Formes de Jacobi de deux variables: Formules de distribution et applications arithmétiques

Abdelmejid Bayad
abayad@maths.univ-evry.fr
Département de mathématiques
Université d'Evry Val d'Essone

26 juin 2005

Table des matières

1 Introduction

Les formes de Jacobi fournissent des outils importants dans de nombreuses branches des mathématiques. Elles constituent un croisement entre fonctions elliptiques et formes modulaires et à ce titre, formes modulaires usuelles et fonctions elliptiques en sont des exemples. Elles apparaissent naturellement dans le développement de Fourier des formes modulaires de Siegel et de toute sorte de formes automorphes. Elles sont liées à des questions importantes de théorie des nombres : Valeurs spéciales de fonctions L, étude de la fonction Zêta de Riemann, sommes de Dedekind, lois de réciprocité, périodes de formes modulaires. La théorie classique des formes de Jacobi **holomorphes, d'une variable**, comme fonctions à valeurs complexes de $\mathcal{H} \times \mathbb{C}$, a été développée par Eichler et Zagier dans [27]. Bien qu'il n'existe pas à notre connaissance de théorie générale, analogue à [27], en dimension supérieure, de nombreux auteurs se sont intéressés aux formes de Jacobi de plusieurs variables. On peut citer notamment Yamazaki, Ziegler et Klingen d'une part [61], [64], [40, 41] et Gritsenko et Krieg, [30], [42], d'autre part. Dans un article consacré au polynôme de périodes des formes paraboliques, [63], Zagier introduit une forme de Jacobi **méromorphe de deux variables** qui joue un rôle crucial dans son travail. Il s'agit de la fonction de trois variables $\tau \in \mathcal{H}, u, v \in \mathbb{C}$ définie pour $\mathrm{Re}(u) < 2\pi \mathrm{Im}(\tau)$ et $-\mathrm{Re}(v) < 2\pi \mathrm{Im}(\tau)$ par

$$F_\tau(u,v) = \sum_{n \geqslant 0} \frac{\eta^{-n}}{q^{-n}\xi - 1} - \sum_{m \geqslant 0} \frac{\xi^m}{q^{-m} - \eta} \quad , (q = e^{2i\pi\tau}, \xi = e^u, \eta = e^v) \ .$$

Cette fonction possède de nombreuses propriétés intéressantes et notamment un prolongement méromorphe pour toute valeur u et v. C'est cette fonction, "convenablement modifiée", qui est au coeur des travaux que nous présentons. Plus précisemment, considérons un réseau complexe L de base $\{\omega_1, \omega_2\}$, $\omega_1/\omega_2 \in \mathcal{H}$, nous définissons la fonction de deux variables

$$D_L(z;\varphi) = \frac{2i\pi}{\omega_2} \exp\left(-\frac{u\mathrm{Re}(v)}{2\pi \mathrm{Im}(\tau)}\right) F_\tau(u,v)$$

où $\tau = \frac{\omega_1}{\omega_2}, u = \frac{2i\pi}{\omega_2} z$ et $v = \frac{2i\pi}{\omega_2}\varphi$. Si la fonction D_L n'est plus analytique ni en v, ni en τ, par contre elle ne dépend pas du choix de la base orientée $\{\omega_1, \omega_2\}$ de L, ce qui justifie notre notation, et possède un grand nombre de propriétés remarquables qui seront présentées dans le paragraphe 2. Parmi ces propriétés deux d'entre elles vont jouer un rôle particulier et seront alternativement utilisées dans les articles joints. Il s'agit de relations de distribution additive et multiplicative, simples, de nature arithmétique, satisfaites par ces fonctions. De manière plus précise si Λ est un réseau de $\mathbb{C}$ tel que $L \subset \Lambda$ et $[\Lambda : L] = l$ on a la relation de distribution additive suivante :

$$\sum_t D_L(lz; \varphi + t) = D_\Lambda(z;\varphi) \quad ,$$

où t parcourt un système complet des représentants dans $\mathbb{C}$ de Λ/L. En outre sous les mêmes hypothèses on obtient la relation de distribution multiplicative :

$$\mathcal{K}(\varphi; L, \Lambda) \prod_t D_L(z+t;\varphi) e(-E_L(t,\varphi)) = D_\Lambda(z;\varphi) \ ,$$

où E_L désigne une $\mathbb{R}$-forme bilinéaire alternée définie sur $\mathbb{C} \times \mathbb{C}$, à valeurs entières sur $L \times L$, précisée en 2.2, $\mathcal{K}(z; L, \Lambda)$ est un quotient de fonctions de Klein associées aux réseaux L et Λ , 2.4, et **enfin où pour tout** x **de** $\mathbb{C}$ **on pose** $e(x) = e^{2i\pi x}$**.**

Une partie importante de notre travail a été consacrée à la découverte des multiples propriétés **"cachées"** satisfaites par les formes D_L. Ces propriétés et certaines de leurs conséquences arithmétiques font l'objet de [7], [14], [16], [17] et [18]. Elles sont rassemblées dans le paragraphe 2 de ce rapport. Dans les paragraphes suivants nous présentons les contributions qu'elles nous ont permis d'apporter aux questions suivantes :

i) Lois de réciprocité quadratiques pour les corps quadratiques imaginaires, [8], (paragraphe 3)

ii) Constructions d'élements de Stickelberger quadratiques et annulation de groupes de classes, [6], [9], [11], (paragraphe 4).

iii) Structure galoisienne des anneaux d'entiers de corps de nombres et construction de bases d'entiers, [10], (paragraphe 5).

iv) Relation de distribution pour la fonction Zêta de Weierstrass, [16], (paragraphe 5).

v) Relation de distribution pour la fonctions de Siegel, [16], (paragraphe 7).

vi) Construction des sommes multiples de Dedekind et Zagier elliptiques, [13], [14], (paragraphe 8).

vii) Construction de sommes multiples d'Apostol elliptiques, [14], (paragraphe 8).

viii) Isogénies entre courbes elliptiques, [14], (paragraphe 9).

On sait que la démonstration du théorème de Stickelberger et l'obtention de nombreux résultats sur la structure galoisienne des anneaux d'entiers de corps de nombres reposent de manière essentielle sur la factorisation en produit d'idéaux premiers des sommes de Gauss. Nous avons construit à l'aide des fonctions D_L certaines résolvantes de Lagrange que nous considérons comme des "sommes de Gauss elliptiques". C'est essentiellement la relation de distribution additive qui nous permet de déterminer leur factorisation en produit d'idéaux premiers et qui constitue ainsi le point important de ii) et iii). Par ailleurs c'est en utilisant la relation de distribution multiplicative qui nous obtenons, Corollaire 6.2.2, une amélioration de résultats de Coates, Kubert et Robert, résultats utilisés par Coates et Wiles dans leur travail sur la conjecture de Birch et Swinnerton-Dyer, [24], [25], par de Shalit, [55], en théorie d'Iwasawa, par Gillard et Robert, [29], dans leur étude du groupe des unités d'extensions abéliennes de corps quadratiques imaginaires. Cette même relation nous permet dans le théorème 7.2.1 de compléter une formule de F. Jarvis et J. Wildeshaus, [38], [39], et [60] en précisant la racine de l'unité qui apparait dans cette formule. Cette formule de distribution est utilisée par ces auteurs dans leur analyse d'un analogue elliptique de la conjecture polylogarithmique de Zagier, [38], [39], [59] et [60]. Enfin c'est en utilisant le théorème du Liouville du résidu et le développement de Laurent des formes $D_L(z, \varphi)$ au voisinage de $z = 0$ que nous donnons une version elliptique des sommes d'Apostol, Dedekind et Zagier.

Ce rapport se termine par deux appendices, paragraphes 9 et 10. Dans le premier nous donnons une formule de distribution additive pour la fonction Zêta de Weierstrass d'où nous déduisons un corollaire 9.2.5 qui généralise un théorème de Schoof, [53]. Ce résultat est un travail soumis pour publication. Dans le second nous donnons une nouvelle démonstration de la loi de réciprocité quadratique pour les corps quadratiques imaginaires qui utilise les formes $D_L(z, \varphi)$.

2 Etude des formes de Jacobi : $D_L(z;\varphi)$

2.1 Généralités sur les formes de Jacobi

La théorie des formes de Jacobi holomorphes, de poids pair et d'indice fini, à une variable est étudiée en détail dans le livre [27]. Par contre il est difficile de trouver une théorie complète sur les formes de Jacobi méromorphes dans la littérature. Neanmoins on peut y trouver l'étude de certaines de ces formes. Dans [36] on étudie certaines formes de Jacobi méromorphes à une variable. En effet, suivant [36] p.128, une forme de Jacobi méromorphe Φ sur $\mathcal{H}\times\mathbb{C}$ est définie comme suit : pour $\tau\in\mathcal{H}$, $z\to\Phi(\tau,z)$ est méromorphe, périodique de périodes $2\pi i\,(\mathbb{Z}\tau+\mathbb{Z})$, de poids k entier et d'indice 0 c'est-à-dire :

$$\Phi\left(\frac{a\tau+b}{c\tau+d},\frac{z}{c\tau+d}\right)=(c\tau+d)^k\Phi\left(\tau,z\right),\forall\begin{pmatrix}a&b\\c&d\end{pmatrix}\in\Gamma,$$

où Γ est un sous-groupe d'indice fini de $\mathrm{SL}_2(\mathbb{Z})$.

La fonction $\wp(\tau,z)$ de Weierstrass en est un exemple de poids 2 et d'indice 0 pour $\Gamma=\mathrm{SL}_2(\mathbb{Z})$.

Dans ce travail nous considérons des formes de Jacobi à deux variables, méromophes par rapport à la première variable et non nécessairement analytique par rapport à la seconde variable. Nous définissons de telles formes Φ de Jacobi sur $\mathcal{H}\times\mathbb{C}^2$ comme suit, $\tau\in\mathcal{H}$, $(z,\varphi)\to\Phi(\tau,z,\varphi)$ est méromorphe par rapport à la variable z et vérifie les conditions suivantes :

pour tout $\rho\in\mathbb{Z}\tau+\mathbb{Z}$

1) $\frac{\Phi(\tau,z+\rho,\varphi)}{\Phi(\tau,z,\varphi)}$ est indépendante de z

2) $\frac{\Phi(\tau,z,\varphi+\rho)}{\Phi(\tau,z,\varphi)}$ est indépendante de φ

3) $\Phi\left(\frac{a\tau+b}{c\tau+d},\frac{z}{c\tau+d},\frac{\varphi}{c\tau+d}\right)=(c\tau+d)^k e(\frac{mz\varphi}{c\tau+d})\Phi\left(\tau,z,\varphi\right),\forall\begin{pmatrix}a&b\\c&d\end{pmatrix}\in\Gamma$, le sous-groupe Γ est d'indice fini dans $\mathrm{SL}_2(\mathbb{Z})$, (de poids k et d'indice m).

Exemple :

$$\Phi(\tau,z,\varphi)=\frac{\theta'(0)\theta(z+\varphi)}{\theta(z)\theta(\varphi)}$$

où θ est le produit triple de Jacobi

$$\theta(z)=q_\tau^{1/8}(e^{z/2}-e^{-z/2})\prod_{n=1}^{\infty}(1-q_\tau^n)(1-q_\tau^n e^z)(1-q_\tau^n e^{-z})$$

est une forme de Jacobi méromorphe par rapport aux deux variables z et φ et vérifiant

$$\Phi(\tau,z+n\tau+s,\varphi+m\tau+r)=q_\tau^{-mn}e^{-mz-n\varphi}\Phi(\tau,z,\varphi),\forall m,n,r,s\in\mathbb{Z}.$$

$$\Phi\left(\frac{a\tau+b}{c\tau+d},\frac{z}{c\tau+d},\frac{\varphi}{c\tau+d}\right)=(c\tau+d)e\left(\frac{z\varphi}{c\tau+d}\right)\Phi\left(\tau,z,\varphi\right),\forall\begin{pmatrix}a&b\\c&d\end{pmatrix}\in\mathrm{SL}_2(\mathbb{Z}),$$

de poids 1 et d'indice 1. Cette forme est étudiée en détail dans [63] elle est utilisée pour la théorie des périodes des formes modulaires.

Dans ce mémoire, nous étudions d'autres formes de Jacobi, notées $D_L(z;\varphi)$ et nous en donnons des applications arithmétiques.

Avant de parler des formes de Jacobi $D_L(z;\varphi)$, précisons quelques définitions et notations.

2.2 Forme E_L

Soit $\mathcal{H}$ le demi-plan supérieur de Poincaré. Pour tout réseau complexe L, si (w_1, w_2) désigne une base de L sur $\mathbb{Z}$ telle que $\mathrm{Im}(w_1/w_2) > 0$, on pose $\tau = w_1/w_2 \in \mathcal{H}$ et on définit l'aire de L par

$$a(L) = \frac{1}{2i}\begin{vmatrix} w_1 & \overline{w}_1 \\ w_2 & \overline{w}_2 \end{vmatrix} = \frac{w_1\overline{w}_2 - w_2\overline{w}_1}{2i} = |w_2|^2\,\mathrm{Im}(\tau);$$

le nombre $a(L)$ est un nombre réel > 0, indépendant du choix de la base (w_1, w_2) de L telle que $\mathrm{Im}(w_1/w_2) > 0$. Il vérifie $a(\lambda L) = |\lambda|^2 a(L)$; pour tout $\lambda \in \mathbb{C}^*$.

On définit alors la forme hermitienne $H_L(u,v) = \frac{\bar{u}v}{a(L)}$, où $(u,v) \in \mathbb{C}\times\mathbb{C}$, et l'on pose $E_L = \mathrm{Im}\, H_L$, de sorte que $E_L(u,v) = \frac{1}{2i}\frac{\bar{u}v - \bar{v}u}{a(L)}$, pour tout $(u,v) \in \mathbb{C}\times\mathbb{C}$.

Notons que E_L :

- vérifie $E_{\lambda L}(\lambda z, \lambda\varphi) = E_L(z,\varphi)$; pour tout $\lambda \in \mathbb{C}^*$;
- est une forme $\mathbb{R}$-bilinéaire alternée ;
- ses valeurs sur $L \times L$ sont entières ;
- vaut -1 sur toutes les bases (w_1, w_2) de L sur $\mathbb{Z}$ telles que $\mathrm{Im}(w_1/w_2) > 0$. D'une façon plus précise : Pour $z, \varphi \in \mathbb{C}$, $z = a\omega_2 + b\omega_1, \varphi = c\omega_2 + d\omega_1$ avec $a, b, c, d \in \mathbb{R}$, on a

$$E_L(z,\varphi) = \frac{\mathrm{Im}\,(\bar{z}\varphi)}{a(L)} = ad - bc.$$

2.3 Fonction êta de Legendre

La fonction êta de Legendre est définie comme suit. Pour $z \in \mathbb{C}$, $z = a_1\omega_1 + a_2\omega_2$ avec $a_1, a_2 \in \mathbb{R}$, on définit

$$\eta(z, L) = a_1\eta(\omega_1, L) + a_2\eta(\omega_2, L)$$

où $\eta(\omega_1, L)$ et $\eta(\omega_2, L)$ désignent les périodes de "deuxième espèce" associées aux périodes de "première espèce" ω_1 et ω_2, c'est-à-dire, $\eta(\omega_i, L)$ $(i = 1, 2)$ est le seul nombre complexe qui satisfait l'égalité

$$\zeta(z + \omega_i, L) = \zeta(z, L) + \eta(\omega_i, L)$$

$(i = 1, 2)$ pour tout $z \in \mathbb{C} \setminus L$, où ζ désigne la fonction zêta de Weierstrass ([45],chapitre 18). Pour donner une jolie expression à la fonction êta de Legendre, nous allons rappeler quelques notions classiques sur les séries. La fonction donnée par la série

$$\sum_{\omega \in L\setminus\{0\}} \frac{1}{\omega^2|\omega|^{2s}}$$

est holomorphe en $s = 0$, donc en particulier on peut définir

$$s_2(L) = \lim_{s\to 0} \sum_{\omega\in L\setminus\{0\}} \frac{1}{\omega^2|\omega|^{2s}}.$$

On peut alors montrer le résultat suivant ([44], Theorem 1.2, p. 226) :

$$\eta(z, L) = s_2(L)z + \frac{\pi}{a(L)}\bar{z}.$$

Cette nouvelle formulation de la fonction êta peut être vue comme une généralisation de la relation de Legendre ([45], p. 241) :

$$\omega_1\eta(\omega_2, L) - \omega_2\eta(\omega_1, L) = 2\pi i.$$

Remarque 2.3.1 *Dans l'appendice 2, nous prouvons une loi de distribution additive satisfaite par la fonction zêta de Weierstrass .*

2.4 Fonctions de Klein

Nos références pour ce paragraphe sont [43] et [44].

Dans la littérature, la fonction de Klein $\mathcal{K}_L(z)$, $z \in \mathbb{C}$, est définie par le produit infini

$$\mathcal{K}_L(z) = ze^{-\frac{1}{2}zz^*} \prod_{\ell\in L,\ell\neq 0} \Big(1 - \frac{z}{\ell}\Big)e^{\frac{z}{\ell}+\frac{1}{2}\left(\frac{z}{\ell}\right)^2} \tag{1.1.1}$$

où, écrivant $z = a_1\omega_1 + a_2\omega_2$ avec $a_1, a_2 \in \mathbb{R}$, on note $z^* = a_1\eta_1 + a_2\eta_2$ pour $\eta_1 = \eta_1(\omega_1, L)$ et $\eta_2 = \eta(\omega_2, L)$ les périodes de "deuxième espèce" associées aux périodes de "première espèce" ω_1 et ω_2. Il faut noter que cette définition a un sens, car l'application $z \mapsto zz^*$ (et donc, d'après (1.1.1), aussi la fonction $z \mapsto \mathcal{K}_L(z)$) ne dépend pas du choix de la base (w_1, w_2) de L telle que $\mathrm{Im}(w_1/w_2) > 0$. En utilisant la fonction êta de Legendre on peut exprimer la fonction $\mathcal{K}_L(z)$ de la manière suivante :

$$\mathcal{K}_L(z) = ze^{-\frac{1}{2}z\eta(z,L)} \prod_{\ell\in L,\ell\neq 0} \Big(1 - \frac{z}{\ell}\Big)e^{\frac{z}{\ell}+\frac{1}{2}\left(\frac{z}{\ell}\right)^2}$$

et comme $s_2(L)$, $a(L)$ et la norme $|z|^2$ ne dépendent pas du choix de la base (w_1, w_2) de L telle que $\mathrm{Im}(w_1/w_2) > 0$, on a la même propriété pour la fonction $\mathcal{K}_L(z)$.

La fonction $\mathcal{K}_L$ vérifie les propriétés suivantes :

a)(Translation) Pour tout $\rho \in L$, on a

$$\mathcal{K}_L(z + \rho) = \chi_L(\rho)e(E_L(\rho, z)/2)\mathcal{K}_L(z),$$

où l'on a posé $\chi_L(\rho) = \begin{cases} 1 & \text{si } \rho \in 2L \\ -1 & \text{si } \rho \in L\setminus 2L. \end{cases}$

Et en fait, pour tous ρ et σ éléments de L, on a

$$\chi_L(\rho+\sigma) = \chi_L(\rho)\chi_L(\sigma)e(E_L(\rho,\sigma)/2).$$

b) Elle est homogène de degré 1, c'est-à-dire, pour tout $\lambda \in \mathbb{C}^*$ et tout $z \in \mathbb{C}$, on a

$$\mathcal{K}_{\lambda L}(\lambda z) = \lambda \mathcal{K}_L(z).$$

2.5 Formes $D_L(z;\varphi)$ de Jacobi et propriétés arithmétiques

Nos principales références pour ce paragraphe sont [7],[14],[16],[17] et [18].
Introduisons la fonction

$$D_L(z;\varphi) = e(E_L(z,\varphi)/2)\frac{\mathcal{K}_L(z+\varphi)}{\mathcal{K}_L(z)\mathcal{K}_L(\varphi)}.$$

où L est un réseau complexe de base (w_1, w_2) telle que $\mathrm{Im}(w_1/w_2) > 0$ et z, φ appartiennent à $\mathbb{C} \setminus L$. On note, dans toute la suite, $\tau = \frac{w_1}{w_2}$.

La fonction D_L est méromorphe par rapport à la première variable, mais elle perd son analyticité vis-à-vis de la seconde variable ; par contre elle vérifie plusieurs **propriétés fondamentales de nature arithmétique et topologique.** Nous en avons découvert un certain nombre.

