Unités elliptiques, corps quadratiques réels, et une formule limite de Kronecker

Henri Darmon
Samit Dasgupta

April 7, 2004

Cet exposé résume l'essentiel des résultats de [DD], auquel on renvoie le lecteur pour les détails et les démonstrations.

Les *unités circulaires* dont il a été question dans l'exposé de Radan Kučera fournissent un outil puissant dans l'étude des corps cyclotomiques. Ces unités explicites, dont les logarithmes s'expriment de façon simple en fonction des valeurs spéciales des séries L de Dirichlet en $s = 1$, engendrent un sous-groupe *d'indice fini* du groupe des unités des extensions abéliennes de $\mathbb{Q}$. Elles ont joué un rôle important dans les travaux de Kummer sur les corps cyclotomiques, et plus récemment dans ceux de Thaine et Kolyvagin qui ont mené à une nouvelle démonstration de la "conjecture principale" de la théorie d'Iwasawa.

Les *unités elliptiques*, dont la construction est basée sur la théorie de la *multiplication complexe*, jouent un peu le même rôle dans l'étude des extensions abéliennes des corps quadratiques imaginaires. Coates et Wiles s'en sont servis dans leurs travaux sur la conjecture de Birch et Swinnerton–Dyer pour les courbes elliptiques à multiplications complexes, et Rubin a pu donner une démonstration complète de la "conjecture principale" d'Iwasawa pour les corps quadratiques imaginaires en adaptant les idèes de Thaine aux unités elliptiques.

On se propose ici d'étendre (de facon, hélas, conjecturale pour le moment) la théorie des unités elliptiques au cas des corps quadratiques réels, pour lesquels la théorie de la multiplication complexe fait défaut.

1 Rappels sur les unités elliptiques

Soit N un entier positif, et soit $\Gamma_0(N) \subset \mathbf{SL}_2(\mathbb{Z})$ le sous-groupe de congruence de Hecke formé des matrices triangulaires supérieures modulo N. On désigne par $Y_0(N)$ la courbe modulaire dont les points complexes s'identifient au quotient

$$Y_0(N)(\mathbb{C}) = \mathcal{H}/\Gamma_0(N), \tag{1}$$

où $\mathcal{H}$ est le demi-plan de Poincaré usuel sur lequel $\Gamma_0(N)$ agit par transformations de Möbius. La courbe $Y_0(N)$ est une courbe algébrique—on en dispose même d'un modèle défini sur $\mathbb{Q}$. On compactifie $Y_0(N)$ en y adjoignant un nombre fini de pointes qui sont en bijection avec les $\Gamma_0(N)$-orbites de $\mathbb{P}_1(\mathbb{Q})$. (Par exemple, lorsque N est sans facteurs carré, ces orbites sont en bijection avec les diviseurs de N, en associant à un diviseur d l'ensemble des éléments de $\mathbb{P}_1(\mathbb{Q})$ de la forme $\frac{a}{d}$ où $\gcd(a,d) = 1$.) Soit $\mathcal{C}_N := \mathbb{P}_1(\mathbb{Q})/\Gamma_0(N)$ l'ensemble des pointes de $X_0(N)$ et soit s_N sa cardinalité.

On appelle *unité modulaire* toute fonction méromorphe sur $X_0(N)$ qui est holomorphe sur $Y_0(N)$; c'est-à-dire toute fonction rationelle sur $X_0(N)$ dont le diviseur est supporté sur $\mathcal{C}_N$, et on désigne par $\mathcal{O}_N^\times$ le groupe mutiplicatif de ces unités. L'application qui à α associe son diviseur donne une *injection*

$$\mathcal{O}_N^\times/\mathbb{C}^\times \longrightarrow \mathrm{Div}^0(\mathcal{C}_N) \tag{2}$$

dont l'image s'identifie au noyau de l'application naturelle de $\mathrm{Div}^0(\mathcal{C}_N)$ dans la Jacobienne $J_0(N)$ de $X_0(N)$. A priori, on pourrait s'attendre à ce que le groupe $\mathcal{O}_N^\times/\mathbb{C}^\times$ soit souvent trivial lorsque le genre de $X_0(N)$ est strictement positif—c'est ce qui arriverait si l'image de $\mathrm{Div}^0(\mathcal{C}_N)$ dans $J_0(N)$ était de rang maximal $s_N - 1$. Le théorème de Manin-Drinfeld [Man] affirme au contraire que $\mathrm{Div}^0(\mathcal{C}_N)$ engendre un sous-groupe *fini* de $J_0(N)$, ce qui implique que

$$\mathrm{rang}(\mathcal{O}_N^\times/\mathbb{C}^\times) = s_N - 1. \tag{3}$$

Les unités modulaires existent donc en abondance. Ces unités remarquables ont trouvé de nombreuses applications arithmétiques, notamment dans les travaux de Beilinson sur les régulateurs et les fonctions zeta des courbes modulaires, de Flach sur le groupe de Selmer du carré symétrique de la représentation ℓ-adique associée à une forme modulaire, ainsi que dans les travaux plus récents de Kato sur la conjecture de Birch et Swinnerton-Dyer sur les extensions abéliennes de $\mathbb{Q}$.

