les sous-espaces propres de $\mathcal{P}_{\bar{\mathbb{Q}}} \otimes_{\bar{\mathbb{Q}}} \left(\mathcal{P}_{\bar{\mathbb{Q}}} \otimes_{\widetilde{\mathbb{T}}_{\bar{\mathbb{Q}}}} \mathcal{P}_{\bar{\mathbb{Q}}}\right)$ sont les $\bar{\mathbb{Q}}$-droites

$$\mathcal{P}_{\bar{\mathbb{Q}}}^{f} \otimes_{\bar{\mathbb{Q}}} \left(\mathcal{P}_{\bar{\mathbb{Q}}}^{g} \otimes_{\widetilde{\mathbb{T}}_{\bar{\mathbb{Q}}}} \mathcal{P}_{\bar{\mathbb{Q}}}^{g}\right)$$

de vecteur directeur $a_f \otimes_{\bar{\mathbb{Q}}} (a_g \otimes_{\widetilde{\mathbb{T}}_{\bar{\mathbb{Q}}}} a_g) = (1 \otimes_{\bar{\mathbb{Q}}} s_{\widetilde{\mathbb{T}}})(A_{f\otimes g\otimes g})$, pour f et g parcourant l'ensemble des formes de Hecke. On a la décomposition en sous-espaces $\widetilde{\mathbb{T}} \otimes \widetilde{\mathbb{T}}$-propres deux à deux orthogonaux

$$\mathcal{P}_{\bar{\mathbb{Q}}} \otimes_{\bar{\mathbb{Q}}} \left(\mathcal{P}_{\bar{\mathbb{Q}}} \otimes_{\widetilde{\mathbb{T}}_{\bar{\mathbb{Q}}}} \mathcal{P}_{\bar{\mathbb{Q}}}\right) = \bigoplus_{f,g} \left(\mathcal{P}_{\bar{\mathbb{Q}}}^{f} \otimes_{\bar{\mathbb{Q}}} \left(\mathcal{P}_{\bar{\mathbb{Q}}}^{g} \otimes_{\widetilde{\mathbb{T}}_{\bar{\mathbb{Q}}}} \mathcal{P}_{\bar{\mathbb{Q}}}^{g}\right)\right),$$

la somme directe portant sur l'ensemble des paires (f, g) de formes de Hecke.

Pour $B \in \mathcal{P}^{\otimes 3}$, on note $\bar{B} = (1 \otimes s_{\widetilde{\mathbb{T}}})(B) \in \mathcal{P} \otimes \left(\mathcal{P} \otimes_{\widetilde{\mathbb{T}}} \mathcal{P}\right)$. Pour f et g deux formes de Hecke, on a donc

$$(\mathbf{1}_f \otimes_{\bar{\mathbb{Q}}} \mathbf{1}_g)(\bar{B}) = (1 \otimes s_{\widetilde{\mathbb{T}}})(B^{f\otimes g\otimes g}) = \overline{B^{f\otimes g\otimes g}}.$$

6.2 Formule de Gross et Kudla

Soient f, g et h trois formes primitives de développements de Fourier à l'infini respectifs :

$$\sum_{m\geq 1} a_m q^m, \quad \sum_{m\geq 1} b_m q^m, \quad \text{et} \quad \sum_{m\geq 1} c_m q^m.$$

Gross et Kudla [11] ont défini la fonction $L(F,s)$ du produit triple $F = f\otimes g\otimes h$ par un produit Eulérien

$$L(F,s) = L_p(F,s)\prod_{l\neq p} L_l(F,s)$$

convergeant pour $Re(s) > \frac{5}{2}$. La définition des facteurs locaux de $L(F,s)$ suit la recette proposée par Serre [45] pour la fonction L de la représentation $\sigma_f\otimes\sigma_g\otimes\sigma_h$ de dimension 8 de $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, où $\sigma_f, \sigma_g, \sigma_h$ sont les représentations de dimension 2 associées respectivement à f, g et h. Plus précisément, les facteurs locaux en un nombre premier l distinct de p sont définis par

$$L_l(F,s) = \prod_{1\leq i,j,k\leq 2} (1-\alpha_{l,i}\beta_{l,j}\gamma_{l,k}l^{-s})^{-1}$$

avec

$$\begin{aligned} 1-a_l x + lx^2 &= (1-\alpha_{l,1}x)(1-\alpha_{l,2}x),\\ 1-b_l x + lx^2 &= (1-\beta_{l,1}x)(1-\beta_{l,2}x),\\ 1-c_l x + lx^2 &= (1-\gamma_{l,1}x)(1-\gamma_{l,2}x). \end{aligned}$$

Le facteur $L_p(F,s)$ est donné par

$$L_p(F,s) = (1+\varepsilon_p p^{-s})^{-1}(1+\varepsilon_p p^{1-s})^{-1}$$

où

$$\varepsilon_p = -a_p b_p c_p = \pm 1$$

(voir [10] paragraphe 1).

Soit $L_\infty(F,s) = (2\pi)^{3-4s}\Gamma(s)\Gamma(s-1)^3$ le facteur archimédien. La fonction $\Lambda(F,s) = L_\infty(F,s)L(F,s)$ admet un prolongement analytique à $\mathbb{C}$ et satisfait l'équation fonctionnelle :

$$\Lambda(F,s) = -\varepsilon_p\, \Lambda(F,4-s). \tag{6.2}$$

(Le lecteur se reportera à [11] proposition 1.1 pour la démonstration de ce fait.)

Lorsque $\varepsilon_p = 1$, on a $L(F,2) = 0$. On suppose désormais que $\varepsilon_p = -1$.

Définition 6.1
On appelle élément diagonal de Gross-Kudla[2] *l'élément*

$$\Delta_3 = \sum_{i=0}^{g} \frac{1}{w_i} x_i^{\otimes 3} \in \mathcal{P}_{\mathbb{Q}}^{\otimes 3}.$$

[2] L'élément Δ_3 est appelé *élément diagonal* et noté Δ dans [11].

La formule de Gross et Kudla ([11] théorème 11.1) s'énonce comme suit :

Théorème 6.2 (Gross-Kudla)
Soient f, g et h trois formes modulaires primitives de poids 2 pour $\Gamma_0(p)$ telles que $\varepsilon_p = -1$. Posons $F = f \otimes g \otimes h$. On a

$$L(F,2) = \frac{(F,F)}{4\pi p}\ \langle \Delta_3^F, \Delta_3^F \rangle^{\otimes 3}.$$

Lorsque $g = h$, on obtient le

Corollaire 6.3 (Gross-Kudla)
Pour $F = f \otimes g \otimes g$, on a

$$L(f,1)L(f \otimes \mathrm{Sym}^2 g, 2) = \frac{(F,F)}{4\pi p}\ \langle \Delta_3^F, \Delta_3^F \rangle^{\otimes 3}.$$

Démonstration. — La représentation l-adique $\sigma_g \otimes \sigma_g$ se décompose comme somme directe de $\mathrm{Sym}^2(\sigma_g)$ et de $\Lambda^2 \sigma_g = \mathbb{Q}_l(-1)$. Par suite, on a

$$L(f \otimes g \otimes g, 2) = L(f,1)L(f \otimes \mathrm{Sym}^2 g, 2)$$

(voir [11] (11.7) p. 200). □

6.3 L'élément diagonal de Gross-Kudla

Soit I_e l'idéal de $\mathbb{T}$ annulateur de l'élément d'enroulement e dont on rappelle la définition dans le paragraphe 5.2. On note $\mathcal{P}_{\mathbb{Q}}^0[I_e]$ l'ensemble des éléments de $\mathcal{P}_{\mathbb{Q}}^0$ annulés par I_e. Considèrons l'élément diagonal de Gross-Kudla $\Delta_3 \in \mathcal{P}_{\mathbb{Q}}^{\otimes 3}$. Posons

$$\bar{\Delta}_3^0 = (\pi^0 \otimes_{\mathbb{Q}} s_{\widetilde{\mathbb{T}}})(\Delta_3) = (\pi^0 \otimes_{\mathbb{Q}} (1 \otimes_{\widetilde{\mathbb{T}}_{\mathbb{Q}}} 1)(\bar{\Delta}_3) \in \mathcal{P}_{\mathbb{Q}}^0 \otimes_{\mathbb{Q}} \left(\mathcal{P}_{\mathbb{Q}} \otimes_{\widetilde{\mathbb{T}}_{\mathbb{Q}}} \mathcal{P}_{\mathbb{Q}} \right).$$

Théorème 6.4
On a

$$\bar{\Delta}_3^0 = \bar{\Delta}_3 - \frac{12}{p-1} a_E \otimes_{\mathbb{Q}} \left(\sum_{i=0}^{g} x_i \otimes_{\widetilde{\mathbb{T}}_{\mathbb{Q}}} \frac{x_i}{w_i} \right)$$

et

$$\bar{\Delta}_3^0 \in \mathcal{P}_{\mathbb{Q}}^0[I_e] \otimes (\mathcal{P}_{\mathbb{Q}}^0 \otimes_{\mathbb{T}_{\mathbb{Q}}} \mathcal{P}_{\mathbb{Q}}^0).$$

Démonstration. — Par définition, on a

$$\pi^0(x) = x - \frac{12}{p-1} \deg(x) a_E \qquad (x \in \mathcal{P}_{\mathbb{Q}}).$$

On a donc

$$\bar{\Delta}_3^0 = \sum_{i=0}^{g}(x_i - \frac{12}{p-1}a_E) \otimes_{\mathbb{Q}} (x_i \otimes_{\widetilde{\mathbb{T}}_{\mathbb{Q}}} \frac{x_i}{w_i}),$$

ce qui prouve la première assertion du théorème 6.4.