Théorème 2.5.1 *La fonction D_L satisfait les propriétés suivantes*

i) Elle ne dépend pas de la base (w_1, w_2) choisie, telle que $\mathrm{Im}(w_1/w_2) > 0$, du réseau L.

ii) Elle ne dépend que de φ modulo L.

iii) On a $D_L(z+\rho;\varphi) = e(E_L(\rho,\varphi))D_L(z;\varphi)$ lorsque $\rho \in L$.

iv) Elle vérifie l'équation fonctionnelle $D_L(z;\varphi)e(-E_L(z,\varphi)) = D_L(\varphi;z)$.

v) Elle est homogène de degré -1, c'est-à-dire $D_{\lambda L}(\lambda z;\lambda\varphi) = \lambda^{-1}D_L(z;\varphi)$ pour tout $\lambda \in \mathbb{C}^*$.

vi) Soit $\mathcal{D} = \sum_{i=1}^{r} n_i(a_i)$ un diviseur principal modulo L, c'est-à-dire, tel que $\sum_{i=1}^{r} n_i = 0$ et $\sum_{i=1}^{r} n_i a_i \in L$. Alors toute fonction elliptique, admettant pour périodes le réseau L et pour diviseur le diviseur $\mathcal{D}$, est égale, à une constante multiplicative non nulle près, à la fonction $g_{\mathcal{D}}(z;L)$ définie par

$$g_{\mathcal{D}}(z;L) = \prod_{a_i \notin L} D_L(z;-a_i)^{n_i}.$$

En outre la fonction $g_{\mathcal{D}}(z;L)$ ne dépend que du diviseur $\mathcal{D}$ modulo le réseau L, c'est-à-dire, si $\mathcal{D}'$ est un autre diviseur vérifiant la condition $\mathcal{D} \equiv \mathcal{D}'(\ mod\ L)$, alors les fonctions $g_{\mathcal{D}}(z,L)$ et $g_{\mathcal{D}'}(z,L)$ coïncident.

vii) Pour tous z et φ appartenant à $\mathbb{C} \setminus L$, on a

$$\wp_L(z) - \wp_L(\varphi) = D_L(z,\varphi)D_L(z,-\varphi).$$

viii) Pour tout $z \in \mathbb{C} \setminus L$ *on a*

$$\wp'_L(z) = -2 \prod_{\bar{t} \in \frac{1}{2}L/L \setminus \{\bar{0}\}} D_L(z;t).$$

ix) Pour $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ *et* $\tau = \frac{w_1}{w_2}$. *On pose* $D_\tau(z;\varphi) = D_{\mathbb{Z}\tau+\mathbb{Z}}(z;\varphi)$. *La forme* $D_\tau(z;\varphi)$ *est modulaire de poids 1 et d'indice 0, c'est-à-dire :*

$$D_{\frac{a\tau+b}{c\tau+d}}\left(\frac{z}{c\tau+d}; \frac{\varphi}{c\tau+d}\right) = (c\tau+d)D_\tau(z;\varphi), \forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}).$$

De plus, on a $D_L(z;\varphi) = \frac{1}{\omega_2} D_\tau\left(\frac{z}{\omega_2}; \frac{\varphi}{\omega_2}\right)$.

x) Elle satisfait une relation de **distribution additive** *lorsque l'on change de réseau. De façon plus précise, soient* L *et* Λ *deux réseaux complexes tels que* $L \subset \Lambda$ *et* $[\Lambda : L] = l$. *Alors on a*

$$\sum_{\bar{t} \in \Lambda/L} D_L(l\varphi; z+t) = D_\Lambda(\varphi; z)$$

Ou encore d'une manière équivalente, grâce à l'équation fonctionelle, on a

$$\sum_{\bar{t} \in \Lambda/L} D_L(z+t; l\varphi) e(-E_L(t, l\varphi)) = D_\Lambda(z;\varphi).$$

Lorsque φ *est un point de torsion du tore* $\mathbb{C}/L$, *l'énoncé de l'égalité ci-dessus est plus simple, mais équivalent, à la formule de Weber classique (3.19)§ 3 p.292 [52] dont on peut trouver une démonstration dans [52].*

xi) Pour deux réseaux complexes L *et* Λ *tels que* $L \subset \Lambda$ *et pour tout* $z \in \mathbb{C} \setminus \Lambda$, *on définit la fonction* $\mathcal{K}(z; L, \Lambda)$ *par*

$$\mathcal{K}(z; L, \Lambda) = \frac{\mathcal{K}_L(z)^{[\Lambda:L]}}{\mathcal{K}_\Lambda(z)}.$$

on a

$$\prod_{\bar{t} \in \Lambda/L \setminus \{\bar{0}\}} D_L(z;t)^{-1} = \mathcal{K}(z; L, \Lambda) \tag{1}$$

ou encore

$$\prod_{\bar{t} \in \Lambda/L \setminus \{\bar{0}\}} D_L(t;z)^{-1} e\left(E_L(t,z)\right) = \mathcal{K}(z; L, \Lambda). \tag{2}$$

xii) Elle satisfait une relation de **distribution multiplicative** *lorsque l'on change de réseau. Soient* L *et* Λ *deux réseaux complexes. Alors, pour tous* z *et* φ *appartenant à* $\mathbb{C} \setminus \Lambda$, *on a*

$$D_\Lambda(z;\varphi) = \mathcal{K}(\varphi; L, \Lambda) \prod_{\bar{t} \in \Lambda/L} D_L(z+t;\varphi) e(-E_L(t,\varphi)). \tag{1}$$

D'une manière équivalente, on a

$$D_\Lambda(z;\varphi) = \mathcal{K}(z; L, \Lambda) \prod_{\bar{t} \in \Lambda/L} D_L(z;\varphi+t). \tag{2}$$

xiii) Elle se décompose en **produit infini**

$$D_L(z,\varphi) = \frac{2\pi i}{w_2} q_{\frac{z}{w_2}}^{\frac{\mathrm{Im}\left(\frac{\varphi}{w_2}\right)}{\mathrm{Im}\,\tau}} \times \frac{\left(q_{\frac{z+\varphi}{w_2}}^{\frac{1}{2}} - q_{\frac{z+\varphi}{w_2}}^{-\frac{1}{2}}\right)}{\left(q_{\frac{z}{w_2}}^{\frac{1}{2}} - q_{\frac{z}{w_2}}^{-\frac{1}{2}}\right)\left(q_{\frac{\varphi}{w_2}}^{\frac{1}{2}} - q_{\frac{\varphi}{w_2}}^{-\frac{1}{2}}\right)}$$

$$\prod_{n\geqslant 1} \frac{(1-q_\tau^n)^2\left(1-q_\tau^n q_{\frac{z+\varphi}{w_2}}\right)\left(1-q_\tau^n q_{\frac{z+\varphi}{w_2}}^{-1}\right)}{\left(1-q_\tau^n q_{\frac{z}{w_2}}\right)\left(1-q_\tau^n q_{\frac{z}{w_2}}^{-1}\right)\left(1-q_\tau^n q_{\frac{\varphi}{w_2}}\right)\left(1-q_\tau^n q_{\frac{\varphi}{w_2}}^{-1}\right)}$$

xiv) Elle possède un **développement de Fourier**

$$D_L(z;\varphi) = \frac{\pi}{w_2} q_{\frac{z}{w_2}}^{\frac{\mathrm{Im}\left(\frac{\varphi}{w_2}\right)}{\mathrm{Im}\,\tau}} \left(cot\left(\frac{\pi z}{w_2}\right) + cot\left(\frac{\pi\varphi}{w_2}\right) + 4\sum_{n=1}^{\infty}\sum_{d|n} sin\left(2d\frac{\pi z}{w_2} + \frac{2n}{d}\frac{\pi\varphi}{w_2}\right) q_\tau^n \right).$$

xv) Elle admet le **développement de Laurent** *suivant :*

$$D_\tau(z;\varphi) = \sum_{k\geqslant 0} d_k(\varphi) z^{k-1}$$

avec

$$d_0(\varphi) = 1, \quad \frac{(k-1)!}{(2\pi i)^k} d_k(\varphi) = \frac{1}{k} B_k\left(\frac{\mathrm{Im}(\frac{\{\varphi\}}{w_2})}{\mathrm{Im}\,\tau}\right) + \frac{q_{\{\varphi\}}}{q_{\{\varphi\}-1}}\left(\frac{\mathrm{Im}(\frac{\{\varphi\}}{w_2})}{\mathrm{Im}\,\tau}\right)^{k-1}$$

$$-\sum_{n\geqslant 1}\left(\frac{q_{\{\varphi\}}q^m}{1-q_{\{\varphi\}}q^m}\left(\frac{\mathrm{Im}(\frac{\{\varphi\}}{w_2})}{\mathrm{Im}\,\tau}+m\right)^{k-1} - \frac{q_{\{\varphi\}}^{-1}q^m}{1-q_{\{\varphi\}}^{-1}q^m}\left(\frac{\mathrm{Im}(\frac{\{\varphi\}}{w_2})}{\mathrm{Im}\,\tau}-m\right)^{k-1}\right), \forall k \geqslant 1$$

Les coefficients satisfont la relation de réccurence suivante

$$d_2(\varphi) = \frac{1}{2}d_1(\varphi)^2 - \frac{1}{2}\wp_L(\varphi), d_{2n}(\varphi) = \frac{(2n-1)}{2}G_{2n}(L) - \frac{1}{2}\sum_{i=1}^{2n-1}(-1)^i d_i(\varphi) d_{2n-i}(\varphi),$$

et où

$$G_{2n}(L) = \sum_{\omega\in L\setminus\{o\}} \frac{1}{|\omega|^{2n}}, \forall n \geqslant 2.$$

xvi) Pour tout $z \in \mathbb{C}\backslash\mathbb{Z}\tau+\mathbb{Z}$. On a alors,

$$\lim_{\mathrm{Im}(\tau)\to\infty} D_\tau(z,\varphi) = \begin{cases} \pi\left(cot(\pi\{\varphi\}) + cot(\pi\{z\})\right) e^{-2i\pi[z_1]\{\varphi_2\}} & si\ (z_1,\varphi_1)\in\mathbb{Z}^2 \\ \pi\left(cot(\pi\{\varphi\}) - i\right) e^{-2i\pi[z_1]\{\varphi_2\}} & si\ \varphi_1\in\mathbb{Z}, z_1\notin\mathbb{Z} \\ \pi\left(cot(\pi\{z\}) - i\right) e^{2i\pi\{\varphi_1\}z_2 - 2i\pi[z_1]\{\varphi_2\}} & si\ z_1\in\mathbb{Z}, \varphi_1\notin\mathbb{Z} \\ 0 & si\ z_1\notin\mathbb{Z}, \varphi_1\notin\mathbb{Z} \end{cases}$$

où l'on a posé $\{z\} = \{z_1\}\tau + \{z_2\}$ et $[z] = [z_1]\tau + [z_2]$, où $\{z_1\}$, $\{z_2\}$ sont les parties fractionnaires de z_1, z_2 (resp. $[z_1], [z_2]$ sont les parties entières de z_1, z_2) habituelles car $z_1, z_2 \in \mathbb{R}$.

xvii) Pour tout $\varphi \in \mathbb{R}\backslash\mathbb{Z}$, *on a*

$$\lim_{\mathrm{Im}(\tau)\to\infty} d_j(\varphi) = \begin{cases} \frac{B_{2l}}{(2l)!}(2\pi i)^{2l} = -2\zeta(2l) & Si\ j = 2l, l \geqslant 0 \\ \pi cot(\pi\varphi) & Si\ j = 1 \\ 0 & Sinon \end{cases}$$

xviii) Pour tout $\varphi = \varphi_1\tau + \varphi_2 \in \mathbb{C}$ *avec* $\varphi_1 \in \mathbb{R}\backslash\mathbb{Z}$, *on a :* $\lim_{\mathrm{Im}(\tau)\to\infty} d_j(\varphi) = \frac{B_j(\{\varphi_1\})}{j!}(2\pi i)^j$, *où* $B_j(X)$ *le* j*-ième polynôme de Bernoulli.*

Application : Pour $\varphi \in \frac{1}{2}L/L\backslash\{\bar{0}\}$ explicitons les formes de Jacobi de " niveau 2"

$$D_\tau(z;\frac{1}{2}) = \frac{1}{z} + 2\sum_{k\geqslant 0}\frac{(2\pi i)^{2k+2}}{(2k+1)!}\left(\frac{B_{2k+2}}{4k+4} + \sum_{m\geqslant 1}\frac{m^{2k+1}q^m}{1+q^m}\right) z^{2k+1}$$

$$D_\tau(z;\frac{\tau}{2}) = \frac{1}{z} + 2\sum_{k\geqslant 0}\frac{(2\pi i)^{2k+2}}{(2k+1)!}\left(\frac{B_{2k+2}(1/2)}{4k+4} + \sum_{m\geqslant 1}(m+1/2)^{2k+1}\frac{q^{2m+1}+q^{m+\frac{1}{2}}}{(1-q^{m+\frac{1}{2}})^2}\right) z^{2k+1}$$

$$D_\tau(z;\frac{\tau+1}{2}) = \frac{1}{z} + 2\sum_{k\geqslant 0}\frac{(2\pi i)^{2k+2}}{(2k+1)!}\left(\frac{B_{2k+2}(1/2)}{4k+4} + \sum_{m\geqslant 1}(m+\frac{1}{2})^{2k+1}\frac{q^{2m+1}-q^{m+\frac{1}{2}}}{(1+q^{m+1/2})^2}\right) z^{2k+1}$$

2.6 Formes de Jacobi p-adiques : Formules de distribution et d'inversion

Nous avons précédemment introduit la notion des formes de Jacobi complexes $D_L(z;\varphi)$ et nous en avons donné les principales propriétés. Nous avons dans [11] et [12] montré comment définir un analogue p-adique de ces formes. Nous avons montré que ces nouvelles fonctions vérifiaient la plupart des propriétés des formes complexes. Nous donnons en particulier dans le théorème 2.6.2 une formule de distribution et une formule d'inversion qui sont satisfaites lors d'un changement de sous-groupe discret. Nous en déduisons le corollaire 2.6.3 qui est un analogue d'une formule de Weber généralisée.

Soit K un corps local de caractéristique résiduelle $p > 0$ et $\overline{K}$ une clôture algébrique fixée de K. Nous désignons par q un élément de K^* de valuation p-adique strictement positive et nous notons v_q la valuation discrète normalisée de K.

Définition 2.6.1 *On associe au sous-groupe discret* $q^{\mathbb{Z}}$ *de* $\overline{K^*}$, *la forme de Jacobi p-adique* $D_{q^{\mathbb{Z}}}(z;\varphi)$ *définie formellement par*

$$D_{q^{\mathbb{Z}}}(z;\varphi) = z^{v_q(\varphi)}\frac{\theta_{q^{\mathbb{Z}}}(z\varphi)}{\theta_{q^{\mathbb{Z}}}(z)\theta_{q^{\mathbb{Z}}}(\varphi)};\ \textit{pour tous}\ z,\varphi \in \overline{K^*}$$

où $\theta_{q^{\mathbb{Z}}}(z) = (z-1)\prod_{n\geqslant 1}\frac{(1-q^n z)(1-q^n z^{-1})}{(1-q^n)^2}$ *c'est la fonction thêta fondamentale associée au sous-groupe discret* $q^{\mathbb{Z}}$ *de* $\overline{K^*}$ *et normalisée par* $\theta'_{q^{\mathbb{Z}}}(1) = 1$.

La forme $D_{q^{\mathbb{Z}}}(z;\varphi)$ est un analogue p-adique à $D_L(z;\varphi)$. Nous démontrons dans [11, 12] le théorème suivant

Théorème 2.6.2 *Soient γ et α des points d'ordre l de $\overline{K^*}/q^{\mathbb{Z}}$, tels que*

$$q^{\mathbb{Z}}\alpha^{\mathbb{Z}} \cap q^{\mathbb{Z}}\gamma^{\mathbb{Z}} = q^{\mathbb{Z}} \ .$$

Alors

i) (Formule de distribution) : Pour tous $z^l \notin q^{\mathbb{Z}}$, $\varphi \notin q^{\mathbb{Z}}\gamma^{\mathbb{Z}}$, on a la relation suivante

$$\sum_t D_{q^{\mathbb{Z}}}(z^l;\varphi t) = D_{q^{\mathbb{Z}}\gamma^{\mathbb{Z}}}(z;\varphi)$$

où t parcourt un système complet T de représentants dans $\overline{K^*}$ de $q^{\mathbb{Z}}\gamma^{\mathbb{Z}}/q^{\mathbb{Z}}$.

ii) (Formule d'inversion) : Pour tous $z \notin q^{\mathbb{Z}}\gamma^{\mathbb{Z}}$, $\varphi^l \notin q^{\mathbb{Z}}$, on a la relation suivante

$$\sum_s D_{q^{\mathbb{Z}}\gamma^{\mathbb{Z}}}(z;\varphi s) = l D_{q^{\mathbb{Z}}}(z;\varphi^l)$$

où s parcourt un système complet de représentants dans $\overline{K^*}$ de $q^{\mathbb{Z}}\alpha^{\mathbb{Z}}\gamma^{\mathbb{Z}}/q^{\mathbb{Z}}\gamma^{\mathbb{Z}}$.

Comme corollaire, on obtient le résultat suivant

Corollaire 2.6.3 *(Formule de Weber p-adique) Pour tout point γ de $\overline{K^*}/q^{\mathbb{Z}}$, d'ordre l, et tout couple z, φ de K tels que $z^l \notin q^{\mathbb{Z}}$ et $\varphi \notin q^{\mathbb{Z}}\gamma^{\mathbb{Z}}$. Alors on a l'égalité :*

$$\sum_{i=0}^{l-1} z^{v_q(\gamma^{li})} \frac{\theta_{q^{\mathbb{Z}}}(z^l\varphi\gamma^i)}{\theta_{q^{\mathbb{Z}}}(z^l)\theta_{q^{\mathbb{Z}}}(\varphi\gamma^i)} = \frac{\theta_{q^{\mathbb{Z}}\gamma^{\mathbb{Z}}}(z\varphi)}{\theta_{q^{\mathbb{Z}}\gamma^{\mathbb{Z}}}(z)\theta_{q^{\mathbb{Z}}\gamma^{\mathbb{Z}}}(\varphi)}$$

3 Lois de réciprocité quadratique de Gauss des corps quadratiques imaginaires

3.1 Introduction

Nous avons dans [8] donné une nouvelle démonstration de la loi de réciprocité quadratique pour les corps quadratiques imaginaires. Cette démonstration utilisait la fonction $\wp_L(z)$ de Weierstrass associé au réseau L.

Nous donnons en appendice 2 une nouvelle démonstration de ces résultats. Cette nouvelle méthode met en évidence l'intérêt des formes de Jacobi complexes dans l'étude de cette question et notamment celui des formes $D_L(z,\varphi)$ de niveau 2. Soit d un entier négatif sans facteur carré et soit K le corps quadratique imaginaire $\mathbb{Q}(\sqrt{d})$, considéré comme plongé dans $\mathbb{C}$. On désigne par O_K l'anneau des entiers de K, c'est un réseau complexe. On choisit une $\mathbb{Z}$ base de O_K, $\{\omega_1, \omega_2\}$ telle que $\mathrm{Im}(\omega_1/\omega_2) > 0$.

