L'accouplement de Weil entre le sous-groupe de Shimura et le sous-groupe cuspidal de $J_0(p)$

Loïc Merel à Paris

Introduction

Soit p un nombre premier ≥ 5. Posons

$$\Gamma_0(p) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z})/p|c\}$$

et

$$\Gamma_1(p) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z})/p|c, p|(d-1)\}.$$

Ces groupes opèrent par homographies sur le demi-plan de Poincaré $\mathfrak{H}$. Notons $Y_0(p)$ et $Y_1(p)$ les surfaces de Riemann quotients $\Gamma_0(p)\backslash\mathfrak{H}$ et $\Gamma_1(p)\backslash\mathfrak{H}$, $X_0(p)$ et $X_1(p)$ leurs compactifiées respectives et *ptes* l'ensemble $\Gamma_0(p)\backslash\mathbf{P}^1(\mathbf{Q}) = \{\Gamma_0(p)0, \Gamma_0(p)\infty\}$ des pointes de $X_0(p)$. Notons $J_0(p)$ et $J_1(p)$ les variétés jacobiennes (vues comme composantes neutres des groupes de Picard) de $X_0(p)$ et $X_1(p)$. Le morphisme analytique de surfaces de Riemann

$$\begin{array}{ll} X_1(p) & \to X_0(p) \\ \Gamma_1(p)z & \mapsto \Gamma_0(p)z \end{array}$$

définit par fonctorialité de Picard un homomorphisme de variétés abéliennes

$$J_0(p) \to J_1(p).$$

Le noyau de cet homomorphisme est par définition le *sous-groupe de Shimura* $\Sigma(p)$ de $J_0(p)$.

Posons $\nu = \mathrm{pgcd}(p-1, 12)$ et $n = \frac{p-1}{\nu}$. Notons U le groupe des puissances ν-ièmes dans $(\mathbf{Z}/p\mathbf{Z})^*$. On définit un isomorphisme canonique de groupes ([7], proposition II.11.6, voir également [5] et section 3.3)

$$\beta_\Sigma \ : \ \mathrm{Hom}(U, \mu_n) \to \Sigma(p)$$

où μ_n désigne le groupe des racines n-ièmes de l'unité dans $\mathbf{C}$. Le sous-groupe de Shimura est donc un groupe cyclique d'ordre n.

Considérons le *sous-groupe cuspidal* $C(p)$ de la jacobienne $J_0(p)$, vue comme variété d'Albanese de $X_0(p)$: c'est le sous-groupe engendré par les classes des diviseurs de degré 0 à support dans les pointes de $X_0(p)$. C'est un groupe cyclique d'ordre n ([7], proposition II.11.1), engendré par la classe du diviseur $(\Gamma_0(p)0) - (\Gamma_0(p)\infty)$. Les accouplements de Weil sur les points de n-torsion de $J_0(p)$ induisent un accouplement bilinéaire

$$C(p) \times \Sigma(p) \to \mu_n.$$

Par bidualité l'isomorphisme β_Σ permet donc de définir un homomorphisme de groupes

$$C(p) \to U.$$

Mazur dans [7] (section II.11) a posé la question suivante : quelle est l'image u du générateur canonique $(\Gamma_0(p)0) - (\Gamma_0(p)\infty)$ de $C(p)$ dans U par cet homomorphisme ? Mazur a signalé ne savoir calculer u dans aucun cas non trivial. Nous donnons dans le théorème 1 ci-dessous une formule permettant de le calculer dans tous les cas. On définit dans la section 4.1 une racine carrée canonique de u dans U notée $\sqrt{u}$.

Théorème 1 *On a dans* $\mathbf{Z}/p\mathbf{Z}$

$$\sqrt{u} = \epsilon\zeta \prod_{l=1}^{\frac{p-1}{2}} l^{-4l}$$

où ϵ *est égal à* -1 *si* $p \in (1+8\mathbf{Z})$*, à* 1 *si* $p \notin (1+8\mathbf{Z})$*, et où* ζ *est la racine cubique de l'unité égale à* 1 *si* $p \notin (1+3\mathbf{Z})$*, et à* $2^{\frac{p-1}{3}}$ *si* $p \in (1+3\mathbf{Z})$*.*

Notons $\mathbf{T}$ *l'algèbre de Hecke* de $J_0(p)$, c'est-à-dire la sous-algèbre de $\mathrm{End}(J_0(p))$ engendrée par l'involution d'Atkin-Lehner W_p et les opérateurs de Hecke T_l, pour l nombre premier $\neq p$ (voir section 5.1). Elle est égale à $\mathrm{End}(J_0(p))$ ([7], proposition II.9.5). Notons $\mathfrak{I}$ *l'idéal d'Eisenstein* de $\mathbf{T}$, i.e. l'idéal engendré par les éléments $1 + W_p$ et $1 + l - T_l$, pour l nombre premier $\neq p$. L'application canonique $\mathbf{Z} \to \mathbf{T}/\mathfrak{I}$ est surjective, de noyau $n\mathbf{Z}$ ([7], proposition II.9.7). Mazur définit un homorphisme surjectif de groupes $\mathfrak{I} \to U$ de noyau $\mathfrak{I}^2$, prenant la valeur $l^{-\nu\frac{l-1}{2}}$ en $1 + l - T_l$, pour l nombre premier différent de 2 et p, la valeur $(-1)^{\frac{p^2-1}{8}} 2^{-\frac{\nu}{2}}$ en $3 - T_2$ et la valeur 1 en $1 + W_p$

(voir [7], section II.18 et la section 5.1 du présent texte). L'image de n par cet homomorphisme est égale à $\sqrt{u}$ (section 5.1).

Si q est un nombre premier divisant n, $q\mathbf{T} + \mathfrak{I}$ est un idéal maximal de $\mathbf{T}$. L'intérêt de l'invariant $\sqrt{u}$ provient du théorème suivant généralisant la proposition II.19.2 de [7].

Théorème 2 *Soit q un nombre premier divisant n. Posons $\mathfrak{q} = q\mathbf{T} + \mathfrak{I}$. Le complété $\mathfrak{q}$-adique $\mathbf{T}_{\mathfrak{q}}$ de $\mathbf{T}$ est isomorphe à $\mathbf{Z}_q$ si et seulement si $\sqrt{u}$ engendre la composante q-primaire de U, ou encore, lorsque $q > 3$, si et seulement si $\prod_{l=1}^{\frac{p-1}{2}} l^l$ n'est pas une puissance q-ième de $\mathbf{Z}/p\mathbf{Z}$.*

On déduit du théorème 2 des critères dont voici des exemples.

Corollaire 1 *Supposons que 3 divise n, i.e. $p \in (1 + 9\mathbf{Z})$. Alors $\mathbf{T}_{3\mathbf{T}+\mathfrak{I}}$ est isomorphe à $\mathbf{Z}_3$ si et seulement si $(\frac{p-1}{3})!$ n'est pas un cube modulo p.*

Supposons que 5 divise n, i.e. $p \in (1 + 5\mathbf{Z})$. Alors $\mathbf{T}_{5\mathbf{T}+\mathfrak{I}}$ est isomorphe à $\mathbf{Z}_5$ si et seulement si $(2\frac{p-1}{5})!\,/(\frac{p-1}{5})!^2$ n'est pas une puissance cinquième modulo p.

On a des critères analogues pour tout nombre premier impair divisant n, voir section 5.2.

Théorème 3 *Supposons que n soit pair, i.e. $p \in (1 + 8\mathbf{Z})$. Alors les conditions suivantes sont équivalentes :*

ı) L'anneau $\mathbf{T}_{2\mathbf{T}+\mathfrak{I}}$ n'est pas isomorphe à $\mathbf{Z}_2$.

ıı) Ou bien $p \in (1 + 16\mathbf{Z})$ et $(\frac{p-1}{4})!$ est un carré modulo p, ou bien $p \in (9 + 16\mathbf{Z})$ et $(\frac{p-1}{4})!$ n'est pas un carré modulo p.

ıı) Le nombre de classes de $\mathbf{Q}(\sqrt{-p})$ est divisible par 8.

ıv) Le nombre p s'écrit sous la forme $x^2 + 32y^2$, avec $(x, y) \in \mathbf{Z}^2$.

v) Le nombre p s'écrit sous la forme $x^2 + 16y^2$, avec $(x, y) \in \mathbf{Z}^2$ et $y \equiv \frac{p-1}{8} \pmod 2$.

vı) Le nombre p s'écrit sous la forme $x^2 - 32y^2$, avec $(x, y) \in \mathbf{Z}^2$ et $|x| \equiv 1 \pmod 4$.

vıı) L'entier -4 est une puissance 8-ième modulo p.

L'équivalence des conditions *ıı)*, *ıv)*, *v)*, *vı)* et *vıı)* est tirée de [1] et [4]. Remarquons que, lorsque $p \in (1 + 8\mathbf{Z})$, le nombre de classes de $\mathbf{Q}(\sqrt{-p})$ est égal au nombre de points de $X_0(p)$ fixés par l'involution W_p ([7], section III.2). Cette observation permet-elle d'obtenir une démonstration directe du théorème 3 ?

Notons comme d'habitude Δ la fonction de Ramanujan. La fonction qui à $z \in \mathfrak{H}$ associe $\Delta(pz)/\Delta(z)$ est modulaire pour $\Gamma_0(p)$. Elle définit par passage aux quotients une fonction rationnelle λ_p sur $X_0(p)$ de diviseur $(p-1)((\Gamma_0(p)\infty)-(\Gamma_0(p)0))$. Sa différentielle logarithmique est holomorphe sur $Y_0(p)$. L'intégrale de cette forme différentielle, divisée par $2\pi i$, le long des cycles de $Y_0(p)$ fournit un homomorphisme de groupes :

$$\bar{\phi}_p \ : \ \mathrm{H}_1(Y_0(p);\mathbf{Z}) \to \mathbf{Z}.$$

Comme le produit d'intersection, noté $\bullet$,

$$\mathrm{H}_1(X_0(p), ptes;\mathbf{Z}) \times \mathrm{H}_1(Y_0(p);\mathbf{Z}) \to \mathbf{Z}$$

est unimodulaire, il existe un unique élément $\mathcal{E} \in \mathrm{H}_1(X_0(p), ptes;\mathbf{Z})$ tel que

$$\bar{\phi}_p(c) = \mathcal{E} \bullet c$$

pour tout $c \in \mathrm{H}_1(Y_0(p);\mathbf{Z})$. Appelons $\mathcal{E}$ l'*élément d'Eisenstein.* Cet élément $\mathcal{E}$ peut aussi être décrit comme l'image, par l'homomorphisme de groupes

$$\lambda_p^* \ : \ \mathrm{H}_1(\mathbf{P}^1(\mathbf{C}), \{0,\infty\};\mathbf{Z}) \to \mathrm{H}_1(X_0(p), ptes;\mathbf{Z})$$

de la classe d'un chemin reliant 0 à ∞ dans $\mathbf{P}^1(\mathbf{C})$ (voir section 2.3). Son bord est égal à $(p-1)((\Gamma_0(p)0)-(\Gamma_0(p)\infty))$ (proposition 9).

Pour $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z})$, le symbole modulaire $\{g0, g\infty\} = \{\frac{b}{d}, \frac{a}{c}\}$ (i.e. la classe dans le groupe d'homologie singulière $\mathrm{H}_1(X_0(p), ptes;\mathbf{Z})$ de l'image dans $X_0(p)$ d'un chemin de $\tilde{\mathfrak{H}}$ reliant $\frac{b}{d}$ à $\frac{a}{c}$) ne dépend que de la classe de g dans $\Gamma_0(p)\backslash SL_2(\mathbf{Z})$, i.e. de l'élément (c,d) de $\mathbf{P}^1(\mathbf{Z}/p\mathbf{Z})$ [6]. Notons-le $\xi(c,d)$.

Théorème 4 *On a*

$$\mathcal{E} = -\sum_{l=1}^{\frac{p-1}{2}} \sum_{h=1}^{\frac{p-1}{2}} \xi(l-h, l+h) + \sum_{l=\frac{p+1}{2}}^{p-1} \sum_{h=1}^{\frac{p-1}{2}} \xi(l-h, l+h).$$

L'intégrale de toute forme différentielle holomorphe sur $X_0(p)$ le long des cycles de classe $\mathcal{E}$ est nulle. De plus $\mathcal{E}$ est l'unique élément de $H_1(X_0(p), ptes;\mathbf{Z})$, à multiplication par un scalaire près, possédant cette propriété.

Le théorème 4 peut être compris comme une version explicite du théorème de Manin-Drinfeld ([3]). On peut encore caractériser l'élément d'Eisenstein, à multiplication par un scalaire près, par le fait qu'il est vecteur propre pour les opérateurs de Hecke T_l avec la valeur propre $1+l$ (l nombre premier $\neq p$). Mais nous n'utiliserons pas les opérateurs de Hecke pour prouver le théorème 4.

Pour prouver le théorème 4, il faut rendre explicite le procédé permettant de passer de $\bar{\phi}_p$ à $\mathcal{E}$. Malheureusement nous ne sommes pas parvenu à accomplir ce programme en restant en niveau p. Nous reposons le problème de l'élément d'Eisenstein dans le contexte du groupe $\Gamma(2) \cap \Gamma_0(p)$ et de la courbe modulaire $X_0(2p, 2)$ associée. Nous nous appuyons alors sur une description de l'homologie de $X_0(2p, 2)$ développée dans la première partie. Signalons que nos méthodes (en particulier le passage d'un groupe Γ à $\Gamma \cap \Gamma(2)$) devraient s'appliquer pour déterminer les éléments d'Eisenstein dans d'autres situations (niveau non premier, poids > 2).

Cet article est divisé en cinq parties. Les résultats de la première partie sont essentiellement de nature topologique. Ils concernent notamment les produits d'intersection pour les courbes modulaires associées aux sous-groupes d'indice fini de $\Gamma(2)$; ces résultats présentent un intérêt indépendamment des autres considérations de cet article. Nous prouvons le théorème 4 dans la deuxième partie. La troisième partie est consacrée à traduire en termes purement algébriques, via la structure complexe des courbes modulaires, la définition géométrique de u. Le théorème 1 apparaît alors comme un corollaire du théorème 4 et est prouvé dans la quatrième partie. La cinquième partie est consacrée à explorer les conséquences des théorèmes 1 et 2 pour l'étude de l'idéal d'Eisenstein.

Nous concluons en donnant le représentant de $\sqrt{u}$ dans $\{0, 1, ..., p-1\}$ pour tout niveau premier $p \leq 250$ et l'indice dans U du sous-groupe engendré par $\sqrt{u}$.

Signalons que nous avons obtenu par des méthodes différentes, reposant sur les opérateurs de Hecke, une généralisation du théorème 4 aux sous-groupes de congruence $\Gamma(N)$ pour N impair.

Je voudrais remercier chaleureusement Joseph Oesterlé, mon directeur de thèse, pour le travail considérable qu'il a accompli en m'aidant à rédiger cet article : d'abord il m'a signalé le lien entre l'invariant de Mazur et l'élément d'Eisenstein et a attiré mon attention sur l'intérêt du groupe $\Gamma(2)$. Certaines

parties de ce texte lui sont largement dues (mentionnons les sections 1.2, 1.3, 3.1 et le lemme 22) ; le reste de l'article a partout bénéficié de ses clarifications et de ses corrections.

1 Résultats topologiques

1.1 Produits d'intersection et sous-groupes de $\Gamma(2)$

Notons $\Gamma(2)$ l'ensemble des matrices de $SL_2(\mathbf{Z})$ congrues à l'identité modulo 2. Soit Γ un sous groupe d'indice fini de $\Gamma(2)$ contenant $-\mathrm{Id}$. Notons Y_Γ la surface de Riemann quotient $\Gamma\backslash\mathfrak{H}$, X_Γ sa compactifieée. Notons π^Γ la surjection canonique

$$\bar{\mathfrak{H}} = \mathfrak{H} \cup \mathbf{P}^1(\mathbf{Q}) \to X_\Gamma.$$

La courbe modulaire $X(2) = X_{\Gamma(2)}$ possède trois pointes : $\Gamma(2)0$, $\Gamma(2)1 = \Gamma(2)(-1)$ et $\Gamma(2)\infty$. Notons P_- (resp. P_+) l'ensemble des pointes de X_Γ dont l'image par le morphisme $\Gamma z \mapsto \Gamma(2)z$ de X_Γ dans $X(2)$ est égale à $\Gamma(2)1$ (resp. à $\Gamma(2)0$ ou à $\Gamma(2)\infty$). Nous allons étudier dans cette section les deux groupes d'homologie relative $\mathrm{H}_1(X_\Gamma - P_-, P_+; \mathbf{Z})$ et $\mathrm{H}_1(X_\Gamma - P_+, P_-; \mathbf{Z})$. Les produits d'intersection définissent un accouplement unimodulaire noté $\bullet$:

$$\mathrm{H}_1(X_\Gamma - P_-, P_+; \mathbf{Z}) \times \mathrm{H}_1(X_\Gamma - P_+, P_-; \mathbf{Z}) \to \mathbf{Z}.$$

Pour $g \in \Gamma(2)$, notons $[g]^0$ (resp. $[g]_0$) la classe dans $\mathrm{H}_1(X_\Gamma - P_-, P_+; \mathbf{Z})$ (resp. $\mathrm{H}_1(X_\Gamma - P_+, P_-; \mathbf{Z})$) de l'image par π^Γ du chemin géodésique reliant $g0$ à $g\infty$ (resp. $g1$ à $g(-1)$). Ces éléments ne dépendent que de la classe Γg de g dans $\Gamma\backslash\Gamma(2)$. Le but de cette section est de prouver les deux théorèmes suivants.

Théorème 5 *Les homomorphismes de groupes*

$$\mathbf{Z}^{(\Gamma\backslash\Gamma(2))} \to H_1(X_\Gamma - P_-, P_+; \mathbf{Z}) \quad \textit{et} \quad \mathbf{Z}^{(\Gamma\backslash\Gamma(2))} \to H_1(X_\Gamma - P_+, P_-; \mathbf{Z})$$

prolongeant les applications qui à Γg associent $[g]^0$ et $[g]_0$ respectivement sont des isomorphismes.

Théorème 6 *Soit g et h deux éléments de $\Gamma(2)$. Le produit d'intersection de l'élément $[g]^0$ de $H_1(X_\Gamma - P_-, P_+; \mathbf{Z})$ et de l'élément $[h]_0$ de $H_1(X_\Gamma - P_+, P_-; \mathbf{Z})$ est donné par la formule*

$$\begin{array}{ll} [g]^0 \bullet [h]_0 = 1 & \textit{si} \quad \Gamma g = \Gamma h \\ [g]^0 \bullet [h]_0 = 0 & \textit{sinon.} \end{array}$$

Démonstration.- Prouvons d'abord le lemme suivant.

Lemme 1 *Le groupe d'homologie* $H_1(X_\Gamma - P_-, P_+; \mathbf{Z})$ *est engendré par* $\{[g]^0 / g \in \Gamma(2)\}$.