Montrons à présent que $\bar{\Delta}_3^0$ est un élément de $\mathcal{P}_{\mathbb{Q}}^0 \otimes_{\mathbb{Q}} (\mathcal{P}_{\mathbb{Q}}^0 \otimes_{\mathbb{T}_{\mathbb{Q}}} \mathcal{P}_{\mathbb{Q}}^0)$.

On a dans $\mathcal{P}_{\bar{\mathbb{Q}}}^0 \otimes_{\bar{\mathbb{Q}}} (\mathcal{P}_{\bar{\mathbb{Q}}} \otimes_{\widetilde{\mathbb{T}}_{\bar{\mathbb{Q}}}} \mathcal{P}_{\bar{\mathbb{Q}}})$

$$\begin{aligned}\bar{\Delta}_3^0 &= \sum_{f,g\in\mathrm{Prim}(p)} (\mathbf{1}_f \otimes \mathbf{1}_g)(\bar{\Delta}_3) + \sum_{f\in\mathrm{Prim}(p)} (\mathbf{1}_f \otimes \mathbf{1}_E)(\bar{\Delta}_3) \\ &= (1 \otimes s_{\widetilde{\mathbb{T}}}) \left(\sum_{f,g\in\mathrm{Prim}(p)} \Delta_3^{f\otimes g\otimes g} + \sum_{f\in\mathrm{Prim}(p)} \Delta_3^{f\otimes E\otimes E} \right).\end{aligned}$$

Pour toute forme primitive f, on a

$$\Delta_3^{f\otimes E\otimes E} = \frac{\langle \Delta_3, a_f \otimes a_E \otimes a_E\rangle^{\otimes 3}}{\langle a_f \otimes a_E \otimes a_E, a_f \otimes a_E \otimes a_E\rangle^{\otimes 3}} (a_f \otimes a_E \otimes a_E).$$

Or

$$\begin{aligned}\langle \Delta_3, a_f \otimes a_E \otimes a_E\rangle^{\otimes 3} &= \sum_{i=0}^{g} \frac{1}{w_i}\langle x_i, a_f\rangle \langle x_i, a_E\rangle^2 \\ &= \langle a_E, a_f\rangle \\ &= 0.\end{aligned}$$

On en déduit que

$$\bar{\Delta}_3^0 = \sum_{f,g\in\mathrm{Prim}(p)} (\mathbf{1}_f \otimes \mathbf{1}_g)(\bar{\Delta}_3). \tag{6.3}$$

En particulier, $\bar{\Delta}_3^0$ est un élément de $\mathcal{P}_{\mathbb{Q}}^0 \otimes_{\mathbb{Q}} (\mathcal{P}_{\mathbb{Q}}^0 \otimes_{\mathbb{T}_{\mathbb{Q}}} \mathcal{P}_{\mathbb{Q}}^0)$.

Rappelons que l'idéal I_e de $\mathbb{T}$ est encore l'annulateur de l'ensemble des formes paraboliques f pour lesquelles $L(f,1) \neq 0$ (voir [24]). On en déduit que, lorsque $f \in \mathrm{Prim}(p)$ est telle que $L(f,1) \neq 0$, le vecteur propre associé a_f est dans $\mathcal{P}_{\mathbb{Q}}^0[I_e]$.

Compte tenu de (6.3), on a

$$\bar{\Delta}_3^0 = \sum_{f,g\in\mathrm{Prim}(p)} \lambda_{f,g}\ a_f \otimes_{\mathbb{Q}} (a_g \otimes_{\mathbb{T}_{\mathbb{Q}}} a_g).$$

Soit $f \in \mathrm{Prim}(p)$ telle que $L(f,1) = 0$. Le corollaire 6.3 de la formule de Gross-Kudla montre que, pour tout $g \in \mathrm{Prim}(p)$, on a

$$(F,F)\langle \Delta_3^F, \Delta_3^F\rangle^{\otimes 3} = 0,$$

où $F = f \otimes g \otimes g$. Or $(F,F) > 0$ et $\langle , \rangle^{\otimes 3}$ est défini positif sur $\mathcal{P}_{\bar{\mathbb{Q}}}^{\otimes 3}$. On en déduit que $\Delta_3^F = 0$ et donc $\lambda_{f,g} = 0$ pour tout $g \in \mathrm{Prim}(p)$ et tout $f \in \mathrm{Prim}(p)$ telle que $L(f,1) = 0$. Finalement,

$$\bar{\Delta}_3^0 = \sum_{\substack{f,g \in \mathrm{Prim}(p) \\ L(f,1) \neq 0}} \lambda_{f,g}\ a_f \otimes_{\bar{\mathbb{Q}}} (a_g \otimes_{\mathbb{T}_{\bar{\mathbb{Q}}}} a_g) \ \in\ \mathcal{P}_{\bar{\mathbb{Q}}}^0[I_e] \otimes_{\bar{\mathbb{Q}}} \left(\mathcal{P}_{\bar{\mathbb{Q}}}^0 \otimes_{\mathbb{T}_{\bar{\mathbb{Q}}}} \mathcal{P}^0 \right).$$

□

Remarque 6.1 La formule de Gross et un théorème de Waldspurger ont permis à Parent de montrer que $\mathcal{P}_{\mathbb{Q}}^0[I_e]$ est le $\mathbb{Q}$-espace vectoriel engendré par l'ensemble des éléments γ_D^0 pour $-D$ parcourant l'ensemble A des discriminants quadratiques imaginaires premiers à p (voir [37] proposition 4.2). Peut-on déterminer explicitement $\bar{\Delta}_3^0$ comme combinaison linéaire d'éléments de $\mathcal{P}_{\mathbb{Q}}^0[I_e] \otimes (\mathcal{P}_{\mathbb{Q}}^0 \otimes_{\mathbb{T}_{\mathbb{Q}}} \mathcal{P}_{\mathbb{Q}}^0)$ du type $\gamma_D^0 \otimes (\Phi_{\mathbb{Q}}^{-1}(u \otimes_{\mathbb{T}_{\mathbb{Q}}} v))$ pour $-D$ discriminant quadratique imaginaire premier à p et $u \otimes_{\mathbb{T}_{\mathbb{Q}}} v \in H_{\mathbb{Q}}^+ \otimes_{\mathbb{T}_{\mathbb{Q}}} H_{\mathbb{Q}}^-$?

6.4 Les éléments y_m

Soit $m > 0$ un entier. Considérons l'élément de $\mathcal{P}$ suivant :

$$y_m = \sum_{i=0}^{g} \left\langle T_m x_i, \frac{x_i}{w_i} \right\rangle \ x_i = \sum_{i=0}^{g} B_{i,i}(m) x_i. \tag{6.4}$$

On a

$$\deg(y_m) = \mathrm{Tr} B(m) \qquad (m \geq 1). \tag{6.5}$$

Posons $y_m^0 = \pi^0(y_m)$.

Rappelons que l'application $\theta : \mathcal{P} \otimes_{\widetilde{\mathbb{T}}} \check{\mathcal{P}} \longrightarrow \mathcal{N}$ est définie par

$$\theta(x_i \otimes_{\widetilde{\mathbb{T}}} \frac{x_j}{w_j}) = \frac{1}{2} + \sum_{k \geq 1} \langle T_k x_i, \frac{x_j}{w_j} \rangle q^k.$$

On en déduit l'égalité

$$y_m = (1 \otimes (a_m \circ \theta))(\bar{\Delta}_3). \tag{6.6}$$

Puisque $\bar{\Delta}_3^0 \in \mathcal{P}_{\mathbb{Q}}^0[I_e] \otimes_{\mathbb{Q}} \left(\mathcal{P}_{\mathbb{Q}}^0 \otimes_{\mathbb{T}_{\mathbb{Q}}} \mathcal{P}_{\mathbb{Q}}^0 \right)$, l'égalité (6.6) entraîne la

Proposition 6.5
Pour tout $m \geq 1$, y_m^0 appartient à $\mathcal{P}_{\mathbb{Q}}^0[I_e]$.