Concrètement, toute famille d'entiers n_d indexés pas les diviseurs d de N, et satisfaisant la condition $\sum_{d|N} n_d = 0$, donne lieu à l'unité modulaire explicite

$$\alpha(\tau) = \prod_{d|N} \Delta(d\tau)^{n_d}, \tag{4}$$

où

$$\Delta(\tau) = q \prod_{n=1}^{\infty} (1-q^n)^{24}, \quad q = e^{2\pi i \tau} \tag{5}$$

est la fonction Δ, l'unique forme modulaire normalisée de poids 12 et de niveau 1. Lorsque N est sans facteurs carrés, les unités de cette forme engendrent un sous-groupe d'indice fini de $\mathcal{O}_N^\times/\mathbb{C}^\times$. Pour plus d'informations sur les unités modulaires le lecteur est invité à consulter le livre de Kubert–Lang [KL].

Soit $K \subset \mathbb{C}$ un corps quadratique imaginaire. On appelle l'*ordre associé* à $\tau \in \mathcal{H} \cap K$ l'ensemble des matrices à coefficients entiers défini par

$$\mathcal{O}_\tau := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}) \quad \text{tel que } N|c \quad \text{et} \quad a\tau + b = \tau(c\tau + d) \right\}. \tag{6}$$

L'application

$$\mathcal{O}_\tau \longrightarrow \mathbb{C}, \qquad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto c\tau + d \tag{7}$$

identifie $\mathcal{O}_\tau$ à un ordre de K (c'est-à-dire, un sous-anneau de K qui est libre de rang deux en tant que $\mathbb{Z}$-module). Inversement, si $\mathcal{O}$ est un ordre de K, (dont on suppose, pour simplifier les énoncés subsequents, que son discriminant D est premier à N) on considère l'ensemble

$$\{\tau \in \mathcal{H} \text{ tel que } \mathcal{O}_\tau = \mathcal{O}\}. \tag{8}$$

Si cet ensemble est non-vide, la matrice de $\mathcal{O}_\tau$ qui correspond à $\sqrt{D} \in \mathcal{O}$ est de la forme

$$\begin{pmatrix} a_\tau & b_\tau \\ c_\tau N & d_\tau \end{pmatrix}, \qquad \text{où} \quad a_\tau^2 \equiv D \pmod{N}. \tag{9}$$

On suppose donc que D possède une racine carrée δ modulo N, que l'on fixe. On pose ensuite

$$\mathcal{H}^{\mathcal{O}} := \{\tau \in \mathcal{H} \qquad \text{tel que} \quad \mathcal{O}_\tau = \mathcal{O} \quad \text{et} \quad a_\tau \equiv \delta \pmod{N}\}. \tag{10}$$

Cet ensemble est préservé par l'action de $\Gamma_0(N)$ par transformations de Möbius.

Pour tout $\tau \in \mathcal{H}^{\mathcal{O}}$, le $\mathbb{Z}$-module engendré par 1 et τ est un $\mathcal{O}$-module projectif Λ_τ dont l'image dans le *groupe de Picard*

$$\mathrm{Pic}(\mathcal{O}) := \{\mathcal{O}\text{-modules projectifs dans } K\}/K^\times, \tag{11}$$

ne dépend que de la $\Gamma_0(N)$-orbite de τ. De surcroît, l'application naturelle

$$\mathcal{H}^{\mathcal{O}}/\Gamma_0(N) \longrightarrow \mathrm{Pic}(\mathcal{O}) \tag{12}$$

qui en résulte est une *bijection*. Le quotient $\mathcal{H}^{\mathcal{O}}/\Gamma_0(N)$ hérite ainsi d'une action naturelle du groupe $\mathrm{Pic}(\mathcal{O})$ dont il sera fait usage dans la suite.