Démonstration.- Ce groupe est l'image de l'homomorphisme de groupes

$$\pi_*^\Gamma \ : \ \mathrm{H}_1(\bar{\mathfrak{H}} - \Gamma(2)1, \Gamma(2)\{0, \infty\}; \mathbf{Z}) \to \mathrm{H}_1(X_\Gamma - P_-, P_+; \mathbf{Z}),$$

déduit fonctoriellement de π^Γ. Il suffit donc de prouver que cette image est engendrée par les classes des chemins géodésiques reliant $g0$ à $g\infty$ ($g \in \Gamma(2)$). Le quadrilatère hyperbolique Q_0de sommets 0, 1, ∞, -1 dans $\bar{\mathfrak{H}}$ est un domaine fondamental pour le groupe $\Gamma(2)/\{\pm \mathrm{Id}\}$. Pour g parcourant $\Gamma(2)$, les quadrilatères hyperboliques gQ_0 constituent un pavage connexe par bords de $\mathfrak{H}$. Notons γ_0 le chemin géodésique de $\bar{\mathfrak{H}}$ reliant 0 à ∞. Pour $g \in \Gamma(2)$, le chemin $g\gamma_0$ relie $g0$ à $g\infty$. Les extrémités de $g\gamma_0$ sont les seuls points de gQ_0 appartenant à $\Gamma(2)0 \cup \Gamma(2)\infty$. Comme $\mathfrak{H}$ est simplement connexe on en déduit que $\mathrm{H}_1(\bar{\mathfrak{H}} - \Gamma(2)1, \Gamma(2)\{0, \infty\}; \mathbf{Z})$ est engendré par les classes des chemins $g\gamma_0$ ($g \in \Gamma(2)$).

Prouvons maintenant le théorème 6.

Notons δ_0 le chemin géodésique de $\bar{\mathfrak{H}}$ reliant 1 à -1. Le chemin $h\delta_0$ est à support dans hQ_0. Les chemins $\pi^\Gamma(g\gamma_0)$ et $\pi^\Gamma(h\delta_0)$ n'ont donc pas de point d'intersection si $\Gamma g \neq \Gamma h$. On a alors

$$[g]^0 \bullet [h]_0 = 0.$$

Si $\Gamma g = \Gamma h$, on constate que les chemins $\pi^\Gamma(g\gamma_0)$ et $\pi^\Gamma(h\delta_0)$ ont un unique point d'intersection (c'est $\pi^\Gamma(gi)$) en lequel ils se coupent transversalement avec pour nombre d'intersection $+1$. On a donc

$$[g]^0 \bullet [h]_0 = 1.$$

Prouvons maintenant le théorème 5.

Le lemme 1 établit que l'application $\mathbf{Z}$-linéaire $\mathbf{Z}^{(\Gamma \backslash \Gamma(2))} \to \mathrm{H}_1(X_\Gamma - P_-, P_+; \mathbf{Z})$ prolongeant l'application $\Gamma g \mapsto [g]^0$ est surjective. Le théorème 6 nous assure que cette application est injective et donc que c'est un isomorphisme de groupes. Le second isomorphisme du théorème 5 résulte alors du théorème 6 et de l'unimodularité de l' accouplement

$$\mathrm{H}_1(X_\Gamma - P_-, P_+; \mathbf{Z}) \times \mathrm{H}_1(X_\Gamma - P_+, P_-; \mathbf{Z}) \to \mathbf{Z}.$$

1.2 La correspondance κ_p

Posons $\Gamma_0(2p,2) = \Gamma_0(p) \cap \Gamma(2)$ et $X_0(2p,2) = X_{\Gamma_0(2p,2)}$. Avec les notations de la section précédente, les ensembles de pointes P_- et P_+ de la courbe modulaire $X_0(2p,2)$ sont

$$P_- = \{\Gamma_0(2p,2)1, \Gamma_0(2p,2)\frac{1}{p}\}$$

et

$$P_+ = \{\Gamma_0(2p,2)0, \Gamma_0(2p,2)\infty, \Gamma_0(2p,2)\frac{1}{2}, \Gamma_0(2p,2)\frac{2}{p}\}.$$

Proposition 1 *Soit f une fonction rationnelle non nulle sur $X_0(p)$. Notons $\pi : X_0(2p,2) \to X_0(p)$ et $\pi' : X_0(2p,2) \to X_0(p)$ les morphismes $\Gamma_0(2p,2)z \mapsto \Gamma_0(p)z$ et $\Gamma_0(2p,2)z \mapsto \Gamma_0(p)\frac{z+1}{2}$. La fonction rationnelle $f_0 = (f \circ \pi)^2/(f \circ \pi')$ n'a ni zéro ni pôle dans P_-.*

Démonstration.- Les fonctions qui à z associent $e^{-\frac{2\pi i}{pz}}$, $e^{2\pi i z}$, $e^{-\frac{2\pi i}{2p(z-1)}}$, $e^{\frac{2\pi i z}{2(-pz+1)}}$ sur $\bar{\mathfrak{H}}$ définissent par passage aux quotients lorsque z tend vers 0, ∞, 1, $\frac{1}{p}$ des uniformisantes locales q_0, q_∞, q_1, $q_{\frac{1}{p}}$ sur $X_0(p)$, $X_0(p)$, $X_0(2p,2)$, $X_0(2p,2)$ au voisinage de $\Gamma_0(p)0$, $\Gamma_0(p)\infty$, $\Gamma_0(2p,2)1$, $\Gamma_0(2p,2)\infty$ respectivement. La proposition se déduit des relations

$$q_0 \circ \pi = q_1^2 \quad \text{et} \quad q_0 \circ \pi' = q_1^4$$

au voisinage de $\Gamma_0(2p,2)1$, et

$$q_\infty \circ \pi = q_{\frac{1}{p}}^2 \quad \text{et} \quad q_\infty \circ \pi' = q_{\frac{1}{p}}^4$$

au voisinage de $\Gamma_0(2p,2)\frac{1}{p}$. Ces relations s'obtiennent par des calculs fastidieux dont voici un exemple pour prouver la dernière égalité. Lorsque z tend vers $\frac{1}{p}$ on a

$$\begin{aligned}
q_\infty(\pi'(\Gamma_0(2p,2)z)) &= q_\infty(\Gamma_0(p)\frac{z+1}{2}) \\
&= q_\infty(\Gamma_0(p)\begin{pmatrix} 2 & -1 \\ -p & \frac{p+1}{2} \end{pmatrix}\frac{z+1}{2}) \\
&= q_\infty(\Gamma_0(p)\frac{2z}{-pz+1}) \\
&= e^{2\pi i \frac{2z}{-pz+1}} \\
&= q_{\frac{1}{p}}^4(\Gamma_0(2p,2)z).
\end{aligned}$$

Corollaire 2 *Notons κ_p la correspondance de $X_0(2p,2)$ dans $X_0(p)$ qui à $\Gamma_0(2p,2)z$ associe $2\pi(\Gamma_0(2p,2)z) - \pi'(\Gamma_0(2p,2)z)$. Les images réciproques par κ_p des diviseurs $(\Gamma_0(p)0)$ et $(\Gamma_0(p)\infty)$ sont à support dans P_+.*

1.3 L'action de la conjugaison complexe sur l'homologie de $X_0(p)$

L'involution $z \mapsto -\bar{z}$ de $\bar{\mathfrak{H}}$ définit par passage aux quotients une involution sur $X_0(p)$: c'est la conjugaison complexe. Cette dernière laisse stable l'ensemble des pointes et définit fonctoriellement une involution sur les groupes d'homologie $\mathrm{H}_1(X_0(p), ptes; \mathbf{Z})$ et $\mathrm{H}_1(X_0(p); \mathbf{Z})$. On notera cette involution par une barre horizontale et on l'appellera encore conjugaison complexe. Son action sur les symboles modulaires est donnée par la formule

$$\overline{\{a, \beta\}} = \{-\alpha, -\beta\}.$$

Nous allons examiner la structure du groupe $\mathrm{H}_1(X_0(p); \mathbf{Z})$, en particulier vis-à-vis de l'action de la conjugaison complexe. Rappelons quelques résultats de cohomologie des groupes cycliques (voir [14], chapitre VIII).

Soit G un groupe à deux éléments. La donnée d'un $\mathbf{Z}[G]$-module équivaut à celle d'un groupe commutatif M muni d'une involution $\mathbf{Z}$-linéaire ι (celle suivant laquelle l'élément non neutre de G opère sur M). Notons M_+ (resp. M_-) l'ensemble des éléments invariants (resp. antiinvariants) par ι. Les groupes de cohomologie $\mathrm{H}^m(G, M)$, pour $m \geq 1$, sont isomorphes à $M_+/(1+\iota)M$ pour m pair et à $M_-/(1-\iota)M$ pour m impair. On dira que M est *acyclique* relativement à ι si ces groupes sont nuls, i.e. si l'on a

$$M_+ = (1+\iota)M \quad \text{et} \quad M_- = (1-\iota)M.$$

Tel est le cas par exemple lorsque M est libre en tant que $\mathbf{Z}[G]$-module, i.e. lorsque M possède une base sur $\mathbf{Z}$ permutée sans point fixe par ι. Si $0 \to M' \to M \to M'' \to 0$ est une suite exacte de $\mathbf{Z}[G]$-modules et si deux de ces modules sont acycliques, le troisième est acyclique. En particulier, si M est acyclique et sans torsion sur $\mathbf{Z}$, M/mM est acyclique pour tout entier $m \in \mathbf{N}$.

On identifie $\mathbf{Z}/p\mathbf{Z}$ à un sous-ensemble de $\mathbf{P}^1(\mathbf{Z}/p\mathbf{Z})$ par l'application $k \mapsto (k, 1)$. Notons ∞ l'élément $(1, 0)$ de $\mathbf{P}^1(\mathbf{Z}/p\mathbf{Z})$. Notons M le sous-groupe de $\mathbf{Z}^{(\mathbf{P}^1(\mathbf{Z}/p\mathbf{Z}))}$ formé des éléments à support dans $\mathbf{P}^1(\mathbf{Z}/p\mathbf{Z}) - \{0, 1, -1, \infty\}$.

Proposition 2 *L'homomorphisme de groupes*

$$\xi \ : \ \mathbf{Z}^{(\mathbf{P}^1(\mathbf{Z}/p\mathbf{Z}))} \to H_1(X_0(p), ptes; \mathbf{Z})$$

prolongeant l'application ξ de $\mathbf{P}^1(\mathbf{Z}/p\mathbf{Z})$ dans $H_1(X_0(p), ptes; \mathbf{Z})$ considérée dans l'introduction induit un homomorphisme de groupes

$$\xi' \ : \ M \to H_1(X_0(p); \mathbf{Z}),$$

lorsqu'on identifie $H_1(X_0(p); \mathbf{Z})$ à un sous-groupe de $H_1(X_0(p), ptes; \mathbf{Z})$.

Démonstration.- Les images par ξ des éléments de $(\mathbf{Z}/p\mathbf{Z})^*$ sont de bord nul. En effet, pour $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z})$ tel que $c \notin p\mathbf{Z}$ et $d \notin p\mathbf{Z}$, on a $\Gamma_0(p)\frac{a}{c} = \Gamma_0(p)0 = \Gamma_0(p)\frac{b}{d}$. Cela prouve la proposition.

Faisons opérer $GL_2(\mathbf{Z})$ à droite sur $\mathbf{Z}^{(\mathbf{P}^1(\mathbf{Z}/p\mathbf{Z}))}$ par

$$(\sum \lambda_x[x]) \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \sum \lambda_x [\frac{ax+c}{bx+d}].$$

Posons $\sigma = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $\tau = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$. On a $a = a\sigma^2 = a\tau^3$, pour tout $a \in \mathbf{Z}^{(\mathbf{P}^1(\mathbf{Z}/p\mathbf{Z}))}$.

Proposition 3 *L'homomorphisme ξ' est surjectif. Son noyau est somme directe des sous-groupes M_σ et M_τ de M fixés par σ et τ respectivement.*

Démonstration.- Le diagramme

$$\begin{array}{ccc} M & \xrightarrow{\xi'} & \mathrm{H}_1(X_0(p); \mathbf{Z}) \\ \downarrow & & \downarrow \\ \mathbf{Z}^{(\mathbf{P}^1(\mathbf{Z}/p\mathbf{Z}))} & \xrightarrow{\xi} & \mathrm{H}_1(X_0(p), ptes; \mathbf{Z}), \end{array}$$

où les flèches verticales sont les injections canoniques est commutatif. D'après un théorème de Manin ([6], théorème 1.9), l'homomorphisme ξ est surjectif et son noyau est engendré par les éléments de $\mathbf{Z}^{(\mathbf{P}^1(\mathbf{Z}/p\mathbf{Z}))}$ invariants par σ ou τ. Si $\sum_{x \in (\mathbf{P}^1(\mathbf{Z}/p\mathbf{Z}))} \lambda_x[x]$ a pour image par ξ un élément de $\mathrm{H}_1(X_0(p); \mathbf{Z})$, on a $\lambda_0 = \lambda_\infty$, et comme $\xi([0] + [\infty]) = 0$ (car $[0]\sigma = [\infty]$), on a $\xi(\sum \lambda_x[x]) = \xi(\sum_{x \neq 0,\infty} \lambda_x[x])$. Comme on a $[\infty]\tau^2 = [0]\tau = [-1]$ et $[-1]\sigma = [1]$, on a $\xi([1]) = \xi([-1]) = 0$. On en déduit l'égalité $\xi(\sum \lambda_x[x]) = \xi'(\sum_{x \neq 0,\infty,1,-1} \lambda_x[x])$. Cela prouve que ξ' est surjectif.

Soit a un élément du noyau de ξ'. D'après le théorème de Manin mentionné ci-dessus, a est dans $\mathbf{Z}^{(\mathbf{P}^1(\mathbf{Z}/p\mathbf{Z}))}$ somme d'un élément a' invariant par σ et d'un élément a'' invariant par τ. Quitte à retrancher à a' un multiple de $\sum_{x\in(\mathbf{P}^1(\mathbf{Z}/p\mathbf{Z}))}[x]$, et à ajouter ce multiple à a'', on peut supposer que a' est à support dans $\mathbf{Z}/p\mathbf{Z}$, donc a'' aussi. Puisque $[\infty]\tau = [0]$ et $[0]\tau = [-1]$, on a $a''_0 = a''_{-1} = 0$ et donc $a'_0 = a'_{-1} = 0$. Comme on a $[-1]\sigma = [1]$, on a $a'_1 = 0$ et donc $a''_1 = 0$. Par conséquent a' appartient à M_σ et a'' à M_τ. On en déduit que le noyau de ξ' est contenu dans $M_\sigma + M_\tau$. L'inclusion inverse résulte du théorème de Manin mentionné ci-dessus. La somme $M_\sigma + M_\tau$ est directe puisqu'aucun élément de non nul de M n'est invariant simultanément par σ et τ. Cela prouve les assertions relatives au noyau de ξ'.

Notons ι l'involution $\sum_x \lambda_x[x] \mapsto \sum_x \lambda_x[\frac{1}{x}]$ de $\mathbf{Z}^{(\mathbf{P}^1(\mathbf{Z}/p\mathbf{Z}))}$. Le sous-groupe M de $\mathbf{Z}^{(\mathbf{P}^1(\mathbf{Z}/p\mathbf{Z}))}$ est stable par ι.

Proposition 4 *Le groupe M muni de l'involution induite par ι est acyclique.*

Démonstration.- Cela résulte de ce que M est un $\mathbf{Z}$-module libre admettant pour base $\mathbf{P}^1(\mathbf{Z}/p\mathbf{Z}) - \{0, 1, -1, \infty\}$ et que ι permute sans point fixe les éléments de cette base.

Lemme 2 *Les sous-groupes M_σ et M_τ de M sont stables par ι. Munis des involutions induites par ι ils sont acycliques.*

Démonstration.- La première assertion résulte des égalités

$$\iota(a)\sigma = \iota(a\sigma) \quad \text{et} \quad \iota(a\tau) = \iota(a)\tau^2 \quad (a \in \mathbf{Z}^{(\mathbf{P}^1(\mathbf{Z}/p\mathbf{Z}))}).$$

Le groupe M_σ (resp. M_τ) est libre sur $\mathbf{Z}$ et admet pour base les éléments de la forme $\sum_{x\in\Omega}[x]$, où Ω est une orbite de σ (resp. de τ) dans $\mathbf{P}^1(\mathbf{Z}/p\mathbf{Z})$ ne rencontrant pas $\{0, 1, -1, \infty\}$. L'involution ι permute ces éléments. Pour prouver la deuxième assertion du lemme il suffit de prouver qu'aucun d'eux n'est fixé par ι. Si $\sum_{x\in\Omega}[x]$ est fixé par ι et si y est un élément de Ω, on a $[\frac{1}{y}] = [y]$ ou $[\frac{1}{y}] = [y]\sigma = [-\frac{1}{y}]$ (resp. $[\frac{1}{y}] = [y]$ ou $[\frac{1}{y}] = [y]\tau = [\frac{-1}{y+1}]$ ou $[\frac{1}{y}] = [y]\tau^2 = [\frac{-(y+1)}{y}]$). Ceci entraîne $y \in \{0, 1, -1, \infty\}$ (resp. $y \in \{0, 1, -1, \infty, -\frac{1}{2}, -2\}$, ce qui est impossible si Ω ne rencontre pas $\{0, 1, -1, \infty\}$. Cela prouve le lemme.

Proposition 5 *Pour tout $a \in M$, on a*

$$\xi'(\iota(a)) = -\overline{\xi'(a)}.$$

Le groupe $H_1(X_0(p);\mathbf{Z})$ muni de l'involution définie par la conjugaison complexe est acyclique.

Démonstration.- Soit $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z})$. On a

$$\overline{\xi(c,d)} = \overline{\{\frac{b}{d}, \frac{a}{c}\}} = \{-\frac{b}{d}, -\frac{a}{c}\} = \{\frac{-b}{d}, \frac{a}{-c}\} = \xi(-c,d).$$

Cela prouve la relation $\overline{\xi([x])} = \xi([-x])$ et donc la relation $\overline{\xi'([x])} = \xi'([-x])$, pour $x \in \mathbf{P}^1(\mathbf{Z}/p\mathbf{Z}) - \{0,1,-1,\infty\}$. On en déduit l'égalité

$$-\overline{\xi'([x])} = -\xi'([-x]) = \xi'([-x]\sigma) = \xi'([\frac{1}{x}]) = \xi'(\iota([x])).$$

Cela prouve la première assertion de la proposition.

Considérons la suite exacte de $\mathbf{Z}[G]$-modules

$$0 \to M_\sigma \oplus M_\tau \to M \xrightarrow{\xi'} \mathrm{H}_1(X_0(p);\mathbf{Z}) \to 0,$$

où G est un groupe d'ordre 2 dont l'élément non neutre opère par $-\iota$ sur M, M_σ et M_τ et par la conjugaison complexe sur $\mathrm{H}_1(X_0(p);\mathbf{Z})$. Comme d'après le lemme 2 et la proposition 4, les $\mathbf{Z}[G]$ modules M, M_σ et M_τ sont acycliques, $\mathrm{H}_1(X_0(p);\mathbf{Z})$ l'est aussi. On en déduit la proposition.

Mentionnons un corollaire (dont nous ne ferons aucun usage) de cette proposition concernant la jacobienne $J_0(p)$ de $X_0(p)$.