D'une façon plus précise, dans toute la suite on prendra

$$\omega_2 = 1 \text{ et } \omega_1 = \begin{cases} \sqrt{d} & \text{si } d \equiv 3 \pmod 4 \\ 1+\sqrt{d} & \text{si } d \equiv 2 \pmod 4 \\ \frac{1+\sqrt{d}}{2} & \text{si } d \equiv 1 \pmod 4 \end{cases} .$$

On sait qu'un système de représentants de $O_K/2O_K$ est donné

$$\{0, \omega_1, \omega_2, \omega_1 + \omega_2\}.$$

On sait aussi que les unités de O_K modulo $2O_K$ sont représentées par :

$$S = \begin{cases} \{1\} & \text{si } d \equiv 1 \pmod 8 \\ \{1, \omega_1\} & \text{si } d \equiv 2 \text{ ou } 3 \pmod 4 \\ \{1, \omega_1, 1+\omega_1\} & \text{si } d \equiv 5 \pmod 8 \end{cases}$$

Pour $\alpha, \beta \in O_K$ on note

$$\alpha = a + b\omega_1, \quad \beta = a' + b'\omega_1 \text{ avec } a, b, a', b' \in \mathbb{Z}.$$

Si $(\alpha, 2) = (\beta, 2) = 1$ il existe $\alpha_0, \beta_0 \in S$ tels que :

$$\alpha \equiv \alpha_0 \pmod{2O_K}, \beta \equiv \beta_0 \pmod{2O_K}.$$

3.2 Définitions

Définition 3.2.1 *Pour $\alpha, \beta \in O_K$, avec $(\alpha, 2) = (\beta, 2) = (\alpha, \beta) = 1$, on définit le symbole quadratique $(\frac{\alpha}{\beta})_2$ par*

$$\left(\frac{\alpha}{\beta}\right)_2 = \prod_{\sigma \in S_\beta} \varepsilon(\alpha, \sigma) \ ,$$

où $\alpha\sigma = \varepsilon(\alpha, \sigma)\gamma(\sigma)$ avec $\varepsilon(\alpha, \sigma) \in \{-1, 1\}$, $\gamma(\sigma) \in S_\beta$ et $S_\beta \cup -S_\beta$ est un système complet de représentants de $O_K/\beta O_K \backslash \{\bar{0}\}$.

3.3 Résultats

Enonçons, maintenant, la loi de réciprocité quadratique pour K.

Théorème 3.3.1 *Soient $\alpha, \beta \in O_K$ tels que $(\alpha, 2) = (\beta, 2) = (\alpha, \beta) = 1$. On a*

$$\boxed{\left(\frac{\alpha}{\beta}\right)_2 \left(\frac{\beta}{\alpha}\right)_2^{-1} = (-1)^{\frac{N(\alpha)-1}{2}\cdot\frac{N(\beta)-1}{2} + \frac{N(\alpha)-1}{2} E_{O_K}\left(\beta - \beta_0, \beta_0 \frac{\omega_1}{2}\right) + \frac{N(\beta)-1}{2} E_{O_K}\left(\alpha - \alpha_0, \alpha_0 \frac{\omega_1}{2}\right)}}$$

Corollaire 3.3.2 *Pour $d \equiv 1 \pmod 8$ et $(\alpha, 2) = (\beta, 2) = (\alpha, \beta) = 1$. On a alors*

$$\boxed{\left(\frac{\alpha}{\beta}\right)_2 \left(\frac{\beta}{\alpha}\right)_2^{-1} = (-1)^{\frac{b}{2}\cdot\frac{b'}{2} + \frac{b}{2}\cdot\frac{a'-1}{2} + \frac{b'}{2}\cdot\frac{a-1}{2}}}$$

Corollaire 3.3.3 *Pour $d \equiv 3 \pmod 4$ et $(\alpha, 2) = (\beta, 2) = (\alpha, \beta) = 1$. On a alors*

$$\boxed{\left(\frac{\alpha}{\beta}\right)_2 \left(\frac{\beta}{\alpha}\right)_2^{-1} = 1}$$

Corollaire 3.3.4 *Pour* $d \equiv 2 \pmod 4$ *et* $(\alpha,2)=(\beta,2)=(\alpha,\beta)=1$. *On a alors*

$$\boxed{\left(\frac{\alpha}{\beta}\right)_2\left(\frac{\beta}{\alpha}\right)_2^{-1}=\begin{cases}1 & si\ \alpha\equiv\beta\equiv 1 \pmod{2O_K}\\ (-1)^{\frac{a-1}{2}} & si\ \alpha\equiv 1 \pmod{2O_K}\ et\ \beta\equiv\omega_1 \pmod{2O_K}\\ (-1)^{\frac{b+b'}{2}} & si\ \alpha\equiv\beta\equiv\omega_1 \pmod{2O_K}\end{cases}}$$

Corollaire 3.3.5 *Pour* $d \equiv 5 \pmod 8$ *et* $(\alpha,2)=(\beta,2)=(\alpha,\beta)=1$. *On a alors*

$$\left(\frac{\alpha}{\beta}\right)_2\left(\frac{\beta}{\alpha}\right)_2^{-1}=\begin{cases}(-1)^{\frac{b}{2}\cdot\frac{b'}{2}+\frac{b}{2}\cdot\frac{a'-1}{2}+\frac{b'}{2}\cdot\frac{a-1}{2}} & si\ \alpha\equiv\beta\equiv 1 \pmod{2O_K}\\ (-1)^{(\frac{a}{2}+\frac{d-5}{8})\cdot(\frac{a'}{2}+\frac{d-5}{8})+(\frac{a}{2}+\frac{d-5}{8})\cdot(\frac{a'}{2}+\frac{b'-1}{2})+(\frac{a'}{2}+\frac{d-5}{8})\cdot(\frac{a}{2}+\frac{b-1}{2})} & si\ \alpha\equiv\beta\equiv\omega_1 \pmod{2O_K}\\ (-1)^{(\frac{a+b}{2}+\frac{d+3}{8})\cdot(\frac{a'+b'}{2}+\frac{d+3}{8})+(\frac{a+b}{2}+\frac{d+3}{8})\cdot\frac{b'-1}{2}+(\frac{a'+b'}{2}+\frac{d+3}{8})\cdot\frac{b-1}{2}} & si\ \alpha\equiv\beta\equiv 1+\omega_1 \pmod{2O_K}\\ (-1)^{\frac{b}{2}\cdot(\frac{a'}{2}+\frac{d-5}{8})+\frac{b}{2}\cdot(\frac{a'}{2}+\frac{b'-1}{2})+(\frac{a'}{2}+\frac{d-5}{8})\cdot\frac{a-1}{2}} & si\ \alpha\equiv 1,\beta\equiv\omega_1 \pmod{2O_K}\\ (-1)^{\frac{b}{2}\cdot(\frac{a'+b'}{2}+\frac{d+3}{8})+\frac{b}{2}\cdot\frac{b'-1}{2}+(\frac{a'+b'}{2}+\frac{d+3}{8})\cdot\frac{a-1}{2}} & si\ \alpha\equiv 1,\beta\equiv 1+\omega_1 \pmod{2O_K}\\ (-1)^{(\frac{a}{2}+\frac{d-5}{8})\cdot(\frac{a'+b'}{2}+\frac{d+3}{8})+(\frac{a}{2}+\frac{d-5}{8})\cdot\frac{b'-1}{2}+(\frac{a'+b'}{2}+\frac{d+3}{8})\cdot(\frac{a}{2}+\frac{b-1}{2})} & si\ \alpha\equiv\omega_1,\beta\equiv 1+\omega_1 \pmod{2O_K}\end{cases}$$

4 Eléments de Stickelberger quadratiques

4.1 Introduction

Le célèbre théorème de Stickelberger fournit des annulateurs du groupe des classes d'idéaux des corps cyclotomiques. La démonstration de ce théorème repose de manière essentielle sur la factorisation en produit d'idéaux premiers des sommes de Gauss, [19], [57].

Pour étudier le cas relatif, lorsqu'on remplace $\mathbb{Q}$ par un corps de nombres F, M.J. Taylor et Ph. Cassou-Noguès ont étudié dans [21] la factorisation en idéaux premiers de certaines résolvantes de Lagrange introduites par Abel et Jacobi. Ces résolvantes sont associées à une courbe elliptique munie d'un point d'ordre premier rationnel sur F. Elles jouent dans ce cas le rôle joué par les sommes de Gauss dans le cas cyclotomique. De telles résolvantes ont été étudiées par S.P. Chan, R. Schertz et A. Srivastav. Nous nous intéressons ici à de nouvelles résolvantes construites à l'aide des formes de Jacobi. Elles généralisent les résolvantes introduites précédemment. Le but de ce paragraphe est de décrire leur factorisation en produit d'idéaux premiers.

Nous disposons de deux manières différentes pour effectuer cette factorisation. La première est analogue à celle utilisée dans l'étude des sommes de Gauss, la deuxième se base essentiellement sur la formule de distribution additive satisfaite par les formes $D_L(z;\varphi)$.

La première méthode est développée dans [6] et [9]. Dans ce qui suit nous développons la deuxième. Nous en déduisons des éléments de Stickelberger quadratiques qui annulent certains groupes de classes dans une situation relative. Cette seconde méthode est développée dans [11] et [18].

4.2 Formules de distribution et d'inversion

Précisons quelques notations et définitions. On fixe un modèle de Weierstrass

$$\left(E, \frac{dx}{y}\right) \begin{cases} y^2 = 4x^3 - g_2(\Omega)x - g_3(\Omega), \\ g_k(\Omega) = d_k \sum\limits_{\rho\in\Omega,\rho\neq 0} \rho^{-2k}, \quad k \in \{2,3\}, \end{cases} \tag{1}$$

de la courbe elliptique E, de façon à ce que le réseau $\Omega \subset \mathbb{C}$ soit formé des périodes complexes de $\left(E, \frac{dx}{y}\right)$ et $d_2 = 60, d_3 = 140$.

On note $F = \mathbb{Q}(g_2(\Omega), g_3(\Omega))$ le corps de définition de ce modèle $\left(E, \frac{dx}{y}\right)$. Pour tout automorphisme $\sigma \in \mathrm{Aut}(\mathbb{C}/F)$ de $\mathbb{C}$ fixant F notons

$$\rho \longmapsto \rho^{[\sigma]}$$

l'application qui à un point $\rho \in \mathbb{C}/\Omega$ fait correspondre son image dans $\mathbb{C}/\Omega$ via l'action de σ sur les coordonnées $(\wp_\Omega(\rho), \wp'_\Omega(\rho))$ de son image dans le modèle de Weierstrass ci-dessus.

Définition 4.2.1 *Soit p un entier > 1. On note*

$$\langle\psi\rangle \subset E[p]$$

un sous-groupe cyclique d'ordre p du groupe $E[p]$ des points de p-torsion de E, de générateur fixé ψ. On désigne par φ un autre point de p-torsion de E, vérifiant $\varphi \notin \langle\psi\rangle$. On définit la fonction

$$z \to D_\Omega(z;\ \varphi, \langle\psi\rangle)$$

comme la forme de Jacobi

$$z \to D_{\Omega+\mathbb{Z}\psi}(z, -\varphi), \quad z \in \mathbb{C}\ ,$$

méromorphe sur $\mathbb{C}$, admettant Ω pour réseau de périodes et de diviseur

$$\sum_{\rho\in\langle\psi\rangle} (\varphi + \rho) - (\rho).$$

Elle est normalisée de sorte que

$$\lim_{z\to 0} zD_\Omega(z; \varphi, \langle\psi\rangle) = 1.$$

On pose dans la suite $\Lambda = \Omega + \mathbb{Z}\psi$.

Les propriétés d'*algébricité* de la fonction elliptique $z \mapsto D_\Omega(z; \varphi, \langle\psi\rangle)$, sont une conséquence de la proposition suivante :

Proposition 4.2.2 *On a les propriétés suivantes*

i) La fonction $z \longmapsto D_\Omega(z; \varphi, \langle\psi\rangle)$ est définie sur le corps $F(E[p])$, extension du corps F obtenue par adjonction des coordonnées des points de p-torsion de E.

ii) Pour tout $\sigma \in \mathrm{Aut}(\mathbb{C}/F)$*, on a*

$$D_\Omega(z;\varphi,\langle\psi\rangle)^\sigma = D_\Omega(z^{[\sigma]};\varphi^{[\sigma]},\langle\psi^{[\sigma]}\rangle)\ .$$

iii) En particulier, la fonction $z \mapsto D_\Omega(z;\varphi,\langle\psi\rangle)$ *est définie sur* $F(\varphi \bmod \Lambda,\ \langle\psi\rangle)$ *plus petite sous-extension de* $F(E[p])/F$ *sur laquelle sont à la fois définis le point (*φ *modulo* Λ*) et le sous-groupe* $\langle\psi\rangle = \Lambda/\Omega$*.*

Soit ℓ un entier > 1 premier à p, soient $\langle\alpha\rangle$ un sous-groupe cyclique de $E[\ell]$ d'ordre ℓ, et $\gamma \in E[\ell]$ un point de ℓ-torsion de E. *On suppose ici que* $\gamma \notin \langle\alpha\rangle$. On note $\mathcal{L}$ le réseau $\Omega + \mathbb{Z}\alpha$.

On a le résultat suivant :

Théorème 4.2.3 *On a*

*i) (***Distribution additive***)*

$$\sum_{t\in\langle\alpha\rangle} D_\Omega(z+t;\varphi,\langle\psi\rangle)e_\ell^\Omega(\gamma,t)^{-1} = D_\Omega\Big(z;\Big[\frac{1}{\ell}\Big]_p\varphi - \Big[\frac{1}{p}\Big]_\ell\gamma,\langle\alpha\rangle\oplus\langle\psi\rangle\Big)$$

où $e_\ell^\Omega : E[\ell]\times E[\ell] \longrightarrow \mu_\ell$ *désigne l'accouplement de Weil.*

*ii) (***Inversion***)On suppose que* (α,γ) *est une base de* $E[\ell]$ *sur* $\mathbb{Z}/\ell\mathbb{Z}$*. Alors, pour tout* $t \in \langle\alpha\rangle$*, on a*

$$\sum_{s\in\langle\gamma\rangle} D_\Omega(z;\Big[\frac{1}{\ell}\Big]_p\varphi - \Big[\frac{1}{p}\Big]_\ell s,\ \langle\alpha\rangle\oplus\langle\psi\rangle\Big)e_\ell^\Omega(s,t) = \ell D_\Omega(z+t;\ \varphi,\langle\psi\rangle)\ .$$

où $\left[\frac{1}{\ell}\right]_p$ *(resp.* $\left[\frac{1}{p}\right]_\ell$*) désigne l'inverse de* ℓ *dans* $\mathbb{Z}/p\mathbb{Z}$ *(resp. de* p *dans* $\mathbb{Z}/\ell\mathbb{Z}$*).*

Il est à remarquer que le membre de gauche de l'égalité (i) du théorème 4.2.3 est une résolvante de Lagrange ou encore une "somme de Gauss elliptique" dont la factorisation en idéaux premiers peut s'obtenir en utilisant le membre de droite de cette égalité.

Définition 4.2.4 *On forme le produit*

$$A_{p,\Omega}(\gamma,\langle\alpha\rangle) = \frac{1}{p}\prod_{\langle\psi\rangle\subset E[p]}\ \prod_{\varphi\mathrm{modulo}\langle\psi\rangle} D_\Omega\Big(\gamma;\Big[\frac{1}{\ell}\Big]_p\varphi - \Big[\frac{1}{p}\Big]_\ell\gamma,\langle\alpha\rangle\oplus\langle\psi\rangle\Big),$$

où φ *parcourt un système de représentants modulo* $\langle\psi\rangle$ *des points de* $E[p]\backslash\langle\psi\rangle$*, tandis que* $\langle\psi\rangle$ *décrit les sous-groupes cycliques d'ordre* p *de* $E[p]$*.*

Il résulte de la proposition 4.2.2 qu'il s'agit d'un élément de

$$F(\gamma \bmod \mathcal{L},\langle\alpha\rangle) \subset F(E[\ell])\ .$$

Compte tenu de cette même proposition 4.2.2 ci-dessus,on obtient

Proposition 4.2.5 *Soient* p *et* ℓ *des nombres premiers, tels que* $(\ell, p(p+1)) = 1$ *et* $\ell \geqslant 5$*. Posons* $N = F(\zeta_\ell + \zeta_\ell^{-1})$*. Alors*

i) $A_{p,\Omega}(\gamma,\langle\alpha\rangle) \in F(E[\ell])$ *;*

ii) si $\sigma \in \mathrm{Gal}\,(F(E[\ell])/F)$ *est défini par*

$$\gamma^{[\sigma]} = a_\sigma \gamma + b_\sigma \alpha, \quad \alpha^{[\sigma]} = \alpha$$

avec $(a_\sigma, b_\sigma) \in (\mathbb{Z}/\ell\mathbb{Z})^2$, $a_\sigma \neq 0$, *on a l'égalité*

$$A_{p,\Omega}(\gamma, \langle\alpha\rangle)^\sigma = e_\ell^\Omega(\gamma, \alpha)^{(p-1)(p+1)a_\sigma b_\sigma} A_{p,\Omega}(a_\sigma \gamma, \langle\alpha\rangle)\ ;$$

iii) $A_{p,\Omega}(-\gamma, \langle\alpha\rangle) = \varepsilon(p) A_{p,\Omega}(\gamma, \langle\alpha\rangle)$ *avec* $\varepsilon(p) = +1$ *(resp. -1) si* $p \geqslant 3$ *(resp.* $p = 2$*), et l'on a*

$$A_{p,\Omega}(\gamma, \langle\alpha\rangle)^\ell \in \begin{cases} F(\zeta_\ell) & \text{pour } p = 2 \\ N & \text{si } p \geqslant 3\ ; \end{cases}$$

iv) l'idéal $(A_{p,\Omega}(\gamma, \langle\alpha\rangle))$ *est un idéal ambige de l'extension* $F(E[\ell])/N$

4.3 Eléments de Stickelberger quadratiques : $\widetilde{\theta}_2(p), p$ premier

Supposons maintenant, dans toute la suite de ce paragraphe que les hypothèses suivantes sont satisfaites :

(H1) *Le point de paramètre complexe* α *est rationnel sur* F .

(H2) *Les entiers* ℓ *et* p *sont des nombres premiers tels que* $(\ell, p(p+1)) = 1$ *et* $\ell \geqslant 5$.

(H3) F *est une extension finie de* $\mathbb{Q}$ *linéairement disjointe de* $\mathbb{Q}(\zeta_\ell)$ *où* ξ_ℓ *est une racine primitive* ℓ*-ième de l'unité.*

On note $\Delta(\Omega) = g_2(\Omega)^3 - 27 g_3(\Omega)^2$ le discriminant du modèle de Weierstrass (1), réseau de périodes Ω, de E et l'on pose

$$\widetilde{n}_p = \frac{(p-1)(p+1)}{12}\ .$$

Pour tout entier t, $1 \leqslant t \leqslant l-1$, on note σ_t l'automorphisme de $\mathbb{Q}(\zeta_l)$ induit par $\zeta_l \mapsto \zeta_l^t$; par abus de notation, σ_t désigne également toute restriction ou prolongement "naturel" de cet automorphisme. On pose $\Gamma = \mathrm{Gal}(N/F)$ où $\Gamma = \{\sigma_t,\ 1 \leqslant t \leqslant (l-1)/2\}$.

Définition 4.3.1 *On définit l'élément de Stickelberger quadratique* $\widetilde{\theta}_2(p)$ *de* $\mathbb{Q}[\Gamma]$ *par :*

$$\widetilde{\theta}_2(p) = \sum_{t=1}^{(l-1)/2} \gamma(t)\sigma_t^{-1}, \quad \sigma_t \in \Gamma$$

avec

$$\gamma(t) = (p^2 - p)\beta(t) + \sum_{s=1}^{p-1} \alpha(t, s)$$

$$\begin{aligned} \beta(t) &= \frac{l}{p}\Big(\frac{t}{l}\{\frac{tp}{l}\} + \inf(0, 1 - \frac{t}{l} - \{\frac{tp}{l}\})\Big) \\ \alpha(t, s) &= -tp\{\frac{a}{lp}\} + lp\inf(\frac{t}{l}, \{\frac{a}{lp}\}) \end{aligned}$$

et

$$a = lsx + pty,$$

où $x, y \in \mathbb{Z}$ *sont choisis tels que* $lx - py = 1$.

On pose $\{z\}$ *la partie fractionnaire du nombre réel* z.

L'élément $\widetilde{\theta}_2(p)$ de $\mathbb{Q}[\Gamma]$ est dit "quadratique" car il satisfait la congruence suivante :

$$\widetilde{\theta}_2(p) \equiv \frac{12\widetilde{n}_p}{\ell} \sum_{t=1}^{(\ell-1)/2} t^2 \sigma_t^{-1} \pmod{\mathbb{Z}[\Gamma]} \tag{6}$$

et que

$$\ell\widetilde{\theta}_2(p) \in \mathbb{Z}[\Gamma] \ .$$

Pour tout idéal premier $\mathfrak{p}$ de F on note $r_\mathfrak{p}$ la valuation $\mathfrak{p}$-adique du discriminant minimal $\mathfrak{D}_{E/F}$ de la courbe E/F.