Démonstration. — En effet, d'après (6.6), on a

$$y_m^0 = \pi^0 \circ (1 \otimes_{\mathbb{Q}} (a_m \circ \theta))(\bar{\Delta}_3) = (1 \otimes_{\mathbb{Q}} (a_m \circ \theta)) \circ (\pi^0 \otimes_{\mathbb{Q}} (1 \otimes_{\widetilde{\mathbb{T}}_{\mathbb{Q}}} 1))(\bar{\Delta}_3).$$

□

6.4.1 Le $\mathbb{T}_{\mathbb{Q}}$-module engendré par $y_m^0,\ m \geq 1$

A une forme linéaire ϕ sur $\mathcal{P}_{\mathbb{Q}}$, on associe la forme modulaire parabolique à coefficients rationnels

$$\mathbf{g}_\phi = (\phi \otimes_{\mathbb{Q}} \theta_{\mathbb{Q}}^0)(\bar{\Delta}_3^0). \tag{6.7}$$

La forme parabolique $\mathbf{g}_\phi$ a pour développement de Fourier à l'infini

$$\sum_{m\geq 1} \phi(y_m^0) q^m. \tag{6.8}$$

En effet, on a :

$$\sum_{m\geq 1} (\phi \otimes_{\mathbb{Q}} (a_m \circ \theta_{\mathbb{Q}}^0))(\bar{\Delta}_3^0)\ q^m = \sum_{m\geq 1} \phi(y_m^0) q^m.$$

Proposition 6.6
Le $\mathbb{Q}$-espace vectoriel engendré par $(y_m^0)_{m\geq 1}$ est égal au $\mathbb{Q}$-espace vectoriel engendré par $(y_m^0)_{1\leq m\leq g+1}$.

Démonstration. — Il suffit de montrer que toute forme linéaire sur l'espace vectoriel engendré par $(y_m^0)_{m\geq 1}$ et qui s'annule en $y_1^0, \ldots, y_{g+1}^0$ est nulle.

Soit ϕ une telle forme linéaire. La forme différentielle ω_ϕ de $X_0(p)$ associée à $\mathbf{g}_\phi$ a pour q-développement

$$\sum_{m\geq 1} \phi(y_m^0) q^m \frac{dq}{q}.$$

Si $\phi(y_1^0) = 0, \ldots, \phi(y_{g+1}^0) = 0$, la forme différentielle holomorphe ω_ϕ a un zéro d'ordre g en l'infini. L'infini n'étant pas un point de Weierstrass de $X_0(p)$ (voir [36]), on en déduit que ω_ϕ est nulle, d'où la proposition. □

Parent [37] a montré que l'ensemble $\{\gamma_D, -D \in A\}$ engendre le $\mathbb{Q}$-espace vectoriel $\mathcal{P}_{\mathbb{Q}}^0[I_e]$ (voir la remarque 6.1). Deux questions restent actuellement ouvertes. L'analogue du résultat de Parent est-il vrai pour $\{y_m^0, 1 \leq m \leq g+1\}$? Le $\mathbb{Q}$-espace vectoriel engendré par $(y_m^0)_{m\geq 1}$ est-il stable sous l'action de $\mathbb{T}_{\mathbb{Q}}$?

Notons $\mathcal{Y}$ le $\mathbb{T}_{\mathbb{Q}}$-module engendré par $(y_m^0)_{m\geq 1}$.

Proposition 6.7
Les conditions suivantes sont équivalentes :

i) les $\mathbb{T}_{\mathbb{Q}}$-modules $\mathcal{Y}$ et $\mathcal{P}_{\mathbb{Q}}^0[I_e]$ sont égaux,

ii) pour toute forme primitive f de poids 2 pour $\Gamma_0(p)$ telle que $L(f,1) \neq 0$, il existe une forme primitive g telle que $L(f \otimes \mathrm{Sym}^2 g, 2) \neq 0$.

Démonstration. — Soit g une forme primitive de poids 2 pour $\Gamma_0(p)$. On a

$$\mathbf{1}_g\ \theta_{\bar{\mathbb{Q}}}(x \otimes_{\tilde{\mathbb{T}}_{\bar{\mathbb{Q}}}} y) = \theta_{\bar{\mathbb{Q}}}(x^g \otimes_{\tilde{\mathbb{T}}_{\bar{\mathbb{Q}}}} y^g) \qquad \left((x,y) \in \mathcal{P}_{\bar{\mathbb{Q}}}{}^2\right).$$

Pour toute forme linéaire ϕ sur $\mathcal{P}_{\mathbb{Q}}$, on a donc

$$\mathbf{1}_g\ \mathbf{g}_\phi = (\phi_{\bar{\mathbb{Q}}} \otimes_{\bar{\mathbb{Q}}} \theta^0_{\bar{\mathbb{Q}}}) \left(\sum_{h \in \mathrm{Prim}(p)} (\mathbf{1}_h \otimes \mathbf{1}_g)(\bar{\Delta}_3) \right). \tag{6.9}$$

Lemme 6.8
Soient f et g deux formes primitives. L'assertion

$$L(f,1)L(f \otimes \mathrm{Sym}^2 g, 2) = 0$$

est équivalente à l'assertion

$$\mathbf{1}_g.\mathbf{g}_{\langle\, .,a_f\rangle} = 0.$$

Démonstration du lemme. — D'après (6.9), on a dans $\mathcal{M}^g_{\bar{\mathbb{Q}}}$

$$\mathbf{1}_g\ \mathbf{g}_{\langle .,a_f\rangle} \quad = \quad \Big(\langle .,a_f\rangle \otimes_{\bar{\mathbb{Q}}} \theta^0_{\bar{\mathbb{Q}}}\Big) \left(\sum_{h \in \mathrm{Prim}(p)} (\mathbf{1}_h \otimes \mathbf{1}_g)(\bar{\Delta}_3) \right).$$

Posons $(\mathbf{1}_h \otimes \mathbf{1}_g)(\bar{\Delta}_3) = \lambda_{h,g}\ a_h \otimes_{\bar{\mathbb{Q}}} (a_g \otimes_{\mathbb{T}_{\bar{\mathbb{Q}}}} a_g)$ avec $\lambda_{h,g} \in \bar{\mathbb{Q}}$. On a alors

$$\mathbf{1}_g\ \mathbf{g}_{\langle .,a_f\rangle} = \lambda_{f,g}\ \langle a_f, a_f\rangle\ \theta^0_{\bar{\mathbb{Q}}}(a_g \otimes_{\mathbb{T}_{\mathbb{Q}}} a_g) = \Big(\langle .,a_f\rangle \otimes_{\bar{\mathbb{Q}}} \theta^0_{\bar{\mathbb{Q}}}\Big)\left(\overline{\Delta^F_3}\right),$$

où l'on pose $F = f \otimes g \otimes g \in (\mathcal{M}^0_{\bar{\mathbb{Q}}})^{\otimes 3}$.

Or l'application

$$\langle .,a_f\rangle \otimes_{\bar{\mathbb{Q}}} \theta^0_{\bar{\mathbb{Q}}} : \mathcal{P}^f_{\bar{\mathbb{Q}}} \otimes_{\bar{\mathbb{Q}}} (\mathcal{P}^0_{\bar{\mathbb{Q}}} \otimes_{\mathbb{T}_{\bar{\mathbb{Q}}}} \mathcal{P}^0_{\bar{\mathbb{Q}}}) \longrightarrow \mathcal{M}^0_{\bar{\mathbb{Q}}}$$

est injective. Par conséquent $\mathbf{1}_g\ \mathbf{g}_{\langle .,a_f\rangle} = 0$ si et seulement si $\overline{\Delta^F} = \lambda_{f,g} a_f \otimes_{\bar{\mathbb{Q}}} (a_g \otimes_{\mathbb{T}_{\bar{\mathbb{Q}}}} a_g) = 0$ *i.e.* si et seulement si $\Delta^F = 0$. Or, d'après le corollaire 6.3, ceci est équivalent à l'assertion

$$L(f,1)L(f \otimes \mathrm{Sym}^2 g, 2) = 0.$$

◇

Les espaces propres pour $\mathbb{T}_{\bar{\mathbb{Q}}}$ de $\mathcal{P}^0_{\bar{\mathbb{Q}}}$ étant des $\bar{\mathbb{Q}}$-droites, la condition i) de la proposition 6.7 est équivalente à la condition i') suivante : pour toute forme primitive f telle que $L(f,1) \neq 0$, il existe $m \geq 1$ tel que $y^f_m \neq 0$. Or d'après le lemme 6.8, la condition ii) est vérifiée si et seulement si pour toute forme primitive f telle que $L(f,1) \neq 0$, il existe une forme primitive g telle que $\mathbf{1}_g \mathbf{g}_{\langle .,a_f\rangle} \neq 0$. Autrement dit, ii) est vraie si et seulement si la forme parabolique $\mathbf{g}_{\langle .,a_f\rangle}$ n'est pas identiquement nulle. Comme

$$\mathbf{g}_{\langle .,a_f\rangle} = \sum_{m \geq 1} \langle y_m, a_f\rangle\ q^m,$$

on en déduit l'équivalence de i) et ii). □

6.4.2 Relation entre y_m et γ_D

Rappelons que $m \geq 1$ est un entier. Posons

$$\epsilon(m) = \begin{cases} 1 & \text{si } m \text{ est un carré} \\ 0 & \text{sinon.} \end{cases}$$

Théorème 6.9
On a

$$y_m = \epsilon(m)\ a_E + \sum_{\substack{(s,d)\in\mathbb{Z}\times\mathbb{N} \\ 4m-s^2=dr^2>0}} \gamma_d.$$