Notons $J_0(p)[2]$ l'ensemble des points de 2-torsion de $J_0(p)$. C'est un $\mathbf{F}_2$-espace vectoriel de dimension $2g$ (où g est le genre de $X_0(p)$), muni d'une forme bilinéaire alternée définie par les accouplements de Weil. Notons $J_0(p)[2](\mathbf{R})$ l'ensemble des points réels de $J_0(p)[2]$.

Corollaire 3 *Le $\mathbf{F}_2$-espace vectoriel $J_0(p)[2](\mathbf{R})$ est un sous-espace vectoriel totalement isotrope maximal de $J_0(p)[2]$ pour la forme bilinéaire définie par les accouplements de Weil.*

Démonstration.- Soient a et b deux points de $J_0(p)[2](\mathbf{R})$. Considérons a comme un élément de $\mathrm{Alb}(X_0(p))$ et b comme un élément de $\mathrm{Pic}^0(X_0(p))$. Avec les notations des numéros 3.1.1 et 3.1.2, a est l'image par l'homomorphisme canonique de groupes $\alpha : \mathrm{H}_1(X_0(p), ptes;\mathbf{R}) \to \mathrm{Alb}(X_0(p))$ d'un élément $x \in \frac{1}{2}\mathrm{H}_1(X_0(p), ptes;\mathbf{Z})$ tel que $x - \bar{x} \in \mathrm{H}_1(X_0(p), ptes;\mathbf{Z})$, et b est l'image par l'isomomorphisme canonique de groupes $\beta : \mathrm{Hom}(\mathrm{H}_1(X_0(p);\mathbf{Z}), \mathbf{U}) \to$

$\mathrm{Pic}^0(X_0(p))$ d'un élément $\phi \in \mathrm{Hom}(\mathrm{H}_1(X_0(p);\mathbf{Z}),\mathbf{U})$ à valeurs dans $\{1,-1\}$ et vérifiant $\phi(y) = \phi(\bar{y})$ ($y \in \mathrm{H}_1(X_0(p);\mathbf{Z})$). D'après la proposition 5, il existe $x_1 \in \mathrm{H}_1(X_0(p), ptes;\mathbf{Z})$ tel que $\bar{x} - x = \bar{x}_1 - x_1$; mais dans ces conditions $2(x - x_1)$ est invariant par la conjugaison complexe, et il existe, toujours d'après la proposition 5, un élément x_2 de $\mathrm{H}_1(X_0(p);\mathbf{Z})$ tel que $2(x - x_1) = x_2 + \bar{x}_2$. L'accouplement de Weil entre a et b est donné ainsi (proposition 10)

$$\begin{aligned} e_2(a,b) &= e_2(\alpha(x),\beta(\phi)) = e_2(\alpha(x-x_1),\beta(\phi)) = e_2(\frac{1}{2}\alpha(x_2+\bar{x}_2),\beta(\phi)) \\ &= \phi(x_2+\bar{x}_2) = \phi(x_2)\phi(\bar{x}_2) = \phi(x_2)^2 = 1. \end{aligned}$$

Cela prouve que $J_0(p)[2](\mathbf{R})$ est un sous-espace vectoriel totalement isotrope de $J_0(p)[2]$; il est donc de dimension $\leq g$ sur $\mathbf{F}_2$. Comme l'espace vectoriel $J_0(p)[2](\mathbf{R})$ contient l'image par α de $\frac{1}{2}\mathrm{H}_1(X_0(p);\mathbf{Z})_+$, qui est de dimension g sur $\mathbf{F}_2$, il est de dimension g sur $\mathbf{F}_2$ et est un sous-espace totalement isotrope maximal de $J_0(p)[2]$.

Remarque.- Soit N un nombre entier > 0 non nécessairement premier. Alors le module $\mathrm{H}_1(X_0(N);\mathbf{Z})$ n'est pas nécessairement acyclique pour la conjugaison complexe ; $J_0(N)[2](\mathbf{R})$ n'est pas nécessairement un sous-espace isotrope de $J_0(N)[2]$ et sa dimension n'est pas nécessairement égale au genre de $X_0(N)$. En effet considérons la courbe modulaire $X_0(15)$, qui est une courbe elliptique. Son discriminant est > 0 et tous ses points d'ordre 2 sont réels.

2 Sommes de Dedekind et éléments d'Eisenstein

2.1 L'homomorphisme de Rademacher

La fonction $z \mapsto \Delta(pz)/\Delta(z)$ sur $\mathfrak{H}$ est modulaire pour $\Gamma_0(p)$ (voir [8]). Sa différentielle logarithmique est égale à $2\pi i E_p(z)\,dz$, où E_p est la série d'Eisenstein de poids 2 pour $\Gamma_0(p)$ dont le terme constant à l'infini est égal à $p-1$. La forme différentielle $E_p(z)\,dz$ définit donc une forme différentielle méromorphe ω_p sur $X_0(p)$, holomorphe sur $Y_0(p)$, à périodes dans $\mathbf{Z}$.

Soit $\gamma \in \Gamma_0(p)$. Pour $z_0 \in \mathfrak{H}$, notons $c_p(\gamma)$ la classe dans $\mathrm{H}_1(Y_0(p),\mathbf{Z})$ de l'image dans $Y_0(p)$ du chemin géodésique reliant z_0 à γz_0 dans $\mathfrak{H}$. Elle ne dépend pas du choix de z_0. Posons

$$\phi_p(\gamma) = \int_{c_p(\gamma)} \omega_p = \int_{z_0}^{\gamma z_0} E_p(z)dz.$$

L'application ϕ_p est un homomorphisme de groupes $\Gamma_0(p) \to \mathbf{Z}$. C'est *l'homomorphisme de Rademacher*. Indiquons ses principales propriétés.

Soient u et v deux nombres entiers premiers entre eux, avec $v \geq 1$. Rappelons que la somme de Dedekind $S(u,v)$ est définie par la formule (voir [12])

$$S(u,v) = \sum_{t=1}^{v-1} \bar{B}_1(\frac{tu}{v})\bar{B}_1(\frac{t}{v})$$

où $\bar{B}_1$ est le premier polynôme de Bernoulli rendu périodique, i.e. l'unique fonction de $\mathbf{R}$ dans $\mathbf{R}$ vérifiant les trois propriétés suivantes : $\bar{B}_1$ est périodique de période 1, on a $\bar{B}_1(0) = 0$, on a $\bar{B}_1(x) = x - \frac{1}{2}$ pour tout $x \in]0,1[$.

Proposition 6 *Soit* $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(p)$.
a) On a

$$\begin{aligned} \phi_p(\gamma) &= \frac{a+d}{c}(p-1) + 12\mathrm{sgn}(c)(S(d,|c|) - S(d,\frac{|c|}{p})) \quad si \quad c \neq 0 \\ \phi_p(\gamma) &= \frac{b}{d}(p-1) \quad si \quad c = 0 \end{aligned}$$

où $\mathrm{sgn}(c)$ *désigne le signe de* c.
b) L'image de ϕ_p *est égale à* $\nu\mathbf{Z}$.
c) On a

$$\phi_p(\gamma) = \phi_p(\begin{pmatrix} a & \frac{c}{p} \\ pb & d \end{pmatrix}).$$

Démonstration.- L'assertion a) est obtenue en combinant les formules (2.1) et (2.2) de [8], section 2 (en réalité ces formules sont extraites de [11]). L'assertion b) traduit le fait que la fonction rationnelle λ_p sur $X_0(p)$ déduite par passage aux quotients de $\Delta(pz)/\Delta(z)$ est une puissance ν-ième. L'assertion c) résulte des propositions 2 et 3 de [8]. Elle provient essentiellement d'une propriété d'antiinvariance de ϕ_p par rapport à l'involution d'Atkin-Lehner.

2.2 L'homomorphisme ψ_p

Soit λ_p la fonction rationnelle $\Gamma_0(p)z \mapsto \Delta(pz)/\Delta(z)$ sur $X_0(p)$. Avec les notations de la section 2.2, posons $\lambda_{2p,2} = (\lambda_p \circ \pi)^2/(\lambda_p \circ \pi')$. C'est une fonction rationnelle sur $X_0(2p,2)$ sans zéro ni pôle sur $X_0(2p,2) - P_+$ (proposition 1). Les calculs de la démonstration de la proposition 1 permettent de montrer

qu'elle prend la valeur 1 sur P_-. Comme sa différentielle logarithmique est égale à $2\pi i {\kappa_p}^*(\omega_p)$, on définit un homomorphisme de groupes

$$\psi_p \ : \ \mathrm{H}_1(X_0(2p,2) - P_+, P_-; \mathbf{Z}) \to \mathbf{Z}$$

en posant

$$\psi_p(c) = \int_c {\kappa_p}^*(\omega_p).$$

L'application $\Gamma(2) \to \mathbf{P}^1(\mathbf{Z}/p\mathbf{Z})$ qui à $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ associe (c,d) définit par passage aux quotients une bijection

$$\Gamma_0(2p,2)\backslash\Gamma(2) \mapsto \mathbf{P}^1(\mathbf{Z}/p\mathbf{Z}).$$

L'élément $[g]_0$ de $\mathrm{H}_1(X_0(2p,2) - P_+, P_-; \mathbf{Z})$ (resp. $[g]^0$ de $\mathrm{H}_1(X_0(2p,2) - P_-, P_+; \mathbf{Z})$) ne dépend que de $\Gamma_0(2p,2)g$, et donc que de l'élément (c,d) de $\mathbf{P}^1(\mathbf{Z}/p\mathbf{Z})$; notons-le $\xi_0(c,d)$ (resp. $\xi^0(c,d)$).

Identifions $\mathbf{Z}/p\mathbf{Z}$ à un sous-ensemble de $\mathbf{P}^1(\mathbf{Z}/p\mathbf{Z})$ par l'application $k \mapsto (k,1)$ et notons ∞ l'élément $(1,0)$ de $\mathbf{P}^1(\mathbf{Z}/p\mathbf{Z})$.

Définissons une fonction $F : \mathbf{P}^1(\mathbf{Z}/p\mathbf{Z}) \to \mathbf{Q}$ comme suit. Posons $F(1) = F(-1) = 0$. Pour $x \in \mathbf{P}^1(\mathbf{Z}/p\mathbf{Z}) - \{1,-1\}$, posons

$$F(x) = 2\sum_{h=1}^{p-1} \bar{B}_1(\frac{hr}{2p})$$

où $r \in (1+2\mathbf{Z})$ est tel que $x = (r-1, r+1)$. On a en particulier

$$F(0) = -\frac{p-1}{2} \quad \text{et} \quad F(\infty) = \frac{p-1}{2}.$$

Considérons la fonction

$$D_2(x) = 2(\bar{B}_1(x) - \bar{B}_1(x+\frac{1}{2})).$$

Elle est périodique de période 1, nulle pour $x = 0$ et $x = 1/2$, égale à -1 sur $]0,1/2[$ et à 1 sur $]1/2,1[$. On notera encore D_2 la fonction qu'elle définit sur $\mathbf{R}/\mathbf{Z}$ par passage aux quotients.

Lemme 3 *Pour tout élément (u,v) de $\mathbf{P}^1(\mathbf{Z}/p\mathbf{Z})$, on a*

$$F(u,v) = \frac{1}{2}\sum_{q=0}^{p-1} D_2(\frac{(u+v)q}{p})D_2(\frac{(u-v)q}{p}).$$

Soit $x \in \mathbf{Z}$ non congru à 0, 1 ou -1 modulo p. On a

$$F(x+p\mathbf{Z}) = \frac{p-1}{2} - 2\sum_{q=1}^{\frac{p-1}{2}} [\frac{q(x+1)}{p}] - [\frac{q(x-1)}{p}],$$

où $[y]$ désigne la partie entière de y ($y \in \mathbf{R}$). La fonction F est donc à valeurs entières.

Démonstration.- Supposons qu'on ait $x \in \mathbf{Z}$ non congru à 0, 1 ou -1 modulo p. Soit $r \in (1+2\mathbf{Z})$ tel que $(r-1, r+1)$ soit un système de coordonnées homogènes du point $x+p\mathbf{Z}$ de $\mathbf{P}^1(\mathbf{Z}/p\mathbf{Z})$, et soit (u,v) un autre tel système de coordonnées. On a les égalités

$$\begin{aligned}
F(x+p\mathbf{Z}) &= 2\sum_{q=1}^{p-1} \bar{B}_1(\frac{qr}{2p}) \\
&= \sum_{q=1}^{2p-1} \bar{B}_1(\frac{qr}{2p})(1 - D_2(\frac{q}{2p})) \\
&= -\sum_{q=1}^{2p-1} \bar{B}_1(\frac{qr}{2p}) D_2(\frac{q}{2p}) \\
&= -\sum_{l=1}^{p-1} \bar{B}_1(\frac{lr}{p}) D_2(\frac{l}{p}) - \sum_{l=1}^{p-1} \bar{B}_1(\frac{lr}{p}+\frac{1}{2}) D_2(\frac{l}{p}+\frac{1}{2}) \\
&= -\sum_{l=0}^{p-1} D_2(\frac{l}{p})(\bar{B}_1(\frac{lr}{p}) - \bar{B}_1(\frac{lr}{p}+\frac{1}{2})) \\
&= -\frac{1}{2}\sum_{l=0}^{p-1} D_2(\frac{l}{p}) D_2(\frac{lr}{p}) \\
&= \frac{1}{2}\sum_{l=0}^{p-1} D_2(\frac{l(u+v)}{p}) D_2(\frac{l(u-v)}{p})
\end{aligned}$$

Cela prouve la première assertion pour $(u,v) \neq 0, 1, -1, \infty$. On vérifie facilement la formule pour les valeurs manquantes. Reprenons notre calcul avec (u,v) égal à $(x,1)$. On a

$$\begin{aligned}
F(x+p\mathbf{Z}) &= \frac{1}{2}\sum_{q=0,2|q}^{2p-1} D_2(\frac{q(1+x)}{2p}) D_2(\frac{q(x-1)}{2p}) \\
&= \frac{1}{2}\sum_{q=1}^{p-1} D_2(\frac{q(1+x)}{2p}) D_2(\frac{q(x-1)}{2p})
\end{aligned}$$

$$= \sum_{q=1}^{\frac{p-1}{2}} D_2(\frac{q(1+x)}{2p})D_2(\frac{q(x-1)}{2p}).$$

Comme $\frac{(x+1)q}{p} - \frac{(x-1)q}{p} < 1$ pour $q = 1, ..., \frac{p-1}{2}$, $D_2(\frac{q(1+x)}{2p})D_2(\frac{q(x-1)}{2p})$ est égal à $+1$ si $[\frac{(x+1)q}{p}] \neq [\frac{(x-1)q}{p}]$ et à -1 sinon. On a donc

$$D_2(\frac{q(1+x)}{2p})D_2(\frac{q(x-1)}{2p}) = 1 - 2([\frac{(x+1)q}{p}] - [\frac{(x-1)q}{p}]).$$

On en déduit le lemme 3.

Proposition 7 *Pour tout $x \in \mathbf{P}^1(\mathbf{Z}/p\mathbf{Z})$, on a*

$$\psi_p(\xi_0(x)) = 6F(x).$$

Démonstration.- Supposons d'abord qu'on ait $x \neq 1, -1$. Soit $r \in (1 + 4\mathbf{Z})$ tel que $x = (r-1, r+1)$. Soit $s \in \mathbf{Z}$ tel que $rs \equiv 1 \pmod{4p}$. Posons

$$\begin{aligned} V(r,s) &= \begin{pmatrix} \frac{1-rs}{2} + s & \frac{1-rs}{2} + s - r + 2 \\ \frac{rs-1}{2} & \frac{rs-1}{2} + r \end{pmatrix} \\ &= \begin{pmatrix} \frac{r-3}{2} & \frac{r-1}{2} \\ \frac{1-r}{2} & \frac{-1-r}{2} \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \frac{s-3}{2} & \frac{s-1}{2} \\ \frac{1-s}{2} & \frac{-1-s}{2} \end{pmatrix}. \end{aligned}$$

On a $V(r,s) \in \Gamma_0(2p, 2)$.

Lemme 4 *Soit $z_0 \in \mathfrak{H}$. L'élément $\xi_0(x)$ de $H_1(X_0(2p,2) - P_+, P_-; \mathbf{Z})$ est la classe de l'image dans $X_0(2p,2)$ du chemin géodésique reliant $V(r,s)z_0$ à z_0.*

Démonstration.- Posons

$$g = \begin{pmatrix} \frac{r-3}{2} & \frac{r-1}{2} \\ \frac{1-r}{2} & \frac{-1-r}{2} \end{pmatrix}.$$

On a $g \in \Gamma(2)$ et $\xi_0(x) = [g]_0$ par définition. Remarquons qu'on a

$$\begin{pmatrix} \frac{r-3}{2} & \frac{r-1}{2} \\ \frac{1-r}{2} & \frac{-1-r}{2} \end{pmatrix}(-1) = \begin{pmatrix} \frac{s-3}{2} & \frac{s-1}{2} \\ \frac{1-s}{2} & \frac{-1-s}{2} \end{pmatrix}(-1) = -1.$$

On en déduit

$$g(-1) = -1 \quad \text{et} \quad g1 = g\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}(-1) = V(r,s)(-1).$$

Or la classe dans $\mathrm{H}_1(X_0(2p,2)-P_+,P_-;\mathbf{Z})$ de l'image du chemin géodésique reliant $V(r,s)z$ à z est indépendante de z, lorsque z parcourt $\mathfrak{H}\cup\{-1\}$. Cela prouve le lemme 4.

