Séminaire Delange-Pisot-Poitou
(Théorie des Nombres)
1980-81

UNE CLASSE DE COURBES ELLIPTIQUES A MULTIPLICATION COMPLEXE

Norbert Schappacher
Göttingen

A. Soient K un corps quadratique imaginaire et $\mathcal{O}$ son anneau d'entiers. Nous fixons une fois pour toutes un plongement de K dans $\mathbb{C}$.

On considère des caractères de Hecke complexes ϕ de K, de conducteur $\mathfrak{f}$, tels que, pour chaque α dans K^* premier à $\mathfrak{f}$, on ait $\phi(\alpha\mathcal{O}) = \alpha$, si $\alpha \equiv 1 \bmod \mathfrak{f}$.

Les courbes elliptiques annoncées par le titre se construisent à partir de tels caractères ϕ : - Soit F une extension finie abélienne de K, telle que le caractère $\psi = \phi \circ N_{F/K}$ de F prenne des valeurs dans K^* en les idéaux entiers de F premiers à son conducteur. Alors F contient forcément le corps de classes de Hilbert H de K. Le caractère ψ détermine une classe de F-isogénie de courbes elliptiques E sur F telles que $\mathrm{End}_F E \cong \mathcal{O}$ et que ψ soit le Grössencharakter attaché à E/F. Cf. [5], §9.

Les notations résumées ci-dessous seront utilisées pendant tout l'exposé:

$$\begin{array}{lcl} E\ /\ F & \psi & \mathrm{End}_F E = \mathcal{O} \\ G=\mathrm{Gal}(F/K)\ \text{abelien} \quad \Big| \ n=[F:K] & \Big| \ N_{F/K} & \psi = \psi_{E/F} \\ \qquad K & \phi & \mathfrak{f} = \mathrm{cond}\ \phi \\ & & \mathfrak{g} = \mathrm{ppcm}(\mathrm{cond}\ F/K, \mathfrak{f}) \end{array}$$

B. EXEMPLE

Si $K = \mathbb{Q}(\sqrt{-p})$ avec p premier, $p \equiv 3 \bmod 4$, $p \geq 7$, et que l'on pose $\phi(\alpha\mathcal{O}) = \pm\alpha \equiv x^2 \pmod{\sqrt{-p}\ \mathcal{O}}$, on obtient $E = A(p)$ sur H , dans les notations de [5].

C. Les courbes elliptiques introduites dans (A) représentent des outils puissants dans l'étude des caractères de Hecke des corps quadratiques imaginaires. Cet exposé va en donner un exemple. D'autre part, elles forment la plus grande classe de courbes elliptiques pour laquelle on sait démontrer le

THÉORÈME DE COATES ET WILES. Si $E(F)$ est infini, alors $L(\psi,1) = 0$. Voir [1] et [2].

Le point essentiel est qu'on contrôle l'arithmétique de E/F par la théorie du corps de classes de K .

D. PLAN DE L'EXPOSÉ

Dans (E), on caractérise les courbes envisagées de différents points de vue. Les données sont ensuite développés -- (F) à (K) -- afin de préparer les énoncés de rationalité, (L), pour les valeurs spéciales de fonctions L : $L(\overline{\phi},1)$ et $L(\overline{\psi},1)$, prédits par la conjecture de Deligne, (M).

E. ÉQUIVALENCES

Soient F une extension abélienne de K ; E une courbe elliptique sur F telle que $\mathrm{End}_F E = \mathcal{O}$, de Grössencharakter associé ψ . Alors les conditions suivantes sont équivalentes:

(1) Il existe un caractère ϕ de K , tel que $\psi = \phi \circ N_{F/K}$.

(2) $F(E_{tors})$, le corps engendré sur F par les coordonnées des points de division de E , est abélien sur K .

(3) Pour tout premier ℓ , la représentation $\mathrm{Ind}_{F/K}\rho_\ell(E)$, induite par rapport à $G(\overline{\mathbb{Q}}/F) \hookrightarrow G(\overline{\mathbb{Q}}/K)$ par la représentation ℓ-adique $\rho_\ell(E)$ attachée à E sur F , est abélienne.

(4) Pour $B = R_{F/K}E$ la restriction de scalaires selon Weil, on a

$$\mathrm{End}_K B \otimes \mathbb{Q} = \prod_{i=1}^{r} T_i =: T \quad ,$$

où chaque T_i $(i = 1,\dots,r)$ est un corps de type CM contenant K, et $\sum_{i=1}^{r} [T_i:K] = n$.