Soit P le point de la courbe elliptique de paramètre complexe α. On désigne par $\mathfrak{R}(E,P)$ l'ensemble des diviseurs premiers $\mathfrak{p}$ de $\mathfrak{D}_{E/F}$, premier à l, pour lesquels la réduction de P modulo $\mathfrak{p}$ est un point régulier de la courbe réduite. On pose

$$\mathfrak{D}_{E/F,reg} = \prod_{\mathfrak{p}\in\mathfrak{R}(E,P)} \mathfrak{p}^{r_\mathfrak{p}}.$$

Si $\mathfrak{a}$ et $\mathfrak{b}$ sont des idéaux fractionnaires de $F(E[\ell])$ écrivons

$$\mathfrak{a} \equiv \mathfrak{b} \pmod{\ell}$$

lorsque les diviseurs de $\mathfrak{a}\mathfrak{b}^{-1}$ divisent ℓ.

Sous les hypothèses (H1) à (H3) précédentes, on a les deux résultats suivants :

Théorème 4.3.2 *Tout idéal premier $\mathfrak{p}$ de $\mathfrak{R}(E,P)$ possède un relèvement $\mathfrak{P}$ dans N tel que :*

$$\Big(A_{p,\Omega}(\gamma,\langle\alpha\rangle)\Big)^l \Big(\mathfrak{D}_{E/F}/(\Delta(\Omega))\Big)^{l\widetilde{n}_p} \equiv \Big(\prod_{\mathfrak{p}\in\mathfrak{R}(E,P)} \mathfrak{P}^{r_\mathfrak{p}}\Big)^{l\widetilde{\theta}_2(p)} \ (mod\ l)$$

Théorème 4.3.3 *On a aussi*

$$\left(\prod_{t=1}^{(\ell-1)/2} A_{p,\Omega}(t\gamma,\langle\alpha\rangle)\right) \equiv \Big((\Delta(\Omega))\mathcal{D}_{E/F}^{-1}\Big)^{\frac{\ell-1}{2}\widetilde{n}_p} \mathcal{D}_{E/F,\mathrm{reg}}^{\frac{(\ell+1)(\ell-1)}{2}\widetilde{n}_p} \pmod{\ell} \ .$$

4.4 Annulation de groupes de classes

Comme dans le cas du théorème de Stickelberger classique le théorème 4.3.2 nous permet d'introduire un sous-quotient du groupe des classes d'idéaux de N annulé par $l\widetilde{\theta}_2(p)$.

On rappelle que l est un nombre fixé, $l \geqslant 5$. Le nombre premier p peut-être considéré comme auxilliaire.

Définition 4.4.1 *On appelle l-groupe des classes du corps de nombres L et l'on note $Cl'(L)$ le quotient du groupe des classes de L par le sous-groupe engendré par les classes des relèvements premiers de l dans L.*

Si M/L est une extension de corps de nombres on note $Cl'(M/L)$ le conoyau de l'homomorphisme induit par l'extension des scalaires de $Cl'(L)$ dans $Cl'(M)$. Soit F tel que $F \cap \mathbb{Q}(\xi_l) = \mathbb{Q}$. A tout couple (E, P) où E est une courbe elliptique définie sur F et P un point rationnel sur F d'ordre l et à tout point $Q \in E[l] \setminus \mathbb{Z}P$ nous associons l'idéal de N

$$\mathfrak{M}(E, P, Q) = \prod_{\mathfrak{p} \in \mathfrak{R}(E,P)} \mathfrak{P}^{r_\mathfrak{p}} \tag{4.4.1}$$

introduit dans le théorème 4.3.2. On remarque que cet idéal est indépendant de p. On déduit de la proposition 4.2.5 et du paragraphe 6.B de [9] les égalités

$$\mathfrak{M}(E, P, a_\omega P + b_\omega Q) = \mathfrak{M}(E, P, Q)^\omega,$$

Pour tout $\omega \in \mathrm{Gal}(F(E[l])/F)$.

Définition 4.4.2 *On désigne par $\mathcal{E}(N)$ (resp. $\mathcal{E}(N/F)$) le sous-groupe de $Cl'(N)$ (resp. $Cl'(N/F)$)) engendré par les images des idéaux $\mathfrak{M}(E, P, Q)$ associés aux couples (E, P) rationnels sur F.*

On déduit immédiatement du théorème 4.3.2

Théorème 4.4.3 *(i) Pour tout nombre premier p tels que $(l, p(p+1)) = 1$, alors pour $p \geqslant 3$ (resp. $p = 2$) l'élément $l\widetilde{\theta}_2(p)$ (resp. $2l\widetilde{\theta}_2(2)$) annule le groupe $\mathcal{E}(N/F)$.*

(ii) On a l'inclusion :

$$\Big(\mathcal{E}(N)\Big)^{\sum_{t=1}^{\frac{l-1}{2}} t^2\sigma_t^{-1}} \subset Cl'(N)^l.$$

Remarque 4.4.4 Il faut noter que pour un corps de nombres F, L. Merel a montré qu'il n'existe qu'un nombre fini de nombres premiers l pour lesquels il existe des couples (E, P) rationnels sur F. La liste de ces nombres premiers l est connue lorsque $F = \mathbb{Q}$ grâce à Mazur et lorsque $F/\mathbb{Q}$ est un corps quadratique grâce à Kamieny.

5 Structure galoisienne des anneaux d'entiers

5.1 Introduction

Dans ce paragraphe nous décrivons notre contribution à l'étude du problème de la structure galoisienne des anneaux d'entiers de corps de nombres attachés aux courbes elliptiques avec ou sans multiplication complexe Nous résolvons ce problème pour une large classe de corps de nombres. Plus précisement, soit L/F une extension abélienne finie. Soit O_L désigne l'anneau des entiers de L et G le groupe de Galois de L/F et $\mathcal{A}_{L/F} = \{x \in F[G] : xO_L \subset O_L\}$ l'ordre associé à L sur F. On a alors les résultats suivants

5.2 Situations cyclotomique et multiplication complexe

Nos références pour cette section sont [20], [22], [23], [28], [52]. Nous rappelons les principaux résultats classiques suivants :

Théorème 5.2.1 *(Hilbert, Leopoldt, Speiser) Soit L/F une extension abélienne finie. Pour $F = \mathbb{Q}$, alors O_L est un $\mathcal{A}_{L/F}$-module libre de rang 1.*

Théorème 5.2.2 *(Chan, Lim) Soit L/F une extension abélienne finie. Pour $L = \mathbb{Q}(\xi_{mn})$, $F = \mathbb{Q}(\xi_m)$, $m, n \geqslant 1$. On a alors, O_L est un $\mathcal{A}_{L/F}$-module libre de rang 1.*

Théorème 5.2.3 *(Cassou-Noguès, Chan, Schertz, Taylor) Soient K un corps quadratique imaginaire, $L = K(\mathfrak{p}^{r+m})$, $F = K(\mathfrak{p}^m)$ où $\mathfrak{p}$ est un idéal premier de K. Alors O_L est un $\mathcal{A}_{L/F}$-module libre de rang 1 dans les cas suivants :*

i) *2 est décomposé et $1 \leqslant m \leqslant r$.*

ii) *2 est ramifié et soit $1 \leqslant m \leqslant r$ lorsque p est décomposé ou $1 \leqslant m \leqslant r-2$ lorsque p est ramifié ou $1 \leqslant m \leqslant r-1$ lorsque p est inerte.*

iii) *2 est inerte et $1 \leqslant m \leqslant r$ avec p est décomposé.*

5.3 Cas des corps de division

Nos références pour ce paragraphe sont [11] et [21].

Soient $l \geqslant 5$ un nombre premier et K un corps de nombres linéairement disjoint à $\mathbb{Q}(\xi_l)$. On désigne par $(E/K, P, l)$ le triplet formé d'une courbe elliptique définie sur K qui est munie d'un point P d'ordre l et rationnel sur K. On désigne par

$$S_{E,l} = \{\mathfrak{p} \text{ premier de } K \text{ tels que } : \quad v_{\mathfrak{p}}(j(E)) < 0 \text{ ou } \mathfrak{p}|l\}\,.$$

Théorème 5.3.1 *On a les propriétés suivantes :*

i) *L'extension $(K(E[l])/K(\xi_l))$ est cyclique de degré l et son groupe de Galois G est représentable matriciellement par*

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}, \text{ avec } b \in \mathbb{F}_l.$$

ii) *L'extension $(K(E[l])/K(\xi_l))$ est non ramifiée en dehors de $S_{E,l}$.*

iii) *Soit $\mathfrak{p} \in S_{E,l}$, non au-dessus de l. Alors on a : $\mathfrak{p}$ se ramifie totalement dans $(K(E[l])/K(\xi_l))$ si et seulement si $(v_{\mathfrak{p}}(j(E)), l) = 1$.*

iv) *On suppose que $(v_{\mathfrak{p}}(j(E)), l) = 1$ pour tout idéal premier $\mathfrak{p}$ au-dessus de l en lequel E à mauvaise réduction en $\mathfrak{p}$. Alors l'extension $(K(E[l])/K(\xi_l))$ est totalement ramifiée en l.*

v) *Soit (l, p) un couple de nombres premiers distincts tels que $(p(p^2-1), l) = 1$. On a alors, d'après la définition 4.2.1, un générateur galoisien pour $K(E[l])/F$*

$$K(E[l]) = F(A_{p,\Omega}(\gamma, \langle\alpha\rangle)), \text{ où } F = K(\xi_l))$$

Notre résultat de structure galoisienne est le suivant :

Théorème 5.3.2 *Soit $L = K(E[l])$ et $F = K(\xi_l)$. On suppose que P définit un point régulier modulo tout premier où E a mauvaise réduction. Pour tout triplet $(E/K, P, l)$ où le discriminant minimal de E sur K possède une décomposition dans O_K de la forme $\mathfrak{p}_0^{r_0}\mathfrak{p}_1^{r_1}...\mathfrak{p}_s^{r_s}$ tel qu'il existe un élément $a \in L$ et $a \notin F$ vérifiant*

$$a^l O_F = \prod_{(r_i,l)=1} \mathfrak{P}_i,$$

où les $\mathfrak{P}_i$ sont les relèvements premiers des $\mathfrak{p}_i$ dans O_F.

On a alors O_L est un $\mathcal{A}_{L/F}$-module libre de rang 1 et engendré par l'élément $\sum_{i=0}^{l-1} a^i$.

6 Amélioration d'un théorème de Coates, Kubert et Robert sur les unités de Stark

6.1 Introduction et généralités

Les résultats contenus dans ce paragraphe sont extraits de [16].

Dans ce travail on montre comment on peut appliquer la formule de distribution multiplicative satisfaite par les formes de Jacobi D_L, contenue dans le théorème 2.5.1, pour améliorer un théorème dû à D. Kubert concernant la formule de distribution satisfaite par les fonctions elliptiques et un résultat de J. Coates, D. Kubert et G. Robert concernant la formule de distribution satisfaite par une certaine fonction $\zeta(z; L, \Lambda)$.

Soient L et Λ deux réseaux complexes tels que $L \subseteq \Lambda$; on remarque qu'alors $[\Lambda : L]$ est fini. A chaque fois qu'on choisit une base ordonnée (w_1, w_2) de L sur $\mathbb{Z}$ de sorte que pour des entiers m et n strictement positifs, le couple (w_1', w_2') définie par

$$w_1' = \frac{w_1}{m}, \qquad w_2' = \frac{w_2}{n},$$

soit une base de Λ sur $\mathbb{Z}$, on dira que le système $\mathcal{R}$ de représentants de Λ/L défini par

$$\mathcal{R} = \left\{ \frac{k}{m}\omega_1 + \frac{k'}{n}\omega_2, 0 \leqslant k \leqslant m-1; 0 \leqslant k' \leqslant n-1 \right\}$$

est **le** système de représentants de Λ/L **adapté** à la base (w_1, w_2). Cette manière de parler est justifiée par le fait suivant, très facile à vérifier : si (w_1, w_2) est une base ordonnée de L sur $\mathbb{Z}$, il peut arriver qu'il n'existe pas un couple ordonné (m, n) d'entiers strictement positifs tels que $(w_1/m, w_2/n)$ soit une base de Λ sur $\mathbb{Z}$. S'il existe un tel couple, il est complètement determiné par la base ordonnée (w_1, w_2) et en outre $[\Lambda : L] = mn$. La théorie des groupes abéliens de type fini assure qu'on peut toujours choisir une base ordonnée (w_1, w_2) de L telle qu'il existe un système de représentants de Λ/L adapté à la base (w_1, w_2), et même avec m divisant n. Cette

dernière condition ne sera pas en général imposée dans la suite(remarquez qu'on peut changer w_1 par $-w_1$, sans changer m ni n). Par contre on choisira (w_1, w_2) telle que $\mathrm{Im}(w_1/w_2) > 0$.

En choisissant une base ordonnée $\mathcal{B} = (w_1, w_2)$ de L sur $\mathbb{Z}$ telle qu'il existe le système de représentants $\mathcal{R}$ de Λ/L adapté à la base $\mathcal{B}$, la racine huitième de l'unité $\epsilon_{\mathcal{B}}(0)$ définie par

$$\epsilon_{\mathcal{B}}(0) = e\left(\frac{3mn + m - n - 3}{8}\right),$$

ne dépend que de $\mathcal{B}$.

6.2 Enoncé des résultats

Si L et Λ sont des réseaux complexes tels que $L \subseteq \Lambda$, on définit la fonction $\mathcal{K}(z; L, \Lambda)$ par l'égalité

$$\mathcal{K}(z; L, \Lambda) = \frac{\mathcal{K}_L(z)^{[\Lambda:L]}}{\mathcal{K}_\Lambda(z)}, \text{ ([44] pp.227–229).}$$

Le théorème que nous obtenons est une relation de distribution multiplicative satisfaite par cette fonction $\mathcal{K}(z; L, \Lambda)$. Ce théorème améliore certains résultats dûs à J. Coates,[24] Appendice, Theorem 8, D. Kubert,[43], Theorem 3.2 et G. Robert [50] relation (1).

Soient L et L' deux réseaux complexes tels que $L \subseteq L'$. On désigne par M un réseau tel que $L \subseteq M$ et $M \cap L' = L$, et on pose $M' = M + L'$; on remarque ainsi que l'inclusion $L' \subset M'$ induit un isomorphisme de groupes $L'/L \simeq M'/M$. Soit $\mathcal{B} = \{w_1, w_2\}$ une base de L sur $\mathbb{Z}$ telle que $\mathrm{Im}(w_1/w_2) > 0$ et de sorte que pour des entiers m et n strictement positifs, le couple $w_1' = w_1/m$, $w_2' = w_2/n$ soit une base de L' sur $\mathbb{Z}$, et soit $\mathcal{R}$ le système de représentants de L'/L adapté à la base (w_1, w_2) ; soit $\tilde{\mathcal{B}} = \{\tilde{w}_1, \tilde{w}_2\}$ une base de M sur $\mathbb{Z}$ telle que $\mathrm{Im}(\tilde{w}_1/\tilde{w}_2) > 0$ et de sorte que pour des entiers $\tilde{m}$ et $\tilde{n}$ strictement positifs, le couple $\tilde{w}_1' = \tilde{w}_1/\tilde{m}$, $\tilde{w}_2' = \tilde{w}_2/\tilde{n}$ soit une base de M' sur $\mathbb{Z}$. On remarque que $\tilde{m}\tilde{n} = mn$.

Théorème 6.2.1 *Sous les hypothèses ci-dessus, pour tout système de représentants $\mathcal{S}$ de M/L, on a l'égalité*

$$\prod_{\alpha \in \mathcal{S}} \mathcal{K}(z + \alpha; L, L')$$

$$= \mathcal{K}(z; M, M') \cdot e(E_L(\sum_{t \in \mathcal{R}} t, \sum_{\alpha \in \mathcal{S}} \alpha)) \cdot \frac{\epsilon_{\mathcal{B}}(0)^{[M:L]}}{\epsilon_{\tilde{\mathcal{B}}}(0)} \cdot \frac{\eta^2(w_1', w_2')^{[M:L]}}{\eta^2(w_1, w_2)^{[M':L]}} \cdot \frac{\eta^2(\tilde{w}_1, \tilde{w}_2)^{[M':M]}}{\eta^2(\tilde{w}_1', \tilde{w}_2')}.$$

Lorsque $[L' : L]$ est impair, on considère la fonction $\zeta(z; L, L')$ définie pour $z \notin L'$ par le produit fini suivant

$$\zeta(z; L, L') = \prod_{\bar{t} \in T} \frac{1}{\wp_L(z) - \wp_L(t)}$$

où T vérifie la réunion disjointe $T \cup -T \cup \{0\} = L'/L$ (voir [44], p. 228).

Corollaire 6.2.2 *(Coates-Kubert-Robert revisité) Sous les hypothèses du théorème précédent et lorsque $[L' : L]$ est impair, on a*

$$\prod_{\alpha \in \mathcal{S}} \zeta(z + \alpha; L, L')$$

$$= \zeta(z; M, M')e(E_L(\sum_{t\in\mathcal{R}} t, \sum_{\alpha\in\mathcal{S}} \alpha)) \cdot \frac{\epsilon_{\mathcal{B}}(0)^{[M:L]}}{\epsilon_{\tilde{\mathcal{B}}}(0)} \cdot \frac{\eta^2(w_1', w_2')^{[M:L]}}{\eta^2(w_1, w_2)^{[M':L]}} \cdot \frac{\eta^2(\tilde{w}_1, \tilde{w}_2)^{[M':M]}}{\eta^2(\tilde{w}_1', \tilde{w}_2')}.$$

Il est à noter que non seulement ce corollaire 6.2.2 améliore les résultats des auteurs précdents, obtenus sous l'hypothèse plus restrictive où $[L' : L]$ est premier avec 6. Mais également il fournit une nouvelle méthode de démonstration. On rappelle que si L est un réseau complexe et (w_1, w_2) et $(\hat{w}_1, \hat{w}_2)$ sont des bases de L sur $\mathbb{Z}$ telles que $\mathrm{Im}(w_1/w_2) > 0$ et $\mathrm{Im}(\hat{w}_1/\hat{w}_2) > 0$, on a $\eta^{24}(w_1, w_2) = \eta^{24}(\hat{w}_1, \hat{w}_2)$. On peut donc définir

$$\Delta(L) = \eta^{24}(w_1, w_2),$$

où (w_1, w_2) est n'importe quelle base de L sur $\mathbb{Z}$ telle que $\mathrm{Im}(w_1/w_2) > 0$. Alors, par élévation à la puissance 12-ième, le corollaire 6.2.2 devient le corollaire suivant, qui est un résultat classique (voir par exemple [55], **p. 50**).

Corollaire 6.2.3 *Soient L et L' deux réseaux complexes tels que $L \subseteq L'$ et $[L' : L]$ est impair. On désigne par M un réseau tel que $L \subseteq M$ et $M \cap L' = L$, et on pose $M' = M + L'$. Alors, pour tout système de représentants $\mathcal{S}$ de M/L, on a*

$$\prod_{\alpha\in\mathcal{S}} \zeta(z + \alpha; L, L')^{12} = \zeta(z; M, M')^{12} \cdot \frac{\Delta(L')^{[M:L]}}{\Delta(L)^{[M':L]}} \cdot \frac{\Delta(M)^{[M':M]}}{\Delta(M')}.$$

Il est à noter que le nombre

$$e(E_L(\sum_{t\in\mathcal{R}} t, \sum_{\alpha\in\mathcal{S}} \alpha)) \cdot \frac{\epsilon_{\mathcal{B}}(0)^{[M:L]}}{\epsilon_{\tilde{\mathcal{B}}}(0)} \cdot \frac{\eta^2(w_1', w_2')^{[M:L]}}{\eta^2(w_1, w_2)^{[M':L]}} \cdot \frac{\eta^2(\tilde{w}_1, \tilde{w}_2)^{[M':M]}}{\eta^2(\tilde{w}_1', \tilde{w}_2')}$$

fournit une racine 12-ième de la quantité

$$\frac{\Delta(L')^{[M:L]}}{\Delta(L)^{[M':L]}} \cdot \frac{\Delta(M)^{[M':M]}}{\Delta(M')}.$$

Il faut dire que, lorsque $[L' : L]$ est premier avec 6, on est proche du remarquable résultat du travail de G. Robert sur la racine 12-ième canonique de la fonction delta ([50]).