Soit $z_0 \in \mathfrak{H}$. Posons $h = \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}$. On a $V(r,s) \in \Gamma_0(2p,2)$ et donc $hV(r,s)h^{-1} \in \Gamma_0(p)$. On en déduit les égalités

$$\begin{aligned}
\psi_p(\xi_0(x)) &= \int_{\xi_0(x)} \kappa_p^*(\omega_p) \\
&= \int_{V(r,s)z_0}^{z_0} (2E_p(z)dz - E_p(\frac{z+1}{2})d(\frac{z+1}{2})) \\
&= 2\int_{V(r,s)z_0}^{z_0} E_p(z)dz - \int_{hV(r,s)z_0}^{hz_0} E_p(z)dz \\
&= -2\phi_p(V(r,s)) + \phi_p(hV(r,s)h^{-1}).
\end{aligned}$$

Calculons chacun des deux termes figurant dans le dernier membre en utilisant la proposition 6. On a

$$\begin{aligned}
\phi_p(V(r,s)) &= \phi_p(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} V(r,s) \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}) \\
&= \phi_p(\begin{pmatrix} s & 2 \\ (rs-1)/2 & r \end{pmatrix}) \\
&= \phi_p(\begin{pmatrix} s & (rs-1)/2p \\ 2p & r \end{pmatrix}) \\
&= \frac{r+s}{2p}(p-1) + 12S(r,2p) - 12S(r,2) \\
&= \frac{r+s}{2p}(p-1) + 12S(r,2p)
\end{aligned}$$

et

$$\begin{aligned}
\phi_p(hV(r,s)h^{-1}) &= \phi_p(\begin{pmatrix} s & 1 \\ rs-1 & r \end{pmatrix}) \\
&= \phi_p(\begin{pmatrix} s & (rs-1)/p \\ p & r \end{pmatrix}) \\
&= \frac{r+s}{p}(p-1) + 12S(r,p) - 12S(r,1) \\
&= \frac{r+s}{p}(p-1) + 12S(r,p).
\end{aligned}$$

On en déduit

$$\frac{1}{12}\psi_p(\xi_0(x)) = S(r,p) - 2S(r,2p)$$

$$
\begin{aligned}
&= \sum_{k=1}^{p-1} \bar{B}_1(\frac{k}{p})\bar{B}_1(\frac{kr}{p}) - 2\sum_{k=1}^{2p-1} \bar{B}_1(\frac{k}{2p})\bar{B}_1(\frac{kr}{2p}) \\
&= \sum_{k=1}^{p-1} (\frac{k}{p} - \frac{1}{2})\bar{B}_1(\frac{kr}{p}) - 2\sum_{k=1}^{2p-1} (\frac{k}{2p} - \frac{1}{2})\bar{B}_1(\frac{kr}{2p}) \\
&= \sum_{k=1}^{p-1} (\frac{k}{p} - \frac{1}{2})\bar{B}_1(\frac{kr}{p}) - \sum_{k=1}^{p-1} (\frac{k}{p} - 1)\bar{B}_1(\frac{kr}{2p}) - \sum_{k=1}^{p-1} \frac{k}{p}\bar{B}_1(\frac{kr}{2p} + \frac{1}{2}) \\
&= \sum_{k=1}^{p-1} (\frac{k}{p} - \frac{1}{2})(\bar{B}_1(\frac{kr}{p}) - \bar{B}_1(\frac{kr}{2p}) - \bar{B}_1(\frac{kr}{2p} + \frac{1}{2})) \\
&\quad + \frac{1}{2}\sum_{k=0}^{p-1} (\bar{B}_1(\frac{kr}{2p}) - \bar{B}_1(\frac{kr}{2p} + \frac{1}{2})) \\
&= \sum_{k=0}^{p-1} \bar{B}_1(\frac{kr}{2p}) \\
&= \frac{1}{2}F(x).
\end{aligned}
$$

Cela prouve la formule figurant dans la proposition 7, pour $x \neq 1, -1$.

Il reste à calculer $\psi_p(\xi_0(1))$ et $\psi_p(\xi_0(-1))$. On a, en posant

$$f(z) = 2E_p(z) - \frac{1}{2}E_p(\frac{z+1}{2})$$

la relation $\overline{f(z)} = f(-\bar{z})$ car f est somme d'une série $\sum_{n=0}^{\infty} a_n e^{\pi i n z}$ où les a_n sont réels. Posons

$$g_1 = \begin{pmatrix} 1 & 0 \\ p+1 & 1 \end{pmatrix} \quad \text{et} \quad g_{-1} = \begin{pmatrix} 1 & 0 \\ -p-1 & 1 \end{pmatrix}.$$

On a, puisque ψ_p est à valeurs réelles,

$$
\begin{aligned}
\psi_p(\xi_0(1)) &= \psi_p([g_1]_0) = \int_{\frac{1}{p+2}}^{\frac{1}{p}} f(z)\,dz \\
&= \overline{\int_{\frac{1}{p+2}}^{\frac{1}{p}} f(z)\,dz} = \int_{\frac{1}{p+2}}^{\frac{1}{p}} f(-\bar{z})\,d\bar{z} \\
&= -\int_{-\frac{1}{p+2}}^{-\frac{1}{p}} f(z')\,dz' = \int_{-\frac{1}{p}}^{-\frac{1}{p+2}} f(z')\,dz' \\
&= \psi_p([g_{-1}]) = \psi_p(\xi_0(-1)).
\end{aligned}
$$

Posons $\sigma = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $\sigma_p = \begin{pmatrix} 1-p & -p \\ p & 1+p \end{pmatrix}$. On a

$$\psi_p(\xi_0(1)) = \int_{g_1\sigma(-1)}^{g_1\sigma 1} f(z)\,dz = -\int_{\sigma_p^{-1}g_1\sigma 1}^{\sigma_p^{-1}g_1\sigma(-1)} f(\sigma_p(z))\,d(\sigma_p(z)).$$

Comme $\sigma_p \in \Gamma_0(p)$ et comme, en posant $h = \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}$, on a $h\sigma_p \in \Gamma_0(p)h$, la forme différentielle $f(z)\,dz$ est invariante par σ_p. Par ailleurs $\sigma_p^{-1}g_1\sigma$ appartient à $\Gamma_0(2p,2)g_{-1}$. Nous avons ainsi

$$\begin{aligned} \psi_p(\xi_0(1)) &= -\int_{g_{-1}1}^{g_{-1}(-1)} f(z)\,dz \\ &= -\psi_p(\xi_0(-1)). \end{aligned}$$

Cela prouve

$$\psi_p(\xi_0(1)) = \psi_p(\xi_0(-1)) = 0,$$

donc la proposition 7.

Proposition 8 *Considérons l'élément*

$$\mathcal{E}_0 = \sum_{x\in\mathbf{P}^1(\mathbf{Z}/p\mathbf{Z})} F(x)\xi^0(x)$$

de $H_1(X_0(2p,2) - P_-, P_+; \mathbf{Z})$. *Pour tout* $c \in H_1(X_0(2p,2) - P_+, P_-; \mathbf{Z})$, *on a*

$$\psi_p(c) = 6\,\mathcal{E}_0 \bullet c.$$

De plus on a

$$\mathcal{E}_0 = -\sum_{l=1}^{\frac{p-1}{2}}\sum_{h=1}^{\frac{p-1}{2}} \xi^0(l-h, l+h) + \sum_{l=\frac{p+1}{2}}^{p-1}\sum_{h=1}^{\frac{p-1}{2}} \xi^0(l-h, l+h).$$

Démonstration.- La première assertion résulte du théorème 6 et de la proposition 7.

On a, en utilisant le lemme 3,

$$\mathcal{E}_0 = \frac{1}{2}\sum_{u=0}^{p-1}\sum_{v=0}^{p-1} D_2(\frac{u+v}{p})D_2(\frac{u-v}{p})\xi^0(u,v)$$

$$
\begin{aligned}
&= -\frac{1}{2}\sum_{l=1}^{p-1}\sum_{h=1}^{p-1} D_2(\frac{l}{p})D_2(\frac{h}{p})\xi^0(l-h,l+h) \\
&= -\sum_{l=1}^{\frac{p-1}{2}}\sum_{h=1}^{\frac{p-1}{2}} \xi^0(l-h,l+h) + \sum_{l=\frac{p+1}{2}}^{p-1}\sum_{h=1}^{\frac{p-1}{2}} \xi^0(l-h,l+h).
\end{aligned}
$$

On en déduit la proposition.

2.3 L'élément d'Eisenstein $\mathcal{E}$

Démontrons le théorème 4. Notons π_* l'homomorphisme de groupes

$$\mathrm{H}_1(X_0(2p,2)-P_-,P_+;\mathbf{Z}) \to \mathrm{H}_1(X_0(p),ptes;\mathbf{Z})$$

déduit fonctoriellement de π. Pour $x \in \mathbf{P}^1(\mathbf{Z}/p\mathbf{Z})$, on a $\pi_*(\xi^0(x)) = \xi(x)$.

Lemme 5 *L'intégrale de toute forme différentielle holomorphe sur $X_0(2p,2)$ le long des cycles de classe $\mathcal{E}_0$ est nulle.*

Démonstration.- Rappelons que la forme différentielle $2\pi i{\kappa_p}^*(\omega_p)$ est égale à la différentielle logarithmique de $\lambda_{2p,2}$. D'après la proposition 1, l'image réciproque de l'ensemble $\{0,\infty\}$ par $\lambda_{2p,2}$ est contenue P_+ et l'image de P_- par $\lambda_{2p,2}$ est égale à $\{1\}$. Notons γ_1 la classe dans $\mathrm{H}_1(\mathbf{P}^1(\mathbf{C})-\{1\},\{0,\infty\};\mathbf{Z})$ d'un chemin de $\mathbf{P}^1(\mathbf{C})$ reliant 0 à ∞ et ne passant pas par 1. Soit $y \in \mathrm{H}_1(X_0(2p,2)-P_+,P_-;\mathbf{Z})$. Notons $\lambda_{2p,2_*}(y)$ la classe dans $\mathrm{H}_1(\mathbf{P}^1(\mathbf{C})-\{0,\infty\},1;\mathbf{Z})$ de l'image d'un chemin de classe y par $\lambda_{2p,2}$. On a, d'après la proposition 8

$$
\begin{aligned}
6\,\mathcal{E}_0 \bullet y &= \psi_p(y) \\
&= \frac{1}{2\pi i}\int_y \frac{d\lambda_{2p,2}}{\lambda_{2p,2}} \\
&= \gamma_1 \bullet \lambda_{2p,2_*}(y) \\
&= \lambda^*_{2p,2}(\gamma_1) \bullet y.
\end{aligned}
$$

On en déduit

$$\lambda^*_{2p,2}(\gamma_1) = 6\mathcal{E}_0.$$

Soit ω une forme différentielle holomorphe sur $X_0(2p,2)$. L'image directe $\lambda_{2p,2_*}(\omega)$ de ω par $\lambda_{2p,2}$ est une forme différentielle holomorphe sur $\mathbf{P}^1(\mathbf{C})$. Elle est donc nulle. On en déduit l'égalité

$$6\int_{\mathcal{E}_0}\omega = \int_{\lambda^*_{2p,2}(\gamma_1)}\omega = \int_{\gamma_1}\lambda_{2p,2_*}(\omega) = 0.$$

Cela prouve le lemme.

On démontre de manière analogue que l'on a $\lambda_p^*(\gamma_1) = \mathcal{E}$ et que l'intégrale de toute forme différentielle holomorphe sur $X_0(p)$ le long des cycles de classe $\mathcal{E}$ est nulle.

Par ailleurs, si ω est une telle forme différentielle, on a

$$\int_{\pi_*(\mathcal{E}_0)} \omega = \int_{\mathcal{E}_0} \pi^*(\omega) = 0.$$

Comme $X_0(p)$ ne posssède que deux pointes, $\mathrm{H}_1(X_0(p); \mathbf{Z})$ est un sous-module de corang 1 de $\mathrm{H}_1(X_0(p), ptes; \mathbf{Z})$. Aucun élément non nul de $\mathrm{H}_1(X_0(p); \mathbf{Z})$ n'annule toutes les intégrales de formes différentielles holomorphes. On en déduit que $\mathcal{E}$ et $\pi_*(\mathcal{E}_0)$ sont proportionnels. La proposition suivante permet de conclure que $\pi_*(\mathcal{E}_0)$ est égal à $\mathcal{E}$. Le théorème 4 résulte alors de la proposition 8.

Proposition 9 *Les bords de $\pi_*(\mathcal{E}_0)$ et $\mathcal{E}$ sont égaux à $(p-1)(\Gamma_0(p)0 - \Gamma_0(p)\infty)$.*

Démonstration.- Il résulte de l'égalité $\lambda_p^*(\gamma_1) = \mathcal{E}$ que le bord de $\mathcal{E}$ est l'image réciproque par λ_p de $(\infty)-(0)$, c'est-à-dire l'opposé du diviseur de λ_p. D'autre part le bord de $\xi(x)$ est nul pour $x \in \mathbf{P}^1(\mathbf{Z}/p\mathbf{Z})$ distinct de 0, ∞, est égal à $(\Gamma_0(p)\infty) - (\Gamma_0(p)0)$ pour $x = 0$ et à $(\Gamma_0(p)0) - (\Gamma_0(p)\infty)$ pour $x = \infty$. Celui de $\pi_*(\mathcal{E}_0) = \sum_{x \in \mathbf{P}^1(\mathbf{Z}/p\mathbf{Z})} F(x)\xi(x)$ est donc $(p-1)(\Gamma_0(p)0 - \Gamma_0(p)\infty)$ puisque l'on a $F(0) = -(p-1)/2$ et $F(\infty) = (p-1)/2$.

On en déduit le théorème 4 et le corollaire suivant.

Corollaire 4 *On a*

$$\mathcal{E} = \sum_{x \in \mathbf{P}^1(\mathbf{Z}/p\mathbf{Z})} F(x)\xi(x).$$

3 Le sous-groupe de Shimura et le sous-groupe cuspidal

3.1 Généralités sur les variétés jacobiennes

Soit X une surface de Riemann compacte connexe et non vide.

3.1.1 Variétés d'Albanese

La variété d'Albanese $\mathrm{Alb}(X)$ de X paramètre par définition les diviseurs de degré 0 de X modulo équivalence linéaire.

Notons $\mathrm{H}^0(X, \Omega^1)$ le $\mathbf{C}$-espace vectoriel des formes différentielles holomorphes sur X et E son dual. On a un isomorphisme canonique de $\mathbf{R}$-espaces vectoriels

$$\begin{array}{rcl} v_{\mathbf{R}} \ : \ \mathrm{H}_1(X;\mathbf{R}) & \to & E \\ c & \mapsto & (\omega \mapsto \displaystyle\int_c \omega). \end{array}$$

Il définit par restriction un isomorphisme v de $\mathrm{H}_1(X;\mathbf{Z})$ sur un réseau L de E. Le groupe de Lie complexe E/L est une variété abélienne [13].

Soit D un diviseur de degré 0 sur X. Soit c une 1-chaîne singulière sur X de bord D. L'élément de E/L : $(\omega \mapsto \int_c \omega) + L$ ne dépend que de la classe $[D]$ de D dans $\mathrm{Alb}(X)$. L'application j : $[D] \mapsto (\omega \mapsto \int_c \omega) + L$ est un isomorphisme de variétés abéliennes de $\mathrm{Alb}(X)$ sur E/L (dû à Abel, voir [10], théorème 2.5).

Notons α l'homomorphisme de groupes composé

$$\mathrm{H}_1(X;\mathbf{R}) \stackrel{v_{\mathbf{R}}}{\to} E \to E/L \stackrel{j^{-1}}{\to} \mathrm{Alb}(X).$$

Soit $P_0 \in X$. L'application i_{P_0} : $X \to \mathrm{Alb}(X)$ qui à P associe la classe du diviseur $(P) - (P_0)$ définit un morphisme $X \to \mathrm{Alb}(X)$.

3.1.2 Variétés de Picard

La variété de Picard $\mathrm{Pic}(V)$ (pour V surface de Riemann ou variété abélienne sur $\mathbf{C}$) paramètre par définition les classes d'isomorphisme de fibrés en droites holomorphes sur V. Sa composante neutre $\mathrm{Pic}^0(V)$ est munie d'une structure naturelle de variété abélienne.

On déduit du morphisme i_{P_0} : $X \to \mathrm{Alb}(X)$ (voir section précédente) un isomorphisme de variétés abéliennes

$$i_{P_0}^* \ : \ \mathrm{Pic}^0(\mathrm{Alb}(X)) \to \mathrm{Pic}^0(X).$$

Cet isomorphisme ne dépend pas du choix du point P_0 choisi. Notons $\mathbf{U}$ l'ensemble des nombres complexes de module 1, vu comme groupe topologique discret. Soit $\chi \in \mathrm{Hom}(L, \mathbf{U})$. Notons R_χ l'espace topologique quotient de $E \times \mathbf{U}$ par la relation d'équivalence qui identifie $(e, \chi(\lambda)u)$ et $(e + \lambda, u)$

$((e,\lambda,u) \in E \times L \times \mathbf{U})$. L'application $R_\chi \to E/L \simeq \mathrm{Alb}(X)$ qui à la classe $[e,u]$ de $(e,u) \in E \times \mathbf{U}$ associe celle de e définit un revêtement principal de $\mathrm{Alb}(X)$ de groupe $\mathbf{U}$.

Notons $\mathcal{L}_\chi$ l'espace topologique quotient de $E \times \mathbf{C}$ par la relation d'équivalence qui identifie $(e, \chi(\lambda)z)$ et $(e+\lambda, z)$ $((e,\lambda,z) \in E \times L \times \mathbf{C})$. C'est un fibré en droites sur $\mathrm{Alb}(X)$ associé au revêtement principal R_χ : la surjection canonique $\mathcal{L}_\chi \to E/L \simeq \mathrm{Alb}(X)$ associe à la classe de (e,z) celle de e.

Soit $\phi \in \mathrm{Hom}(\mathrm{H}_1(X;\mathbf{Z}),\mathbf{U})$. Le composé $\phi \circ v^{-1}$ est un élément de $\mathrm{Hom}(L,\mathbf{U})$. L'application qui à ϕ associe la classe du fibré $i_{P_0}^* \mathcal{L}_{\phi \circ v^{-1}}$ définit un isomorphisme de groupes

$$\beta \ : \ \mathrm{Hom}(\mathrm{H}_1(X;\mathbf{Z}),\mathbf{U}) \to \mathrm{Pic}^0(X).$$

Remarque.- Soit $\phi \in \mathrm{Hom}(\mathrm{H}_1(X;\mathbf{Z}),\mathbf{U})$. Posons $\chi = \phi \circ v^{-1}$. Considérons le revêtement principal R'_χ de X image réciproque de R_χ par i_{P_0}. Le fibré $i_{P_0}^* \mathcal{L}_\chi$ s'identifie au fibré en droites associé à R'_χ. Soit c un chemin fermé de X et $\bar{c}$ sa classe dans $\mathrm{H}_1(X;\mathbf{Z})$. Le chemin c se relève en un chemin $\tilde{c}$ de R'_χ. L'application de monodromie qui à $\bar{c}$ associe $\tilde{c}(1)/\tilde{c}(0)$ est un homomorphisme de groupes $\mathrm{H}_1(X;\mathbf{Z}) \to \mathbf{U}$. Cet homomorphisme coïncide avec ϕ. En effet le composé de $\tilde{c}$ avec l'application canonique $R'_\chi \to R_\chi$ est un chemin de la forme $t \mapsto [e+\delta(t), u]$, où e est un élément de E, u un élément de U et $\delta(t)$ l'élément $\omega \mapsto \int_{c|[0,t]} \omega$ de E. On a

$$[e+\delta(1), u] = [e+v(c), u] = [e, \chi(v(c))u] = [e, \phi(c)u].$$

On en déduit

$$\tilde{c}(1)/\tilde{c}(0) = \phi(c).$$

L'isomorphisme de groupes $\beta : \mathrm{Hom}(\mathrm{H}_1(X;\mathbf{Z}),\mathbf{U}) \to \mathrm{Pic}^0(X)$ considéré ici coïncide donc avec celui défini dans [5].

3.1.3 Accouplements de Weil

Soient A et B deux variétés abéliennes sur $\mathbf{C}$. Soit π une isogénie $A \to B$. Notons $A^\vee = \mathrm{Pic}^0(A)$ et $B^\vee = \mathrm{Pic}^0(B)$ les variétés abéliennes duales de A et B et $\pi^\vee$ l'isogénie $B^\vee \to A^\vee$ duale de π.

Soit $P \in \mathrm{Ker}\,\pi$. Soit $Q \in \mathrm{Ker}\,\pi^\vee$. Soient $\mathcal{L}$ un fibré en droites sur B de classe Q et $\pi^*(\mathcal{L})$ son image réciproque par π sur A. Comme $Q \in \mathrm{Ker}\,\pi^\vee$, ce fibré est trivial. Il existe donc une application holomorphe $f : A \to \mathcal{L}$ relevant π. La fonction $R \mapsto f(R+P)/f(R)$ sur A est à valeurs dans les

racines de l'unité, donc constante. Sa valeur est par définition l'*accouplement de Weil* $e_\pi(P,Q)$ de P et Q relativement à π. Cette définition diffère par le signe de celle de [9], paragraphe 16.