Démonstration. — Rappelons que

$$y_m = \sum_{i=0}^{g} B_{i,i}(m) x_i.$$

D'après (4.21), on a

$$\begin{aligned} B_{i,i}(m) &= \frac{1}{2w_i}\mathrm{Card}\{b \in R_i = M_{i,i}\ ;\ N(b) = m\} \\ &= \frac{1}{2w_i} \sum_{\substack{s\in\mathbb{Z} \\ s^2\leq 4m}} \mathrm{Card}(A_i(s,m)) \end{aligned}$$

où

$$A_i(s,m) = \{b \in R_i\ ;\ N(b) = m, \mathrm{Tr}(b) = s\}.$$

Rappelons quelques faits essentiels (voir la démonstration de [10] proposition 1.9). Posons $D = 4m - s^2$. Lorsque $D = 0$, ce qui est possible si et seulement si m est un carré, $A_i(s,m)$ n'a qu'un seul élément. Lorsque $D > 0$, tout élément b de $A_i(s,m)$ donne lieu à un plongement f_b a priori non optimal de l'ordre $\mathcal{O}_{-D}$ de discriminant $-D$ dans R_i. Le groupe $\Gamma_i = R_i^*/\langle\pm 1\rangle$ agit par conjugaison sur $A_i(s,m)$ ainsi que sur l'ensemble des plongements de $\mathcal{O}_{-D}$ dans R_i. Les orbites de $A_i(s,m)$ sous l'action de Γ_i sont en correspondance bijective avec les plongements de $\mathcal{O}_{-D}$ dans R_i modulo conjugaison par R_i^*. Soit $\mathcal{O}_{-d}$ un ordre de discriminant $-d$ contenant $\mathcal{O}_{-D}$, *i.e.* tel que d divise D et D/d est un carré. Tout plongement de $\mathcal{O}_{-D}$ dans R_i s'étend en $h_i(d)$ plongements optimaux de $\mathcal{O}_{-d}$ dans R_i modulo conjugaison par R_i^*. Le stabilisateur de $b \in A_i(s,m)$ sous l'action de Γ_i est d'ordre $u(-d)$. On a donc

$$\mathrm{Card}(A_i(s,m)) = w_i \sum_{\substack{d\in\mathbb{N};\exists r\in\mathbb{N}; \\ dr^2=D}} \frac{h_i(-d)}{u(-d)}.$$

Finalement, pour tout entier $m > 0$, on a

$$\begin{aligned} y_m &= \sum_{4m=s^2} \sum_{i=0}^{g} \frac{x_i}{2w_i} + \sum_{i=0}^{g} \sum_{\substack{(s,d)\in\mathbb{Z}\times\mathbb{N} \\ \exists r>0;\ 4m-s^2=dr^2>0}} \frac{h_i(-d)}{2u(-d)} x_i \\ &= \epsilon(m)\ a_E + \sum_{\substack{(s,d)\in\mathbb{Z}\times\mathbb{N} \\ 4m-s^2=dr^2>0}} \sum_{i=0}^{g} \frac{h_i(-d)}{2u(-d)} x_i. \end{aligned}$$

Ceci montre le théorème. □

Remarque 6.2 Le raisonnement précédent est celui qui donne la formule d'Eichler pour la trace de T_m (voir [7] ou [10]). On retrouve cette formule en identifiant les degrés de chacun des membres de l'égalité du théorème.

Remarque 6.3 Puisque pour tout entier $d < 0$, l'élément γ_d^0 est dans $\mathcal{P}^0[I_e]$, le théorème 6.9 donne une nouvelle preuve de la proposition 6.5 [3].

Table 6.1 On a

$$\begin{aligned}
y_1 &= a_E + 2\gamma_3 + \gamma_4 \\
y_2 &= 2\gamma_4 + 2\gamma_7 + \gamma_8 \\
y_3 &= 3\gamma_3 + 2\gamma_8 + 2\gamma_{11} + \gamma_{12} \\
y_4 &= a_E + 2\gamma_3 + \gamma_4 + 2\gamma_7 + 2\gamma_{12} + 2\gamma_{15} + \gamma_{16} \\
y_5 &= 4\gamma_4 + 2\gamma_{11} + 2\gamma_{16} + 2\gamma_{19} + \gamma_{20} \\
y_6 &= 2\gamma_8 + 2\gamma_{15} + 2\gamma_{20} + 2\gamma_{23} + \gamma_{24} \\
y_7 &= 6\gamma_3 + \gamma_7 + 2\gamma_{12} + 2\gamma_{19} + 2\gamma_{24} + 2\gamma_{27} + \gamma_{28} \\
y_8 &= 2\gamma_4 + 4\gamma_7 + \gamma_8 + 2\gamma_{16} + 2\gamma_{23} + 2\gamma_{28} + 2\gamma_{31} + \gamma_{32} \\
y_9 &= a_E + 2\gamma_3 + \gamma_4 + 2\gamma_8 + 2\gamma_{11} + 2\gamma_{20} + 2\gamma_{27} + 2\gamma_{32} + 2\gamma_{35} + \gamma_{36} \\
y_{10} &= 4\gamma_4 + 2\gamma_{15} + 2\gamma_{24} + 2\gamma_{31} + 2\gamma_{36} + 2\gamma_{39} + \gamma_{40} \\
y_{11} &= 2\gamma_7 + 2\gamma_8 + \gamma_{11} + 2\gamma_{19} + 2\gamma_{28} + 2\gamma_{35} + 2\gamma_{40} + 2\gamma_{43} + \gamma_{44} \\
y_{12} &= 3\gamma_3 + 2\gamma_8 + 2\gamma_{11} + 3\gamma_{12} + 2\gamma_{23} + 2\gamma_{32} + 2\gamma_{39} + 2\gamma_{44} + 2\gamma_{47} + \gamma_{48} \\
y_{13} &= 6\gamma_3 + 4\gamma_4 + 2\gamma_{12} + 2\gamma_{16} + 2\gamma_{27} + 2\gamma_{36} + 2\gamma_{43} + 2\gamma_{48} + 2\gamma_{51} + \gamma_{52}.
\end{aligned}$$

Corollaire 6.10
Si $\mathcal{Y} = \mathcal{P}^0_{\mathbb{Q}}[I_e]$ et si f est une forme modulaire primitive de poids 2 pour $\Gamma_0(p)$ telle que $L(f,1) \neq 0$, alors il existe $d \leq 4g+4$ tel que $L(f \otimes \varepsilon_d, 1) \neq 0$.

Démonstration. — Soit f une forme primitive. D'après [18] théorème B, il existe une infinité de discriminants $-D < 0$ premiers à p tels que $L(f \otimes \varepsilon_D, 1) \neq 0$. Choisissons un tel discriminant $-D$. Si $L(f,1) \neq 0$, on a $\mathbf{1}_f \left(\mathcal{P}^0_{\mathbb{Q}}[I_e] \right) \neq 0$ et

[3] On rappelle que γ_d est nul si $-d$ n'est pas un discriminant quadratique imaginaire (se reporter à la remarque 5.1).

donc $\mathcal{Y}^f_{\bar{\mathbb{Q}}} \neq 0$. D'après la proposition 6.6, il existe alors $m \in \{1, \ldots, g+1\}$ tel que $y^f_m \neq 0$. Or d'après le théorème 6.9,

$$y^f_m = \sum_{\substack{(s,d)\in\mathbb{Z}\times\mathbb{N} \\ 4m-s^2=dr^2>0}} \gamma^f_d.$$

On en déduit qu'il existe $d \leq 4m \leq 4g+4$ tel que $\gamma^f_d \neq 0$ c'est-à-dire, d'après la formule de Gross-Zhang énoncée au théorème 5.2, tel que $L(f \otimes \varepsilon_d, 1) \neq 0$. $\square$

6.5 Points rationnels de certaines courbes modulaires

Nous allons à présent utiliser la proposition 6.5 pour étudier la géométrie en caractéristique p du morphisme ϕ^e_P de $X_0(p)$ dans le quotient d'enroulement J_e de sa jacobienne.

6.5.1 Morphisme d'enroulement

On renvoie à la première partie de ce document pour la définition d'immersion formelle. Le critère d'immersion formelle donné dans ce paragraphe est un cas particulier du théorème 1.10 du chapitre 1. Toutefois on peut en trouver une démonstration indépendante dans [37] proposition 3.2.

Le *quotient d'enroulement* est la variété abélienne (voir [24])

$$J_e = J_0(p)/I_e J_0(p).$$

Nous reprenons ici les notations du chapitre 1 : on note $X_0(p)_{\mathbb{Z},\text{lisse}}$ la partie lisse de la normalisation $X_0(p)_{\mathbb{Z}}$ de $\mathbb{P}^1_{\mathbb{Z}}$ dans $X_0(p)$ via $X_0(p) \longrightarrow X_0(1) \cong \mathbb{P}^1_{\mathbb{Q}}$. Soient K un corps p-adique d'anneau des entiers $\mathcal{O}_K$, $k_{\mathfrak{p}}$ son corps résiduel et P un point K-rationnel de $X_0(p)$. Rappelons que $X_0(p)_{\mathcal{O}_K}$ désigne le schéma sur Spec $\mathcal{O}_K$ obtenu par extension des scalaires de $X_0(p)_{\mathbb{Z}}$ à $\mathcal{O}_K$ et $J_0(p)_{\mathcal{O}_K}$ (resp. $J_{e,\mathcal{O}_K}$) le modèle de Néron de $J_0(p)$ (resp. J_e) sur $\mathcal{O}_K$. On note $P_{\mathcal{O}_K}$ la section de $X_0(p)_{\mathcal{O}_K}$ sur $\mathcal{O}_K$ définie par P et $P_{k_{\mathfrak{p}}} = P_{\bar{\mathbb{F}}_p}$ sa réduction modulo p. Supposons que P est ordinaire en caractéristique p, c'est-à-dire que sa réduction $P_{k_{\mathfrak{p}}}$ n'est pas un point double de $X_0(p)_{\bar{\mathbb{F}}_p}$.