7 Formule de distribution pour la fonction φ de Siegel

7.1 Introduction

Les résultats contenus dans ce paragraphe sont comme précédemment démontrés dans [16]. Le théorème 7.2.1 contient une formule de distribution que satisfait la fonction φ_L de Siegel. Cette formule améliore celle établie par F. Jarvis [38, 39] et J. Wildeshaus [60]. Les formules données dans le théorème 0.1 de [39] et le théorème 0.2 de [38] sont les mêmes mais le principe de démonstration n'est pas le même. En outre elles sont "exactes" à une racine de l'unité près.

Nous proposons ici une nouvelle façon de procèder qui nous permet également de déterminer la racine de l'unité qui manquait aux formules de F. Jarvis.

On utilise cette formule de distribution pour l'analyse de l'analogue elliptique de la conjecture polylogarithmique de Zagier, voir [38], [39], [59], [60].

7.2 Enoncé du résulat

Soit L un réseau complexe. Si (w_1, w_2) désigne une base de L telle que $\mathrm{Im}(w_1/w_2) > 0$, rappelons que la fonction de Siegel associée à L et à la base (w_1, w_2) de L est définie par

$$\varphi_L(z; w_1, w_2) = \mathcal{K}_L(z)\eta^2(w_1, w_2), \tag{4.1}$$

où η est la fonction de Dedekind, dont le carré a été défini dans (1.11). La fonction φ_L de Siegel est homogène de degré -1. Elle s'exprime à l'aide des formes de Jacobi introduites précédemment.

Pour tout diviseur $\mathcal{D} = \sum_{i=1}^{r} n_i(a_i)$ de $\mathbb{C}$, principal ou non, on définit la forme

$$\varphi_L(\mathcal{D}; w_1, w_2) = \prod_{a_i \notin L} \varphi_L(a_i; w_1, w_2)^{n_i}, \tag{4.2}$$

et pour tout $t \in \mathbb{C}$, on pose

$$\mathcal{D} \oplus t = \sum_{i=1}^{r} n_i(a_i + t).$$

Théorème 7.2.1 *Soient L et Λ deux réseaux complexes tels que $L \subseteq \Lambda$; soit $\mathcal{B} = (w_1, w_2)$ une base ordonnée de L sur $\mathbb{Z}$ telle que $\mathrm{Im}(w_1/w_2) > 0$ et de sorte que pour des entiers m et n strictement positifs, le couple $w_1' = w_1/m, w_2' = w_2/n$ soit une base de Λ sur $\mathbb{Z}$, et soit $\mathcal{R}$ le système de représentants de Λ/L adapté à la base (w_1, w_2). Alors on a*

$$\varphi_\Lambda(\mathcal{D}; w_1', w_2') = \epsilon_{\mathcal{B}}(0)^2 \cdot e(E_L(\sum_{t\in\mathcal{R}} t, y)) \cdot \prod_{t\in\mathcal{R}} \varphi_L(\mathcal{D} \oplus t; w_1, w_2)$$

pour tout diviseur $\mathcal{D} = (x + y) + (x - y) - 2(x) - 2(y) + 2(0)$ vérifiant

$$Supp(\mathcal{D}) \cap \Lambda = \{0\}.$$

Remarque 7.2.2 Notons que Ce nombre complexe $\epsilon_{\mathcal{B}}(0)^2 e(E_L(\sum_{t\in\mathcal{R}} t, y))$ ne figurait pas dans la formule originale de Jarvis, il dépend du choix de la base $\mathcal{B}$ de L telle qu'il existe le système de représentants $\mathcal{R}$ de Λ/L adapté à la base $\mathcal{B}$. Lorsque y est la deuxième coordonnée d'un point de s-division de la courbe elliptique $\mathbb{C}/L$, ce nombre est une racine $8s$-ième de l'unité.

8 Sommes d'Apostol–Dedekind–Zagier elliptiques multiples

8.1 Introduction

Les sommes d'Apostol-Dedekind-Zagier ont plusieurs applications dans divers domaines : Lois de réciprocité quadratiques [46], calcul du nombre des classes des corps quadratiques et fonctions L [47], étude du problème des nombres aléatoires (ou pseudo-aléatoires)[26], la formule de partition de Hardy-Ramanujan [33], [48], formule d'indice de Hirzebruch, évaluant la signature de certains invariants d'homologie de variétés différentielles à l'aide de la fonction cotangente, géométrie algébrique (Théorème de Riemann-Roch) [4], [31],[32], étude de la cohomologie d'Eisenstein de $\mathrm{SL}_2(\mathbb{Z})$ [46] pour $\mathrm{SL}_2(\mathbb{O}_K)$($K$ corps quadratique imaginaire) voir [54, 58]...etc.

Pour plus d'informations sur les applications des sommes de Dedekind en théorie des nombres se reporter aux livres [35, 37].

L'objectif de ce paragraphe est d'introduire puis étudier des analogues elliptiques aux sommes multiples d'Apostol-Dedekind-Zagier. Ces nouvelles sommes sont définies en terme de formes de Jacobi à deux variables $D_\tau(z;\varphi)$ où τ appartient au demi-plan de Poincaré. Pour φ fixé et $\mathrm{Im}(\tau)\to\infty$, ces sommes redonnent les sommes multiples de Dedekind étudiées par Zagier [62] ainsi que les sommes d'Apostol [1, 2]. Nous démontrons une loi de réciprocité "à la Dedekind" satisfaite par ces sommes.

Le long de ce paragraphe on considère L un réseau complexe et $O_L=\{x\in L | xL\in L\}$ ordre associé à L, p, a_0, a_1, a_2, ..., a_n éléments non nuls de $O_L\backslash O_L^\times$ et deux à deux premiers entre eux.

8.2 Sommes elliptiques multiples de Dedekind à paramètre [13]

On considère le réseau complexe $L=\mathbb{Z}\tau+\mathbb{Z}$.

Définition 8.2.1 *Pour tout p élément non nul de $O_L\backslash O_L^\times$ et tout entier naturel m, on fixe E_p un système de représentants de $L/pL\backslash\{0\}$, on définit la somme elliptique de Dedekind $d(p;a_1,...,a_n;m,\varphi,z,\tau)$ paramétrée par les complexes φ, z :*

$$d(p;a_1,...,a_n;m,\varphi,z,\tau)=\frac{1}{p}\sum_{w\in E_p} e\left(E_L(w,\varphi)\right) D_\tau\left(z+\frac{w}{p};\varphi\right)^m\prod_{k=1}^n D_\tau\left(a_k\frac{w}{p};\varphi\right).$$

Définition 8.2.2 *Pour tout $n\in\mathbb{N}$ et $a_0,a_1,\ldots,a_n\in O_L\backslash O_L^\times$, on définit les $M_k(a_0,\ldots,a_n;\varphi,\tau)$ par :*

$$a_0a_1\cdots a_n\prod_{k=0}^n zD_\tau\left(a_kz;\varphi\right)=\sum_{k\geqslant 0}M_k(a_0,\ldots,a_n;\varphi,\tau)z^k.$$

On a

Proposition 8.2.3 *Pour tout $n\in\mathbb{N}$ et $a_0,a_1,\ldots,a_n\in O_L\backslash O_L^\times$, les coefficients $M_k(a_0,\ldots,a_n;\varphi,\tau)$ vérifient les relations :*

$$\begin{aligned} M_k(a_0,\ldots,a_n;\varphi,\tau) &= \sum_{\substack{i_0+\cdots+i_n=k\\ 0\leqslant i_0,\ldots,i_n\leqslant k}} a_0^{i_0}\cdots a_n^{i_n}d_{i_0}(\varphi)\cdots d_{i_n}(\varphi);\\ M_k(a_0,\ldots,a_n;-\varphi,\tau) &= (-1)^kM_k(a_0,\ldots,a_n;\varphi,\tau).\end{aligned}$$

On a le résultat suivant

Théorème 8.2.4 *(loi de réciprocité) Soit $d \in O_L \backslash O_L^{\times}$ non nul tels que $a_0 + ... + a_n + m \equiv 0 \pmod{dO_L}$. Alors, pour tout φ paramètre de point de d-division non nul de $\mathbb{C}/L$,*

i) Si $m = 0$, on a : $\displaystyle\sum_{k=0}^{n} d(a_k; a_0, \cdots, \check{a}_k, \cdots, a_n; 0, \varphi, z, \tau) = -\frac{M_n(a_0, \cdots, a_n; \varphi, \tau)}{a_0 a_1 \cdots a_n}.$

ii) Si $1 \leqslant m \leqslant d$ et z tel que $a_0 \cdots a_n z \notin L$, on a :

$$-\sum_{k=0}^{n} d(a_k; a_0, \cdots, \check{a}_k, \cdots, a_n; m, \varphi, z, \tau) =$$

$$\sum_{l=0}^{m-1} \frac{1}{l!} \frac{d^l}{dx^l} \left\{ \prod_{i=0}^{n} D_\tau (a_i x, \varphi) \right\}_{|x=-z} M_{m-l-1}(\overbrace{1, \cdots, 1}^{m \ fois}; \varphi, \tau) + \sum_{l=0}^{n} \frac{1}{l!} \frac{d^l}{dx^l} \left\{ D_\tau (x; \varphi)^m \right\}_{|x=z} \frac{M_{n-l}(a_0, \cdots a_n; \varphi, \tau)}{a_0 a_1 \cdots a_n}.$$

On observe que les hypothèses du théorème 8.2.4 impliquent que la somme $d(a_k; a_0, \cdots, \check{a}_k, \cdots, a_n; 0, \varphi, z, \tau)$ ne dépend pas du choix du système E_{a_k}.

8.3 Sommes elliptiques d'Apostol-Dedekind-Zagier [13]

Définissons les sommes elliptiques multiples d'Apostol-Dedekind-Zagier et montrons qu'elles satisfont une loi de réciprocité.

Définition 8.3.1 *Soient p élément non nul de $O_L \backslash O_L^{\times}$ et m, k deux entiers naturels. On fixe E_p un système de représentants de $L/pL\backslash\{0\}$. On définit la somme elliptique multiple d'Apostol-Dedekind-Zagier (paramétrée par φ) associée aux entiers $p; a_1, ..., a_n$ non nuls de $O_L \backslash O_L^{\times}$, par*

$$S_k(p; a_1, ..., a_n; m, \varphi, \tau) = \frac{1}{p} \sum_{w \in E_p} e\left(E_L(w, \varphi)\right) \frac{1}{k!} \frac{d^k}{dz^k} \left\{ D_\tau \left(z + \frac{w}{p}; \varphi \right)^m \right\}_{|z=0} \prod_{j=1}^{n} D_\tau \left(a_j \frac{w}{p}; \varphi \right).$$

Théorème 8.3.2 *(loi de réciprocité) Soient $d \in O_L \backslash O_L^{\times}$ et $m \in \mathbb{N}$ tels que $a_0 + ... + a_n + m \equiv 0 \pmod{dO_L}$. Alors, pour tout φ paramètre de point de d-division non nul de $\mathbb{C}/L$ et tout $k \in \mathbb{N}$, on a*

(1) $$Si\ m = 0 : -\sum_{l=0}^{n} S_k(a_l; a_0, \cdots, \check{a}_l, \cdots, a_n; m, \varphi, \tau) = \begin{cases} 0 & si \ \ k \geqslant 1 \\ \frac{M_n(a_0, \cdots, a_n; \varphi, \tau)}{a_0 a_1 \cdots a_n} & si\ k = 0 \end{cases}.$$

(2) $$Si\ m \geqslant 1 : -\sum_{l=0}^{n} S_k(a_l; a_0, \cdots, \check{a}_l, \cdots, a_n; m, \varphi, \tau) = \sum_{l=0}^{n} C_{k+l}^{l} \frac{M_{n-l}(a_0, \cdots a_n; \varphi, \tau)}{a_0 a_1 \cdots a_n} M_{m+k+l}(\overbrace{1, \cdots, 1}^{m \ fois}; \varphi, \tau)$$
$$+ \sum_{l=0}^{m-1} (-1)^k C_{k+l}^{l} M_{m-l-1}(\overbrace{1, \cdots, 1}^{m \ fois}; \varphi, \tau) \frac{M_{n+k+l+1}(a_0, \cdots a_n; \varphi, \tau)}{a_0 a_1 \cdots a_n}$$

On observe que les hypothèses du théorème 8.3.2 impliquent que la somme $S(a_k; a_0, \cdots, \check{a}_k, \cdots, a_n; 0, \varphi, z, \tau)$ ne dépend pas du choix du système E_{a_k}.

8.4 Application 1 : Sommes multiples de Dedekind-Zagier à paramètre [14]

Dans ce paragraphe on se donne $a_0, \cdots, \cdots, a_n$ entiers naturels deux à deux premiers entre eux et strictement supérieur à 1. Nous nous intéréssons ici aux sommes suivantes, à paramètres $\varphi \in \mathbb{R}\backslash\mathbb{Z}$ et $m \in \mathbb{N}$, qui généralisent celles étudiées par D. Zagier [62](correspondant à $\varphi = \frac{1}{2}$)

$$d(a_l; a_0, \cdots, \check{a}_l, \cdots, a_n; m, \varphi) = \frac{1}{a_l} \sum_{k=1}^{a_l-1} \left(\cot(\frac{\pi k}{a_l}) + \cot(\pi\varphi) \right)^m \prod_{0 \leqslant j \neq l \leqslant n} \left(\cot(\frac{\pi k a_j}{a_l}) + \cot(\pi\varphi) \right)$$

Quand $\mathrm{Im}(\tau) \to \infty$, le théorème 8.2.4 donne une version plus générale au résultat de Zagier [62].

Théorème 8.4.1 *Soient $m \in \mathbb{N}$, $d \geqslant 2$ divisant a_0+...+a_n+m. Alors pour tout $\varphi = \frac{k}{d}$,$1 \leqslant k \leqslant d-1$, on obtient*

$$\sum_{l=0}^{n} d(a_l; a_0, \cdots, \check{a}_l, \cdots, a_n; m, \varphi) = \frac{sin(\pi\varphi(n+m+1))}{sin(\pi\varphi)^{m+n+1}} - i^{n+m} \frac{l_{n+m}(\overbrace{1, \cdots, 1}^{m \ \ fois}, a_0, \cdots a_n; \varphi)}{a_0 \cdots a_n}.$$

Où l' on a posé

$$\frac{l_{n+m}(\overbrace{1, \cdots, 1}^{m \ \ fois}, a_0, \cdots a_n; \varphi = \frac{k}{d})}{a_0 \cdots a_n} = (-i)^{n+m} Res \left((cot(z) + cot(\pi\varphi))^m \prod_{j=0}^{n} cot(a_j z) + cot(\pi\varphi) \right)_{|z=0}.$$

Remarque 8.4.2 On sait que pour n pair on a $l_n(a_0, \ldots, a_n, \varphi = \frac{1}{2}) = L_k(p_1, \ldots, p_k)$, $k = \frac{n}{2}$ où p_i, $i = 1, \ldots, k$ est le i-ème polynôme élémentaire symétrique en a_0,...,a_n et L_k le polynôme de Hirzebruch connu par les topologues [34].

8.5 Application 2 : Sommes classiques d'Apostol, [14].

On applique le théorème 8.3.2, pour $n = 1$ et $m = 1$ ou 2. On obtient le résultat suivant

Corollaire 8.5.1 *Soient a_0, a_1 éléments non nuls de $O_L\backslash O_L^\times$. Alors, pour tout φ paramètre de point de 2-division non nul de $\mathbb{C}/L$ et tout $k \in \mathbb{N}^*$, on a*

i) Si $a_0 + a_1 \equiv 1 \pmod{2O_L}$, alors $S_k(a_0, a_1; 1, \varphi, \tau) + S_k(a_1, a_0; 1, \varphi, \tau)$ est égale à

$$\begin{cases} 0 & \text{si } k \text{ est impair} \\ -\frac{1}{a_0 a_1} \left(\sum_{i=0}^{l+1} d_{2i}(\varphi) d_{2l+2-2i}(\varphi) a_0^{2i} a_1^{2l+2-2i} + (2l+1) d_{2l+2}(\varphi) \right) & \text{si } k = 2l \end{cases}$$

ii) Si $a_0 + a_1 \equiv 0 \pmod{2O_L}$, alors $S_k(a_0, a_1; 2, \varphi, \tau) + S_k(a_1, a_0; 2, \varphi, \tau)$ est égale à

$$\begin{cases} 0 & \text{si } k \text{ est pair} \\ -\frac{2l}{a_0 a_1} \left((2l+1) G_{2l+2}(L) - \sum_{i=0}^{l+1} d_{2i}(\varphi) d_{2l+2-2i}(\varphi) a_0^{2i} a_1^{2l+2-2i} \right) & \text{si } k = 2l-1. \end{cases}$$

En particulier si $\varphi = \frac{1}{2}$ et $\mathrm{Im}(\tau) \to \infty$ on déduit de ce corollaire un résultat connu sur les sommes classiques d'Apostol [1] p.149. Plus precisément, on obtient

Corollaire 8.5.2 *(Apostol revisité) Pour a_0, a_1 entiers naturels premiers entre eux et strictement supérieur à 1, on a l'égalité suivante*

$$s_k(a_0,a_1)+s_k(a_1,a_0) = \begin{cases} \frac{(-1)^l 4^{l+1}}{a_0 a_1}\left(\sum_{i=0}^{l+1}\frac{B_{2i}}{(2i)!}\frac{B_{2l+2-2i}}{(2l+2-2i)!}a_0^{2i}a_1^{2l+2-2i} - \frac{B_1 B_{2l+1}}{(2l+1)!}a_0 a_1^{2l+1} + (2l+1)\frac{B_{2l+2}}{(2l+2)!}\right) & \\ 0 & \end{cases}$$

où l'on a posé

$$s_k(a_0,a_1) = \frac{1}{k! a_0}\sum_{t=0}^{a_0-1}\cot^{(k)}\left(\frac{\pi t}{a_0}\right)\cot\left(\frac{\pi a_1 t}{a_0}\right).$$

Ceci peut être formulé d'une autre manière équivalente

Corollaire 8.5.3 *Pour a_0, a_1 entiers naturels premiers entre eux et > 1 , on a*

$$\tilde{s}_k(a_0,a_1)+\tilde{s}_k(a_1,a_0) = \begin{cases} \frac{(-1)^l (2\pi)^{2l+1}}{a_0 a_1}\left(\sum_{i=0}^{l+1}\frac{B_{2i}}{(2i)!}\frac{B_{2l+2-2i}}{(2l+2-2i)!}a_0^{2i}a_1^{2l+2-2i} + (2l+1)\frac{B_{2l+2}}{(2l+2)!}\right) & \text{Si } k = 2l \\ 0 & \text{Si } k \text{ impair} \end{cases}$$

où l'on a posé

$$\tilde{s}_k(a_0,a_1) = \frac{1}{a_0}\sum_{t=0}^{a_0-1}\zeta\left(k+1,\frac{t}{a_0}\right)\cot\left(\frac{\pi a_1 t}{a_0}\right)$$

et $\zeta(s,x) := \sum_{n=0}^{\infty}(n+x)^{-s}$ est la fonction zêta d'Hurwitz définie pour $R(s) > 1$ et $x \neq 0, -1, -2, \cdots$

Ce dernier corollaire se déduit immédiatement du corollaire 8.5.2 et de la formule suivante

$$\frac{\pi^{k+1}\cot^{(k)}(\pi x)}{k!} = (-1)^k\zeta(k+1,x) - \zeta(k+1,1-x), \forall x, |x| < 1, k \in \mathbb{N}^*.$$

9 Appendice 1 : Fonction zêta de Weierstrass et isogénies entre courbes elliptiques

Notre référence pour cet appendice est [15].

Le résultat principal de ce paragraphe est une relation de distribution additive satisfaite par la fonction zêta de Weierstrass et les conséquences que l'on peut en tirer pour la détermination des isogénies entre courbes elliptiques.

Il existe essentiellement deux algorithmes pour déterminer les isogénies entre courbes elliptiques. L'algorithme CCR et celui d'Atkin, [5], [53].

Pour l'algorithme CCR, le coeur en est l'évaluation des quantités

$$S_\Lambda(k) = \sum_{\bar{t}\in\Lambda/L\setminus\{0\}} \wp_L(t)^k$$

qui permettent de déterminer le polynôme $H(X) = \prod_{\bar{t}\in\Lambda/L\setminus\{0\}} (X - \wp_L(t))\,.$

Dans l'algorithme d'Atkin, l'idée essentielle est de calculer la série $H(\wp_L(z))$ et d'en déduire $H(X)$.