3.1.4 Application aux variétés jacobiennes

Soit l un nombre entier > 0. Pour A variété abélienne notons A_l l'ensemble des points de l-torsion de A.

Appliquons les résultats du numéro précédent au cas où $A = B = \mathrm{Alb}(X)$, et où π est l'isogénie multiplication par l. Identifions $A^\vee = B^\vee = \mathrm{Pic}^0(\mathrm{Alb}(X))$ à $\mathrm{Pic}^0(X)$ par $i^*_{P_0}$ (voir numéro 3.1.2). On obtient alors un accouplement

$$e_l \ : \ \mathrm{Alb}(X)_l \times \mathrm{Pic}^0(X)_l \to \mu_l.$$

Soit $x \in \mathrm{H}_1(X;\mathbf{Z})$. Soit $\phi \in \mathrm{Hom}(\mathrm{H}_1(X;\mathbf{Z}),\mu_l) \subset \mathrm{Hom}(\mathrm{H}_1(X;\mathbf{Z}),\mathbf{U})$. Alors $\alpha(x/l)$ est un élément de $\mathrm{Alb}(X)_l$ et $\beta(\phi)$ est un élément de $\mathrm{Pic}^0(X)_l$.

Proposition 10 *On a*

$$e_l(\alpha(x/l),\beta(\phi)) = \phi(x).$$

Démonstration.- Via les isomorphismes considérés

$$\mathrm{Pic}^0(X) \simeq \mathrm{Pic}^0(\mathrm{Alb}(X)) \simeq \mathrm{Pic}^0(E/L),$$

l'élément $\beta(\phi)$ correspond à la classe du fibré en droites $\mathcal{L}_{\phi\circ v^{-1}}$ sur E/L défini au numéro 3.1.2. Notons m_l l'isogénie de multiplication par l de E/L et $q : \mathcal{L}_{\phi\circ v^{-1}} \to E/L$ la projection canonique. Comme ϕ est à valeurs dans μ_l, on définit une application holomorphe $f : E/L \to \mathcal{L}_{\phi\circ v^{-1}}$ en posant $f(e+L) = [le,1]$. On a $q\circ f = m_l$, donc f est un relèvement de m_l. L'élément $\alpha(x/l)$ de $\mathrm{Alb}(X)_l$ s'identifie à lélément $(v(x)/l)+L$ de E/L et on a, pour tout $e \in E$

$$\begin{array}{rcl} f(e+(v(x)/l)+L) & = & [le+v(x),1] \\ & = & [le,\phi(x)] \\ & = & \phi(x)f(e+L). \end{array}$$

On en déduit la proposition par définition des accouplements de Weil.

3.2 Le sous-groupe cuspidal de $\mathbf{Alb}(X_0(p))$

Notons $\{0,\infty\}$ la classe dans $\mathrm{H}_1(X_0(p), ptes; \mathbf{Z})$ de l'image du chemin géodésique reliant 0 à ∞ dans $\bar{\mathfrak{H}}$. L'élément $\omega \mapsto -\int_{\{0,\infty\}} \omega$ de E est l'image par l'isomorphisme canonique $v_{\mathbf{R}} : \mathrm{H}_1(X_0(p); \mathbf{R}) \to E$ (voir le numéro 3.1.1) d'un élément $\mathbf{e}$ de $\mathrm{H}_1(X_0(p); \mathbf{R})$ appelé par Mazur ([7], section II.18) l'*élément d'enroulement* (*winding element*).

Si y est un nombre rationnel de dénominateur premier à p, l'image dans $X_0(p)$ du chemin géodésique reliant 0 à y dans $\bar{\mathfrak{H}}$ est un lacet. Notons $\{0, y\}$ sa classe dans $\mathrm{H}_1(X_0(p); \mathbf{Z})$. Cette définition coïncide avec celle de l'introduction lorsqu'on identifie $\mathrm{H}_1(X_0(p); \mathbf{Z})$ à un sous-groupe de $\mathrm{H}_1(X_0(p), ptes; \mathbf{Z})$.

Proposition 11 *On a*

$$\mathbf{e} = -\frac{1}{p-1} \sum_{x=1}^{p-1} F(x + p\mathbf{Z})\{0, \frac{1}{x}\}.$$

Démonstration.- Rappelons (corollaire 4) que l'élément d'Eisenstein est donné par la formule

$$\mathcal{E} = \sum_{y \in \mathbf{P}^1(\mathbf{Z}/p\mathbf{Z})} F(y)\xi(y).$$

Comme on a $\xi(0) = \{0,\infty\}$, $\xi(\infty) = -\{0,\infty\}$, $F(0) = -\frac{p-1}{2}$, $F(\infty) = \frac{p-1}{2}$ et comme pour $x = 1, 2, ..., p-1$, $\xi(x + p\mathbf{Z})$ coïncide avec le symbole modulaire $\{0, \frac{1}{x}\}$, l'élément d'Eisenstein s'écrit

$$\mathcal{E} = -(p-1)\{0,\infty\} + \sum_{x=1}^{p-1} F(x + p\mathbf{Z})\{0, \frac{1}{x}\}.$$

On a $\int_{\mathcal{E}} \omega = 0$ pour toute forme différentielle holomorphe ω sur $X_0(p)$, donc l'élément

$$\omega \mapsto -\int_{\{0,\infty\}} \omega$$

de E coïncide avec

$$\omega \mapsto \frac{1}{p-1} \sum_{x=1}^{p-1} -F(x + p\mathbf{Z}) \int_{\{0,\frac{1}{x}\}} \omega.$$

Cela prouve la proposition.

Notons C la classe du diviseur $(\Gamma_0(p)0) - (\Gamma_0(p)\infty)$ dans $\mathrm{Alb}(X_0(p))$. Notons α l'homomorphisme de groupes défini dans le numéro 3.1.1

$$\mathrm{H}_1(X_0(p);\mathbf{R}) \to \mathrm{Alb}(X_0(p)).$$

On a

$$C = \alpha(\mathbf{e}) = \alpha(-\frac{1}{p-1}\sum_{x=1}^{p-1} F(x+p\mathbf{Z})\{0,\frac{1}{x}\}).$$

Remarque.- L'élément $n\mathbf{e}$ appartient à $\mathrm{H}_1(X_0(p);\mathbf{Z})$ (proposition 6). Cela ne se déduit apparemment pas simplement de la proposition 11.

3.3 Le sous-groupe de Shimura de $\mathbf{Pic}^0(X_0(p))$

Considérons les courbes modulaires $X_0(p)$ et $X_1(p)$. Le morphisme de dégénérescence $\pi_p \ : \ X_1(p) \to X_0(p)$ définit par fonctorialité un homomorphisme de variétés abéliennes $\pi_p^* \ : \ \mathrm{Pic}^0(X_0(p)) \to \mathrm{Pic}^0(X_1(p))$ et un homomorphisme de groupes

$$\pi_{p*} \ : \ \mathrm{H}_1(X_1(p);\mathbf{Z}) \to \mathrm{H}_1(X_0(p);\mathbf{Z}).$$

D'après [5], on a le diagramme commutatif

$$\begin{array}{ccc} \mathrm{Hom}(\mathrm{H}_1(X_0(p);\mathbf{Z}),\mathbf{U}) & \overset{Hom(\pi_{p*},1)}{\to} & \mathrm{Hom}(\mathrm{H}_1(X_1(p);\mathbf{Z}),\mathbf{U}) \\ \downarrow & & \downarrow \\ \mathrm{Pic}^0(X_0(p)) & \overset{\pi_p^*}{\to} & \mathrm{Pic}^0(X_1(p)), \end{array}$$

où les flèches verticales sont les isomorphismes canoniques du numéro 3.1.2.

L'application

$$\alpha_0 \ : \ \Gamma_0(p) \to \mathrm{H}_1(X_0(p);\mathbf{Z})$$

(resp.

$$\alpha_1 \ : \ \Gamma_1(p) \to \mathrm{H}_1(X_1(p);\mathbf{Z}))$$

qui à γ associe la classe de l'image dans $X_0(p)$ (resp. $X_1(p)$) du chemin géodésique reliant z_0 à γz_0 dans $\bar{\mathfrak{H}}$ (cette classe ne dépend pas du choix de z_0 dans $\bar{\mathfrak{H}}$) est un homomorphisme surjectif de groupes ([6]). Le noyau $K_0(p)$ de α_0 (resp. $K_1(p)$ de α_1) est engendré par les éléments de trace égale à $-2,-1,0,1$ ou 2 et par les commutateurs de $\Gamma_0(p)$ (resp. de $\Gamma_1(p)$) ([6]). L'application $\Gamma_0(p) \to (\mathbf{Z}/p\mathbf{Z})^*$ qui à $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ associe $d + p\mathbf{Z}$ définit par

passage aux quotients un isomorphisme de groupes $\Gamma_0(p)/\Gamma_1(p) \to (\mathbf{Z}/p\mathbf{Z})^*$. L'image de $K_0(p)$ est égale à l'ensemble $\mu_\nu(p)$ des racines ν-ièmes de l'unité dans $(\mathbf{Z}/p\mathbf{Z})^*$, où comme dans l'introduction $\nu = \mathrm{pgcd}(p-1, 12)$. On résume cela par le diagramme commutatif de suites exactes suivant :

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & K_1(p) & \to & K_0(p) & \to & \mu_\nu(p) & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & \Gamma_1(p) & \to & \Gamma_0(p) & \to & (\mathbf{Z}/p\mathbf{Z})^* & \to & 0 \\
 & & \downarrow \alpha_1 & & \downarrow \alpha_0 & & \downarrow t_\nu & & \\
 & & \mathrm{H}_1(X_1(p);\mathbf{Z}) & \overset{\pi_{p*}}{\to} & \mathrm{H}_1(X_0(p);\mathbf{Z}) & \overset{\theta}{\to} & U & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

où U est le groupe des puissances ν-ièmes de $(\mathbf{Z}/p\mathbf{Z})^*$ et t_ν est l'élévation à la puissance ν. L'homomophisme θ est déterminé par les autres homomorphismes du diagramme. Il associe à la classe commune dans $\mathrm{H}_1(X_0(p);\mathbf{Z})$, pour $z_0 \in \bar{\mathfrak{H}}$, de l'image dans $X_0(p)$ d'un chemin reliant z_0 à $\begin{pmatrix} a & b \\ c & d \end{pmatrix} z_0$ dans $\bar{\mathfrak{H}}$, l'élément $d^\nu + p\mathbf{Z}$ de U. En particulier, en prenant $z_0 = 0$, on voit qu'il associe à $\{0, \frac{b}{d}\}$ le nombre $d^\nu + p\mathbf{Z}$. Comme U est un groupe cyclique d'ordre $n = (p-1)/\nu$, il résulte de l'exactitude de la dernière ligne du diagramme ci-dessus que l'application

$$\mathrm{Hom}(U, \mu_n) \to \mathrm{Pic}^0(X_0(p))$$

qui à λ associe $\beta(\lambda \circ \theta)$ définit un isomorphisme de groupes

$$\beta_\Sigma \ : \ \mathrm{Hom}(U, \mu_n) \simeq \Sigma(p).$$

Remarque.- On peut remplacer dans ce qui précède U par $(\mathbf{Z}/p\mathbf{Z})^*/\mu_\nu(p)$ en remplaçant t_ν par la surjection canonique $(\mathbf{Z}/p\mathbf{Z})^* \to (\mathbf{Z}/p\mathbf{Z})^*/\mu_\nu(p)$. Ce point de vue a été adopté dans [7] et [5].

3.4 L'invariant de Mazur

Par définition l'invariant u de Mazur est l'unique élément u de U vérifiant pour tout élément $\lambda \in \mathrm{Hom}(U, \mu_n)$

$$e_n(C, \beta_\Sigma(\lambda)) = \lambda(u).$$

Proposition 12 *On a*

$$u = \theta(n\mathbf{e}).$$

Démonstration.- En effet, d'après la proposition 10 et la section 3.2, on a, pour tout $\lambda \in \mathrm{Hom}(U, \mu_n)$,

$$\begin{aligned} e_n(C, \beta_\Sigma(\lambda)) &= e_n(\alpha(\mathbf{e}), \beta(\lambda \circ \theta)) \\ &= \lambda(\theta(n\mathbf{e})). \end{aligned}$$

Cela prouve la proposition.

4 La racine carrée de l'invariant de Mazur

4.1 La définition de la racine carrée de u

Notons $\mathrm{H}_1(X_0(p); \mathbf{Z})_+$ et $\mathrm{H}_1(X_0(p); \mathbf{Z})_-$ les sous-groupes de $\mathrm{H}_1(X_0(p); \mathbf{Z})$ formés par les éléments invariants et antinvariants respectivement par l'action de la conjugaison complexe. D'après la proposition 4 tout élément de $\mathrm{H}_1(X_0(p); \mathbf{Z})_+$ (resp. $\mathrm{H}_1(X_0(p); \mathbf{Z})_-$) est de la forme $x + \bar{x}$ (resp. $x - \bar{x}$) avec $x \in \mathrm{H}_1(X_0(p); \mathbf{Z})$. On a

$$\theta(\overline{\{0, \frac{a}{b}\}}) = \theta(\{0, \frac{-a}{b}\}) = b^\nu + p\mathbf{Z} = \theta(\{0, \frac{a}{b}\}).$$

On en déduit que $\mathrm{H}_1(X_0(p); \mathbf{Z})_-$ est dans le noyau de θ. Si deux éléments x et y de $\mathrm{H}_1(X_0(p); \mathbf{Z})$ vérifient $x + \bar{x} = y + \bar{y}$, on a $x - y \in \mathrm{H}_1(X_0(p); \mathbf{Z})_-$ et donc $\theta(x) = \theta(y)$. Cela permet de définir un homomorphisme de groupes

$$\theta_+ \ : \ \mathrm{H}_1(X_0(p); \mathbf{Z})_+ \to U$$

par la formule

$$\theta_+(x + \bar{x}) = \theta(x).$$

Comme $n\mathbf{e}$ est invariant par la conjugaison complexe, on définit une racine carrée canonique de u dans U en posant

$$\sqrt{u} = \theta_+(n\mathbf{e}).$$

On fera le lien entre cette définition et la section II.18 de [7] dans la section 5.1. D'après la proposition 11, $n\mathbf{e}$ est égal à $-\frac{1}{\nu}\sum_{x=1}^{p-1} F(x + p\mathbf{Z})\{0, \frac{1}{x}\}$. Comme la fonction F est à valeur dans $\mathbf{Z}$ mais pas en général dans $\nu\mathbf{Z}$, cette écriture de $n\mathbf{e}$ ne permet pas de caluler directement $\sqrt{u}$. On peut calculer facilement $\sqrt{u}$ à une racine douzième (donc ν-ième) de l'unité près. Nous allons consacrer l'essentiel de nos efforts dans cette partie à déterminer cette racine douzième.

4.2 Les homomorphismes χ, χ_3 et χ_4

Reprenons toutes les notations de la section 1.3. En particulier M est le sous-groupe de $\mathbf{Z}^{(\mathbf{P}^1(\mathbf{Z}/p\mathbf{Z}))}$ formé des éléments à support dans $(\mathbf{Z}/p\mathbf{Z})^* - \{1, -1\}$.

Pour $\bar{a}$ et $\bar{b}$ dans $\mathbf{Z}/p\mathbf{Z}$, notons $[\bar{a}, \bar{b}]$ la réduction modulo p de l'intervalle de nombres entiers $[a, b]$, où a et b sont les représentants de $\bar{a}$ et $\bar{b}$ dans $\{-p, ..., -1\}$ et $\{1, 2, ..., p\}$ respectivement.

Notons μ_4' (resp. μ_3') l'ensemble des racines quatrièmes (resp. cubiques) primitives de l'unité de $\mathbf{Z}/p\mathbf{Z}$. Il est non vide si et seulement si on a $4|\nu$ (resp. $3|\nu$). Il est formé des éléments de $(\mathbf{Z}/p\mathbf{Z})^*$ fixés par σ (resp. par τ).

Introduisons les homomorphismes de groupes suivants :

$$\begin{array}{rccc} \chi : & M & \to & (\mathbf{Z}/p\mathbf{Z})^* \\ & \sum \lambda_x [x] & \mapsto & \prod x^{\lambda_x}, \end{array}$$

$$\begin{array}{rccc} \chi_3 : & M & \to & \mu_3(\mathbf{Z}/p\mathbf{Z}) \\ & \sum \lambda_x [x] & \mapsto & \prod\limits_{x_3 \in \mu_3'} \prod\limits_{y \in [-x_3, x_3]} x_3^{\lambda_{y\sigma} - \lambda_y} \end{array}$$

et

$$\begin{array}{rccc} \chi_4 : & M & \to & \mu_4(\mathbf{Z}/p\mathbf{Z}) \\ & \sum \lambda_x [x] & \mapsto & x_4^{\lambda_{x_4} - \lambda_{-x_4} + \sum_{y \in [-x_4, x_4]} \lambda_{y\sigma} - \lambda_y}, \end{array}$$

où x_4 est une racine quatrième primitive de l'unité, s'il en existe, 1 sinon. L'homomorphisme χ_4 ne dépend pas du choix de x_4.

Lemme 6 *Soit $a \in M_\tau$. On a*

$$\chi(a) = \chi_3(a) \quad \textit{et} \quad \chi_4(a) = 1.$$

Démonstration.- Posons $a = \sum \lambda_x [x]$. On a

$$\chi_3(a) = \prod_{x_3 \in \mu_3'} \Big(\prod_{y \in [-x_3 - 1, x_3 - 1]} x_3^{\lambda_{(y+1)\sigma}} \prod_{y \in [-x_3, x_3]} x_3^{-\lambda_y} \Big).$$

Comme $(y+1)\sigma = y\tau$ et que l'on a $\lambda_{y\tau} = \lambda_y$, on en déduit

$$\chi_3(a) = \prod_{x_3 \in \mu_3'} x_3^{\lambda_{-x_3\sigma} - \lambda_{x_3}} = \prod_{x_3 \in \mu_3'} x_3^{\lambda_{x_3^2} - \lambda_{x_3}} = \prod_{x_3 \in \mu_3'} x_3^{\lambda_{x_3}}.$$

Cela prouve la première égalité. Un calcul analogue à celui qui précède fournit l'égalité

$$\chi_4(a) = x_4^{\lambda_{x_4} - \lambda_{-x_4} + \lambda_{-x_4\sigma} - \lambda_{x_4}} = 1.$$

Lemme 7 *Soit $a \in M_\sigma$. On a*

$$\chi(2a) = \chi_4(2a) \quad \textit{et} \quad \chi_3(a) = 1.$$

Démonstration.- Posons $a = \sum \lambda_x[x]$. On a $\chi_4(2a) = x_4^{2\lambda_{x_4} - 2\lambda_{-x_4}}$. Par ailleurs σ opère sans point fixe sur $(\mathbf{Z}/p\mathbf{Z})^* - \mu_4'$. Si R est un système de représentants de $(\mathbf{Z}/p\mathbf{Z})^* - \mu_4'$ modulo σ, on a

$$\chi(2a) = \prod x^{2\lambda_x} = \chi_4(2a) \prod_{x \in R} x^{2\lambda_x} (x\sigma)^{2\lambda_{x\sigma}} = \chi_4(2a)\,;$$

en effet on a $\lambda_x = \lambda_{x\sigma}$ et $x(x\sigma) = -1$.