F. Voici comment on peut visualiser les r corps T_i à partir des données ϕ et F : ψ étant $\phi\circ N_{F/K}$, on voit facilement que l'ensemble des caractères ϕ' de K satisfaisant $\psi = \phi'\circ N_{F/K}$ est $\{\phi\chi : \chi \in \hat{G}\}$. Les corps T_i $(i = 1,\dots,r)$ correspondent alors aux orbites de cet ensemble sous $\mathrm{Aut}_K\mathbb{C}$. Ainsi, si $T_1 = K(\phi)$ et $[T_1:K] = n_1$, on aura que

$$\{\phi^\sigma : \sigma \in \mathrm{Aut}_K\mathbb{C}\} = \{\phi,\phi\chi_2,\dots,\phi\chi_{n_1}\} .$$

Ensuite $T_2 = K(\phi\chi_{n_1+1})$, pour un certain χ_{n_1+1}, etc.

Si l'on est dans le cas particulier où F égale H, le corps de classes de Hilbert de K, il est démontré dans [6], que $r = 1$.

G. Appelons $\tilde{\psi}$ (resp. $\tilde{\phi}$) les quasi-caractères d'idèles attachés -- selon [7], Th. 10 -- à E/F (resp. B/K). On a donc

$$\tilde{\psi} : F_{\mathbb{A}}^{*} \to K^{*} , \tilde{\psi}|_{F^*} = N_{F/K} \quad ;$$

et de $\psi \otimes N^{-1}_{F\otimes\mathbb{R}/K\otimes\mathbb{R}}$ se déduisent, par les deux plongements possibles de K dans $\mathbb{C}$, les deux caractères complexes ψ et $\overline{\psi}$. De même, $\tilde{\phi} : K_{\mathbb{A}}^{*} \to T^{*}$, $\tilde{\phi}|_{K^*} = (\text{diag.})$; et les caractères complexes $\phi\chi$, pour $\chi \in \hat{G}$, ainsi que leurs conjugués complexes, se déduisent de $\tilde{\phi} \otimes (\text{compos. à } l'\infty)^{-1}$ par les différents $\mathbb{Q}$-homomorphismes de $T = \Pi\, T_i$ dans $\mathbb{C}$.

H. Soit $\mathfrak{a}$ un idéal entier de K premier à G (notation de (A)). L'action de l'endormorphisme $\tilde{\phi}(\mathfrak{a})$ sur un point de G-division P de B est alors donnée par le symbole d'Artin $\sigma_{\mathfrak{a}}$ de l'idéal $\mathfrak{a}$:

$$\tilde{\phi}(\mathfrak{a})(P) = P^{\sigma_{\mathfrak{a}}} \quad .$$

$\tilde{\phi}(\mathfrak{a})$ induit donc une isogénie $E \to E^{\sigma_{\mathfrak{a}}}$. (Si $\mathfrak{a}$ est une norme de F, alors $E^{\sigma_{\mathfrak{a}}} = E$ et on voit aussitôt que $\tilde{\psi} = \tilde{\phi}\circ N_{F/K}$).

I. DU POINT DE VUE ANALYTIQUE...

Choisissons un plongement de F dans $\mathbb{C}$ qui est compatible au plongement fixé de K, et tel que l'invariant j algébrique de E s'identifie à l'invariant modulaire $j(\mathcal{O})$. Choisissons également une forme différentielle de première espèce ω de E définie sur F. Le couple (E,ω) détermine donc, par la théorie de Weierstrass, un réseau L du plan complexe qui, dans notre cas, s'écrit sous la forme $L = \Omega\mathcal{O}$, pour un $\Omega \in \mathbb{C}^*$. On fixe un des $|\mathcal{O}^*|$ choix possibles de la période Ω.

Pour $\mathfrak{a}$ comme dans (H), on note $(E^{\mathfrak{a}}, \omega^{\mathfrak{a}})$ le modèle conjugué de (E,ω) par $\sigma_{\mathfrak{a}}$. Soit $L_{\mathfrak{a}}$ le réseau dans $\mathbb{C}$ correspondant. Définissons $\Lambda(\mathfrak{a}) \in F^*$ par la formule

$$\Lambda(\mathfrak{a})\omega = \tilde{\phi}(\mathfrak{a})^*(\omega^{\mathfrak{a}}) .$$