Par ailleurs, la théorie du corps de classe identifie $\mathrm{Pic}(\mathcal{O})$ au groupe de Galois d'une extension abélienne H de K, appelée le *corps d'anneau* ("ring class field") associé à $\mathcal{O}$. Si $\mathfrak{p}$ est un idéal de K relativement premier au discriminant de $\mathcal{O}$, l'isomorphism de réciprocité

$$\mathrm{rec} : \mathrm{Pic}(\mathcal{O}) \longrightarrow \mathrm{Gal}(H/K) \tag{13}$$

associe à la classe de $\mathfrak{p} \cap \mathcal{O}$ l'élément de Frobenius en $\mathfrak{p}$ dans $\mathrm{Gal}(H/K)$.

L'unité modulaire α évaluée en $\tau \in \mathcal{H}^{\mathcal{O}}/\Gamma_0(N)$ donne lieu à l'*unité elliptique*

$$u(\alpha, \tau) := \alpha(\tau) \in \mathbb{C}^\times. \tag{14}$$

Cet invariant jouit des propriétés suivantes:

1. Après s'être fixé un plongement complexe $H \subset \mathbb{C}$, l'élément $u(\alpha, \tau)$ appartient à $H^\times$. Plus précisément,

$$u(\alpha, \tau) \in \mathcal{O}_H[1/N]^\times, \qquad \text{et} \qquad \frac{u(\alpha, \tau)^\sigma}{u(\alpha, \tau)} \in \mathcal{O}_H^\times, \tag{15}$$

   pour tout $\sigma \in \mathrm{Gal}(H/K)$, où $\mathcal{O}_F$ désigne comme d'habitude l'anneau des entiers du corps de nombres F.

2. (Loi de réciprocité de Shimura). Les applications (flèches horizontales) sont compatibles aux actions dans le diagramme suivant.

$$\begin{array}{ccc} \mathrm{Pic}(\mathcal{O}) & \xrightarrow{\mathrm{rec}} & \mathrm{Gal}(H/K) \\ \circlearrowleft & & \circlearrowleft \\ \mathcal{H}^{\mathcal{O}}/\Gamma_0(N) & \xrightarrow{\alpha} & H^\times. \end{array} \tag{16}$$

3. (Première formule limite de Kronecker). Etant donné $\tau \in \mathcal{H}^{\mathcal{O}}$, soit $Q_\tau(x,y)$ l'unique forme quadratique positive satisfaisant

$$Q_\tau(\tau,1)=0 \text{ et } \mathrm{Disc}(Q_\tau)=D. \tag{17}$$

Cette forme quadratique est à coefficients entiers, et elle est même *primitive*:

$$Q_\tau(x,y)=Ax^2+Bxy+Cy^2, \quad \gcd(A,B,C)=1, \tag{18}$$

avec

$$N|A, \quad \text{et} \quad B\equiv\delta \pmod N. \tag{19}$$

On introduit les fonctions zeta

$$\zeta_\tau(s):=\sum Q_\tau(m,n)^{-s}, \quad \zeta(\alpha,\tau,s):=\sum_{d|N} n_d d^{-s}\zeta_{d\tau}(s), \tag{20}$$

où la première somme se fait sur tous les couples d'entiers (m,n) différents de $(0,0)$. Le formule de Kronecker affirme alors que

$$\zeta'(\alpha,\tau,0)=\frac{1}{12}\log|u(\alpha,\tau)|^2. \tag{21}$$

Ce sont toutes ces propriétés qu'on aimerait étendre aux corps quadratiques réels.

2 Corps quadratiques réels

Soit K un corps quadratique réel muni d'un plongement $K\subset\mathbb{R}$. Tout comme dans le cas imaginaire, on associe à tout ordre $\mathcal{O}$ de K le groupe de Picard de $\mathcal{O}$, pris cette fois au *sens étroit*

$$\mathrm{Pic}^+(\mathcal{O}):=\{\mathcal{O}\text{-modules projectifs dans } K\}/K_+^\times, \tag{22}$$

où $K_+^\times$ désigne le groupe multiplicatif des éléments *totalement positifs* de K. La théorie du corps de classe fournit, comme en (13), un isomorphisme

$$\mathrm{rec}:\mathrm{Pic}^+(\mathcal{O})\longrightarrow\mathrm{Gal}(H/K), \tag{23}$$

où H est une extension abélienne de K, appelée corps d'anneau (au sens étroit) associé à $\mathcal{O}$.

On se propose de construire au moyen de l'unité modulaire α des éléments explicites de $H^\times$. On se heurte d'emblée à certaines difficultés évidentes:

1. D'une part, le demi-plan de Poincaré ne contient aucun élément appartenant à un corps quadratique réel.

2. D'autre part, on dispose du résultat négatif suivant qui vient de la transcendance et qui a été mentionné dans l'exposé de Michel Waldschmidt:

   Théorème 2.1. *Si $\tau \in \mathcal{H}$ est un nombre algébrique qui n'est pas quadratique, alors $\alpha(\tau)$ est transcendant.*

Comme on le verra plus bas, il faudra donc remplacer l'évaluation de α dans la formule (14) par une opération plus compliquée qui fait intervenir *l'intégration*, tant *complexe* que *p-adique*.