L'égalité $\chi_3(a) = 1$ se déduit immédiatement de la relation $\lambda_x = \lambda_{x\sigma}$ et de la définition de χ_3.

Lemme 8 *Soit $a \in \nu M$. On a*

$$\chi_3(a) = \chi_4(a) = 1.$$

Démonstration.- Les homomorphismes χ_3 et χ_4 sont à valeurs dans les racines ν-ièmes de l'unité. On en déduit le lemme.

Rappelons que ι est l'involution de $\mathbf{Z}^{(\mathbf{P}^1(\mathbf{Z}/p\mathbf{Z}))}$ qui à $\sum \lambda_x[x]$ associe $\sum \lambda_x[\frac{1}{x}]$ (voir section 1.3). Cette involution laisse stable M. Notons M_+ l'ensemble des éléments de M fixés par ι.

Lemme 9 *Soit $a \in M_+$. On a*

$$\chi(a) = \chi_3(a) = \chi_4(a) = 1.$$

Démonstration.- Posons $a = \sum \lambda_x[x]$. On a $x\sigma = \iota(-x)$, d'où $\lambda_{x\sigma} = \lambda_{-x}$ pour tout x. Par ailleurs, si $x_4 \in \mu_4'$, on a $-x_4 = \iota(x_4)$ et donc $\lambda_{x_4} = \lambda_{-x_4}$. Les relations $\chi_3(a) = 1$ et $\chi_4(a) = 1$ résultent alors des définitions de χ_3 et de χ_4. Comme M est acyclique pour l'involution ι, il suffit de démontrer l'égalité $\chi(a) = 1$ lorsque a est de la forme $[x] + \iota([x]) = [x] + [\frac{1}{x}]$. Or, dans ce cas, on a $\chi(a) = x\frac{1}{x} = 1$.

4.3 La détermination de la racine carrée de u

Démontrons le théorème 1. Reprenons les notations des sections 1.3 et 4.2. Alors

$$\mathcal{F} \;=\; -\sum_{x \in (\mathbf{Z}/p\mathbf{Z})^*} F(x)[x]$$

$$= \sum_{l=1}^{\frac{p-1}{2}} \sum_{h=1,h\neq l}^{\frac{p-1}{2}} [\frac{l-h}{l+h}] - \sum_{l=\frac{p+1}{2}}^{p-1} \sum_{h=1,h\neq p-l}^{\frac{p-1}{2}} [\frac{l-h}{l+h}]$$

est un élément de M. On a $\xi'(\mathcal{F}) = (p-1)\mathbf{e}$ (proposition 11). Posons

$$\mathcal{F}' = \sum_{l=1}^{\frac{p-1}{2}} \sum_{h=1,h\neq l}^{\frac{p-1}{2}} [\frac{l-h}{l+h}] = \sum_{x\in(\mathbf{Z}/p\mathbf{Z})^*} F'(x)[x].$$

L'élément $\mathcal{F}'$ appartient à M.

Lemme 10 *On a*

$$\mathcal{F}' - \iota(\mathcal{F}') = \mathcal{F},$$

et $F'(-x) = F'(x)$ *pour* $x \in (\mathbf{Z}/p\mathbf{Z})^* - \{1, -1\}$.

Démonstration.- La première égalité résulte facilement du calcul suivant

$$\iota(\mathcal{F}') = \sum_{l=1}^{\frac{p-1}{2}} \sum_{h=1,h\neq l}^{\frac{p-1}{2}} [\frac{l+h}{l-h}] = \sum_{l=1}^{\frac{p-1}{2}} \sum_{h=\frac{p+1}{2},h\neq p-l}^{p-1} [\frac{l-h}{l+h}].$$

La seconde égalité résulte de l'échange de l et h dans la formule qui définit $\mathcal{F}'$.

Si $p \in (3+4\mathbf{Z})$, $(\mathbf{Z}/p\mathbf{Z})^* - \{1, -1\}$ admet une partition en parties à 4 éléments de la forme $\{x, -x, \frac{1}{x}, -\frac{1}{x}\}$, et peut donc s'écrire $A \cup \iota(A)$, où A est disjoint de $\iota(A)$ et est stable par σ. Posons dans ce cas

$$\mathcal{G} = \sum_{x\in A} [x].$$

Si $p \in (1+4\mathbf{Z})$, posons

$$\mathcal{G} = 0.$$

Dans les deux cas $\mathcal{G}$ est un élément de M_σ et en particulier on a $\xi'(\mathcal{G}) = 0$.

Lemme 11 *Il existe* $\mathcal{F}_0 \in M$, $k_\sigma \in M_\sigma$, $k_\tau \in M_\tau$ *et* $k_+ \in M_+$ *tels que*

$$\mathcal{F}' = \nu\mathcal{F}_0 + 2k_\sigma + k_\tau + k_+ + \mathcal{G}.$$

Démonstration.- L'élément $\mathcal{F}'-\mathcal{G}-\iota(\mathcal{F}'-\mathcal{G})$ est égal à $\mathcal{F}-\sum_{x\in(\mathbf{Z}/p\mathbf{Z})^*-\{1,-1\}}[x]$ si $p\in(3+4\mathbf{Z})$, à $\mathcal{F}$ si $p\in(1+4\mathbf{Z})$. D'après le lemme 3, il appartient à $2M$. Il s'écrit donc $2\mathcal{F}_1$ avec $\mathcal{F}_1\in M$. Son image par ξ' est égale à $\xi'(\mathcal{F})$; c'est un élément de $\nu\mathrm{H}_1(X_0(p);\mathbf{Z})$ invariant par la conjugaison complexe. Comme $\mathrm{H}_1(X_0(p);\mathbf{Z})$ est acyclique, il peut s'écrire

$$\nu(\xi'(\mathcal{F}_0)+\overline{\xi'(\mathcal{F}_0)})=\nu\xi'(\mathcal{F}_0-\iota(\mathcal{F}_0)),$$

avec $\mathcal{F}_0\in M$. L'élément $\mathcal{F}_1-\frac{\nu}{2}(\mathcal{F}_0-\iota(\mathcal{F}_0))$ appartient au noyau de ξ'. Cet élément est antiinvariant par ι. Comme $\ker\xi'$ est acyclique pour ι (section 1.3), il existe $k\in\ker\xi'$ tel que

$$\mathcal{F}_1-\frac{\nu}{2}(\mathcal{F}_0-\iota(\mathcal{F}_0))=k-\iota(k).$$

En d'autres termes, $\mathcal{F}'-\mathcal{G}-\nu\mathcal{F}_0-2k$ appartient à M_+. On a $\ker\xi'=M_\sigma\oplus M_\tau$ (proposition 3). Par conséquent k est somme d'un élément k_σ de M_σ et d'un élément $k'=\frac{1}{2}k_\tau$ de M_τ. Cela prouve le lemme.

Conservons jusqu'à la fin de cette section les notations du lemme 11.

Lemme 12 *On a*

$$\sqrt{u}=\chi(\nu\mathcal{F}_0).$$

Démonstration.- On a

$$\xi'(k_\sigma)=\xi'(k_\tau)=\xi'(\mathcal{G})=0$$

et

$$\xi'(k_+)+\overline{\xi'(k_+)}=0,$$

d'où (lemmes 10 et 11)

$$\xi'(\mathcal{F}_0)+\overline{\xi'(\mathcal{F}_0)}=\frac{1}{\nu}(\xi'(\mathcal{F}')+\overline{\xi'(\mathcal{F}')})=\frac{1}{\nu}(\xi'(\mathcal{F}'-\iota(\mathcal{F}')))=\frac{1}{\nu}\xi'(\mathcal{F})=n\mathbf{e}.$$

On en déduit

$$\sqrt{u}=\theta(\xi'(\mathcal{F}_0))=\chi(\mathcal{F}_0)^\nu=\chi(\nu\mathcal{F}_0).$$

Lemme 13 *On a*

$$\chi(\mathcal{G})=(-1)^{\frac{p-3}{4}}$$

si $p\in(3+4\mathbf{Z})$ *et*

$$\chi(\mathcal{G})=1$$

si $p\in(1+4\mathbf{Z})$.

Démonstration.- Si $p \in (1+4\mathbf{Z})$, c'est évident. Si $p \in (3+4\mathbf{Z})$ l'ensemble $(\mathbf{Z}/p\mathbf{Z})^* - \{1,-1\}$ compte $p-3$ éléments. Comme $\mathcal{G}$ est la somme de la moitié des orbites de σ sur $(\mathbf{Z}/p\mathbf{Z})^* - \{1,-1\}$ et comme $\chi([x]+[x\sigma]) = -1$, on a la formule annoncée.

Lemme 14 *On a*

$$\chi(\mathcal{F}') = -2^{\frac{p-1}{2}} \prod_{l=1}^{\frac{p-1}{2}} l^{-4l}.$$

Démonstration.- On a dans $(\mathbf{Z}/p\mathbf{Z})^*$

$$\begin{aligned}
\chi(\mathcal{F}') &= \prod_{l=1}^{\frac{p-1}{2}} \prod_{h=1,h\neq l}^{\frac{p-1}{2}} \frac{l-h}{l+h} \\
&= \prod_{l=1}^{\frac{p-1}{2}} \frac{l!2l(l-1)!(\frac{p-1}{2}-l)!(-1)^{\frac{p-1}{2}-l}}{(\frac{p-1}{2}+l)!} \\
&= 2^{\frac{p-1}{2}} \prod_{l=1}^{\frac{p-1}{2}} (l!^2(\frac{p-1}{2}-l)!^2(-1)^{\frac{p-1}{2}-l}(-1)^{\frac{p-1}{2}-l+1}) \\
&= 2^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}} \prod_{l=1}^{\frac{p-1}{2}} \frac{l!^2(\frac{p+1}{2}-l)!^2}{(\frac{p+1}{2}-l)^2} \\
&= \frac{2^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}}}{(\frac{p-1}{2})!^2} \prod_{l=1}^{\frac{p-1}{2}} l!^4 \\
&= \frac{2^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}}}{(\frac{p-1}{2})!^2} \prod_{l=1}^{\frac{p-1}{2}} l^{-4l}.
\end{aligned}$$

On a $(\frac{p-1}{2})!^2 \equiv -(-1)^{\frac{p-1}{2}} \pmod{p}$. On en déduit le lemme.

Lemme 15 *On a*

$$\chi_3(\mathcal{G}) = \chi_4(\mathcal{G}) = 1.$$

Démonstration.- Si $p \in (1+4\mathbf{Z})$, on a $\mathcal{G} = 0$, d'où le lemme. Si $p \in (3+4\mathbf{Z})$, on $\chi_4(\mathcal{G}) = 1$ par définition de χ_4. Comme $\mathcal{G} \in M_\sigma$, on a $\chi_3(\mathcal{G}) = 1$ d'après le lemme 7.

Lemme 16 *On a*

$$\chi(2k_\sigma) = 1.$$

Démonstration.- Par application du lemme 7, on a $\chi(2k_\sigma) = \chi_4(2k_\sigma)$. On peut donc supposer $p \in (1+4\mathbf{Z})$. D'après les lemmes 6, 8, 9 et 15, on a

$$\chi_4(\nu\mathcal{F}_0) = \chi_4(k_+) = \chi_4(k_\tau) = \chi_4(\mathcal{G}) = 1.$$

On en déduit la relation

$$\chi_4(\mathcal{F}') = \chi_4(2k_\sigma).$$

On a, en utilisant le lemme 10,

$$\begin{aligned}
\chi_4(\mathcal{F}') &= x_4^{F'(x_4)-F'(-x_4)+\sum_{x\in[-x_4,x_4]} F'(x\sigma)-F'(x)} \\
&= x_4^{\sum_{x\in[-x_4,x_4]} F'(\iota(x))-F'(x)} \\
&= x_4^{\sum_{x\in[-x_4,x_4]} -F(x)} \\
&= x_4^{\sum_{x\in[0,x_4]} -2F(x)}.
\end{aligned}$$

D'après le lemme 3, on a $F(x) \equiv \frac{p-1}{2} \equiv 0 \pmod 2$. On en déduit le lemme.

Pour $x \in \mathbf{Z}/p\mathbf{Z}$, notons $R(x)$ le plus petit représentant ≥ 0 de x dans $\mathbf{Z}$.

Lemme 17 *On a*

$$\chi(k_\tau) = \prod_{x_3\in\mu_3'} \prod_{q=1}^{\frac{p-1}{2}} x_3^{R(qx_3)},$$

Démonstration.- On a (lemme 6)

$$\chi(k_\tau) = \chi_3(k_\tau).$$

D'après les lemmes 6, 8, 9 et 15, on a

$$\chi_3(\nu\mathcal{F}_0) = \chi_3(k_+) = \chi_3(2k_\sigma) = \chi_3(\mathcal{G}) = 1.$$

On en déduit la relation

$$\chi_3(\mathcal{F}') = \chi_3(k_\tau)^2.$$

Comme M_+ est dans le noyau de χ_3 (lemme 9), on a

$$\chi_3(\mathcal{F}) = \chi_3(\mathcal{F}' - \iota(\mathcal{F}')) = \chi_3(\mathcal{F}')^2 = \chi_3(k_\tau)^4 = \chi_3(k_\tau).$$

Calculons $\chi_3(\mathcal{F})$ en utilisant le lemme 3. On a

$$\begin{aligned}
\chi_3(\mathcal{F}) &= \prod_{x_3\in\mu_3'}\prod_{x\in[-x_3,x_3]} x_3^{-F(x)}\\
&= \prod_{x_3\in\mu_3'}\prod_{x\in[2,x_3]}\prod_{q=1}^{\frac{p-1}{2}} x_3^{[\frac{q(R(x)+1)}{p}]-[\frac{q(R(x)-1)}{p}]}\\
&= \prod_{x_3\in\mu_3'}\prod_{q=1}^{\frac{p-1}{2}} x_3^{[\frac{q(R(x_3)+1)}{p}]+[\frac{qR(x_3)}{p}]}\\
&= \prod_{x_3\in\mu_3'}\prod_{q=1}^{\frac{p-1}{2}} x_3^{[\frac{qR(x_3)}{p}]+(q-1)-[\frac{qR(x_3^2)}{p}]}\\
&= \prod_{x_3\in\mu_3'}\prod_{q=1}^{\frac{p-1}{2}} x_3^{-[\frac{qR(x_3)}{p}]}\\
&= \prod_{x_3\in\mu_3'}\prod_{q=1}^{\frac{p-1}{2}} x_3^{-qR(x_3)+R(qx_3)}\\
&= \prod_{x_3\in\mu_3'}\prod_{q=1}^{\frac{p-1}{2}} x_3^{R(qx_3)}.
\end{aligned}$$

Poursuivons la preuve du théorème 1. Posons

$$\zeta' = \prod_{x_3\in\mu_3'}\prod_{q=1}^{\frac{p-1}{2}} x_3^{R(qx_3)}.$$

On a

$$\sqrt{u} = \chi(\nu\mathcal{F}_0) = \chi(\mathcal{F}')\chi^{-1}(2k_\sigma)\chi^{-1}(k_\tau)\chi^{-1}(k_+)\chi^{-1}(\mathcal{G}).$$

On a (lemmes 9 et 16)

$$\chi(k_+) = \chi(2k_\sigma) = 1.$$

On a donc (lemmes 13, 14 et 17)

$$\sqrt{u} = -\zeta' 2^{\frac{p-1}{2}}\eta\prod_{l=1}^{\frac{p-1}{2}} l^{-4l},$$

où $\eta = (-1)^{\frac{p-3}{4}}$ si $p \in (3+4\mathbf{Z})$ et $\eta = 1$ si $p \in (1+4\mathbf{Z})$. On a $2^{\frac{p-1}{2}} \equiv 1 \pmod p$ si $p \in (1+8\mathbf{Z})$ ou $p \in (-1+8\mathbf{Z})$ et $2^{\frac{p-1}{2}} \equiv -1 \pmod p$ sinon. En examinant les congruences possibles de p modulo 8 on constate que $-\eta 2^{\frac{p-1}{2}}$ est égal à 1 sauf si $p \in (1+8\mathbf{Z})$ auquel cas on a $-\eta 2^{\frac{p-1}{2}} = -1$. Cela prouve le théorème 1 à la détermination de la racine cubique ζ' près.

4.4 La détermination de la racine cubique

On se place dans cette section dans le cas $p \in (1+3\mathbf{Z})$. Pour $x \in \mathbf{Z}/p\mathbf{Z}$, rappelons que nous notons $R(x)$ le plus petit représentant ≥ 0 de x. Fixons x_3 une racine cubique primitive de l'unité dans $\mathbf{Z}/p\mathbf{Z}$. Posons $\bar{x}_3 = x_3^2$. Nous allons prouver que la racine cubique ζ' de la section précédente est égale à la racine cubique ζ de l'introduction.

Proposition 13 *On a dans* $\mathbf{Z}/p\mathbf{Z}$

$$2^{\frac{p-1}{3}} = \prod_{l=1}^{\frac{p-1}{2}} x_3^{R(lx_3)} \prod_{l=1}^{\frac{p-1}{2}} \bar{x}_3^{R(l\bar{x}_3)}.$$

Démonstration.- Nous allons d'abord examiner le membre de gauche de l'égalité ci-dessus. Pour $(u,v,w) \in (\mathbf{Z}/6\mathbf{Z})^3$, posons

$$A(u,v,w) = \{a \in (\mathbf{Z}/p\mathbf{Z})^* / (R(a), R(ax_3), R(a\bar{x}_3)) \in u \times v \times w\}.$$

Remarquons qu'on a $R(a) + R(ax_3) + R(a\bar{x}_3) = p$ ou $2p$. Si $u+v+w \neq 1$ ou 2, on a donc $A(u,v,w) = \emptyset$. Posons

$$A = \cup_{(u,v,w) \in \{1,2,4,5\} \times \{0,1,3,4\} \times \{0,2,3,5\}} A(u,v,w).$$

Lemme 18 *Les ensembles* A, x_3A *et* $\bar{x}_3A$ *forment une partition de* $(\mathbf{Z}/p\mathbf{Z})^*$.

Démonstration.- L'ensemble A est formé des éléments a de $(\mathbf{Z}/p\mathbf{Z})^*$ vérifiant $R(a) \equiv 1$ ou $-1 \pmod 3$, $R(ax_3) \equiv 0$ ou $1 \pmod 3$ et $R(a\bar{x}_3) \equiv -1$ ou $0 \pmod 3$. Comme $R(a) + R(ax_3) + R(a\bar{x}_3) \equiv 1$ ou $-1 \pmod 3$, $(R(a), R(ax_3), R(a\bar{x}_3))$ est congru à l'un des triplets suivants modulo 3 : $(1,0,0)$, $(1,1,0)$, $(1,1,-1)$, $(-1,0,0)$, $(-1,0,-1)$, $(-1,1,-1)$. A permutation circulaire près c'est l'ensemble des triplets (u,v,w) vérifiant $u+v+w = 1$ ou -1. L'ensemble x_3A (resp. $\bar{x}_3A$) est défini par $(R(ax_3), R(a\bar{x}_3), R(a))$ (resp. $(R(a\bar{x}_3), R(a), R(ax_3))$) vérifiant les mêmes congruences. Après permutation circulaire dans les triplets ci-dessus, on obtient une partition de

l'ensemble des éléments (x, y, z) de $(\mathbf{Z}/3\mathbf{Z})^3$ vérifiant $x + y + z = 1$ ou -1. On en déduit le lemme.