Cette constante $\Lambda(\mathfrak{a})$ dépend du choix de ω : si l'on passe de ω à $\alpha\omega$ $(\alpha \in F^*)$, $\Lambda(\mathfrak{a})$ se multiplie par $\alpha^{(1-\sigma_{\mathfrak{a}})}$. On voit tout de suite que $\Lambda(\mathfrak{a})$ est un homomorphisme croisé par l'action de G :

$$\Lambda(\mathfrak{a}\mathfrak{b}) = \Lambda(\mathfrak{a})^{\sigma_{\mathfrak{b}}}\Lambda(\mathfrak{b}) .$$

Nous avons le diagramme commutatif suivant

$$\begin{tikzcd} E \arrow[r, "\text{Weierstrass}"] \arrow[d, "\tilde{\phi}(\mathfrak{a})"'] & \mathbb{C}/L \arrow[d, "\cdot\Lambda(\mathfrak{a})"] \\ E^{\mathfrak{a}} \arrow[r, "\text{Weierstrass}"'] & \mathbb{C}/L_{\mathfrak{a}} \end{tikzcd} .$$

La théorème principal de la multiplication complexe des courbes elliptiques -- [8], Th. 5.4 -- dit que $L_{\mathfrak{a}}$ s'écrit $L_{\mathfrak{a}} = \Lambda(\mathfrak{a})\Omega\mathfrak{a}^{-1}$. En d'autres termes, $\tilde{\phi}(\mathfrak{a})$ induit une isogénie $E \to E^{\mathfrak{a}}$ de noyau isomorphe à $\mathfrak{a}^{-1}/\mathcal{O}$.

J. Posons $\Phi(\mathfrak{a}) = \tilde{\phi}(\mathfrak{a})\Lambda(\mathfrak{a})^{-1} \in (T \otimes_K F)^*$. Alors il est facile de voir que $\Phi(\mathfrak{a})$ dépend uniquement de $\sigma_{\mathfrak{a}}|_F \in G$. (Ceci n'est pas vrai au niveau des $\Lambda(\mathfrak{a})$!).

On obtient donc une application

$$\Phi : G \to (T \otimes_K F)^* ,$$

qui est visiblement un 1-cocycle, si l'on munit $(T \otimes_K F)^*$ de l'action de G qui est triviale sur T et naturelle sur F. Une légère généralisation du "théorème 90" de Hilbert fournit donc un élément x de $(T \otimes_K F)^*$ (bien détermine à T^* près) tel que $\Phi(\sigma) = x^{(\sigma-1)}$, pour tout $\sigma \in G$.

K. On note ε un élément de $J := \mathrm{Hom}_K(T,\mathbb{C})$. Par le plongement choisi de F dans $\mathbb{C}$ -- voir (I) -- $T \otimes_K F$ s'injecte dans $T \otimes_K \mathbb{C} = \mathbb{C}^J$.

On associe donc à ε la composante x_ε de l'élément x construit plus haut. De même, ϕ_ε est l'élément de $\{\phi\chi : \chi \in \hat{G}\}$ qui se déduit de $\tilde{\phi}$ au moyen de ε - voir (G). Enfin, notons T_ε l'image de ε.

La forme différentielle $\eta_\varepsilon = \sum_{\sigma\in G} (x^\sigma)_\varepsilon\, \omega^\sigma \in H^0(B,\Omega^1/T_\varepsilon)$ est une forme propre pour l'action de T. Plus précisément, on a $\tilde{\phi}(\mathfrak{a})^*(\eta_\varepsilon) = \phi_\varepsilon(\mathfrak{a})\cdot\eta_\varepsilon$. On deduit de cela que, pour chaque cycle $c \in H_1(B,\mathbb{Z})$, l'intégrale $\int_c \eta_\varepsilon$ vaut $x_\varepsilon \Omega$, à un élément de T_ε^* près: $(\int_c \eta_\varepsilon)_\varepsilon \underset{T^*}{\sim} x\Omega \in (T \otimes_K \mathbb{C})^*$.

L. <u>THÉORÈMES DE RATIONALITÉ</u>
<u>On garde les notations précédentes</u>

1) $$(L(\overline{\phi}_\varepsilon,1))_\varepsilon \underset{T}{\sim} x\Omega \in (T \otimes_K \mathbb{C})^*$$

2) $$L(\overline{\psi},1) \underset{K}{\sim} \delta \,.\, \prod_{\mathfrak{a}}(\Lambda(\mathfrak{a})\Omega)$$

où $\delta = \det_{i,\sigma}(f_i^\sigma) \neq 0$, <u>pour un système</u> $\mathcal{O}$-<u>libre d'éléments</u> $f_i \in F$ $(i = 1,\dots,n)$; <u>et</u> $\mathfrak{a}$ <u>décrit un ensemble d'idéaux entiers de</u> K <u>premiers à</u> G <u>dont les symboles d'Artin couvrent</u> G <u>sans répétition</u>.