Soient

$$\begin{array}{rccc} \phi_P \ : & X_0(p) & \longrightarrow & J_0(p) \\ & Q & \longmapsto & [(Q)-(P)] \end{array}$$

et ϕ^e_P le morphisme de $X_0(p)$ vers J_e obtenu en composant ϕ_P et le morphisme quotient $J_0(p) \twoheadrightarrow J_e$. Puisque P est ordinaire en caractéristique p, ces morphismes s'étendent en des morphismes de schémas sur $\mathcal{O}_K$ que nous noterons encore respectivement

$$\phi_P : X_0(p)_{\mathcal{O}_K,\text{lisse}} \longrightarrow J_0(p)_{\mathcal{O}_K}$$

et

$$\phi^e_P : X_0(p)_{\mathcal{O}_K,\text{lisse}} \longrightarrow J_{e,\mathcal{O}_K}.$$

Notons $j_0, \ldots, j_g$ les invariants supersinguliers associés respectivement à $x_0, \ldots, x_g$. Pour $j \in \mathbb{P}^1(\bar{\mathbb{F}}_p)$ non supersingulier, on définit l'application

$$\begin{array}{rccc} \iota_j \ : & \mathcal{P} & \longrightarrow & \bar{\mathbb{F}}_p \\ & \sum_{i=0}^g \lambda_i x_i & \longmapsto & \sum_{i=0}^g \frac{\lambda_i}{j-j_i}. \end{array} \tag{6.10}$$

Proposition 6.11
Soit $j \in \mathbb{P}^1(\bar{\mathbb{F}}_p)$ l'invariant associé au point $P_{k_\mathfrak{p}}$. S'il existe $x \in \mathcal{P}^0[I_e]$ tel que $\iota_j(x) \neq 0$ alors ϕ_P^e est une immersion formelle au point $P_{k_\mathfrak{p}}$.

Démonstration. — Voir chapitre 1 théorème 1.10 ou [37] proposition 3.2. □

6.5.2 Méthode de Momose-Parent

Soit $r > 1$ un entier. Considérons la courbe modulaire $X_0(p^r)^+$ quotient de la courbe modulaire $X_0(p^r)$ par l'involution d'Atkin-Lehner w_{p^r}. On dit qu'un point $\mathbb{C}$-rationnel de $X_0(p^r)$ est *trivial* si c'est une pointe ou si la courbe elliptique sous-jacente est à multiplication complexe.

S'inspirant des travaux de Momose [31, 32, 33], Parent (voir [37] proposition 3.1) montre la

Proposition 6.12 (Parent)
Supposons que $p \geq 11$. Si pour tout $P \in X_0(p)_{\mathbb{Z},\text{lisse}}(\mathbb{Z}_p)$ le morphisme ϕ_P^e est une immersion formelle en $P_{\mathbb{F}_p}$ alors les points $\mathbb{Q}$-rationnels de $X_0^+(p^r)$ sont triviaux.

Posons $\mathcal{A}$ l'ensemble des nombres premiers p qui sont simultanément un carré modulo $3, 4, 7$ et un carré modulo au moins cinq des nombres suivants : $8, 11, 19, 43, 67, 163$. L'ensemble $\mathcal{A}$ a pour densité $7/2^9$. En appliquant le critère de la proposition 6.11 à des combinaisons linéaires bien choisies des éléments $\gamma_D^0 \in \mathcal{P}_\mathbb{Q}^0[I_e]$, Parent montre le théorème suivant (voir [37] théorème 1.1) :

Théorème 6.13 (Parent)
Si $p \geq 11$, $p \neq 13$ et $p \notin \mathcal{A}$, alors $X_0^+(p^r)(\mathbb{Q})$ est trivial pour tout entier $r > 1$.

Remarque 6.4 Soit $X_{\text{split}}(p)$ la courbe modulaire sur $\mathbb{Q}$ classifiant les courbes elliptiques généralisées munies d'une paire non ordonnée d'isogénies de degré p. La courbe $X_{\text{split}}(p)$ est isomorphe à $X_0^+(p^2)$ sur $\mathbb{Q}$. Le théorème 6.13 appliqué à $r = 2$ entraîne donc que les points $\mathbb{Q}$-rationnels de $X_{\text{split}}(p)$ sont triviaux lorsque $p \geq 11$, $p \neq 13$ et $p \notin \mathcal{A}$.

Comme alternative aux éléments γ_D^0, nous proposons de considérer des éléments de $\mathcal{Y}$.

6.5.3 Utilisation d'éléments de $\mathcal{Y}$

Soient $j \in \mathbb{P}^1(\bar{\mathbb{F}}_p)$ un invariant non supersingulier et $m > 0$ un entier. Soit λ l'application naturelle de $\mathbb{Q}$ dans $\mathbb{P}^1(\mathbb{F}_p)$ définie par $\lambda(a/b) = ab^{-1}$ si $(b,p) = 1$ et $\lambda(a/b) = \infty$ sinon, pour tout couple (a,b) d'entiers premiers entre eux. On notera encore ι_j l'application $\lambda \otimes \iota_j : \mathcal{P}_{\mathbb{Q}} \longrightarrow \mathbb{P}^1(\bar{\mathbb{F}}_p)$. Remarquons que comme $y_m^0 \in \mathcal{P}^0\big[\frac{1}{n\delta}\big]$, $\iota_j(y_m^0)$ est dans $\bar{\mathbb{F}}_p$ dès lors que $p > 3$. On suppose désormais que $p > 3$.

Considérons la forme parabolique à coefficients dans $\bar{\mathbb{F}}_p$ définie par

$$\mathbf{g}_j = (\iota_j \otimes_{\mathbb{Q}} \theta_{\mathbb{Q}}^0)(\bar{\Delta}_3^0) \in \mathcal{M}_{\bar{\mathbb{F}}_p}^0. \tag{6.11}$$

Cette forme modulaire a pour q-développement

$$\sum_{m \geq 1} \iota_j(y_m^0)\, q^m. \tag{6.12}$$

Proposition 6.14
Si $\mathbf{g}_j \neq 0$ alors ϕ_P^e est une immersion formelle au point de $X_0(p)_{\bar{\mathbb{F}}_p}$ d'invariant modulaire j.

Démonstration. — Rappelons que l'application qui à une forme parabolique sur $\bar{\mathbb{F}}_p$ associe son q-développement est injective (voir le paragraphe 4.1). La proposition résulte alors de (6.12) et des propositions 6.5 et 6.11. □

Dans $\bar{\mathbb{F}}_p$, on a l'égalité

$$\iota_j(y_m^0) = \sum_{i=0}^{g} \frac{B_{i,i}(m)}{j - j_i} + 12\ \mathrm{Tr}(B(m)) \sum_{i=0}^{g} \frac{1}{w_i(j - j_i)}. \tag{6.13}$$

En effet,

$$y_m^0 = y_m - \frac{12}{p-1} \deg(y_m) a_E,$$

et

$$\iota_j(a_E) = \sum_{i=0}^{g} \frac{1}{w_i(j - j_i)}.$$

Le terme $\sum_{i=0}^{g} \frac{1}{w_i(j-j_i)}$ n'étant pas facile à calculer en pratique, nous introduisons d'autres éléments de $\mathcal{P}_{\mathbb{Q}}^0[I_e]$.

Pour $m > 0$ et $k > 0$ deux entiers tels que $k \leq m$, on considère l'élément

$$y_{k,m} = \mathrm{Tr}\ B(m) y_k - \mathrm{Tr}\ B(k) y_m. \tag{6.14}$$

Puisque $y_{k,m} \in \mathcal{P}^0[I_e]$, on déduit immédiatement des propositions 6.5 et 6.11 le

Corollaire 6.15
Supposons qu'il existe $k, m \geq 1$ tel que $\iota_j(y_{k,m}) \neq 0$ dans $\bar{\mathbb{F}}_p$. Alors ϕ_P^e est une immersion formelle au point de $X_0(p)_{\bar{\mathbb{F}}_p}$ d'invariant modulaire j.

On a

$$\iota_j(y_{k,m}) = \sum_{i=0}^{g} \frac{\mathrm{Tr}\ B(m)\ B_{i,i}(k) - \mathrm{Tr}\ B(k)\ B_{i,i}(m)}{j - j_i}. \tag{6.15}$$

6.5.4 Calcul pratique de $\iota_j(y_{k,m})$

Les calculs que nous décrivons dans ce paragraphe sont inspirés de la méthode du graphe de Mestre et Oesterlé [28]. En combinant les résultats de ces calculs au théorème 6.13 dû à Parent, on obtient le théorème 6.16 ci-dessous.