9.1 Introduction

Les séries d'Eisenstein associées au réseau L, sont définies par

$$E_k(z,L) = \lim_{s\to 0+} \sum\nolimits^{(e)}_{w\in L} (w+z)^{-k}|w+z|^{-s}, k = 1, ... \tag{9.1.2}$$

où $\sum^{(e)}$ est la sommation d'Eisenstein donnée par

$$\sum\nolimits^{(e)} = \sum_m\nolimits^{(e)} \sum_n\nolimits^{(e)} = \lim_{M\to\infty} \sum_{m=-M}^{m=M} \left(\lim_{N\to\infty} \sum_{n=-N}^{n=N} \right). \tag{9.1.3}$$

On définit également les fonctions de Weierstrass suivantes

$$\sigma_L(z) = z \prod_{\ell\in L,\ell\neq 0} \Big(1 - \frac{z}{\ell}\Big) e^{\frac{z}{\ell} + \frac{1}{2}\left(\frac{z}{\ell}\right)^2}, \zeta(z,L) = \frac{\sigma'_L(z)}{\sigma_L(z)}, \wp_L(z) = -\zeta'(z,L). \tag{9.1.4}$$

Le but ce paragraphe est de répondre aux questions simples suivantes :

(1) Soit Λ un réseau complexe tel que $\Lambda \supset L$.

Evaluer les sommes

$$\sum_{\bar{t}\in\Lambda/L} \Big(\zeta(z+t,L) - \eta(t,L)\Big), \sum_{\bar{t}\in\Lambda/L} \wp_L(z+t)^k$$

respectivement en fonction de $\zeta(z,\Lambda)$ et $\wp_\Lambda(z)$.

(2) Décrire explicitement les dérivées $\wp_L^{(2k-2)}(z)$ en fonction de $\wp_L(z)$.

La réponse à (1) fournit une bonne méthode pour contrôler le polynôme suivant

$$H(X) = \prod_{\bar{t}\in\Lambda/L\setminus\{0\}} (X - \wp_L(t))\,.$$

Dans le cas particulier où $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\frac{\omega_2}{l}, L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2, l \in \mathbb{N}, l \geqslant 2$, on retrouve les résultats les plus significatifs connus sur les algorithmes CCR et Atkin. De (1) et (2) on déduit des versions trigonométriques à ces algorithmes, ceci permet d'expliciter les isogénies entre les courbes singulières réelles

$$E_n(\mathbb{R}) : y^2 = x^3 - \frac{n^4}{3}x - \frac{2n^6}{27}, n \in \mathbb{N}^*$$

et la courbe

$$E_1(\mathbb{R}) : y^2 = x^3 - \frac{1}{3}x - \frac{2}{27}.$$

9.2 Résultats

Le premier résultat est une relation de distribution additive simple et de nature arithmétique.

Théorème 9.2.1 *(Relation de distribution) Pour tout réseau complexe $\Lambda \supset L$ on a*

$$\sum_{\bar{t}\in\Lambda/L}\Big(\zeta(z+t,L)-\eta(t,L)\Big)=\zeta(z,\Lambda)+\Big([\Lambda:L]s_2(L)-s_2(\Lambda)\Big)z,$$

où

$$s_2(L)=\lim_{s\to 0}\sum_{\omega\in L\setminus\{0\}}\frac{1}{\omega^2|\omega|^{2s}}.$$

On pose

$$E_1^*(z,L)=\zeta(z,L)-\eta(z,L), E_n^*(z,L)=E_n(z,L), \forall n\geqslant 2.$$

Du théorème 9.2.1, on déduit

Corollaire 9.2.2 *(Distribution pour les séries d'Eisenstein)Pour tout réseau complexe $\Lambda \supset L$ on a*

$$\sum_{\bar{t}\in\Lambda/L}E_n^*(z+t,L)=E_n^*(z,\Lambda), \forall n\geqslant 1.$$

Corollaire 9.2.3 *On a*

(i)
$$\prod_{\bar{t}\in\Lambda/L\setminus\{0\}}\Big(\wp_L(z)-\wp_L(t)\Big)=\mathcal{K}(z;L,\Lambda)^{-2}$$

(ii) En outre, si $[\Lambda:L]$ est impair

$$\zeta(z;L,\Lambda)=\mathcal{K}(z;L,\Lambda)^{-1}$$

On peut écrire ce corollaire de manière équivalente

Corollaire 9.2.4 *On a*

(i)
$$\prod_{\bar{t}\in\Lambda/L\setminus\{0\}}\Big(\wp_L(z)-\wp_L(t)\Big)=e^{([\Lambda:L]s_2(L)-s_2(\Lambda))z^2}\frac{\sigma_\Lambda(z)^2}{\sigma_L(z)^{2[\Lambda:L]}}$$

(ii) En outre, si $[\Lambda:L]$ est impair

$$\prod_{\bar{t}\in\Lambda/L\setminus\{0\}/\pm 1}\Big(\wp_L(z)-\wp_L(t)\Big)=e^{\frac{1}{2}([\Lambda:L]s_2(L)-s_2(\Lambda))z^2}\frac{\sigma_\Lambda(z)}{\sigma_L(z)^{[\Lambda:L]}}$$

On peut écrire ce corollaire comme une série

Corollaire 9.2.5 *On a*

$$\prod_{\bar{t}\in\Lambda/L\setminus\{0\}}\Big(\wp_L(z)-\wp_L(t)\Big)=z^{2-2[\Lambda:L]}e^{([\Lambda:L]s_2(L)-s_2(\Lambda))z^2-2\sum\limits_{k\geqslant 1}\frac{[\Lambda:L]G_{2k+2}(L)-s_2(\Lambda)}{2k+2}z^{2k+2}}$$

En outre si $[\Lambda:L]$ *est impair*

$$\prod_{\bar{t}\in\Lambda/L\setminus\{0\}/\pm 1}\Big(\wp_L(z)-\wp_L(t)\Big)=z^{1-[\Lambda:L]}e^{\frac{1}{2}([\Lambda:L]s_2(L)-s_2(\Lambda))z^2-\sum\limits_{k\geqslant 1}\frac{[\Lambda:L]G_{2k+2}(L)-s_2(\Lambda)}{2k+2}z^{2k+2}}$$

Remarque 9.2.6 Le corollaire 9.2.5 nous fournit une bonne méthode pour déterminer le polynôme suivant

$$H(X)=\prod_{\bar{t}\in\Lambda/L\setminus\{0\}}(X-\wp_L(t))\,.$$

Connaître ce polynôme permet de déterminer explicitement l'isogénie Φ de degré $[\Lambda:L]$ et de noyau Λ/L entre les deux courbes elliptiques $\mathbb{C}/L\to\mathbb{C}/\Lambda$. Ce corollaire est essentiel pour l'algorithme d'Atkin, qui consiste à calculer la série $H(\wp_L(z))$ et d'en déduire $H(X)$. Atkin ne fournit pas cette série mais il établit un algorithme [5] qui lui permet de déterminer les coefficients de $H(X)$. Ici nous fournissons cette série. En effet,

$$H(\wp_L(z))=z^{2-2[\Lambda:L]}e^{([\Lambda:L]s_2(L)-s_2(\Lambda))z^2}\exp\Big(-2\sum_{k\geqslant 1}\frac{[\Lambda:L]G_{2k+2}(L)-s_2(\Lambda)}{2k+2}z^{2k+2}\Big).$$

Un cas particulier du corollaire 9.2.5 est démontré, dans le cas particulier où $\Lambda=\mathbb{Z}\omega_1+\mathbb{Z}\frac{\omega_2}{l}, L=\mathbb{Z}\omega_1+\mathbb{Z}\omega_2, l\in\mathbb{N}, l\geqslant 2$, par R. Schoof [53], Theorem 8.3.

Pour préciser notre résultat concernant l'algorithme CCR, on définit les séries d'Eisenstein multiples associées au réseau complexe L par :

$$G_n(i,L)=\sum_{\substack{0\leqslant j_1,\ldots,j_i\leqslant n\\ j_1+\ldots+j_i=n}}(2j_1-1)\ldots(2j_l-1)G_{2j_1}(L)\ldots G_{2j_i}(L),\forall i\geqslant 1, n\in\mathbb{N}^*,$$

$$G_n(0,L)=\begin{cases}1 & \text{Si } n=0\\ 0 & \text{Sinon}\end{cases}$$

où l'on a posé $G_0(L)=-1$ et $G_2(L)=0$ et $G_{2n}(L)=\sum\limits_{\omega\in L\setminus\{0\}}\frac{1}{\omega^{2n}}, \forall n\geqslant 2$.

On a le résultat

Théorème 9.2.7 *Pour tout réseau complexe* $\Lambda\supset L$ *on a les égalités*

$$\frac{1}{(2k-1)!}\wp_L^{(2k-2)}(z)=\sum_{i=0}^{k}a_i(k,L)\wp_L(z)^i,\forall k\in\mathbb{N}^*.$$

et

$$\sum_{\bar{t}\in\Lambda/L} \wp_L(z+t)^k = \sum_{i=0}^{k} b_i(k,\Lambda)\wp_\Lambda(z)^i$$

où les $a_i(k,L), i = k, k-1, ..., 0$ *et les* $b_i(k,\Lambda), i = k, \cdots, 1, \forall k \geqslant 1$ *sont donnés par la résolution des systèmes triangulaires suivants*

$$\begin{cases} a_k(k,L) = 1 \\ \sum_{i=0}^{k-j} a_{i+j}(k,L)G_i(i+j,L) = 0, \quad \forall 1 \leqslant j \leqslant k-1 \text{ si } k \geqslant 2 \\ \sum_{i=0}^{k} a_i(k,L)G_i(i,L) = G_{2k}(L). \end{cases}$$

$$\begin{cases} b_k(k,\Lambda) = 1, b_0(1,\Lambda) = s_2(\Lambda) - s_2(L)[\Lambda : L] \quad \forall k \in \mathbb{N} \\ \sum_{l=j}^{k} b_l(k,\Lambda)G_{l-j}(l,\Lambda) = G_{k-j}(k,L), \qquad \forall 1 \leqslant j \leqslant k. \end{cases}$$

Pour trouver le terme $b_0(k,\Lambda)$ *on complète ce dernier système avec l'équation*

$$\sum_{i=j}^{k} a_i(k,L)b_j(i,\Lambda) = a_j(k,\Lambda), \forall 0 \leqslant j \leqslant k, \forall k \geqslant 2.$$

En particulier, on obtient

$$\sum_{\bar{t}\in\Lambda/L\setminus\{\bar{0}\}} \wp_L(t)^k = -G_k(k,L) + \sum_{j=0}^{k} b_j(k,\Lambda)G_j(j,L), \forall k \in \mathbb{N}.$$

9.3 Isogénies entre certaines courbes singulières réelles

Nous allons expliciter les isogénies entre les courbes singulières

$$E_n(\mathbb{R}) : y^2 = x^3 - \frac{n^4}{3}x - \frac{2n^6}{27}, n \in \mathbb{N}^*$$

et la courbe

$$E_1(\mathbb{R}) : y^2 = x^3 - \frac{1}{3}x - \frac{2}{27}.$$

Pour cela, considérons $\Lambda = \mathbb{Z}\tau + \mathbb{Z}\frac{1}{n}$, et $L = \mathbb{Z}\tau + \mathbb{Z}$ où n est un entier naturel $\geqslant 2$. En effectuant $\operatorname{Im}\tau \to \infty$, on déduit du paragraphe 9.2 le polynôme

$$h(X) = \prod_{t=1}^{n-1} \left(X - \frac{1}{sin(\frac{\pi t}{n})^2} \right)$$

qui vaut

$$h(X)=\frac{1}{2n^2}\left(X^n-\sum_{k=0}^{n}(-1)^{n-k}C_{2n}^{2k}(X-1)^k\right)$$

ou encore

$$h(X)=-\frac{1}{2n^2}\sum_{j=0}^{n-1}\left(\sum_{k=j}^{n}(-1)^{n-j}C_k^jC_{2n}^{2k}\right)X^j.$$

Ce polynôme permet d'obtenir l'expression de l'isogénie φ de degré n et de noyau $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$ entre les courbes singulières $E_1(\mathbb{R})$ et $E_n(\mathbb{R})$. Plus précisément, on a

$$\text{(5.4)}\qquad\begin{cases}\varphi\Big(x(t),y(t)\Big)=\left(X(t)=-\dfrac{1}{3}+\dfrac{1}{n^2}\dfrac{\Big(\frac{1}{3}+x(t)\Big)^n}{h\Big(\frac{1}{3}+x(t)\Big)},Y(t)=-\dfrac{1}{2n\pi}X^{'}(t)\right),\\ \forall t\in\mathbb{R}\backslash\mathbb{Z}.\\ \varphi\Big(\dfrac{-1}{3},0\Big)=\Big(\dfrac{-n^2}{3},0\Big).\end{cases}$$

10 Appendice 2 : Une nouvelle démonstration des lois de réciprocité quadratique de Gauss des corps quadratiques imaginaires

Dans cet appendice nous utilisons les formes de Jacobi de niveau 2 pour démontrer la loi de réciprocité quadratique pour un corps quadratique imaginaire K.

Commençons par préciser la notion de niveau.

Pour tout réseau complexe L , si (w_1,w_2) désigne une base de L sur $\mathbb{Z}$ telle que $\mathrm{Im}(w_1/w_2)>0$, on pose $\tau=w_1/w_2\in\mathcal{H}$. Soient N un entier naturel $\geqslant 2$ et φ le paramètre d'un point de $\mathbb{C}/L$ d'ordre N . Pour fixer les idées, on prend $\varphi=\frac{k}{N}\omega_1+\frac{l}{N}\omega_2, 0\leqslant k,l\leqslant N-1$. Nous associons à la paire (L,φ) la fonction

$$f_{(k,l)}(.,\tau):\quad z\in\mathbb{C}\setminus L\mapsto D_L(z;\varphi)=e(E_L(z,\varphi)/2)\frac{\mathcal{K}_L(z+\varphi)}{\mathcal{K}_L(z)\mathcal{K}_L(\varphi)}.$$

La fonction $f_{(k,l)}(.,\tau)$ est méromorphe sur $\mathbb{C}$, ne dépend que de φ modulo L et vérifie

$$f_{(k,l)}(z+\rho,\tau)=e(E_L(\rho,\varphi))f_{(k,l)}(z,\tau)=exp\left(-2i\pi\frac{(la-kb)}{N}\right)f_{(k,l)}(z,\tau),$$

pour tout élément $\rho=a\omega_1+b\omega_2$ de L.

On sait que pour tout $A=\begin{pmatrix}a&b\\c&d\end{pmatrix}\in\mathrm{SL}_2(\mathbb{Z})$, on a

$$D_{\frac{a\tau+b}{c\tau+d}}\left(\frac{z}{c\tau+d};\frac{\varphi}{c\tau+d}\right)=(c\tau+d)D_\tau(z;\varphi).$$

Par conséquent,

$$f_{(k,l)}\left(\frac{z}{c\tau+d};\frac{a\tau+b}{c\tau+d}\right)=(c\tau+d)f_{(k,l)A}(z;\tau).$$

Donc, $f_{(k,l)}$ est modulaire pour $\Gamma(N)$ de poids 1 et d'indice 0. Cela vient du fait que, pour tout $A=\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in\Gamma(N)$ on a :

$$(k,l)\begin{pmatrix}a & b\\ c & d\end{pmatrix}\equiv(k,l)\pmod N.$$

On dit alors que la forme modulaire $f_{(k,l)}$ ou $D_L(z;\varphi)$ est de **niveau N.**

10.1 Forme de Jacobi de "niveau 2" et symbole quadratique de Legendre

Dans ce paragraphe, on fixe un réseau complexe L et une base (w_1,w_2) de L sur $\mathbb{Z}$ telle que $\mathrm{Im}(w_1/w_2)>0$.

Théorème 10.1.1 *Il existe une unique fonction $f_L(z;\frac{w_1}{2},\frac{w_2}{2})$, ayant les propriétés suivantes :*
1) $z\to f_L(z;\frac{w_1}{2},\frac{w_2}{2})$ est impaire et périodique de périodes L.
2) $z\to f_L(z;\frac{w_1}{2},\frac{w_2}{2})$ est de diviseur $(0)+(\frac{w_1+w_2}{2})-(\frac{w_1}{2})-(\frac{w_2}{2})$.
3) (Normalisation)

$$\lim_{z\to 0}\frac{f_L(z;\frac{w_1}{2},\frac{w_2}{2})}{z}=D_L(\frac{w_2}{2};\frac{w_1}{2}).$$

Plus important, cette fonction satisfait les propriétés suivantes
4) $f_L(z;\frac{w_1}{2}+\rho,\frac{w_2}{2}+\rho')=e(E_L(\rho',\frac{w_1}{2}))f_L(z;\frac{w_1}{2},\frac{w_2}{2});\forall\rho,\rho'\in L$.
5) $f_L(z;\frac{w_1}{2},\frac{w_2}{2})=if_L(z;\frac{w_2}{2},\frac{w_1}{2})$
6) $f_L(z;\frac{w_1}{2},\frac{w_2}{2}).f_L(z+\frac{w_1}{2};\frac{w_1}{2},\frac{w_2}{2})=1$
7) $f_L(z;\frac{w_1}{2},\frac{w_2}{2}).f_L(z+\frac{w_2}{2};\frac{w_1}{2},\frac{w_2}{2})=-1$
8) $f_L(\lambda z;\lambda\frac{w_1}{2},\lambda\frac{w_2}{2})=f_\Lambda(z;\frac{w_1}{2},\frac{w_2}{2})$, où $\Lambda=\lambda^{-1}L;\forall\lambda\in\mathbb{C}^*,(\lambda,2)=1$.
9) (Formule produit)

$$f_\Lambda(z;\frac{w_1}{2},\frac{w_2}{2})=\prod_{\bar{t}\in\Lambda/L}f_L(z+t;\frac{w_1}{2},\frac{w_2}{2});$$

Pour tout Λ réseau complexe contenant L tel que $[\Lambda:L]$ est impair.

En fait cette fonction est donnée par

$$f_L(z;\frac{w_1}{2},\frac{w_2}{2})=\frac{D_L(z;\frac{w_1+w_2}{2})D_L(\frac{w_2}{2};\frac{w_1}{2})}{D_L(z;\frac{w_1}{2})D_L(z;\frac{w_2}{2})}.$$

Preuve :

Si une telle fonction existe, les propriétés 1), 2) et 3) assurent qu'elle est unique. Comme la fonction $z\to D_L(z;\varphi)$ vérifie

$$D_L(z+\rho;\varphi)=e(E_L(\rho,\varphi))D_L(z;\varphi),D_L(z;\varphi+\rho)=D_L(z;\varphi),\forall\rho\in L,$$

on a alors $z \to \frac{D_L(z;\frac{w_1+w_2}{2})D_L(\frac{w_2}{2};\frac{w_1}{2})}{D_L(z;\frac{w_1}{2})D_L(z;\frac{w_2}{2})}$ qui satisfait justement 1) , 2) et 3). D'où l'existence et l'unicité.

Les autres propriétés 4), 5), 6), 7) et 8), découlent de celles de la fonction $z \to D_L(z;\varphi)$.

Montrons le 9).– Etant donné la formule produit

$$D_\Lambda(z;\varphi) = \mathcal{K}(\varphi;L,\Lambda) \prod_{\bar{t}\in\Lambda/L} D_L(z+t;\varphi)e(-E_L(t,\varphi))$$

satisfaite par $D_L(z;\varphi$, on obtient

$$f_\Lambda(z;\frac{w_1}{2},\frac{w_2}{2}) = \frac{\mathcal{K}(\frac{w_1+w_2}{2};L,\Lambda)}{\mathcal{K}(\frac{w_1}{2};L,\Lambda)\mathcal{K}(\frac{w_2}{2};L,\Lambda)}.\frac{D_\Lambda(\frac{w_2}{2};\frac{w_1}{2})}{D_L(\frac{w_2}{2};\frac{w_1}{2})^{[\Lambda:L]}}.\prod_{\bar{t}\in\Lambda/L} f_L(z+t;\frac{w_1}{2},\frac{w_2}{2})$$

Or, en utilisant le fait que $\mathcal{K}(z;L,\Lambda) = \frac{\mathcal{K}_L(z)^{[\Lambda:L]}}{\mathcal{K}_\Lambda(z)}$ et $D_L(z;\varphi) = e(E_L(z,\varphi)/2)\frac{\mathcal{K}_L(z+\varphi)}{\mathcal{K}_L(z)\mathcal{K}_L(\varphi)}$, on obtient assez facilement que

$$\frac{\mathcal{K}(\frac{w_1+w_2}{2};L,\Lambda)}{\mathcal{K}(\frac{w_1}{2};L,\Lambda)\mathcal{K}(\frac{w_2}{2};L,\Lambda)}.\frac{D_\Lambda(\frac{w_2}{2};\frac{w_1}{2})}{D_L(\frac{w_2}{2};\frac{w_1}{2})^{[\Lambda:L]}} = 1.$$

Ce qui termine la preuve du théorèm 10.1.1.