M. On vérifie que 1) équivaut à la conjecture de Deligne, [3], 2.8, pour le motif $R_{K/\mathbb{Q}} H_1(B)$. En fait, on a $H_1(B) = M(\phi^{-1})$ dans les notations de [3], 8.1. De même, 2) équivaut à la conjecture pour $R_{F/\mathbb{Q}} H_1(E)$, le terme à droit de 2) étant celui de la proposition 8.16 de [3].

N. La démonstration des énoncés de (L) repose sur deux résultats cruciaux.

1) Pour $\sigma \in G$, posons $L(\phi,\sigma,s) = \sum_{\sigma_{\mathfrak{a}}=\sigma} \phi(\mathfrak{a})N\mathfrak{a}^{-s}$, pour $\mathrm{Re}(s)$ assez grande, pour obtenir une fonction L partielle par prolongement analytique. Elle se décompose en somme de séries d'Eisenstein: Soit $\rho \in \Omega K^*$ tel que $\frac{\rho}{\Omega}\mathcal{O} = \frac{\mathfrak{h}}{\mathcal{G}}$, pour un idéal entier $\mathfrak{h}$ de K premier à $\mathcal{G}$.

On notera $\mathcal{B}$ un ensemble d'idéaux entiers $\mathfrak{b}$ de K premiers à $\mathcal{G}$ représentant les classes de rayon $\mathrm{mod}.\mathcal{G}$ de K dont le symbole d'Artin fixe F.

Finalement, E_1 est la série d'Eisenstein dont la valeur en L et $z \notin L$ serait $E_1(z,L) = \sum_{\omega\in L} (z+\omega)^{-1}$, si cette dernière serie convergeait... -- voir [9], III -- et on note E_1^* la fonction L-périodique déduite de E_1 : [9], VI §2.

Alors on trouve, pour tout $\varepsilon \in \mathrm{Hom}_K(T,\mathbb{C})$ et tout $(\mathfrak{a},\mathcal{G}) = 1$, la formule

$$\frac{\phi_\varepsilon(\mathfrak{a}\mathfrak{h})}{\Lambda(\mathfrak{a})\rho} L(\overline{\phi}_\varepsilon,\sigma_{\mathfrak{a}\mathfrak{h}},1) = \sum_{\mathfrak{b}\in\mathcal{B}} E_1^*(\phi_\varepsilon(\mathfrak{b})\Lambda(\mathfrak{a})\rho,L_{\mathfrak{a}}) .$$

Notons $E(\mathfrak{a},\mathfrak{b})$ les termes de la somme à droite. Ils ne dépendent pas, en fait, de ε.

2) On démontre (voir [4], §6) que $E(\mathfrak{a},\mathfrak{b})$ appartient au corps des rayons modulo $\mathcal{G}$ de K, et que

$$E(\mathcal{O},\mathfrak{b})^{\sigma_{\mathfrak{a}}} = E(\mathfrak{a},\mathfrak{b}) = E(\mathfrak{a},\mathcal{O})^{\sigma_{\mathfrak{b}}} .$$

Pour plus de détails de la démonstration de (L), voir [4], §7.

REFERENCES

[1] Arthaud, N., On Birch and Swinnerton-Dyer's Conjecture for elliptic curves with complex multiplication, II; à paraître.

[2] Coates, M. et Wiles, A., On the Conjecture of Birch and Swinnerton-Dyer. Inventiones Math. 39 (1977), 223-251.

[3] Deligne, P., Valeurs de fonctions L et périodes d'intégrales. Proc. Symp. in Pure Math. 33 (1979), Part 2, 313-346.

[4] Goldstein, C. et Schappacher, N., Séries d'Eisenstein et fonctions L de courbes elliptiques à multiplication complexe; à paraître, Crelle.

[5] Gross, B., Arithmetic on elliptic curves with complex multiplication. Springer Lect. Notes Math. 776 (1980).

[6] Rohrlich, D., Galois Conjugacy of unramified twists of Hecke characters. Duke Math. J. 47 (1980).

[7] Serre, J.-P. et Tate, J., Good reduction of abelian varieties. Ann. of Math. 88 (1968), 492-517.

[8] Shimura, G., Introduction to the arithmetic theory of automorphic functions. Princeton U. Press, 1971.

[9] Weil, A., Elliptic functions according to Eisenstein and Kronecker. Springer Ergebn. 88 (1976).

Norbert Schappacher
Mathematisches Institut der Universität
Bunsenstr. 3-5
D-3400 Göttingen