Pour $x \in (\mathbf{Z}/p\mathbf{Z})^*$ notons $\epsilon(x)$ l'unique élément de $\{1, x_3, \bar{x}_3\}$ vérifiant $x \in \epsilon(x)A$.

Lemme 19 *Soit $x \in (\mathbf{Z}/p\mathbf{Z})^*$. On a*

$$x^{\frac{p-1}{3}} = \prod_{a \in A} \epsilon(xa).$$

Démonstration.- On a

$$x^{\frac{p-1}{3}} \prod_{a \in A} a = \prod_{a \in A} ax = \prod_{a \in A} a \prod_{a \in A} \epsilon(xa).$$

On en déduit le lemme.

Par conséquent on a

$$2^{\frac{p-1}{3}} = \prod_{a \in A} \epsilon(2a).$$

On a

$$2A = \cup_{(u,v,w) \in \{1,2,3,4\} \times \{0,1,2,5\} \times \{0,3,4,5\}} A(u, v, w).$$

On a donc

$$2^{\frac{p-1}{3}} = x_3^{|x_3 A \cap 2A|} \bar{x}_3^{|\bar{x}_3 A \cap 2A|}.$$

En comparant les définitions de $x_3 A$, de $\bar{x}_3 A$ et de $2A$ on obtient

$$\begin{array}{rcl} x_3 A \cap 2A & = & \cup_{(u,v,w) \in \{1,3,4\} \times \{0,2,5\} \times \{4,5\}} A(u, v, w) \\ \bar{x}_3 A \cap 2A & = & \cup_{(u,v,w) \in \{2,3\} \times \{1,2,5\} \times \{0,3,4\}} A(u, v, w) \end{array}$$

Pour $(u, v, w) \in (\mathbf{Z}/6\mathbf{Z})^3$, posons

$$\eta(u, v, w) = x_3^{|A(u,v,w)|} \bar{x}_3^{|A(u,w,v)|}.$$

Lemme 20 *Pour $(u, v, w) \in (\mathbf{Z}/6\mathbf{Z})^3$, La fonction η est invariante (resp. transformée en son inverse) par permutation paire (resp. impaire) de ses arguments. Si u, v et w ne sont pas deux à deux distincts ou si $u+v+w \neq 1$ ou 2, on a $\eta(u, v, w) = 1$. On a de plus*

$$\eta(u, v, w) = \eta(1 - u, 1 - v, 1 - w).$$

Démonstration.- Seule la dernière identité est non trivialement satisfaite. Elle provient de la bijection entre $A(u,v,w)$ et $A(1-u,1-v,1-w)$ donnée par $a \mapsto p-a$.

En transformant $\bar{x}_3 A \cap 2A$ par $a \mapsto p-a$, puis par $a \mapsto \bar{x}_3 a$ on obtient que le cardinal de $\bar{x}_3 A \cap 2A$ est égal au cardinal de

$$\cup_{(u,v,w)\in\{1,4,3\}\times\{0,5,2\}\times\{5,4\}} A(u,v,w).$$

Compte-tenu de la nécessaire congruence $R(y) + R(yx_3) + R(y\bar{x}_3) \equiv 1$ ou $2 \pmod 6$, $2^{\frac{p-1}{3}}$ est égal au produit des valeurs de η calculées en les triplets suivants $(1,2,4)$, $(1,2,5)$, $(3,0,4)$, $(3,0,5)$, $(3,5,5)$, $(4,0,4)$, $(4,5,5)$, $(4,5,4)$. En utilisant les relations vérifiées par η énoncées dans le lemme précédent on obtient

$$\begin{aligned} 2^{\frac{p-1}{3}} &= \eta(1,2,4)\eta(3,0,5)\eta(1,2,5)\eta(3,0,4) \\ &= \eta(2,0,5)\eta^2(1,2,4)\eta(3,4,1) \\ &= \eta(2,0,5)\eta(2,1,4)\eta(4,1,3). \end{aligned}$$

Venons-en au second membre de l'égalité figurant dans l'identité que nous voulons démontrer. On a

$$\prod_{l=1}^{\frac{p-1}{2}} x_3^{R(lx_3)} \prod_{l=1}^{\frac{p-1}{2}} \bar{x}_3^{R(l\bar{x}_3)} = x_3^{r_1+r_2}\bar{x}_3^{s_1+s_2},$$

où r_1 (resp. r_2) est le nombre d'éléments l de $(\mathbf{Z}/p\mathbf{Z})^*$ tels que $R(l) < \frac{p}{2}$ et $R(lx_3) \equiv 1 \pmod 3$ (resp. $R(l\bar{x}_3) \equiv -1 \pmod 3$) et où s_1 et s_2 sont définis par les mêmes conditions que r_1 et r_2 en échangeant les rôles joués par x_3 et $\bar{x}_3$. Cela se réécrit en posant $q = 2l$: r_1 (resp. r_2) est le nombre d'éléments q de $(\mathbf{Z}/p\mathbf{Z})^*$ tels que $R(q) \equiv 0 \pmod 2$ et $R(qx_3) \equiv 1$ ou $2 \pmod 6$ (resp. $R(q\bar{x}_3) \equiv 3$ ou $4 \pmod 6$). Par conséquent $x_3^{r_1+r_2}\bar{x}_3^{s_1+s_2}$ est le produit des valeurs de η calculées en les triplets (u,v,w) suivants (compte-tenu de la relation nécessaire $u+v+w=1$ ou 2) : $(0,1,0)$, $(0,1,1)$, $(0,2,0)$, $(0,2,5)$, $(2,1,4)$, $(2,1,5)$, $(2,2,3)$, $(2,2,4)$, $(4,1,2)$, $(4,1,3)$, $(4,2,1)$, $(4,2,2)$, $(0,4,3)$, $(0,3,4)$, $(0,5,3)$, $(0,4,4)$, $(2,2,3)$, $(2,3,3)$, $(2,1,4)$, $(2,2,4)$, $(4,0,3)$, $(4,1,3)$, $(4,5,4)$, $(4,0,4)$. En éliminant d'abord les triplets formés de trois éléments non deux à deux distincts, puis en appliquant les relations satisfaites par η on trouve

$$\prod_{l=1}^{\frac{p-1}{2}} x_3^{R(lx_3)} \prod_{l=1}^{\frac{p-1}{2}} \bar{x}_3^{R(l\bar{x}_3)} = \eta(0,2,5)\eta(2,1,4)^2\eta(2,1,5)\eta(4,1,3)^2\eta(0,5,3)\eta(4,0,5)$$

$$
\begin{aligned}
&= \eta(0,2,5)^2\eta(2,1,4)\eta(4,1,3)\\
&= \eta(2,0,5)\eta(2,1,4)\eta(4,1,3)\\
&= 2^{\frac{p-1}{3}}.
\end{aligned}
$$

Cela prouve la proposition 13 et achève de prouver le théorème 1.

5 Application à l'étude de l'idéal d'Eisenstein

5.1 L'idéal d'Eisenstein de l'algèbre de Hecke

Soit l un nombre premier différent de p. On a deux morphismes de dégénérescence $X_0(pl) \to X_0(p)$. Le premier associe à $\Gamma_0(pl)z$ le point $\Gamma_0(p)z$, le second associe à $\Gamma_0(pl)z$ le point $\Gamma_0(p)lz$. La correspondance composée du premier morphisme avec la correspondance inverse du second morphisme est la correspondance de Hecke, notée T_l, de $X_0(p)$. Cette correspondance définit un endomorphisme encore noté T_l sur $J_0(p)$ (les opérateurs obtenus en considérant les fonctorialités de Picard et d'Albanese sont identiques). Considérons l'involution W_p de $X_0(p)$ qui à $\Gamma_0(p)z$ associe $\Gamma_0(p)\frac{-1}{pz}$. Elle définit une involution de $J_0(p)$ encore notée W_p. *L'algèbre de Hecke* $\mathbf{T}$ est par définition la sous-algèbre commutative de $\mathrm{End}(J_0(p))$ engendrée par les opérateurs de Hecke T_l ($l \neq p$) et l'involution W_p. Elle est égale à $\mathrm{End}(J_0(p))$ ([7], proposition II.9.5).

Considérons l'idéal de $\mathbf{T}$ engendré par les $1 + l - T_l$ (l nombre premier différent de p) et $1 + W_p$. C'est *l'idéal d'Eisenstein* $\mathfrak{I}$ de $\mathbf{T}$. On a $\mathbf{T}/\mathfrak{I} \simeq \mathbf{Z}/n\mathbf{Z}$ ([7], proposition II.9.7), où n est, comme dans l'introduction, le numérateur de $(p-1)/12$.

Rappelons que $\mathrm{H}_1(X_0(p);\mathbf{Z})_-$ désigne le sous-groupe de $\mathrm{H}_1(X_0(p);\mathbf{Z})$ formé des éléments antiinvariants par la conjugaison complexe et que $\mathbf{e}$ désigne l'élément d'enroulement de $\frac{1}{n}\mathrm{H}_1(X_0(p);\mathbf{Z})$ (voir section 3.2).

Comme $\mathrm{H}_1(X_0(p);\mathbf{R})$ s'interprète comme l'espace tangent en 0 de $J_0(p)$, on a une action de $\mathbf{T}$ sur $\mathrm{H}_1(X_0(p);\mathbf{R})$. Cette action coïncide avec l'action provenant fonctoriellement des correspondances T_l et W_p. Elle commute à l'action de la conjugaison complexe.

L'homomorphisme de groupes $\theta : \mathrm{H}_1(X_0(p);\mathbf{Z}) \to U$, défini dans la section 3.3, est surjectif. Le lemme 18.7 de [7] affirme que le noyau de θ est égal à $\mathrm{H}_1(X_0(p);\mathbf{Z})_- + \mathfrak{I}\mathrm{H}_1(X_0(p);\mathbf{Z})$. Le fait que ce noyau contienne $\mathrm{H}_1(X_0(p);\mathbf{Z})_-$ n'apparait pas clairement dans la démonstration de Mazur. Cela résulte directement de l'acyclicité de $\mathrm{H}_1(X_0(p);\mathbf{Z})$ vis-à-vis de la conjugaison complexe (proposition 5).

Mazur définit l'homomorphisme d'enroulement ([7], section II.18)

$$\begin{array}{rcl} w_+ \ : \ \mathfrak{I} & \to & \mathrm{H}_1(X_0(p);\mathbf{Z})_+ \\ t & \mapsto & t\mathbf{e}. \end{array}$$

Pour l nombre premier $\neq p$, on a

$$(1+l-T_l)\mathbf{e} = -\sum_{k=1}^{l-1}\{0,\frac{k}{l}\} \quad \text{et} \quad (1+W_p)\mathbf{e} = 0.$$

Cela se déduit de calculs élémentaires sur les symboles modulaires (voir [6], Théorème 3.3). On en déduit les égalités, pour $l \neq 2$,

$$(1+l-T_l)\mathbf{e} = -2\sum_{k=1}^{\frac{l-1}{2}}\{0,\frac{k}{l}\} + \sum_{k=1}^{\frac{l-1}{2}}(\{0,\frac{k}{l}\} - \{0,-\frac{k}{l}\}).$$

La seconde somme est antiinvariante par la conjugaison complexe. On en déduit les égalités, en notant θ_+ l'homomorphisme défini dans la section 4.1, (pour $l \neq 2$)

$$\theta_+ \circ w_+(1+l-T_l) = l^{-\nu(\frac{l-1}{2})} \quad \text{et} \quad \theta_+ \circ w_+(1+W_p) = 1,$$

(voir [7], lemme II.18.7, proposition II.18.8 et proposition II.18.9).

L'homomorphisme $\theta_+ \circ w_+$ est surjectif. En effet, soit l un nombre premier impair dont la réduction modulo p engendre $(\mathbf{Z}/p\mathbf{Z})^*$ et tel que $(l-1)/2$ soit premier à $p-1$. Il en existe d'après le théorème de Dirichlet. Alors $\theta_+ \circ w_+(1+l-T_l)$ engendre U.

Le noyau de $\theta_+ \circ w_+$ est égal à $\mathfrak{I}^2$, cela résulte de [7], théorème II.18.10 et proposition II.18.9. On déduit de $\theta_+ \circ w_+$, par passage aux quotients, un isomorphisme de groupes

$$\mathfrak{I}/\mathfrak{I}^2 \simeq U.$$

On a

$$\sqrt{u} = \theta_+ \circ w_+(n).$$

Soit q un nombre premier divisant n. Considérons l'idéal $\mathfrak{q}$ de $\mathbf{T}$ engendré par $\mathfrak{I}$ et q. C'est un idéal premier. Posons

$$\mathbf{T}_\mathfrak{q} = \lim_{\leftarrow} \mathbf{T}/\mathfrak{q}^i\mathbf{T}.$$

L'anneau $\mathbf{T}_\mathfrak{q}$ est muni d'une structure naturelle de $\mathbf{Z}_q$ module libre de rang fini.

Démontrons le théorème 2.

Supposons d'abord que $\sqrt{u}$ engendre la composante q-primaire de U. L'homomorphisme de groupe $\theta_+ \circ w_+$ définit par passage aux quotients un isomorphisme de groupes entre $\mathfrak{I}/\mathfrak{q}\mathfrak{I}$ et U/U^q, donc le groupe $\mathfrak{I}/\mathfrak{q}\mathfrak{I}$ est engendré par l'image de n. Comme $q|n$, et que l'on a $\mathfrak{q} = q\mathbf{T} + \mathfrak{I}$, le $\mathbf{T}$-module $\mathfrak{q}/\mathfrak{q}^2$ est engendré par $q + \mathfrak{q}^2$. Comme $\mathbf{T}/\mathfrak{q}$ est isomorphe à $\mathbf{Z}/q\mathbf{Z}$ (c'est un résultat facile qu'on peut établir indépendamment de [7]), $\mathfrak{q}/\mathfrak{q}^2$ est cyclique d'ordre q. Par conséquent $\mathbf{T}_\mathfrak{q}$ est isomorphe à $\mathbf{Z}_q$.

Réciproquement, supposons que $\mathbf{T}_\mathfrak{q}$ soit isomorphe à $\mathbf{Z}_q$. Comme l'anneau $\mathbf{T}/\mathfrak{I}$ est isomorphe à $\mathbf{Z}/n\mathbf{Z}$, l'anneau $\mathbf{T}_\mathfrak{q}/\mathfrak{I}\mathbf{T}_\mathfrak{q}$ est isomorphe à $\mathbf{Z}/q^a\mathbf{Z}$, où q^a est la plus grande puissance de q qui divise n. Dans ces conditions $\mathfrak{I}\mathbf{T}_\mathfrak{q}$ s'identifie à l'idéal $q^a\mathbf{Z}_q = n\mathbf{Z}_q$ de $\mathbf{Z}_q$. Par suite le groupe $\mathfrak{I}/\mathfrak{q}\mathfrak{I}$, qui est cyclique d'ordre q, est engendré par l'image canonique de n. On en déduit que U/U^q est engendré par l'image de $\sqrt{u}$.

Comme $(\sqrt{u})^2 = u$, on obtient immédiatement le corollaire suivant qui est la proposition II.19.2 de [7].

Corollaire 5 *Soit q un nombre premier impair divisant n. L'anneau $\mathbf{T}_\mathfrak{q}$ est isomorphe à $\mathbf{Z}_q$ si et seulement si u engendre la composante q-primaire de U.*

Remarque.- Comme u est le carré d'un élément de U, il ne peut engendrer la composante 2-primaire de U si cette composante est non triviale. Comme les accouplements de Weil sont des formes bilinéaires alternées, le fait que u soit le carré d'un élément de U peut se déduire de ce que, si $2|n$, les sous-groupes $\Sigma(p)$ et $C(p)$ de $J_0(p)$ ont un point d'ordre 2 en commun.

5.2 Calcul de la racine de u modulo les puissances q-ièmes

Lemme 21 *Soit a un entier naturel $< p/2$. On a*

$$(2a)!\,(\frac{p-1}{2})! \equiv a!\,(\frac{p-1}{2}+a)!\,2^{2a} \pmod{p}.$$

Démonstration.- On a dans $\mathbf{Z}/p\mathbf{Z}$

$$\begin{aligned} a!\,(\frac{p-1}{2}+a)!\,2^{2a} &= (\frac{p-1}{2})! \prod_{0<k\leq a} 2k \prod_{0<k\leq a} 2(k+\frac{p-1}{2}) \\ &= (\frac{p-1}{2})! \prod_{0<k\leq 2a, k\in 2\mathbf{Z}} k \prod_{0<k\leq 2a, k\in 2\mathbf{Z}} (p-1+k) \end{aligned}$$

$$\equiv \quad (\frac{p-1}{2})!\,(2a)! \pmod p.$$

Rappelons que $(\frac{p-1}{2})!$ est une racine quatrième de l'unité modulo p vérifiant

$$(\frac{p-1}{2})!^{\,2} = -(-1)^{\frac{p-1}{2}}.$$

Proposition 14 *Soit q un nombre impair > 0 divisant n. Notons u_q l'élément de $\mathbf{Z}/p\mathbf{Z}$ défini par*

$$\prod_{k=1}^{q-1}(k\frac{p-1}{q})!^{\,6k}.$$

Alors $u_q\sqrt{u}$ est une puissance q-ième de $\mathbf{Z}/p\mathbf{Z}$.