Définissons, maintenant, le symbole quadratique de Legendre associé au réseau L. Grâce au lemme de Gauss généralisé, on a

Définition 10.1.2 *Pour $\alpha,\beta \in L$, avec $(\alpha,2) = (\beta,2) = 1$, on définit le symbole quadratique $(\frac{\alpha}{\beta})_2$ par*

$$\Big(\frac{\alpha}{\beta}\Big)_2 = \prod_{\sigma\in S_\beta} \varepsilon(\alpha,\sigma)\ ,$$

où $\alpha\sigma = \varepsilon(\alpha,\sigma)\gamma(\sigma)$ avec $\varepsilon(\alpha,\sigma) \in \{-1,1\}$, $\gamma(\sigma) \in S_\beta$ et $\{S_\beta, -S_\beta\}$ est un système complet de représentants de $L/\beta L\backslash\{0\}$.

Formulons, d'une autre manière le symbole $\Big(\frac{\alpha}{\beta}\Big)_2$. Comme la fonction $z \to f_L(z;\frac{w_1}{2},\frac{w_2}{2})$ est impaire, alors

$$\Big(\frac{\alpha}{\beta}\Big)_2 = \prod_{\sigma\in S_\beta} \frac{f_L(\alpha\sigma;\alpha\frac{w_1}{2},\alpha\frac{w_2}{2})}{f_L(\gamma(\sigma);\alpha\frac{w_1}{2},\alpha\frac{w_2}{2})}$$

ou encore

$$\Big(\frac{\alpha}{\beta}\Big)_2 = \prod_{\sigma\in S_\beta} \frac{f_L(\alpha\sigma;\alpha\frac{w_1}{2},\alpha\frac{w_2}{2})}{f_L(\sigma;\alpha\frac{w_1}{2},\alpha\frac{w_2}{2})}$$

En utilisant la formule produit safisfaite par f_L, Théorème 10.1.1, on obtient que

$$\Big(\frac{\alpha}{\beta}\Big)_2 = \prod_{\sigma\in S_\beta} \Big\{\frac{f_L(\sigma;\frac{w_1}{2},\frac{w_2}{2})}{f_L(\sigma;\alpha\frac{w_1}{2},\alpha\frac{w_2}{2})} \prod_{t\in S_\alpha} f_L(\sigma+t;\frac{w_1}{2},\frac{w_2}{2})f_L(\sigma-t;\frac{w_1}{2},\frac{w_2}{2})\Big\}$$

Ce qui permet de démontrer l'égalité suivante :

$$\Big(\frac{\alpha}{\beta}\Big)_2\Big(\frac{\beta}{\alpha}\Big)_2^{-1} = (-1)^{\frac{N(\alpha)-1}{2}\cdot\frac{N(\beta)-1}{2}} \prod_{\sigma\in S_\beta} \frac{f_L(\sigma;\frac{w_1}{2},\frac{w_2}{2})}{f_L(\sigma;\alpha\frac{w_1}{2},\alpha\frac{w_2}{2})} \prod_{t\in S_\alpha} \frac{f_L(t;\beta\frac{w_1}{2},\beta\frac{w_2}{2})}{f_L(t;\frac{w_1}{2},\frac{w_2}{2})}.$$

Ainsi, pour obtenir une loi de réciprocité quadratique il suffit d'évaluer la quantité

$$\prod_{\sigma\in S_\beta} \frac{f_L(\sigma;\frac{w_1}{2},\frac{w_2}{2})}{f_L(\sigma;\alpha\frac{w_1}{2},\alpha\frac{w_2}{2})} \prod_{t\in S_\alpha} \frac{f_L(t;\beta\frac{w_1}{2},\beta\frac{w_2}{2})}{f_L(t;\frac{w_1}{2},\frac{w_2}{2})}.$$

Cette quantité vérifie la propriété suivante :

Proposition 10.1.3 *Soient $\alpha,\beta,\alpha_0,\beta_0 \in L$ tels que $(\alpha,2)=(\beta,2)=1$ et $\alpha\equiv\alpha_0 \pmod{2L}$, $\beta\equiv\beta_0 \pmod{2L}$. On a alors l'égalité*

$$\prod_{\sigma\in S_\beta} \frac{f_L(\sigma;\frac{w_1}{2},\frac{w_2}{2})}{f_L(\sigma;\alpha\frac{w_1}{2},\alpha\frac{w_2}{2})} \prod_{t\in S_\alpha} \frac{f_L(t;\beta\frac{w_1}{2},\beta\frac{w_2}{2})}{f_L(t;\frac{w_1}{2},\frac{w_2}{2})} =$$

$$(-1)^{\frac{N(\alpha)-1}{2}E_L\left(\beta-\beta_0,\beta_0\frac{\omega_1}{2}\right)+\frac{N(\beta)-1}{2}E_L\left(\alpha-\alpha_0,\alpha_0\frac{\omega_1}{2}\right)}$$

$$\times \prod_{\sigma\in S_\beta} \frac{f_L(\sigma;\frac{w_1}{2},\frac{w_2}{2})}{f_L(\sigma;\alpha_0\frac{w_1}{2},\alpha_0\frac{w_2}{2})} \prod_{t\in S_\alpha} \frac{f_L(t;\beta_0\frac{w_1}{2},\beta_0\frac{w_2}{2})}{f_L(t;\frac{w_1}{2},\frac{w_2}{2})}.$$

Preuve : C'est une conséquence immédiate des propriétés 1) et 4) données dans le théorème 10.1.1 satisfaites par la fonction $z \to f_L(z;\frac{w_1}{2},\frac{w_2}{2})$.

En conclusion, à l'aide des propriétés simples de la forme de Jacobi f_L de niveau 2, on obtient le résultat suivant : Pour tout $\alpha,\beta,\alpha_0,\beta_0 \in L$ tels que $(\alpha,2)=(\beta,2)=1$ et $\alpha\equiv\alpha_0 \pmod{2L}$, $\beta\equiv\beta_0 \pmod{2L}$, on a

$$\Big(\frac{\alpha}{\beta}\Big)_2\Big(\frac{\beta}{\alpha}\Big)_2^{-1} = (-1)^{\frac{N(\alpha)-1}{2}\cdot\frac{N(\beta)-1}{2}+\frac{N(\alpha)-1}{2}E_L\left(\beta-\beta_0,\beta_0\frac{\omega_1}{2}\right)+\frac{N(\beta)-1}{2}E_L\left(\alpha-\alpha_0,\alpha_0\frac{\omega_1}{2}\right)}$$

$$\times \prod_{\sigma\in S_\beta} \frac{f_L(\sigma;\frac{w_1}{2},\frac{w_2}{2})}{f_L(\sigma;\alpha_0\frac{w_1}{2},\alpha_0\frac{w_2}{2})} \prod_{t\in S_\alpha} \frac{f_L(t;\beta_0\frac{w_1}{2},\beta_0\frac{w_2}{2})}{f_L(t;\frac{w_1}{2},\frac{w_2}{2})}.$$

L'objectif du paragraphe suivant est le calcul explicite du produit

$$\prod_{\sigma\in S_\beta} \frac{f_L(\sigma;\frac{w_1}{2},\frac{w_2}{2})}{f_L(\sigma;\alpha_0\frac{w_1}{2},\alpha_0\frac{w_2}{2})} \prod_{t\in S_\alpha} \frac{f_L(t;\beta_0\frac{w_1}{2},\beta_0\frac{w_2}{2})}{f_L(t;\frac{w_1}{2},\frac{w_2}{2})},$$

Pour tout couple α_0,β_0 d'unités de L modulo $2L$.

Remarque 10.1.4 *Le calcul fait dans le paragraphe suivant ne concerne que les réseaux L qui sont des anneaux d'entiers de corps quadratiques imaginaires.*

10.2 Enoncé et preuve de la loi de réciprocité quadratique dans un corps quadratique imaginaire

Les notations sont celles du paragraphe 3.

Soient $K = \mathbb{Q}(\sqrt{d})$, $d < 0$ entier relatif sans facteur carré. On note par $O_K = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ l'anneau des entiers de K, avec $\mathrm{Im}(\omega_1/\omega_2) > 0$. Comme prédemment, paragraphe 3 on choisit

$$\omega_2 = 1, \omega_1 = \begin{cases} \sqrt{d} & \text{si } d \equiv 3 \pmod 4 \\ 1+\sqrt{d} & \text{si } d \equiv 2 \pmod 4 \\ \frac{1+\sqrt{d}}{2} & \text{si } d \equiv 1 \pmod 4 \end{cases}.$$

On sait que

$$O_K/2O_K = \{0, \omega_1, \omega_2, \omega_1+\omega_2\}.$$

On sait aussi que les unités de O_K modulo $2O_K$ sont données par

$$\Big(O_K/2O_K\Big)^* = \begin{cases} \{1\} & \text{si } d \equiv 1 \pmod 8 \\ \{1, \omega_1\} & \text{si } d \equiv 2 \text{ ou } 3 \pmod 4 \\ \{1, \omega_1, 1+\omega_1\} & \text{si } d \equiv 5 \pmod 8 \end{cases}$$

Dans toute la suite du paragraphe, pour $\alpha, \beta, \alpha_0, \beta_0 \in O_K$ tels que $(\alpha, 2) = (\beta, 2) = 1$ et $\alpha \equiv \alpha_0 \pmod{2O_K}$, $\beta \equiv \beta_0 \pmod{2O_K}$, α_0, β_0 unités de O_K modulo $2O_K$, on pose

$$c(\alpha, \beta) = \prod_{\sigma \in S_\beta} \frac{f_{O_K}(\sigma; \frac{w_1}{2}, \frac{w_2}{2})}{f_{O_K}(\sigma; \alpha_0\frac{w_1}{2}, \alpha_0\frac{w_2}{2})} \prod_{t \in S_\alpha} \frac{f_{O_K}(t; \beta_0\frac{w_1}{2}, \beta_0\frac{w_2}{2})}{f_{O_K}(t; \frac{w_1}{2}, \frac{w_2}{2})}$$

et l'on note

$$\alpha = a + b\omega_1, \quad \beta = a' + b'\omega_1 \text{ avec } a, b, a', b' \in \mathbb{Z}.$$

Rappelons, maintenant, la loi de réciprocité quadratique pour les corps quadratiques imaginaires, que nous souhaitons démontrer.

Théorème 10.2.1 *(Loi de réciprocité quadratique dans $\mathbb{Q}(\sqrt{d})$, $d < 0$) Soient $\alpha, \beta \in O_K$, $(\alpha, 2) = (\beta, 2) = 1$. On a alors*

$$\boxed{\Big(\frac{\alpha}{\beta}\Big)_2 \Big(\frac{\beta}{\alpha}\Big)_2^{-1} = (-1)^{\frac{N(\alpha)-1}{2}\cdot\frac{N(\beta)-1}{2} + \frac{N(\alpha)-1}{2}E_{O_K}(\beta-\beta_0, \beta_0\frac{\omega_1}{2}) + \frac{N(\beta)-1}{2}E_{O_K}(\alpha-\alpha_0, \alpha_0\frac{\omega_1}{2})}}$$

Pour la démonstration de ce théorème nous avons besoin des lemmes suivants

Lemme 10.2.2 *Pour $d < 0$ entier relatif sans facteur carré et $d \equiv 5 \pmod 8$.*

(i)
$$\prod_{\sigma \in S_\beta} \frac{f_{O_K}(\sigma; \frac{w_1}{2}, \frac{w_2}{2})}{f_{O_K}(\sigma; \alpha_0\frac{w_1}{2}, \alpha_0\frac{w_2}{2})} = \begin{cases} 1 & si\ \alpha_0 = 1 \\ \frac{\mathcal{K}_{O_K}(\frac{\omega_2}{2})\mathcal{K}_{O_K}(\beta\frac{\omega_1+\omega_2}{2})}{\mathcal{K}_{O_K}(\frac{\omega_1+\omega_2}{2})\mathcal{K}_{O_K}(\beta\frac{\omega_2}{2})} & si\ \alpha_0 = \omega_1 \\ \frac{\mathcal{K}_{O_K}(\frac{\omega_1}{2})\mathcal{K}_{O_K}(\beta\frac{\omega_1+\omega_2}{2})}{\mathcal{K}_{O_K}(\frac{\omega_1+\omega_2}{2})\mathcal{K}_{O_K}(\beta\frac{\omega_1}{2})} & si\ \alpha_0 = 1+\omega_1 \end{cases}$$

(ii) $$\frac{\mathcal{K}_{O_K}(\alpha\frac{\omega_i}{2})}{\mathcal{K}_{O_K}(\alpha\frac{\omega_1+\omega_2}{2})} =$$

$$\chi_{O_K}\Big((\alpha-\alpha_0)\frac{\omega_j}{2}\Big)(-1)^{\frac{N(\alpha-\alpha_0)}{4}}\cdot\frac{\mathcal{K}_{O_K}(\alpha_0\frac{\omega_i}{2})}{\mathcal{K}_{O_K}(\alpha_0\frac{\omega_1+\omega_2}{2})},$$

avec $\{i,j\}=\{1,2\}$ *et où* $\alpha\equiv\alpha_0 \pmod{2O_K}$ *et* $\alpha_0\in\{1,\omega_1,1+\omega_1\}$

(iii) $\mathcal{K}_{O_K}(\frac{\omega_1^2}{2})=(-1)^{\frac{d-5}{8}}e(\frac{d-5}{32})\mathcal{K}_{O_K}(\frac{\omega_1+\omega_2}{2})$, $\mathcal{K}_{O_K}(\frac{\omega_1^2+\omega_1}{2})=i\mathcal{K}_{O_K}(\frac{\omega_2}{2})$, $\mathcal{K}_{O_K}(\frac{(\omega_1+\omega_2)^2}{2}) = -e(\frac{d+3}{32})\mathcal{K}_{O_K}(\frac{\omega_1}{2})$.

Preuve : Lorsque $\alpha_0=1$ le (i) du lemme 10.2.2 est clair. Comme $f_{O_K}(z;\frac{w_1}{2},\frac{w_2}{2})=\frac{D_{O_K}(z;\frac{w_1+w_2}{2})D_{O_K}(\frac{w_2}{2};\frac{w_1}{2})}{D_{O_K}(z;\frac{w_1}{2})D_{O_K}(z;\frac{w_2}{2})}$, alors pour $\alpha_0=\omega_1$, on a

$$\prod_{\sigma\in S_\beta}\frac{f_{O_K}(\sigma;\frac{w_1}{2},\frac{w_2}{2})}{f_{O_K}(\sigma;\alpha_0\frac{w_1}{2},\alpha_0\frac{w_2}{2})}=\prod_{\sigma\in S_\beta}\Big(\frac{D_{O_K}(\sigma;\frac{w_1+w_2}{2})}{D_{O_K}(\sigma;\frac{w_1}{2})}\Big)^2\cdot\Big(\frac{\mathcal{K}_{O_K}(\frac{w_1+w_2}{2})}{\mathcal{K}_{O_K}(\frac{w_1}{2})}\Big)^{N(\beta)-1}.$$

Grâce à la propriété xi) précisée dans le paragraphe 2.5 des formes de Jacobi $D_{O_K}(z,\varphi)$, on obtient

$$\prod_{\sigma\in\beta^{-1}O_K/O_K\setminus\{0\}}\frac{D_{O_K}(\frac{w_1+w_2}{2};\sigma)}{D_{O_K}(\frac{w_2}{2};\sigma)}=\frac{\mathcal{K}(\frac{w_2}{2};O_K,\beta^{-1}O_K)}{\mathcal{K}(\frac{w_1+w_2}{2};O_K,\beta^{-1}O_K)}$$

et de l'égalité

$$\mathcal{K}_{\beta^{-1}O_K}(z)=\beta^{-1}\mathcal{K}_{O_K}(z)$$

on déduit alors le (i) pour $\alpha_0=\omega_1$. Le reste du (i) s'obtient par les mêmes techniques de calcul.

Le (ii) et (iii) du lemme 10.2.2 se déduisent du fait que

$\mathcal{K}_{O_K}(z+\rho)=\chi_{O_K}(\rho)e(E_{O_K}(\rho,z)/2)\mathcal{K}_{O_K}(z)$, où $\chi_{O_K}(\rho)=\begin{cases}1 & \text{si } \rho\in 2O_K\\ -1 & \text{si } \rho\in O_K\setminus 2O_K.\end{cases}$

Lemme 10.2.3 *Pour $d<0$ entier relatif sans facteur carré. on a*

1) $\boxed{c(\alpha,\beta)=1}$ *si* $d\not\equiv 5 \pmod 8$

2) Sinon, pour $d\equiv 5 \pmod 8$, *on a :*

$$c(\alpha,\beta)=\begin{cases}1 & si\ \alpha\equiv\beta\equiv 1 \pmod{2O_K}\\ \chi_{O_K}(\frac{\alpha-\omega_1}{2}\omega_1)\chi_{O_K}(\frac{\beta-\omega_1}{2}\omega_1)(-1)^{\frac{N(\alpha-\omega_1)+N(\beta-\omega_1)}{4}} & si\ \alpha\equiv\beta\equiv\omega_1 \pmod{2O_K}\\ \chi_{O_K}(\frac{\alpha-(1+\omega_1)}{2}\omega_2)\chi_{O_K}(\frac{\beta-(1+\omega_1)}{2}\omega_2)(-1)^{\frac{N(\alpha-(1+\omega_1))+N(\beta-(1+\omega_1))}{4}} & si\ \alpha\equiv\beta\equiv 1+\omega_1 \pmod{2O_K}\\ \chi_{O_K}(\frac{\alpha-1}{2}\omega_1)(-1)^{\frac{N(\alpha-1)}{4}} & si\ \alpha\equiv 1,\beta\equiv\omega_1 \pmod{2O_K}\\ \chi_{O_K}(\frac{\alpha-1}{2}\omega_2)(-1)^{\frac{N(\alpha-1)}{4}} & \alpha\equiv 1,\beta\equiv 1+\omega_1 \pmod{2O_K}\\ \chi_{O_K}(\frac{\alpha-\omega_1}{2}\omega_2)\chi_{O_K}(\frac{\beta-(1+\omega_1)}{2}\omega_1)(-1)^{\frac{N(\alpha-\omega_1)+N(\beta-(1+\omega_1))}{4}} & \alpha\equiv\omega_1,\beta\equiv 1+\omega_1 \pmod{2O_K}\end{cases}$$

Démonstration : Le cas où $d \equiv 1 \pmod 8$. Puisque $\left(O_K/2O_K\right)^* = \{1\}$ alors $\alpha_0 = \beta_0 = 1$. Dans ce cas, le (1) découle de la définition de $c(\alpha, \beta)$.

Pour $d \equiv 2$ ou $3 \pmod 4$, on a $\left(O_K/2O_K\right)^* = \{1, \omega_1\}$. Grâce aux propriétés de la fonction $f_{O_K}(z; \frac{w_1}{2}, \frac{w_2}{2})$, il est assez facile de vérifier que que l'on a aussi : $c(\alpha, \beta) = 1$.

Nous nous propososns de détailler le cas où $d \equiv 5 \pmod 8$. Pour cela nous allons nous servir du lemme 10.2.2.

- Si $\alpha \equiv \beta \equiv 1 \pmod{2O_K}$, on a alors $\alpha_0 = \beta_0 = 1$, le lemme 10.2.2 permet de conclure.
- Si $\alpha \equiv \beta \equiv \omega_1 \pmod{2O_K}$, on a alors $\alpha_0 = \beta_0 = \omega_1$. D'après le lemme 10.2.2 on obtient

$$c(\alpha, \beta) = \frac{\mathcal{K}_{O_K}(\beta\frac{\omega_1+\omega_2}{2})}{\mathcal{K}_{O_K}(\beta\frac{\omega_2}{2})} \cdot \frac{\mathcal{K}_{O_K}(\alpha\frac{\omega_2}{2})}{\mathcal{K}_{O_K}(\alpha\frac{\omega_1+\omega_2}{2})}.$$

Pour conclure, on utilise la propriété de translation satisfaite par $\mathcal{K}_{O_K}$, avec $\rho = \frac{\alpha-\alpha_0}{2}$, puis $\rho = \frac{\beta-\beta_0}{2}$.