Avant de décrire cette procédure, on remarque que la difficulté 1 disparaît quand on remplace le demi-plan de Poincaré par une variante p-adique

$$\mathcal{H}_p := \mathbb{P}_1(\mathbb{C}_p) - \mathbb{P}_1(\mathbb{Q}_p), \tag{24}$$

où $\mathbb{C}_p$ désigne le complété de $\bar{\mathbb{Q}}_p$ pour la valuation p-adique. Ce "demi-plan" non-archimédien contient de nombreux éléments appartenant à K, pourvu que p soit *inerte* ou *ramifié* dans K, ce que l'on suppose désormais. On supposera même, pour simplifier un peu les énoncés, que p est *inerte* dans K, et qu'il ne divise pas N.

Pour tout $\tau \in \mathcal{H}_p \cap K$, on définit alors comme en (6)

$$\mathcal{O}_\tau := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}[1/p]) \ \text{ tel que } \ N|c \ \text{ et } \ a\tau + b = \tau(c\tau + d) \right\}. \tag{25}$$

C'est un p-ordre de K, c'est-à-dire, un sous-anneau de K qui contient $\mathbb{Z}[1/p]$ et qui est libre de rang deux en tant que module sur ce sous-anneau.

Inversement, en se fixant un p-ordre $\mathcal{O}$ de K de discriminant $D > 0$ premier à N,

$$D \equiv \delta^2 \pmod{N}, \tag{26}$$

on définit comme en (10)

$$\mathcal{H}_p^{\mathcal{O}} := \{\tau \in \mathcal{H}_p \quad \text{tel que} \quad \mathcal{O}_\tau = \mathcal{O} \quad \text{et} \quad a_\tau \equiv \delta \pmod{N}\}. \tag{27}$$

Cet ensemble est préservé par l'action du groupe

$$\Gamma = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}_2(\mathbb{Z}[1/p]) \ \text{ tel que } N|c \right\}, \tag{28}$$

et le quotient $\mathcal{H}_p^{\mathcal{O}}/\Gamma$ hérite comme en (12) d'une action du groupe de Picard $\mathrm{Pic}^+(\mathcal{O})$. (Il convient ici de remarquer que, parce que p est inerte dans K,

$$\mathrm{Pic}^+(\mathcal{O}) = \mathrm{Pic}^+(\mathcal{O} \cap \mathcal{O}_K). \tag{29}$$

Ainsi il n'y a pas de différence, du point de vue des groupes de Picard, à travailler avec un ordre au sens usuel, ou avec le p-ordre qui s'en déduit en rendant p inversible.)

On veut associer à tout $\tau \in \mathcal{H}_p^{\mathcal{O}}/\Gamma$ un élément explicite

$$u(\alpha, \tau) \in \mathbb{C}_p^\times, \tag{30}$$

que l'on appellera *unité spéciale*, et qui jouit (*conjecturalement*) de propriétés semblables à celles des unités elliptiques.

3 Construction des unités spéciales

Le construction de $u(\alpha, \tau)$ se fait en cinq étapes.

1. On suppose d'abord, sans perte essentielle de généralité, que l'unité α satisfait la propriété suivante

   Hypothèse 3.1. *Il existe un élément ξ de $\mathbb{P}_1(\mathbb{Q})$ tel que α n'ait ni zéro ni pôle en en toute pointe qui est Γ-équivalente à ξ.*

   Cette hypothèse est satisfaite, par exemple, pour l'unité modulaire

   $$\alpha(\tau) = \Delta(\tau)^2 \Delta(2\tau)^{-3} \Delta(4\tau), \quad \text{avec } \xi = \infty, \tag{31}$$

   ou encore pour l'unité modulaire donnée en (4) avec $\xi = \infty$ dès lors que N est sans facteurs carrés et que

   $$\sum_{d|N} d n_d = 0. \tag{32}$$

   En général on peut se ramener à ce cas en exprimant α—ou tout au moins, une puissance α^e—comme un produit d'unités modulaires, invariantes éventuellement par un sous-groupe de congruence plus petit, et satisfaisant l'Hypothèse 3.1.