Démonstration.- Pour $0 < i < q$, posons

$$b_i = \prod_{0<l<p/2, l\equiv i \pmod q} l.$$

On a

$$\sqrt{u} \equiv \zeta \prod_{i=1}^{q-1} b_i^{-4i} \pmod{(\mathbf{Z}/p\mathbf{Z})^{*q}}.$$

Pour $0 \leq j < q$, posons

$$\begin{aligned} a_j &= \prod_{\frac{jp}{2q}<l<(j+1)p/2q} l \\ &= \frac{((j+1)\frac{p-1}{2q})!}{(j\frac{p-1}{2q})!}. \end{aligned}$$

On a

$$\begin{aligned} q^{\frac{p-1}{2q}} a_j &\equiv \prod_{\frac{jp}{2q}<l<(j+1)p/2q} ql \pmod p \\ &\equiv \prod_{\frac{jp}{2}<x<(j+1)p/2, x\equiv 0 \pmod q} x \pmod p. \end{aligned}$$

Si $j = 2k$, on déduit de l'égalité précédente

$$q^{\frac{p-1}{2q}} a_j \equiv \prod_{0<x<p/2, x\equiv -k \pmod q} x \pmod p$$

$$\equiv \quad b_{q-k} \pmod p.$$

Si $j = 2k-1$, on obtient de façon analogue

$$q^{\frac{p-1}{2q}} a_j \equiv (-1)^{\frac{p-1}{2q}} b_k \pmod p.$$

Introduisons ces expressions dans la formule de $\sqrt{u}$ modulo $(\mathbf{Z}/p\mathbf{Z})^{*q}$ ci-dessus. On a les congruences modulo les puissances q-ièmes de $(\mathbf{Z}/p\mathbf{Z})^*$

$$\begin{aligned}
\prod_{i=1}^{q-1} b_i^i &\equiv \prod_{k=1}^{\frac{q-1}{2}} ((-q)^{\frac{p-1}{2q}} a_{2k-1})^k \prod_{k=1}^{\frac{q-1}{2}} (q^{\frac{p-1}{2q}} a_{2k})^{q-k} \\
&\equiv \prod_{k=1}^{\frac{q-1}{2}} (\frac{a_{2k-1}}{a_{2k}})^k \\
&\equiv \prod_{k=1}^{\frac{q-1}{2}} (\frac{(2k\frac{p-1}{2q})!^{\,2}}{((2k-1)\frac{p-1}{2q})!\,((2k+1)\frac{p-1}{2q})!})^k \\
&\equiv \prod_{k=1}^{\frac{q-1}{2}} \frac{(2k\frac{p-1}{2q})!^{\,2k}}{((2k-1)\frac{p-1}{2q})!^{\,2k-1}} \\
&\equiv \prod_{k=1}^{\frac{q-1}{2}} (2k\frac{p-1}{2q})!^{\,2k} ((q-2k)\frac{p-1}{2q})!^{\,2k-q} \\
&\equiv \prod_{k=1}^{\frac{q-1}{2}} ((k\frac{p-1}{q})!\,(\frac{p-1}{2} - k\frac{p-1}{q})!\,)^{2k}.
\end{aligned}$$

En utilisant le lemme 21 et la relation

$$((\frac{p-1}{2} - k\frac{p-1}{q})!\,(\frac{p-1}{2} + k\frac{p-1}{q})!\,)^2 \equiv 1 \pmod p,$$

on obtient la congruence suivante modulo les puissances q-ièmes de $(\mathbf{Z}/p\mathbf{Z})^*$

$$\prod_{i=1}^{q-1} b_i^i \equiv \prod_{k=1}^{\frac{q-1}{2}} (k\frac{p-1}{q})!^{\,2k} ((k\frac{p-1}{q})!^{\,2k} 2^{4\frac{p-1}{q}k^2} / (2k\frac{p-1}{q})!^{\,2k}).$$

Utilisons la relation

$$\sum_{k=1}^{\frac{q-1}{2}} 4k^2 \frac{p-1}{q} = \frac{(q^2-1)(p-1)}{6},$$

et, pour $k > \frac{q}{4}$, la relation

$$(2k\frac{p-1}{q})! \equiv (p-1-2k\frac{p-1}{q})! \pmod p.$$

On obtient les congruences modulo les puissances q-ièmes de $(\mathbf{Z}/p\mathbf{Z})^*$

$$\begin{aligned}\prod_{i=1}^{q-1} b_i^i &\equiv 2^{\frac{(q^2-1)(p-1)}{6}} \prod_{k=1}^{\frac{q-1}{2}} (k\frac{p-1}{q})!^{\,4k} \prod_{k=1}^{\frac{q-1}{2}} (k\frac{p-1}{q})!^{\,-k} \\ &\equiv 2^{\frac{(q^2-1)(p-1)}{6}} \prod_{k=1}^{\frac{q-1}{2}} (k\frac{p-1}{q})!^{\,3k}\end{aligned}$$

Remarquons que, modulo les puissances q-ièmes de $(\mathbf{Z}/p\mathbf{Z})^*$, $2^{\frac{(q^2-1)(p-1)}{6}}$ est congru à $2^{\frac{p-1}{3}}$ si $3|q$ et à 1 sinon ou encore est congru à ζ (cf théorème 1). De plus on a les congruences modulo les puissances q-ièmes de $(\mathbf{Z}/p\mathbf{Z})^*$

$$\begin{aligned}\prod_{k=1}^{\frac{q-1}{2}} (k\frac{p-1}{q})!^{\,12k} &\equiv \prod_{k=1}^{\frac{q-1}{2}} (k\frac{p-1}{q})!^{\,6k} \prod_{k=\frac{q+1}{2}}^{q-1} (p-1-k\frac{p-1}{q})!^{\,6(q-k)} \\ &\equiv \prod_{k=1}^{\frac{q-1}{2}} (k\frac{p-1}{q})!^{\,6k} \prod_{k=\frac{q+1}{2}}^{q-1} (k\frac{p-1}{q})!^{\,6k} \\ &\equiv \prod_{k=1}^{q-1} (k\frac{p-1}{q})!^{\,6k}.\end{aligned}$$

On en déduit le lemme.

Corollaire 6 *Soit q un nombre premier impair divisant n. Alors $\mathbf{T}_{q\mathbf{T}+\mathfrak{I}}$ est isomorphe à $\mathbf{Z}_q$ si et seulement si*

$$\prod_{k=1}^{q-1} (k\frac{p-1}{q})!^{\,k}$$

n'est pas une puissance q-ième modulo p.

Démonstration.- Cela résulte directement de la proposition 14 et du théorème 2 si $q > 3$. Si $q = 3$, alors on a $p \in (1 + 9\mathbf{Z})$. D'après la proposition 14 et le théorème 2, $\mathbf{T}_{3\mathbf{T}+\mathfrak{I}}$ est isomorphe à $\mathbf{Z}_3$ si et seulement si $\prod_{k=1}^{2}(k\frac{p-1}{3})!^{\,6k}$

n'est pas une puissance neuvième de $\mathbf{Z}/p\mathbf{Z}$, ou encore si et seulement si $\prod_{k=1}^{2}(k\frac{p-1}{3})!^{\,k}$ n'est pas un cube de $\mathbf{Z}/p\mathbf{Z}$.

Remarque.- On peut remplacer dans le corollaire 6 et dans la proposition 14 l'expression

$$\prod_{k=1}^{q-1}(k\frac{p-1}{q})!^{\,k} \quad \text{par} \quad \prod_{k=1}^{\frac{q-1}{2}}(k\frac{p-1}{q})!^{\,2k}.$$

L'expression alors obtenue est plus utile pour obtenir des critères dans des cas particuliers comme ci-dessous.

Exemple.- 1) Supposons que $p \in (1+5\mathbf{Z})$. Par application du corollaire 6, $\mathbf{T}_{5\mathbf{T}+\mathfrak{J}}$ est isomorphe à $\mathbf{Z}_5$ si et seulement si

$$(\frac{p-1}{5})!\,(2\frac{p-1}{5})!^{\,2}$$

n'est pas une puissance 5-ième modulo p, ou encore, après élévation au cube, si et seulement si

$$(2\frac{p-1}{5})!\,/(\frac{p-1}{5})!^{\,2}$$

n'est pas une puissance 5-ième modulo p.

2) Supposons qu'on ait $p \in (1+9\mathbf{Z})$, $\mathbf{T}_{3\mathbf{T}+\mathfrak{J}}$ est isomorphe à $\mathbf{Z}_3$ si et seulement si

$$(\frac{p-1}{3})!$$

n'est pas un cube modulo p. Cela résulte du corollaire 6 et de la remarque qui suit.

Jusqu'à la fin de cette section, plaçons-nous dans la situation $p \in (1+8\mathbf{Z})$ (i.e. l'ordre de U est pair).

Proposition 15 *Supposons qu'on ait $p \in (9+16\mathbf{Z})$ (resp. $p \in (1+16\mathbf{Z})$). L'anneau $\mathbf{T}_{2\mathbf{T}+\mathfrak{J}}$ est isomorphe à $\mathbf{Z}_2$ si et seulement si $(\frac{p-1}{4})!$ est (resp. n'est pas) un carré modulo p.*

Démonstration.- D'après le théorème 2, $\mathbf{T}_{2\mathbf{T}+\mathfrak{J}}$ est isomorphe à $\mathbf{Z}_2$ si et seulement si $\sqrt{u}$ n'est pas un carré de U, i.e. si et seulement si $\sqrt{u}$ n'est pas une puissance huitième de $\mathbf{Z}/p\mathbf{Z}$, ou encore d'après le théorème 1 si et seulement si $-\prod_{l=1}^{\frac{p-1}{2}} l^{4l}$ n'est pas une puissance huitième de $\mathbf{Z}/p\mathbf{Z}$.

On a

$$\begin{aligned}
-\prod_{l=1}^{\frac{p-1}{2}} l^{4l} &\equiv -\prod_{l=1, l\in(1+2\mathbf{Z})}^{\frac{p-1}{2}} l^4 \pmod{((\mathbf{Z}/p\mathbf{Z})^*)^8} \\
&\equiv -\frac{(\frac{p-1}{2})!^4}{(2^{\frac{p-1}{4}})^4(\frac{p-1}{4})!^4} \pmod{((\mathbf{Z}/p\mathbf{Z})^*)^8} \\
&\equiv -(\frac{p-1}{4})!^4 \pmod{((\mathbf{Z}/p\mathbf{Z})^*)^8}
\end{aligned}$$

Si $p \in (9+16\mathbf{Z})$ (resp. $p \in (1+16\mathbf{Z})$) alors -1 est une puissance quatrième qui n'est pas (resp. est) une puissance huitième modulo p. Par conséquent $\mathbf{T}_{2\mathbf{T}+\mathfrak{J}}$ est isomorphe à $\mathbf{Z}_2$ si et seulement $(\frac{p-1}{4})!$ est (resp. n'est pas) un carré modulo p.

Prouvons maintenant le théorème 3. Rappelons qu'on a $p \in (1+8\mathbf{Z})$.

D'après [4] les conditions *iii)* et *iv)* sont équivalentes. D'après [1] les conditions *iv)*, *v)*, *vi)* et *viii)* sont équivalentes. Le théorème 3, dont la preuve se rapporte maintenant à l'équivalence des conditions *i)*, *ii)* et *iii)*, résulte de la proposition 15 combinée avec le lemme suivant dont l'énoncé et la démonstration m'ont été communiqués par Oesterlé.

Lemme 22 *Si $p \in (1+16\mathbf{Z})$ (resp. $p \in (9+16\mathbf{Z})$), 8 divise le nombre de classes h de $\mathbf{Q}(\sqrt{-p})$ si et seulement si $(\frac{p-1}{4})!$ est (resp. n'est pas) un carré modulo p.*

Démonstration.- D'après le théorème 3 de [2], section V.4, on a

$$h = \frac{1}{2} \sum_{0<x<2p, x\in(1+2\mathbf{Z})} (-1)^{\frac{x-1}{2}} \left(\frac{x}{p}\right),$$

où $\left(\frac{\cdot}{p}\right)$ est le symbole de Legendre modulo p. On a donc

$$\begin{aligned}
h &= \frac{1}{2}\Big(\sum_{0<x<p, x\in(1+2\mathbf{Z})} (-1)^{\frac{x-1}{2}} \left(\frac{x}{p}\right) + \sum_{0<x<p, x\in 2\mathbf{Z}} (-1)^{\frac{x}{2}} \left(\frac{x}{p}\right)\Big) \\
&= \frac{1}{2} \sum_{x=1}^{p-1} \epsilon(x) \left(\frac{x}{p}\right)
\end{aligned}$$

où $\epsilon(x) = 1$ (resp. $\epsilon(x) = -1$) si x est congru à 0 ou 1 (resp. 2 ou 3) modulo 4. Comme $p \in (1+4\mathbf{Z})$, on a $\left(\frac{-1}{p}\right) = 1$. On en déduit la formule

$$h = \sum_{0<x<p, x\in 4\mathbf{Z}} \left(\frac{x}{p}\right) - \sum_{0<x<p, x\in(2+4\mathbf{Z})} \left(\frac{x}{p}\right)$$

$$= \Big(\frac{2}{p}\Big)\Big(\sum_{0<x<p/2, x\in 2\mathbf{Z}}\Big(\frac{x}{p}\Big) - \sum_{0<x<p/2, x\in(1+2\mathbf{Z})}\Big(\frac{x}{p}\Big)\Big).$$

Or on a

$$\sum_{x=1}^{\frac{p-1}{2}}\Big(\frac{x}{p}\Big) = \frac{1}{2}\sum_{x=1}^{\frac{p-1}{2}}\Big(\Big(\frac{x}{p}\Big) + \Big(\frac{p-x}{p}\Big)\Big) = \frac{1}{2}\sum_{x=1}^{p-1}\Big(\frac{x}{p}\Big) = 0.$$

On en déduit

$$\begin{aligned} h &= \Big(\frac{2}{p}\Big)2\sum_{0<x<p/2, x\in 2\mathbf{Z}}\Big(\frac{x}{p}\Big) \\ &= 2\Big(\frac{2}{p}\Big)^2\sum_{0<x<p/4}\Big(\frac{x}{p}\Big) \\ &= 2\sum_{0<x<p/4}\Big(\frac{x}{p}\Big). \end{aligned}$$

On a les congruences suivantes modulo 4

$$\begin{aligned} \Big(\frac{(\frac{p-1}{4})!}{p}\Big) &\equiv \prod_{0<x<p/4}\Big(\frac{x}{p}\Big) \\ &\equiv \prod_{0<x<p/4}\Big(1 + \Big(\Big(\frac{x}{p}\Big) - 1\Big)\Big) \\ &\equiv 1 + \sum_{0<x<p/4}\Big(\Big(\frac{x}{p}\Big) - 1\Big) \\ &\equiv 1 + \frac{1}{2}h - \frac{p-1}{4}. \end{aligned}$$

On en déduit le lemme.

Remarque.- Soit p un nombre premier de la forme $p = t^2 + 64$ avec $t \in \mathbf{Z}$. D'après le théorème 3, $\mathbf{T}_{2\mathbf{T}+\mathfrak{I}}$ est isomorphe à $\mathbf{Z}_2$ si et seulement si $p \in (9 + 16\mathbf{Z})$ (i.e. $t \equiv \pm 3 \pmod 8$). Cette assertion avait été prouvée dans la section III.7 de [7], en admettant que les courbes elliptiques de Setzer-Neumann de conducteur p satisfont la conjecture de Taniyama-Weil.

5.3 Tables

Pour chaque nombre premier p compris entre 5 et 250 nous donnons la valeur du numérateur n de $(p-1)/12$, le représentant de $\sqrt{u}$ dans $\{1, 2, ..., p-1\}$ et

la décomposition en produit de facteurs premiers de l'indice i du sous-groupe de $(\mathbf{Z}/p\mathbf{Z})^{*\nu}$ engendré par $\sqrt{u}$.

p	5	7	11	13	17	19	23	29	31	37	41	43	47
n	1	1	5	1	4	3	11	7	5	3	10	7	23
$\sqrt{u}$	1	1	5	1	4	7	16	23	1	26	37	35	14
i	1	1	1	1	1	1	1	1	5	1	2	1	1

p	53	59	61	67	71	73	79	83	89	97	101	103	107
n	13	29	5	11	35	6	13	41	22	8	25	17	53
$\sqrt{u}$	10	3	58	9	6	65	22	49	57	64	16	1	76
i	1	1	1	1	1	1	1	1	1	1	1	17	1

p	109	113	127	131	137	139	149	151	157	163	167	173	179
n	9	28	21	65	34	23	37	25	13	27	83	43	89
$\sqrt{u}$	27	85	107	52	16	106	102	9	16	22	87	57	108
i	1	2	7	5	2	1	1	1	1	1	1	1	1

p	181	191	193	197	199	211	223	227	229	233	239	241	
n	15	95	16	49	33	35	37	113	19	58	119	10	
$\sqrt{u}$	48	12	143	54	121	123	171	78	53	107	109	201	
i	5	1	1	1	3	5	1	1	1	1	1	1	

Les tables figurant dans l'introduction de [7] nous indiquent les seuls cas (pour $p < 250$) où les complétions en $\mathfrak{q}$ de l'algèbre de Hecke ne sont pas isomorphes à $\mathbf{Z}_q$ proviennent de $p = 31$, 41, 103, 113, 127, 131, 137, 181, 199 et 211, et $q = 5$, 2, 17, 2, 7, 5, 2, 5, 3 et 5 respectivement. Cela est confirmé par les tables ci-dessus. Ajoutons que nous avons poursuivi les calculs pour $250 < p < 1000$. L'indice i est toujours égal à 1 excepté dans les cas suivants :

p	257	271	281	313	337	353	401	409	457	487	521	523	541
i	2^6	3^2	5	2	2	2^3	5^2	2.17	2	3	2	3	3.5

p	569	571	577	593	661	683	691	701	733	751	761	809	857
i	2	5	2	2	11	11	5	5	61	5	2.5.19	2	2

p	881	911	919	941	953	971							
i	2	7	3	5	2	5							

References

[1] Barrucand P., Cohn H. Note on prime of type x^2+32y^2, class number, and residuacity. *Journal für die reine und angewandte Mathematik*, 238:67–70, 1969.

[2] Borevitch Z.I., Chafarevitch I.R. *Théorie des nombres.* Gauthier-Villars, Paris, 1967.

[3] Drinfeld V. Two theorems on modular curves. *Functional analysis and its applications*, 7:155–156, 1973.

[4] Hasse H. Über die Klassenzahl des Körper $P(\sqrt{-p})$ mit einer Primzahl $p \equiv 1 \pmod{2^3}$. *Aequationes mathematicae*, 3:165–169, 1969.

[5] Ling S., Oesterlé J. The Shimura subgroup of $J_0(N)$. In *Courbes modulaires et courbes de Shimura*, volume 196-197, pages 171–203. Astérisque, 1991.

[6] Manin Y. Parabolic points and zeta function of modular curves. *Math. USSR Izvestija*, 6(1):19–64, 1972.

[7] Mazur B. Modular curves and the Eisenstein ideal. *Pub. math. de l'IHES*, 47:33–186, 1977.

[8] Mazur B. On the arithmetic of special values of L functions. *Inv. math.*, 55:207–240, 1979.

[9] Milne J.S. Abelian varieties. In Cornell and Silverman, editors, *Arithmetic geometry*, chapter 5, pages 103–150. Springer Verlag, 1986.

[10] Milne J.S. Jacobian varieties. In Cornell and Silverman, editors, *Arithmetic geometry*, chapter 7, pages 167–212. Springer Verlag, 1986.

[11] Rademacher H. Zur Theorie der Modulfunktionen. *Journal für die reine und angewandte Mathematik*, 167:312–336, 1931.

[12] Rademacher H., Grosswald E. *Dedekind sums.* Number 16 in Carus mathematical monographs. Math. association of America, 1972.

[13] Rosen M. Abelian varieties over $\mathbf{C}$. In Cornell and Silverman, editors, *Arithmetic geometry*, chapter 4, pages 79–101. Springer Verlag, 1986.

[14] Serre J-P. *Corps locaux.* Hermann, Paris, 1968.

Adresse : Problèmes diophantiens, Institut de mathématiques, Université Pierre et Marie Curie, 4 place Jussieu, 75252 Paris cedex 05, France. e-mail : merel@moka.ccr.jussieu.fr.

Running title : Sous-groupe de Shimura et sous-groupe cuspidal

Abstract : We calculate an invariant defined by Mazur, which characterizes the Weil pairing between the Shimura and cuspidal subgroups of the jacobian of the modular curve $X_0(p)$. As a direct application our formula gives information about the completion of the Hecke algebra at Eisenstein primes.