On note p_0 le nombre premier 4532193519. Soit $\mathcal{C}$ l'ensemble des nombres premiers p qui sont simultanément un carré modulo $3, 4, 7$ et tels que l'une des conditions suivantes est vérifiée :

1. p carré modulo $11, 19, 23, 43, 67, 163$, non carré modulo 8 ;
2. p carré modulo $8, 11, 19$, et au moins deux des nombres premiers $43, 67, 163$, et vérifiant l'une des conditions suivantes
   (a) p carré modulo 5 ;
   (b) p non carré modulo 5 et 23 ;
   (c) p non carré modulo 5 et carré modulo $23, 59, 71$;
   (d) p non carré modulo $5, 59, 71$ et carré modulo 23 ;
3. p carré modulo $5, 8, 11, 43, 67, 163$, non carré modulo 19 et
   (a) p carré modulo 23 ;
   (b) ou p non carré modulo 23 et $\left(\frac{p}{31}\right)\left(\frac{p}{36319}\right)\left(\frac{p}{p_0}\right) = 1$;
4. p carré modulo $5, 8, 19, 43, 67, 163$, non carré modulo 11 et p carré modulo au moins un des nombres : $23, 797$.

Théorème 6.16
Si $p > 19$ et $p \notin \mathcal{C}$, alors les points $\mathbb{Q}$-rationnels de $X_0^+(p^r)$ sont triviaux pour tout entier $r > 1$.

La densité de l'ensemble des premiers p intervenant dans le théorème 6.16 est égale à $1 - 5/2^9$.

Description des calculs

Soient m un entier et $\phi_m \in \mathbb{Z}[X, Y]$ le polynôme modulaire d'ordre m (voir [16] 5.2). Le polynôme ϕ_m est symétrique. Soient E et E' des courbes elliptiques sur $\bar{\mathbb{F}}_p$ d'invariants modulaires respectifs j_E et $j_{E'}$. Si p ne divise pas m, les courbes elliptiques E et E' sont m-isogènes sur $\bar{\mathbb{F}}_p$ si et seulement si $\phi_m(j_E, j_{E'}) = 0$ dans $\bar{\mathbb{F}}_p$. Une courbe elliptique E est donc m-isogène à elle-même si et seulement si son invariant j_E est racine de $\phi_m(X, X)$ dans $\bar{\mathbb{F}}_p$.

Par ailleurs, supposons que m n'est pas un carré et qu'il existe une m-isogénie f d'une courbe elliptique E sur $\bar{\mathbb{F}}_p$ dans elle-même. D'après le théorème de relèvement de Deuring (voir [16] théorème 14), il existe alors un ordre quadratique imaginaire $\mathcal{O} = \mathbb{Z}[\tau]$ possédant un élément de norme m et une courbe elliptique

E_τ à multiplication par $\mathcal{O}$ qui a bonne réduction isomorphe à E_i en un idéal $\mathfrak{p}$ au-dessus de p. L'invariant j_i est donc la réduction en $\mathfrak{p}$ de $j(\tau) = j_{E_\tau}$.

On suppose désormais, pour simplifier les calculs, que m est sans facteur carré et n'est pas divisible par p.

On peut donc déterminer les invariants supersinguliers $j_i, 0 \leq i \leq g$, pour lesquels $B_{i,i}(m) \neq 0$ de deux façons différentes : soit en déterminant les racines dans $\bar{\mathbb{Q}}$ de $\phi_m(X, X)$, soit en déterminant les ordres quadratiques imaginaires possédant un élément de norme m. D'après un résultat de Kronecker (voir [16] théorème 11), la multiplicité $n_m(\tau)$ de la racine $j(\tau)$ de $\phi_m(X, X)$ est égale au nombre d'éléments de $\mathbb{Z}[\tau]$ de norme m à multiplication par une unité près. L'invariant $j(\tau)$ est supersingulier en caractéristique p si et seulement si p est inerte ou ramifié dans $\mathbb{Q}(\tau)$ (voir [16] théorème 12). Dans ce cas, si $j(\tau) \equiv j_i \mod \mathfrak{p}$, on a $B_{i,i}(m) = n_m(\tau)$.

Calcul de $\iota_j(y_{k,m})$ pour k, m dans $\{2, 3, 5, 6, 7\}$

On suppose $p > 7$.

Table 6.2

$$
\begin{aligned}
\phi_2(X,X) &= -(X-1\,728)(X+3\,375)^2(X-8\,000)\\
\phi_3(X,X) &= -X(X-54\,000)(X+32\,768)^2(X-8\,000)^2\\
\phi_5(X,X) &= -(X-1\,728)^2(X-287\,496)^2(X+32\,768)^2(X+884\,736)^2\ P_1\\
\phi_6(X,X) &= (X-8\,000)^2\ P_1^2\ P_2\ P_3^2\ P_4^2\\
\phi_7(X,X) &= -(X+3\,375)(X-16\,581\,375)X^2(X-54\,000)^2\\
&\quad \times (X+12\,288\,000)^2(X+884\,736)^2\ P_2^2
\end{aligned}
$$

où

$$
\begin{aligned}
P_1 &= X^2 - 1\,264\,000\ X - 681\,472\,000\\
P_2 &= X^2 - 4\,834\,944\ X + 14\,670\,139\,392\\
P_3 &= X^2 + 191\,025\ X - 121\,287\,375\\
P_4 &= X^3 + 3\,491\,750\ X^2 - 5\,151\,296\,875\ X + 12\,771\,880\,859\,375.
\end{aligned}
$$

Les ordres associés aux racines des facteurs de degré 1 de $\phi_2, \phi_3, \phi_5, \phi_6$ et ϕ_7 sont donnés dans la littérature (voir par exemple [1] 7.2.3).

Pour $i \in \{1, \ldots, 4\}$, notons α_i une racine de P_i dans $\bar{\mathbb{Q}}$. En déterminant les ordres de corps quadratiques imaginaires possédant un élément de norme $5, 6$ et 7, on trouve que, quitte à échanger les racines conjuguées, on a

$$
\begin{aligned}
\alpha_1 &= j\left(\sqrt{-5}\right)\\
\alpha_2 &= j\left(\sqrt{-6}\right)\\
\alpha_3 &= j\left(\frac{1+\sqrt{-15}}{2}\right)\\
\alpha_4 &= j\left(\frac{1+\sqrt{-23}}{2}\right).
\end{aligned}
$$

Les conditions sur p pour que les courbes elliptiques ayant ces racines pour invariant soient supersingulières en caractéristique p sont résumées dans le tableau 6.1 de la page 108. Pour un invariant $j(\tau)$, on note $-D<0$ le discriminant du corps quadratique $\mathbb{Q}(\tau)$. Les coefficients de la dernière colonne sont par définition égaux à 1 lorsque l'invariant correspondant est supersingulier et 0 sinon.

TAB. 6.1 – Invariants supersinguliers pour lesquels $B(i,i)\neq 0$.

$j(x_i)$	D	supersingulier pour	coeff
$1\,728 = j(\sqrt{-1})$ $287\,496 = j(2\sqrt{-1})$	4	$p=2$ ou $p\equiv 3 \mod 4$	a
$-3\,375 = j(\frac{1+\sqrt{-7}}{2})$ $16\,581\,375 = j(\sqrt{-7})$	7	$p=7$ ou p non carré mod 7	b
$8\,000 = j(\sqrt{-2})$	8	$p=2$ ou $p\equiv 5,7 \mod 8$	c
$0 = j(\frac{1+\sqrt{-3}}{2})$ $54\,000 = j(\sqrt{-3})$ $-12\,288\,000 = j(\frac{1+3\sqrt{-3}}{2})$	3	$p=3$ ou $p\equiv 2 \mod 3$	d
$-32\,768 = j(\frac{1+\sqrt{-11}}{2})$	11	$p=11$ ou p non carré mod 11	e
$-884\,736 = j(\frac{1+\sqrt{-19}}{2})$	19	$p=19$ ou p non carré mod 19	f
$\alpha_1 = j(\sqrt{-5})$	20	$p=5$ ou $[p\equiv 3 \mod 4$ et p carré mod 5] ou $[p\equiv 1 \mod 4$ et p non carré mod 5]	g
$\alpha_2 = j(\sqrt{-6})$	24	$p=2,3$ ou $[p\equiv 2 \mod 3$ et $p\equiv 1,7 \mod 8]$ ou $[p\equiv 1 \mod 3$ et $p\equiv 3,5 \mod 8]$	h
$\alpha_3 = j\left(\frac{1+\sqrt{-15}}{2}\right)$	15	$p=3,5$ ou $[p\equiv 1 \mod 3$ et p non carré mod 5] ou $[p\equiv 2 \mod 3$ et p carré mod 5]	v
$\alpha_4 = j\left(\frac{1+\sqrt{-23}}{2}\right)$	23	$p=23$ ou p non carré mod 23	w

Les contraintes de congruence sur p résumées dans le tableau 6.1 montrent, en particulier, que $a=c$ équivaut à $h=d$, et que $a=d$ équivaut à $v=g$. On peut écrire cela sous la forme

$$h=||a-c|-d|, \quad \text{et} \quad v=||a-d|-g|.$$

Les valeurs de $B_{i,i}(m)$ pour $j_i\equiv j(\tau)$ sont données dans le tableau 6.2

Posons

$$Q_m(j)=\sum_{i=0}^{g}\frac{B_{i,i}(m)}{j-j_i}.$$

On a

$$\iota_j(y_{k,m})=\operatorname{Tr} B(m)Q_k(j)-\operatorname{Tr} B(k)Q_m(j).$$

TAB. 6.2 – Valeurs de $B(i,i)$ pour $i \in \{0,\dots,g\}$.