2. On introduit l'unité modulaire

$$\alpha^*(z) := \frac{\alpha(z)}{\alpha(pz)} \tag{33}$$

invariante sous le groupe $\Gamma_0(Np)$. La dérivée logarithmique $d\log\alpha$ (resp. $d\log\alpha^*$) est une série d'Eisenstein de poids deux sur $\Gamma_0(N)$ (resp. sur $\Gamma_0(Np)$) de termes constants nuls aux pointes de $\Gamma\xi$. La proposition suivante construit, à partir des périodes (complexes) de $d\log\alpha^*$ entre ces pointes un système canonique de mesures p-adiques sur $\mathbb{P}_1(\mathbb{Q}_p)$.

Proposition 3.2. *Il existe un unique système de mesures p-adiques $\mu_{x\to y}$ sur $\mathbb{P}_1(\mathbb{Q}_p)$, indexées par des éléments x, y de $\Gamma\xi$, et satisfaisant les axiomes suivants:*

(a) Pour tout $x, y \in \Gamma\xi$, on a $\mu_{x\to y}(\mathbb{P}_1(\mathbb{Q}_p)) = 0$.

(b)

$$\mu_{x\to y}(\mathbb{Z}_p) = \frac{1}{2\pi i}\int_x^y d\log\alpha^*(z) \in \mathbb{Z} \subset \mathbb{Z}_p. \tag{34}$$

(c) Pour tout $\gamma \in \Gamma$ et tout sous-ensemble compact ouvert U de $\mathbb{P}_1(\mathbb{Q}_p)$,

$$\mu_{\gamma x\to\gamma y}(\gamma U) = \mu_{x\to y}(U). \tag{35}$$

La démonstration (élémentaire) de cette proposition est expliquée dans [DD], §2.1. La vérification de la propriété de distribution satisfaite par $\mu_{x\to y}$ fait intervenir de facon essentielle l'invariance de $d\log\alpha^*(z)$ sous l'opérateur de Hecke U_p.

C'est à travers l'axiome (b) de la proposition 3.2 qu'interviennent les périodes complexes de $d\log\alpha$. Ces périodes, ui sont des entiers, se calculent par des formules explicites où interviennent des *sommes de Dedekind*, et que l'on pourra trouver dans [DD], §2.5 ou encore dans [Maz].

3. On introduit l'intégration p-adique en posant, pour tout $x, y \in \Gamma\xi$ et pour tout $\tau_1, \tau_2 \in \mathcal{H}_p$,

$$\int_{\tau_1}^{\tau_2}\int_x^y d\log\alpha := \int_{\mathbb{P}_1(\mathbb{Q}_p)} \log_p\left(\frac{t-\tau_2}{t-\tau_1}\right) d\mu_{x\to y}(t) \in \mathbb{C}_p, \tag{36}$$

où $\log_p : \mathbb{C}_p^\times \longrightarrow \mathbb{C}_p$ est une branche du logarithme p-adique déterminée par la condition

$$\log_p(p) = 0. \tag{37}$$

La definition (36) a l'inconvénient de dépendre du choix d'un logarithme p-adique, c'est-à-dire, d'une "uniformisante" de $\mathbb{C}_p^\times$. Parce que les mesures $\mu_{x\to y}$ sont à valeurs dans $\mathbb{Z}$ (et non seulement $\mathbb{Z}_p$) on peut de toute façon faire mieux, en posant

$$⨍_{\tau_1}^{\tau_2}\int_x^y d\log\alpha := ⨍_{\mathbb{P}_1(\mathbb{Q}_p)}\left(\frac{t-\tau_2}{t-\tau_2}\right)d\mu_{x\to y}(t) \in \mathbb{C}_p^\times, \tag{38}$$

où l'intégrale de droite est une "intégrale de Riemann multiplicative" dans laquelle on a remplacé les limites usuelles de sommes de Riemann par des limites de produits correspondants. C'est dans cette définition plus fine que l'intégralité des mesures $\mu_{x\to y}$ joue un rôle essentiel. On remarque ici que si τ_1 et τ_2 appartiennent à $K_p \cap \mathcal{H}_p$, où K_p désigne le complété de K pour la valuation p-adique, alors l'intégrale de (38) appartient à $K_p^\times$.

4. L'intégrale multiplicative (38) permet d'associer à $\tau \in \mathcal{H}_p$ un deux-cocycle

$$\kappa_\tau \in Z^2(\Gamma, K_p^\times) \tag{39}$$

par la règle

$$\kappa_\tau(\gamma_1,\gamma_2) := ⨍_\tau^{\gamma_1\tau}\int_{\gamma_1\xi}^{\gamma_1\gamma_2\xi} d\log\alpha \in K_p^\times. \tag{40}$$

Soit

$$\mathrm{ord}_p : K_p^\times \longrightarrow \mathbb{Z} \subset K_p \tag{41}$$

l'homomorphisme habituel.