Grâce au lemme 10.2.2, les autres sous-cas restants se déduisent de la même manière que ci-dessus.

Le théorème principal de ce paragraphe nous dit en fait que, dans tous les cas

$$c(\alpha, \beta) = 1.$$

Démonstration du théorème principal.— Grâce aux lemmes 10.2.2 (i) et 10.2.3 pour démontrer notre résultat il suffit de montrer que

$$\boxed{c(\alpha, \beta) = 1, \forall \alpha, \beta \in O_K, (\alpha, 2) = (\beta, 2) = 1.}$$

Pour se faire il suffit d'appliquer la partie (ii) du lemme 10.2.2.

Corollaire 10.2.4 *Pour $d \equiv 1 \pmod 8$ et $(\alpha, 2) = (\beta, 2) = 1$. On a alors*

$$\boxed{\left(\frac{\alpha}{\beta}\right)_2 \left(\frac{\beta}{\alpha}\right)_2^{-1} = (-1)^{\frac{b}{2}\cdot\frac{b'}{2} + \frac{b}{2}\cdot\frac{a'-1}{2} + \frac{b'}{2}\cdot\frac{a-1}{2}}}$$

Preuve : Elle découle du fait que

$$\frac{N(\alpha)-1}{2} \equiv \frac{b}{2} \pmod 2 \text{ et } E_{O_K}(\alpha - \alpha_0, \alpha_0\frac{\omega_1}{2}) = \frac{a-1}{2}, \quad \alpha_0 = 1 \text{ car } \left(O_K/2O_K\right)^* = \{1\}.$$

Corollaire 10.2.5 *Pour $d \equiv 3 \pmod 4$ et $(\alpha, 2) = (\beta, 2) = 1$. On a alors*

$$\boxed{\left(\frac{\alpha}{\beta}\right)_2 \left(\frac{\beta}{\alpha}\right)_2^{-1} = 1}$$

Preuve : Il suffit d'utiliser que $\frac{N(\alpha)-1}{2} \equiv 0 \pmod 2$

Corollaire 10.2.6 *Pour* $d \equiv 2 \pmod 4$ *et* $(\alpha,2)=(\beta,2)=1$. *On a alors*

$$\boxed{\left(\frac{\alpha}{\beta}\right)_2\left(\frac{\beta}{\alpha}\right)_2^{-1} = \begin{cases} 1 & si\ \alpha \equiv \beta \equiv 1 \pmod{2O_K} \\ \left(-1\right)^{\frac{a-1}{2}} & si\ \alpha \equiv 1 \pmod{2O_K}\ et\ \beta \equiv \omega_1 \pmod{2O_K} \\ \left(-1\right)^{\frac{b+b'}{2}} & si\ \alpha \equiv \beta \equiv \omega_1 \pmod{2O_K} \end{cases}}$$

Preuve : On utilise que

$$\frac{N(\alpha)-1}{2} \equiv \begin{cases} 0 & \text{si } \alpha \equiv 1 \pmod{2O_K} \\ 1 & \text{si } \alpha \equiv \omega_1 \pmod{2O_K} \end{cases} \pmod 2$$

et

$$E_{O_K}(\alpha-\alpha_0,\alpha_0\frac{\omega_1}{2}) \equiv \begin{cases} \frac{a-1}{2} & \text{si } \alpha \equiv 1 \pmod{2O_K} \\ \frac{b-1}{2} & \text{si } \alpha \equiv \omega_1 \pmod{2O_K} \end{cases} \pmod 2$$

Corollaire 10.2.7 *Pour* $d \equiv 5 \pmod 8$ *et* $(\alpha,2)=(\beta,2)=1$. *On a alors*

$$\boxed{\left(\frac{\alpha}{\beta}\right)_2\left(\frac{\beta}{\alpha}\right)_2^{-1} = \begin{cases} (-1)^{\frac{b}{2}\cdot\frac{b'}{2}+\frac{b}{2}\cdot\frac{a'-1}{2}+\frac{b'}{2}\cdot\frac{a-1}{2}} & si\ \alpha \equiv \beta \equiv 1 \pmod{2O_K} \\ (-1)^{(\frac{a}{2}+\frac{d-5}{8})\cdot(\frac{a'}{2}+\frac{d-5}{8})+(\frac{a}{2}+\frac{d-5}{8})\cdot(\frac{a'}{2}+\frac{b'-1}{2})+(\frac{a'}{2}+\frac{d-5}{8})\cdot(\frac{a}{2}+\frac{b-1}{2})} & si\ \alpha \equiv \beta \equiv \omega_1 \pmod{2O_K} \\ (-1)^{(\frac{a+b}{2}+\frac{d+3}{8})\cdot(\frac{a'+b'}{2}+\frac{d+3}{8})+(\frac{a+b}{2}+\frac{d+3}{8})\cdot\frac{b'-1}{2}+(\frac{a'+b'}{2}+\frac{d+3}{8})\cdot\frac{b-1}{2}} & si\ \alpha \equiv \beta \equiv 1+\omega_1 \pmod{2O_K} \\ (-1)^{\frac{b}{2}\cdot(\frac{a'}{2}+\frac{d-5}{8})+\frac{b}{2}\cdot(\frac{a'}{2}+\frac{b'-1}{2})+(\frac{a'}{2}+\frac{d-5}{8})\cdot\frac{a-1}{2}} & si\ \alpha \equiv 1, \beta \equiv \omega_1 \pmod{2O_K} \\ (-1)^{\frac{b}{2}\cdot(\frac{a'+b'}{2}+\frac{d+3}{8})+\frac{b}{2}\cdot\frac{b'-1}{2}+(\frac{a'+b'}{2}+\frac{d+3}{8})\cdot\frac{a-1}{2}} & si\ \alpha \equiv 1, \beta \equiv 1+\omega_1 \pmod{2O_K} \\ (-1)^{(\frac{a}{2}+\frac{d-5}{8})\cdot(\frac{a'+b'}{2}+\frac{d+3}{8})+(\frac{a}{2}+\frac{d-5}{8})\cdot\frac{b'-1}{2}+(\frac{a'+b'}{2}+\frac{d+3}{8})\cdot(\frac{a}{2}+\frac{b-1}{2})} & si\ \alpha \equiv \omega_1, \beta \equiv 1+\omega_1 \pmod{2O_K} \end{cases}}$$

Preuve : Elle se déduit de

$$\frac{N(\alpha)-1}{2} \equiv \begin{cases} \frac{b}{2} & \text{si } \alpha \equiv 1 \pmod{2O_K} \\ \frac{a}{2}+\frac{d-5}{5} & \text{si } \alpha \equiv \omega_1 \pmod{2O_K} \\ \frac{a+b}{2}+\frac{d+3}{8} & \text{si } \alpha \equiv 1+\omega_1 \pmod{2O_K} \end{cases} \pmod 2$$

et

$$E_{O_K}(\alpha-\alpha_0,\alpha_0\frac{\omega_1}{2}) \equiv \begin{cases} \frac{a-1}{2} & \text{si } \alpha \equiv 1 \pmod{2O_K} \\ \frac{a}{2}+\frac{b-1}{2} & \text{si } \alpha \equiv \omega_1 \pmod{2O_K} \\ \frac{b-1}{2} & \text{si } \alpha \equiv 1+\omega_1 \pmod{2O_K} \end{cases} \pmod 2$$

Références

[1] Apostol, T. M, *Generalized Dedekind sums and transformation formulae of certain Lambert series*, Duke Math. J, **17**, 1950, 147–157.

[2] T. M Apostol, *Theorems on generalized Dedekind Sums*, Pacific. J. Math, **2** (1952) 1–9.

[3] M.F. Atiyah, *The Logarithm of the Dedekind η-Function*, Math. Ann, **278**, (1987), 335-380.

[4] M.F. Atiyah, F. Hirzebruch, *Riemann-Roch theorems for differentiable manifolds*, Bull. Amer. Math.Soc, **65**, 1959, 276-281.

[5] A.O.L Atkin, *The number of points on an elliptic curve modulo a prime*, Draft, (1988).

[6] A. Bayad, *Résolvantes elliptiques et éléments de Stickelberger*, Pub.école doctorale de mathématiques de Bordeaux I, 1992.

[7] A. Bayad, *Sommes de Dedekind elliptiques et formes de Jacobi*, Ann. Instit. Fourier, Vol. **51**, Fasc. 1, 2001, 29-42.

[8] A. Bayad, *Loi de réciprocité quadratique dans les corps quadratiques imaginaires*, Ann. Inst. Fourier, tome **45** (5), 1995, 1223–1237.

[9] A. Bayad, W. Bley, Ph. Cassou-Noguès, *Sommes arithmétiques et éléments de Stickelberger*, J. of Algebra, t. **179** ((1)), 1996, 145–190.

[10] A. Bayad, *Structure galoisienne d'anneaux d'entiers et courbes elliptiques sans multiplication complexe*, Journal of Number Theory Vol. **52**, No**2**,1995, 267-279.

[11] A. Bayad, *Valuation p-adique et relation de distribution additive pour certaines fonctions q-périodiques*, Journal of Number Theory Vol. **65**, No**1**, 1997, 1-22.

[12] A. Bayad, *Formes de Jacobi et formules de Weber p-adiques*, Journal de Théorie des nombres de Bordeaux No**11**, 1999, 317-329.

[13] A. Bayad, *Sommes elliptiques multiples d'Apostol-Dedekind-Zagier*, C.R.A.S Paris, Ser. I **339**, fascicule 7, Série I, 2004, 457-462.

[14] A. Bayad, *Applications aux sommes elliptiques multiples d'Apostol-Dedekind-Zagier*, C.R.A.S Paris, Ser. I **339**, fascicule 8, Série I, 2004, 529-532.

[15] A. Bayad, *Propriétés et applications arithmétques de la la fonction zêta de Weierstrass* , soumis au Journal of Number Theory.

[16] A. Bayad, E.J Gomez-Ayala, *Formes de Jacobi et formules de distribution*, Journal of Number theory **109** (2004), 136-162.

[17] A. Bayad, G. Robert, *Note sur une forme de Jacobi méromorphe*, C.R.A.S Paris, **325**,1997, 455-460.

[18] A. Bayad, G. Robert, *Amélioration d'une congruence pour certaines éléments de Stickelberger quadratiques*, Bulletin de la société mathématique de france, No. **125**, 1997, 249-267.

[19] J. Brinkhuis, *Gauss sums and their prime factorization*, L'enseignement mathématique, 36 (1990), 39-51.

[20] Ph. Cassou-Noguès, M.J. Taylor, *Elliptic functions and rings of integers*, Prog. in Math. 66, Basel-Stuttgart-Boston 1987.

[21] Ph. Cassou-Noguès, M.J. Taylor, *Un élément de Stickelberger quadratique*, Journal of Number Theory (3),**37** (1991), 307-342.

[22] S-P Chan, *Modular functions, elliptic functions and Galois module structure*, J. Reine Angew. Math. (1987), 67-82.

[23] S-P Chan and C-H Lim, *Relative Galois module structure of rings of integers of cyclotomic fields*, J. Reine Angew. Math.**434** (1993), 205-230.

[24] J. Coates, *Elliptic curves with complex multiplication and Iwasawa theory*, Bull. London. Math. Soc,**23**, (1991), 321–350.

[25] J. Coates, A. Wiles, *On the conjecture of Birch and Swinnerton-Dyer*, Invent. Math,**39**,(1979), 223–251.

[26] U. Dieter,*Pseudo-random numbers : the exact distribution of pairs*, Math.of Computation,**25**, 1971.

[27] M. Eichler, D. Zagier, *The theory of Jacobi forms*, Birkhauser-Verlag Progress in mathematics, 0055, 1985

[28] C. Greither, D. R. Replogle, K. Rubin, and A. Srivastav, *Swan Modules and Hilbert-Speiser number fields*, J. Num. Theory**79** (1999), 164-173.

[29] R. Gillard, G. Robert, *Groupes d'unités elliptiques*, Bull. Soc. Math. France,**107**, (1979), 305–317.

[30] V. Gritsenko, *Fourier-Jacobi functions of n*, J. Sov.Math,**53**, (1991), 243–252.

[31] G. Harder, *Periods Integrals of Cohomology Classes which are represented by Eisenstein Series*, Proc. Bombay Colloquium, Berlin-Heidelberg-New York, (1979).

[32] G. Harder, *Periods Integrals of Eisenstein Cohomology Classes which are special values of some L-functions*, Number theory related to Fermat's last theorem, 103-142. In Koblitz, N. (ed.) Boston-Basel-Stuttgart : Birkhauser, (1982).

[33] G.H Hardy, S. Ramanujan, *Asymptotic formulae in combinatory analysis*, Proc. London math. Soc (2), **17**, 1918, 75-115.

[34] F. Hirzebruch, *Topological methods in algebraic geometry* , Third Enlarged Edition. Berlin-Heidelberg-New York ; Springer, 1966.

[35] F. Hirzebruch, *The signature theorem : reminiscences and recreation* , Prospects in Mathematics. Ann. of Math.Studies 70, 3-31, Princeton University Press, Princeton, 1971.

[36] F. Hirzebruch, T. Berger and R. Jung, *Manifolds and Modular forms* , Aspects of Math.E. 20,Vieweg (1992).

[37] F. Hirzebruch and D. Zagier, *The Atiyah-Singer Theorem and Elementary Number Theory*, Math. Lecture Series 3, Publish or Perish Inc, 1974.

[38] F. Jarvis, *A distribution relation on elliptic curves*, Bull. London. Math. Soc, **32**, (2000), 146–154.

[39] F. Jarvis, *An elementary proof of a distribution relation on elliptic curves*, Manuscripta Math, **103**, (2000), 329–337.

[40] H. Klingen, *Metriserung theorie und Jacobiformen*, Abh. Math. Semin.Univ.Hamburg, **57**, (1987), 395–417.

[41] H. Klingen, *Automorphic forms and functions with respect to the Jacobi group*, Math Ann, **306**, (1996), 675–690.

[42] A. Krieg, *Jacobi Forms of Several Variables and Maaβ spaces*, J. of Number Theory, **56**, (1996), 242–255.

[43] D. Kubert, *Product formulae on elliptic curves*, Invent. Math. t. **117**, 1994, 227–273.

[44] D. Kubert, S. Lang, *Modular units*, Grundlehren der Mathematischen Wissenschaften, **244**, Springer- Verlag, 1981.

[45] S. Lang, *Elliptic functions*, Addison-Wesley, 1973.

[46] C. Meyer, *Über einige Anwendungen Dedekindscher Summen*, J.Reine angew. Math. **198**, (1957), 143-203.

[47] C. Meyer, *Über die Bildung von Klasseninvarianten binarer quadratischer Formen mittels Dedekinkscher Summen*, Abh. math. Sem. Univ. Hamburg. 27 Heft 3/4, (1964), 206-230.

[48] H. Rademacher, *On the partition function $p(n)$*, Proc. London math. Soc (2), **43**, 1937, 241-254.

[49] G. Robert, *Unités elliptiques*, Bull.Soc. Math. France, Mémoire **36**,(1973).

[50] G. Robert, *Concernant la relation de distribution satisfaite par la fonction φ associée à un réseau complexe*, Invent. Math. t. **100**, 1990, 231–257.

[51] K. Rolshausen, N. Schappacher, *On the second K-group of an elliptic curve*, J. reine angew. Math, **495**, (1998), 61–77.

[52] R. Schertz, *Galoismodulstruktur und Elliptische Funktionen*, Journal of Number Theory, **39** (1991), 285 - 326.

[53] R.Schoof, *Counting points on elliptic curves over finite fields*, Journal de Théorie des nombres de Bordeaux, **7**, (1995), 219-254.

[54] R.Sczech, *Dedekindsummen mit elliptischen Funktionen*, Invent.math, **76**, (1984), 523-551.

[55] E. de Shalit, *Iwasawa theory of elliptic curves with complex multiplication*, Academic Press, Orlando, (1987).

[56] A. Srivastav, M.J. Taylor, *Elliptic curves with complex multiplication and Galois module structure*, Invent. Math. t. **99**, 1990, 165–184.

[57] L. Washington, *Introduction to cyclotomic fields*, Graduate texts in mathematics, Vol **83**, Springer-Verlag, New York-Berlin-Heidelberg-Tokyo.

[58] U. Weselmann, *EisensteinKohomologie und Dedekindsummen für GL_2 über imaginär-quadratischen Zahlenkörpern*, J. reine. angew. Math. 389, (1988), 90–121.

[59] J. Wildeshaus, *On an elliptic analogue of Zagier's Conjecture*, Duke Math. J. **87**, (1997), 355–407.

[60] J. Wildeshaus, *Variations of Hodge-de Rham structure and elliptic modular units*, in "Regulators in analysis, geometry and number theory", A. Reznikov, N. Schappacher (eds.), Progr. Math. **171**, Birkhäuser, Boston, (1999), 295–324.

[61] T. Yamazaki, *Jacobi forms and a Maaβ relation for Eisenstein series*, J. Fac. sci. Univ. Tokyo, sect. IA, **33**, 1986,295–310.

[62] D. Zagier, *Higher order Dedekind sums*, Math.Ann, **202**, 1973, 149-172.

[63] D. Zagier, *Periods of modular forms and Jacobi theta functions*, Invent.math, **104**, 1991, 449-465.

[64] C. Ziegler, *Jacobi Forms of Higher degree*, Abh. Math. Sem. Univ. Hamburg, **59**, 1989, 191–224.

11 Liste de publications

[Ba1] *Structure galoisienne d'anneaux d'entiers et courbes elliptiques sans multiplication complexe*, Journal of Number Theory Vol. **52**, No 2, 1995, 267-279.

[Ba2](En collaboration avec Ph. Cassou-Noguès et W. Bley)
Sommes arithmétiques et éléments de Stickelberger, Journal of Algebra, Vol. **179**, 1996, 145-190.

[Ba3] *Loi de réciprocité quadratique dans les corps quadratiques imaginaires*, Annales Institut Fourier, Vol. **45**, Fasc. 5, 1995, 1223-1237.

[Ba4] *Valuation p-adique et relation de distribution additive pour certaines fonctions q-périodiques*, Journal of Number Theory Vol. **65**, No 1, 1997, 1-22.

[Ba5] (En collaboration avec G. Robert)
Amélioration d'une congruence pour certaines éléments de Stickelberger quadratiques, Bulletin de la société mathématique de france, No. **125**, 1997, 249-267.

[Ba6] (En collaboration avec G. Robert) *Note sur une forme de Jacobi méromorphe*, C.R.A.S Paris, Ser. I **325**, 1997, 455-460.

[Ba7] *Formes de Jacobi et formules de Weber p-adiques*,
Journal de Théorie des nombres de Bordeaux No **11**, 1999, 317-329.

[Ba8] *Sommes de Dedekind elliptiques et formes de Jacobi*,
Annales Institut Fourier, t. **51**, 2001, fascicule 1, 29-42.

[Ba9] *Sommes elliptiques multiples d'Apostol-Dedekind-Zagier*,
C.R.A.S Paris, Ser. I **339**, fascicule 7, 2004, 457-462.

[Ba10] *Applications aux sommes elliptiques multiples d'Apostol-Dedekind-Zagier*,
C.R.A.S Paris, Ser . I **339**, fascicule 8, 2004, 529-532.

[Ba11] (En collaboration avec Jésus Gomez-Ayala)
Formes de Jacobi et formules de distribution,
Journal of Number theory **109** (2004), 136-162.

[Ba12](En collaboration avec Ludovic Perret)
A differential approach to a polynomial equivalence problem,
Communication in 2004 IEEE International Symposium on InformationTheory.

[Ba13] *Propriétés et applications arithmétques de la la fonction zêta de Weierstrass* , soumis.

[Ba14] *Arithmétique et topologie des formes de Jacobi.*
En préparation(En collaboration avec Philippe Cassou-Noguès).

[Ba15] *Résolvantes elliptiques et éléments de Stickelberger*,
Pub. Ecole doctorale de mathématique Bordeaux I, Thèse, 1992.

[Ba16] *Théorème de Stickelberger elliptique*,
Revue Arithmétique de Caen, 1993.