$j(x_i)$	D	coeff	$B_{i,i}(2)$	$B_{i,i}(3)$	$B_{i,i}(5)$	$B_{i,i}(6)$	$B_{i,i}(7)$
1728	4	a	1		2		
287496	4	a			2		
-3375	7	b	2				1
16581375	7	b					1
8000	8	c	1	2		2	
0	3	d		1			2
54000	3	d		1			2
-12288000	3	d					2
-32768	11	e		2	2		
-884736	19	f			2		2
α_1	20	g			1	2	
α_2	24	h				1	2
α_3	15	v				2	
α_4	23	w				2	

Table 6.3

$$\begin{aligned}
\mathrm{Tr}\, B(2) &= a+2b+c\\
\mathrm{Tr}\, B(3) &= 2c+2d+2e\\
\mathrm{Tr}\, B(5) &= 4a+2e+2f+2g\\
\mathrm{Tr}\, B(6) &= 2c+4g+2||a-c|-d|+4||a-d|-g|+6w\\
\mathrm{Tr}\, B(7) &= 2b+6d+2f+4||a-c|-d|.
\end{aligned}$$

Table 6.4

$$\begin{aligned}
Q_2(j) &= \frac{a}{j-1728}+\frac{2b}{j+3375}+\frac{c}{j-8000}\\
Q_3(j) &= \frac{2c}{j-8000}+\frac{d}{j}+\frac{d}{j-54000}+\frac{2e}{j+32768}\\
Q_5(j) &= \frac{2a}{j-1728}+\frac{2a}{j-287496}+\frac{2e}{j+32768}+\frac{2f}{j+884736}+\frac{gP_1'(j)}{P_1(j)}\\
Q_6(j) &= \frac{2c}{j-8000}+\frac{2g\,P_1'(j)}{P_1(j)}+\frac{h\,P_2'(j)}{P_2(j)}+\frac{2v\,P_3'(j)}{P_3(j)}+\frac{2w\,P_4'(j)}{P_4(j)}\\
Q_7(j) &= \frac{b}{j+3375}+\frac{b}{j-16581375}+\frac{2d}{j}+\frac{2d}{j-54000}+\frac{2d}{j+12288000}\\
&\quad+\frac{2f}{j+884736}+\frac{2h\,P_2'(j)}{P_2(j)}
\end{aligned}$$

où

$$h=||a-c|-d|, \quad \text{et} \quad v=||a-d|-g|.$$

À titre d'exemple, calculons $\iota_j(y_{k,m})$ pour $k,m \in \{2,3,5,6,7\},\ k \leq m$, lorsque $(a,b,c,d,e,f,g,w) = (0,0,1,0,0,0,0,0)$. On a

$$\begin{aligned}
Q_2(j) &= \frac{1}{j-8000} && \text{Tr } B(2) = 1\\
Q_3(j) &= \frac{2}{j-8000} && \text{Tr } B(3) = 2\\
Q_5(j) &= 0 && \text{Tr } B(5) = 0\\
Q_6(j) &= \frac{2}{j-8000} + \frac{P_2'(j)}{P_2(j)} && \text{Tr } B(6) = 4\\
Q_7(j) &= \frac{2\,P_2'(j)}{P_2(j)} && \text{Tr } B(7) = 4.
\end{aligned}$$

On a alors

$$\iota_j(y_{2,3}) = \iota_j(y_{2,5}) = \iota_j(y_{3,5}) = \iota_j(y_{5,6}) = \iota_j(y_{5,7}) = 0$$

et $\iota_j(y_{2,6})$, $\iota_j(y_{3,6})$, $\iota_j(y_{2,7})$, $\iota_j(y_{3,7})$ et $\iota_j(y_{6,7})$ sont, à multiplication par une puissance de 2 près, égaux à

$$Q(j) = \frac{2}{j-8000} - \frac{P_2'(j)}{P_2(j)} = \frac{-2^{12}\ (13.181\ j + 2^6.3^3.7.13.29)}{(j-8000)P_2(j)}.$$

On a $p \neq 13$ car $g = 0$ or $13 \equiv 1 \mod 4$ et 13 n'est pas un carré modulo 5. De même, on a $p \neq 181$ car 181 n'est pas un carré modulo 7 mais $b = 0$. Par conséquent $Q(j)$ s'annule en

$$j_0 \equiv -(181)^{-1}.2^6.7.29. \mod p.$$

On suppose désormais $(a,b,c,d,e,f,g,w) \neq (0,0,1,0,0,0,0,0)$. On fait parcourir au 8-uplet (a,b,c,d,e,f,g,w) les différentes valeurs possibles par ordinateur. On constate que lorsque $p > 19$ et $(a,b,c,d) \neq (0,0,0,0)$, les fractions $\iota_j(y_{k,m})$ pour k,m parcourant $\{2,3,5,6,7\}$ ne s'annulent pas simultanément modulo p. En effet les facteurs premiers du résultant de deux telles fractions ne répondent pas aux conditions de congruence imposées par la valeur du 8-uplet (a,b,c,d,e,f,g,w).

Lorsque $(a,b,c,d) = (0,0,0,0)$, on obtient les résultats résumés dans le tableau 6.3 page 111. Dans ce tableau, le symbole $*$ signifie que le coefficient peut prendre indifféremment la valeur 0 ou 1. On rappelle que $p_0 = 4532193519$. Lorsque $\iota_j(y_{k,m})$ n'est pas une fraction identiquement nulle, on note $n_{k,m}$ le degré de son numérateur. Lorsque $n_{k,m} = 2$ on note $d_{k,m}$ le discriminant du numérateur (dans $\mathbb{Z}$). Dans ce cas, $\iota_j(y_{k,m})$ a un zéro dans $\mathbb{F}_p$ si et seulement si $d_{k,m}$ est un carré modulo p. Pour (e,f,g,w) distincts des quadruplets listés dans le tableau 6.3 page 111, les fractions $\iota_j(y_{k,m}),\ k,m \in \{2,3,5,6,7\}$, ne s'annulent pas simultanément.

Par exemple, lorsque $(a,b,c,d,e,f,g,w) = (0,0,0,0,0,0,1,0)$, on a

$$\iota_j(y_{5,6}) = \frac{4P_1'}{P_1} - \frac{4P_3'}{P_3} = 2^2.5^2.11^2.13.37\ \frac{x^2 + 2.5.11.x + 2^7.3^3.5^3.11.41}{P_1P_3}.$$

TAB. 6.3 – Résultats des calculs pour $(a,b,c,d) = (0,0,0,0)$.

e	f	g	w	Résultat
0	0	0	$*$	$\iota_j(y_{k,m}) = 0$ $(k,m \in \{2,3,5,6,7\})$
		1	0	$n_{5,6} = 2,\ d_{5,6} = r^2.11.59.71,$
				$\iota_j(y_{k,m}) = 0$ $(k,m) \neq (5,6)$
		1	1	$n_{5,6} = 5,\ \iota_j(y_{k,m}) = 0$ $(k,m) \neq (5,6)$
0	1	0	0	$\iota_j(y_{k,m}) = 0$ $(k,m \in \{2,3,5,6,7\})$
		0	1	$\iota_j(y_{5,6}) = \iota_j(6,7)$ $n_{5,6} = 2,$
				$d_{5,6} = r'^2.5.31.36319.p_0$
				$\iota_j(y_{k,m}) = 0$ $(k,m) \neq (5,6),(6,7)$
1	0	0	0	$\iota_j(y_{k,m}) = 0$ $(k,m \in \{2,3,5,6,7\})$
		0	1	$\iota_j(3,6) = \iota_j(5,6),\ n_{5,6} = 2,$
				$d_{5,6} = r''^2.3.5.797$
				$\iota_j(y_{k,m}) = 0$ $(k,m) \neq (3,6),(5,6)$

Analyse des résultats

On suppose $p > 19$. Soit $j \in \mathbb{F}_p$. Les calculs décrits plus haut montrent en particulier que lorsque l'une des conditions suivantes sur (a,b,c,d,e,f,g,w) est satisfaite, il existe $k,m \in \{2,3,5,6,7\}$ tels que $\iota_j(y_{k,m}) \neq 0$:

1. $(a,b,c,d) \neq (0,0,0,0)$ et $(a,b,c,d,e,f,g,w) \neq (0,0,1,0,0,0,0,0)$;
2. $(a,b,c,d) = (0,0,0,0)$ et $(e,f,g) \neq (0,0,0)$;
3. $(a,b,c,d) = (0,0,0,0)$ et $(e,f,g,w) \neq (0,0,1,1)$;
4. $(a,b,c,d) = (0,0,0,0)$ et $[(e,f,g,w) \neq (0,0,1,0)$ ou $\left(\frac{p}{59}\right)\left(\frac{p}{71}\right) = 1]$;
5. $(a,b,c,d) = (0,0,0,0)$ et $(e,f,g,w) \neq (0,1,0,0)$;
6. $(a,b,c,d) = (0,0,0,0)$ et $[(e,f,g,w) \neq (0,1,0,1)$ ou $\left(\frac{p}{31}\right)\left(\frac{p}{36319}\right)\left(\frac{p}{p_0}\right) = 1]$;
7. $(a,b,c,d) = (0,0,0,0)$ et $(e,f,g,w) \neq (1,0,0,0)$;
8. $(a,b,c,d) = (0,0,0,0)$ et $[(e,f,g,w) \neq (1,0,0,1)$ ou p est un carré modulo $797]$.