Théorème 3.3. *L'image naturelle des 2-cocycles* $\mathrm{ord}_p(\kappa_\tau)$ *et* $\log_p(\kappa_\tau)$ *dans* $H^2(\Gamma, K_p)$ *est triviale. En particulier, il existe un sous-groupe fini* U *de* $K_p^\times$ *et un élément* ξ_τ *de* $C^1(\Gamma, K_p^\times)$ *tel que*

$$\kappa_\tau = d\xi_\tau \pmod U. \tag{42}$$

Ce théorème est démontré dans [DD], §2.3. (Cf. aussi le §3.3 pour $\mathrm{ord}_p(\kappa_\tau)$, et le §4.3 pour $\log_p(\kappa_\tau)$.) Les démonstrations données dans

[DD] sont constructives et il en ressort des formules explicites pour ξ_τ. Par exemple, la formule pour $\log_p(\xi_\tau)$ fait intervenir des périodes de séries d'Eisenstein de poids pair ≥ 2 qui s'expriment au moyen de certaines sommes de Dedekind généralisées.

On remarque que la formule (42) ne détermine ξ_τ qu'à multiplication près par des éléments de $\hom(\Gamma, K_p^\times/U)$. Heureusement, on sait que l'abélianisée de Γ est un groupe *fini* ([Me], [Se]). En élargissant éventuellement le sous-groupe fini U de $K_p^\times$, l'invariant ξ_τ est alors défini sans ambiguité.

5. Soit Γ_τ le stabilisateur de τ dans Γ pour l'action de ce groupe sur $\mathcal{H}_p$. Le groupe $\Gamma_\tau/\langle\pm 1\rangle$ est libre de rang un, et ses deux générateurs correspondent aux unités fondamentales de $\mathcal{O}$ de norme 1. On fixe le choix d'un générateur γ_τ en se donnant une unité fondamentale ϵ de norme 1 de $\mathcal{O}$ et en exigeant que

$$\gamma_\tau \begin{pmatrix} \tau \\ 1 \end{pmatrix} = \epsilon \begin{pmatrix} \tau \\ 1 \end{pmatrix}. \tag{43}$$

On pose alors

$$u(\alpha, \tau) = \xi_\tau(\gamma_\tau) \in K_p^\times/U. \tag{44}$$

On peut vérifier ([DD], Chapitre 2) que l'invariant $u(\alpha, \tau)$ ne dépend que de α et de l'image de τ dans $\mathcal{H}_p^{\mathcal{O}}/\Gamma$, et pas des autres choix qui ont été faits au cours de sa construction.

Remarque 3.4. La définition de $u(\alpha, \tau)$ est calquée sur celle des points de Stark-Heegner sur les courbes elliptiques modulaires définis dans [Dar1] et dans le Chapitre 9 de [Dar2]. Dans cette construction la série d'Eisenstein $d\log\alpha^*$ est remplacée par la forme parabolique de poids deux sur $\Gamma_0(Np)$ associée à une courbe elliptique de conducteur Np.

Le corps d'anneau H associé à $\mathcal{O}$ est muni d'une involution canonique τ_∞ fournie par la conjugaison complexe, qui a priori dépend d'un plongement de H dans $\mathbb{C}$ (mais ne dépend pas en fin de compte de ce choix). On se donne aussi un plongement $H \longrightarrow \mathbb{C}_p$.

La conjecture principale de [DD] (énoncée dans le §2.4) prédit que les éléments $u(\alpha, \tau)$ se comportent comme des unités elliptiques, à cela près qu'il s'agit de p-unités et non d'unités de H.

Conjecture 3.5. *L'élément $u(\alpha,\tau)$ appartient à $\mathcal{O}_H[1/p]^\times$, et*

$$\tau_\infty u(\alpha,\tau) = u(\alpha,\tau)^{-1}. \tag{45}$$

De plus les éléments $u(\alpha,\tau)$ satisfont un loi de réciprocité de Shimura *selon laquelle les applications sont compatibles aux actions dans le diagramme suivant:*

$$\begin{array}{ccc} \mathrm{Pic}^+(\mathcal{O}) & \xrightarrow{\mathrm{rec}} & \mathrm{Gal}(H/K) \\ \circlearrowleft & & \circlearrowleft \\ \mathcal{H}_p^{\mathcal{O}}/\Gamma & \xrightarrow{u(\alpha,-)} & H^\times. \end{array} \tag{46}$$

4 Fonctions L

On associe comme avant à $\tau \in \mathcal{H}_p^{\mathcal{O}}$ une forme quadratique Q_τ à coefficients rationnels de discriminant $D = \mathrm{Disc}(\mathcal{O})$. (Par convention, le discriminant d'un p-ordre de K est un entier premier à p.) A priori les coefficients de Q_τ appartiennent à $\mathbb{Z}[1/p]$. On suppose qu'ils appartiennent en fait à $\mathbb{Z}$. Cela peut toujours s'arranger, quitte à remplacer τ par un élément de la Γ-orbite de τ ou de $p\tau$. Une fois cette condition satisfaite, la matrice γ_τ de l'équation (43) appartient à $\mathbf{SL}_2(\mathbb{Z})$, et agit donc par multiplication à gauche sur les vecteurs colonnes non-nuls de $\mathbb{Z}^2$. Soit

$$\mathcal{W} := (\mathbb{Z}^2 - \{(0,0)\})/\langle\gamma_\tau\rangle \tag{47}$$

un choix de représentants pour cette action. Comme dans l'équation (20), on pose

$$\zeta_\tau(s) := \sum_{\mathcal{W}} \mathrm{sgn}(Q_\tau(m,n))|Q_\tau(m,n)|^{-s}, \qquad \zeta(\alpha,\tau,s) := \sum_{d|N} n_d d^s \zeta_{d\tau}(s). \tag{48}$$

Cette définition ressemble en tous points à celles de la formule (20), à ceci près que

1. La forme quadratique $Q_\tau(x,y)$, qui est indéfinie, est constante sur les γ_τ-orbites de $(\mathbb{Z}^2 - \{0\})$. Il est donc essentiel, pour obtenir une expression convergente, de restreindre la somme à $\mathcal{W}$ et non à $\mathbb{Z}^2 - \{0\}$ tout entier.

2. La forme quadratique Q_τ prend des valeurs entières tant positives que négatives, ce qui rend nécessaire la valeur absolue. La présence du terme $\mathrm{sgn}(Q_\tau(m,n))$ implique que les fonctions $\zeta_\tau(s)$ s'expriment comme combinaison linéaire des fonctions $\zeta(K,\chi,s)$ où les χ parcourent les caractères *impairs* de $\mathrm{Gal}(H/K)$, c'est-à-dire, ceux pour lesquels $\chi(\tau_\infty) = -1$. En particulier, les $\zeta_\tau(s)$ sont partout holomorphes, même en $s = 1$. On remarque que pour s un entier positif *impair*

$$\zeta_\tau(s) = \sum_{\mathcal{W}} Q(m,n)^{-s}. \tag{49}$$

Le théorème suivant est démontré dans le Chapitre 3 de [DD]:

Théorème 4.1. $\zeta(\alpha,\tau,0) = \frac{1}{12}\,\mathrm{ord}_p(u(\alpha,\tau))$.

Ce résultat permet d'étudier la factorisation des idéaux principaux engendrés par les $u(\alpha,\tau)$ et de relier cette factorisation à *l'élément de Brumer-Stickelberger* dans l'anneau de groupe $\mathbb{Z}[\mathrm{Gal}(H/K)]$ qui a été introduit dans l'exposé de Cornelius Greither. On obtient ainsi le théorème suivant dans la direction de la conjecture de Brumer-Stark (cf. [DD], §3.4).

Théorème 4.2. *Si la conjecture 3.5 est vraie, alors l'élément de Brumer-Stickelberger* $\theta(H/K) \in \mathbb{Z}[\mathrm{Gal}(H/K)]$ *annule* $\mathrm{Pic}(\mathcal{O}_H) \otimes \mathbb{Z}[1/2]$*, la partie impaire du groupe de classes de* H*.*

Une démonstration de la conjecture 3.5 fournirait ainsi une preuve de la conjecture de Brumer-Stark pour les corps d'anneau de corps quadratiques réels dans la lignée de la démonstration de Stickelberger pour le cas abélien sur $\mathbb{Q}$ qu'a rappelé Greither dans son exposé. Les p-unités $u(\alpha,\tau)$ joueraient, dans cette approche, le rôle des sommes de Gauss dans la démonstration de Stickelberger.

Les travaux de Wiles [Wi] fournissent une démonstration de la conjecture de Brumer-Stark pour H/K qui ne s'appuie sur aucune conjecture. L'interêt du Théorème 4.2 réside dans le lien qu'il établit entre la Conjecture 3.5 et d'autres conjectures plus classiques. Il serait bien entendu plus interessant de disposer d'une implication dans le sens inverse!