Posons $\mathcal{B}$ l'ensemble des nombres premiers $p > 19$ qui sont simultanément un carré modulo $3, 4$ et 7 et qui vérifient l'une des conditions suivantes :

i) p carré modulo $5, 11, 19$, et 23 et non carré modulo 8,

ii) p est un carré modulo $5, 8, 11$ et 19;

iii) p carré modulo $8, 11$ et 19, non carré modulo $5, 23$;

iv) p carré modulo $8, 11, 19, 23, 59, 71$, non carré modulo 5;

v) p carré modulo $8, 11, 19, 23$, non carré modulo $5, 59, 71$;

vi) p carré modulo $5, 8, 11, 23$, non carré modulo 19;

vii) p carré modulo $5, 8, 11$, non carré modulo $19, 23$ et $\left(\frac{p}{31}\right)\left(\frac{p}{36319}\right)\left(\frac{p}{p_0}\right) = 1$;

viii) p carré modulo $5, 8, 19, 23$, non carré modulo 11;

ix) p carré modulo $5, 8, 19, 797$, non carré modulo $11, 23$.

L'ensemble $\mathcal{B}$ est de densité $15/2^8$.

Lemme 6.17
Si $p > 19$ et $p \notin \mathcal{B}$, alors il existe $(k, m) \in \{2, 3, 5, 6, 7\}^2$ tel que $\iota_j(y_{k,m}) \neq 0$.

Démonstration du lemme. — On vérifie que si $p \notin \mathcal{B}$, le 8-uplet (a, b, c, d, e, f, g, w) associé à p vérifie l'une des conditions 1. à 8. ◇

On déduit de ce lemme et de la proposition 6.15, la proposition suivante.

Proposition 6.18
Si $p > 19$ et $p \notin \mathcal{B}$, alors ϕ_P^e est une immersion formelle en tout point P de $X_0(p)_{\mathbb{F}_p}(\mathbb{F}_p)$. En particulier, pour tout $r > 1$, les points de $X_0^+(p^r)$ sont soit des pointes soit des points à multiplication complexe.

L'ensemble $\mathcal{C}$ est égal à $\mathcal{A} \cup \mathcal{B}$. En combinant le théorème 6.13 et la proposition 6.18, on obtient le théorème 6.16.

Bibliographie

[1] H. Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993.

[2] R. F. Coleman. Effective Chabauty. *Duke Math. J.*, 52(3) :765–770, 1985.

[3] C. Cornut. *Réduction de familles de points CM*. PhD thesis, Université de Strasbourg.

[4] J. E. Cremona. Modular symbols for $\Gamma_1(N)$ and elliptic curves with everywhere good reduction. *Math. Proc. Cambridge Philos. Soc.*, 111(2) :199–218, 1992.

[5] 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.

[6] F. Diamond and J. Im. Modular forms and modular curves. In *Seminar on Fermat's Last Theorem (Toronto, ON, 1993–1994)*, volume 17 of *CMS Conf. Proc.*, pages 39–133. Amer. Math. Soc., Providence, RI, 1995.

[7] M. Eichler. Zur Zahlentheorie der Quaternionen-Algebren. *J. Reine Angew. Math.*, 195 :127–151 (1956), 1955.

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

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

[10] 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.

[11] 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.

[12] A. Grothendieck. Éléments de géométrie algébrique. I. Le langage des schémas. *Inst. Hautes Études Sci. Publ. Math.*, (4) :228, 1960.

[13] S. Kamienny. Torsion points on elliptic curves over fields of higher degree. *Internat. Math. Res. Notices*, (6) :129–133, 1992.

[14] K. Kato. p-adic Hodge theory and values of Zeta functions of modular forms. à paraître, Astérisque.

[15] 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.

[16] S. Lang. *Elliptic functions*, volume 112 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1987. With an appendix by J. Tate.

[17] J.-C. Lario and J. Quer. Table of some hecke operator's eigenvalues. Non publiée.

[18] W. Luo and D. Ramakrishnan. Determination of modular forms by twists of critical L-values. *Invent. Math.*, 130(2) :371–398, 1997.

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

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

[21] B. Mazur. Rational isogenies of prime degree (with an appendix by D. Goldfeld). *Invent. Math.*, 44(2) :129–162, 1978.

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

[23] 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.

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

[25] L. Merel. Sur la nature non-cyclotomique des points d'ordre fini des courbes elliptiques. *Duke Math. J.*, 110(1) :81–119, 2001. With an appendix by E. Kowalski and P. Michel.

[26] L. Merel and W. A. Stein. The field generated by the points of small prime order on an elliptic curve. *Internat. Math. Res. Notices*, (20) :1075–1082, 2001.

[27] Loïc 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.

[28] J.-F. Mestre and J. Oesterlé. Courbes elliptiques de conducteur premier.

[29] J. S. Milne. Jacobian varieties. In *Arithmetic geometry (Storrs, Conn., 1984)*, pages 167–212. Springer, New York, 1986.

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

[31] F. Momose. Rational points on the modular curves $X_{\mathrm{split}}(p)$. *Compositio Math.*, 52(1) :115–137, 1984.

[32] F. Momose. Rational points on the modular curves $X_0^+(p^r)$. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, 33(3) :441–466, 1986.

[33] F. Momose. Rational points on the modular curves $X_0^+(N)$. *J. Math. Soc. Japan*, 39(2) :269–286, 1987.

[34] J. Oesterlé. Torsion des courbes elliptiques sur les corps de nombres.

[35] A. P. Ogg. Rational points on certain elliptic modular curves. In *Analytic number theory (Proc. Sympos. Pure Math., Vol XXIV, St. Louis Univ., St. Louis, Mo., 1972)*, pages 221–231. Amer. Math. Soc., Providence, R.I., 1973.

[36] A. P. Ogg. On the Weierstrass points of $X_0(N)$. *Illinois J. Math.*, (29) :31–35, 1978.

[37] P. Parent. Towards the triviality of $X_0^+(p^r)(\mathbf{q})$ for $r > 1$. *Compositio Math.* à paraître.

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

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

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

[41] 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).

[42] M. Rebolledo Hochart. Corps engendré par les points de 13-torsion des courbes elliptiques. *Acta Arith.*, 109(3) :219–230, 2003.

[43] K. Ribet. Endomorphisms of semi-stable abelian varieties over number fields. *Ann. of Math.*, 101 :555–562, 1975.

[44] D. E. Rohrlich. Modular curves, Hecke correspondence, and L-functions. In *Modular forms and Fermat's last theorem (Boston, MA, 1995)*, pages 41–100. Springer, New York, 1997.

[45] J.-P. Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4) :259–331, 1972.

[46] Jean-Pierre Serre. *Œuvres. Vol. III.* Springer-Verlag, Berlin, 1986. 1972–1984.

[47] J. Tilouine. Hecke algebras and the Gorenstein property. In *Modular forms and Fermat's last theorem (Boston, MA, 1995)*, pages 327–342. Springer, New York, 1997.

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

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

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

Index

Résumé

Nous étudions ici le groupe libre engendré par les classes d'isomorphisme de courbes elliptiques supersingulières en caractéristique p, appelé *module supersingulier*. Nous le comparons à d'autres modules de Hecke : l'homologie de la courbe modulaire $X_0(p)$ et l'ensemble des formes modulaires de poids 2 et de niveau p. Nous donnons des interprétations et des applications des formules de Gross et Gross-Kudla concernant les fonctions L de formes modulaires. Les liens entre le module supersingulier et la géométrie de $X_0(p)$ nous permettent d'appliquer ces résultats à l'étude des points rationnels de certaines courbes modulaires. Reprenant une méthode de Momose et Parent, nous déterminons notamment un ensemble infini de nombres premiers p pour lesquels le quotient de $X_0(p^r)$ $(r > 1)$ par l'opérateur d'Atkin-Lehner n'a pour points rationnels que les pointes et les points CM.

Mots clefs.— courbes elliptiques, courbes modulaires, formes modulaires, fonctions L, module supersingulier, variétés abéliennes, symboles modulaires.

Abstract

We study here the free group generated by isomorphism classes of supersingular elliptic curves in positive characteristic p, called the *supersingular module*. We compare it with others Hecke modules : the homology of modular curve $X_0(p)$ and the set of modular forms of weight 2 and level p. We give several interpretations and applications of Gross and Gross-Kudla's formulas about L-functions of modular forms. Using the links between supersingular module and geometry of $X_0(p)$ we apply these results in order to study the rational points on certain modular curves. Following the method of Momose and Parent, we determinate an infinite set of primes p for which the quotient of $X_0(p^r)$ $(r > 1)$ by the Atkin-Lehner operator has no rational points other than cups and CM points.

Keywords.— abelian varieties, elliptic curves, modular curves, modular forms, modular symbols, L-functions, supersingular module.