D'après les travaux de Siegel et Deligne-Ribet, il existe une fonction analytique de la variable $s \in \mathbb{Z}_p$, appelée fonction zeta p-adique, et que l'on notera $\zeta_p(\alpha,\tau,s)$, qui est définie par la propriété d'interpolation suivante

$$\zeta_p(\alpha,\tau,s) = (1 - p^{-2s})\zeta(\alpha,\tau,s), \tag{50}$$

pour tout entier négatif $s \equiv 0 \pmod{p-1}$. (La fonction $\zeta_p(\alpha, \tau, s)$, si elle existe, est bien entendu unique puisque les entiers négatifs divisibles par $p-1$ sont denses dans $\mathbb{Z}_p$. Toute la difficulté est d'en démontrer l'existence.) Le lecteur notera que la fonction $\zeta_p(\alpha, \tau, s)$ s'annule en $s = 0$ à cause du facteur Eulérien qui apparaît dans (50).

Le théorème suivant, qui figure dans la thèse du second auteur [Das] et dont la démonstration est reproduite dans le Chapitre 4 de [DD], établit un lien entre les unités $u(\alpha, \tau)$ et les valeurs spéciales de la fonction $\zeta_p(\alpha, \tau, s)$ en $s = 0$.

Théorème 4.3. *Si on pose* $|x|^2 := \mathrm{Norme}_{K_p/\mathbb{Q}_p}(x)$*, alors*

$$\zeta_p'(\alpha, \tau, 0) = -\frac{1}{12} \log_p |u(\alpha, \tau)|^2. \tag{51}$$

L'existence d'une p-unité de H satisfaisant la propriété (45) de la conjecture 3.5 ainsi que les théorèmes 4.1 et 4.3 a été conjecturée par Gross dans [Gr1] et [Gr2] (conjecture de Gross-Stark p-adique). La Conjecture 3.5 impliquerait donc la conjecture de Gross-Stark p-adique—mais elle est plus forte que celle-ci, puisqu'elle permet de calculer par un procédé analytique l'unité de Gross-Stark elle-même, et non seulement sa "valeur absolue".

Remarque 4.4. Le théorème 4.3 est une variante naturelle de la formule limite de Kronecker (21) pour les corps quadratiques réels. Le lecteur en trouvera des variantes plus classiques, où n'intervient pas d'analyse p-adique, dans le livre de Siegel [Sie] ou encore dans [Za].

References

[Dar1] H. Darmon. *Integration on $\mathcal{H}_p \times \mathcal{H}$ and arithmetic applications*. Ann. of Math. (2) **154** (2001), no. 3, 589–639.

[Dar2] H. Darmon. *Rational points on modular elliptic curves*. NSF-CBMS Lecture Notes, à paraître.

[Das] S. Dasgupta, Thèse de Doctorat, Berkeley. En cours.

[DD] H. Darmon et S. Dasgupta. *Elliptic units for real quadratic fields*. à paraître.

[Gr1] B.H. Gross. *p-adic L-series at $s = 0$*. J. Fac. Sci. Univ. Tokyo Sect. IA Math. 28 (1981), no. 3, 979–994 (1982).

[Gr2] B.H. Gross. *On the values of abelian L-functions at $s = 0$*. J. Fac. Sci. Univ. Tokyo Sect. IA Math. 35 (1988), no. 1, 177–197.

[Hida] H. Hida. *Elementary theory of L-functions and Eisenstein series*. London Math. Society Student Texts. **26**. Cambridge University Press, 1993.

[KL] D.S. Kubert, S. Lang. Modular units. Grundlehren der Mathematischen Wissenschaften, 244. Springer-Verlag, New York-Berlin, 1981.

[Man] J.I. Manin, *Parabolic Points and Zeta Functions of Modular Curves.* Izv. Akad. Nauk SSSR Ser. Mat. **36** (1972), no. 1, 19–66.

[Maz] B. Mazur. *On the arithmetic of special values of L functions.* Invent. Math. **55** (1979), no. 3, 207–240.

[Me] J. Mennicke. *On Ihara's modular group*. Invent. Math **4** (1967) 202-228.

[Se] J.-P. Serre, *Le problème des groupes de congruence pour* $\mathbf{SL}_2$. Ann. of Math (2) **92** (1970) 489–527.

[Sie] C.L. Siegel. Advanced analytic number theory. Second edition. Tata Institute of Fundamental Research Studies in Mathematics, 9. Tata Institute of Fundamental Research, Bombay, 1980.

[Wi] A. Wiles. *On a conjecture of Brumer*. Ann. of Math. (2) 131 (1990), no. 3, 555–565. (Reviewer: Alexey A. Panchishkin) 11R42 (11R23)

[Za] D. Zagier. *A Kronecker limit formula for real quadratic fields*. Math. Ann. **213** (1975), 153–184.