Séries d'Eisenstein et fonctions L de courbes elliptiques à multiplication complexe

Par *Catherine Goldstein* d'Orsay et *Norbert Schappacher**) de Göttingen

Introduction

Soit K un corps quadratique imaginaire, muni d'un plongement dans $\mathbb{C}$. Eisenstein fut le premier à démontrer, dans un langage légèrement différent, des résultats d'algébricité concernant les valeurs spéciales de fonctions L d'un Grössencharakter de K aux points entiers naturels, dans la moitié droite de la bande critique de ces fonctions (voir à ce propos le résumé de Weil dans [26]). Longtemps négligé, cet aspect du travail d'Eisenstein fut redécouvert par Birch et Swinnerton-Dyer [2] et Damerell [8]. Il fut ensuite généralisé aux corps de type CM dans [20], papier qui s'inscrit dans le cadre d'une importante série de résultats d'algébricité dus à Shimura.

Le but du présent article est de préciser — tout en utilisant essentiellement les mêmes méthodes — les résultats d'Eisenstein et de Damerell et de les relier d'une part à la conjecture de Birch et Swinnerton-Dyer sur les courbes elliptiques et d'autre part à la conjecture de Deligne, [9].

Soit φ un caractère de Hecke de K de conducteur $\mathfrak{f}$. Supposons que $\varphi((\alpha))=\alpha$ pour tout $\alpha \in K^*$ avec $\alpha \equiv 1 \bmod^{\times} \mathfrak{f}$. Les valeurs de φ sur les idéaux de K premiers à $\mathfrak{f}$ ne se trouvent en général pas dans K^*. Mais il existe clairement une extension abélienne finie F de K (contenant nécessairement le corps de classes de Hilbert de K) telle que le Grössencharakter ψ de F donné par

$$\psi = \varphi \circ N_{F/K}$$

prenne dans K^* ses valeurs aux idéaux de F premiers à son conducteur. Par la théorie de la multiplication complexe, il existe alors une courbe elliptique E définie sur F, à multiplication complexe par l'anneau $\mathfrak{o}$ des entiers de K, dont le Grössencharakter sur F au sens de Deuring soit précisément ψ.

Soient j et k deux entiers avec $0 < \frac{k}{2} < j \leqq k$. Nous allons prouver des résultats précis de rationalité pour les valeurs spéciales $L(\bar{\psi}^k, j)$ d'une part, voir (7. 1) et (7. 3), et $L(\bar{\varphi}^k, j)$ d'autre part, voir (9. 1). Nos théorèmes démontrent la conjecture de Deligne

*) Supporté par Deutsche Forschungsgemeinschaft.

0075-4102/81/0327-0008$02.00

— [9], 2. 8 — pour des motifs adaptés à ces valeurs, voir (9. 3), (9. 7). En particulier, nous vérifions l'énoncé de rationalité pour $L(\psi, 1)$, $L(\bar{\psi}, 1)$ contenu dans la conjecture de Birch et Swinnerton-Dyer pour E/F — ou, ce qui revient au même, pour B/K, où B est la restriction de scalaires de E, au sens de Weil, par rapport à l'extension F/K. Bien que le résultat (9. 3), relatif à la conjecture de Deligne, contienne essentiellement tous les autres, nous avons préféré privilégier le point de vue de l'arithmétique de la courbe E/F et donc établir d'abord les propriétés des $L(\bar{\psi}^k, j)$ pour réserver le point de vue de Deligne à un paragraphe complémentaire (§ 9).

Mentionnons ici notre résultat final relatif à $L(\bar{\psi}, 1)$: La variété abélienne B/K, restriction de scalaires de E, a des multiplications complexes par K, ce qui induit une structure de K-espace vectoriel sur l'homologie rationnelle $H_1(B(\mathbb{C}), \mathbb{Q})$. Les formes différentielles $H^0(B, \Omega^1_{/K})$ étant munies de l'action naturelle de K, l'accouplement d'intégration

$$H_1(B(\mathbb{C}), \mathbb{Q}) \times H^0(B, \Omega^1_{/K}) \xrightarrow{\int} \mathbb{C}$$

est K-bilinéaire.

Soit Ω_B un complexe non nul — bien déterminé à un élément de K^* près — représentant le déterminant de $\int$, calculé dans des bases K-rationnelles: Alors

$$\frac{L(\bar{\psi}, 1)}{\Omega_B}$$

appartient à K.

Il semble probable que nos résultats peuvent aussi être démontrés, sans l'intermédiaire des séries d'Eisenstein, par les méthodes de Shimura, voir [21], [22].

La classe des courbes E/F construites plus haut est la plus grande classe de courbes elliptiques dont l'arithmétique est maîtrisée par la théorie du corps de classes de K: voir (4. 1). Elle fut introduite par Shimura et étudiée notamment par N. Arthaud [1] dans sa généralisation du théorème de Coates et Wiles [6] (cf. aussi le travail de K. Rubin en cours de préparation*)). Nous empruntons à Arthaud en particulier les fonctions L «partielles»: voir § 5. Enfin, si le discriminant de K est premier, les «$\mathbb{Q}$-courbes» de B. Gross [10] sont les exemples typiques des courbes considérées ici. Son travail a d'ailleurs beaucoup influencé la présentation de nos résultats.

Nous tenons à remercier cordialement John Coates qui a proposé et orienté ce travail, ainsi que Benedict Gross pour ses amicaux conseils pendant la préparation de la version finale de cet article.

Conseils au lecteur. Nous avons regroupé dans la partie I (§§ 1, 2, 3) des résultats relatifs aux séries d'Eisenstein, valables pour toute courbe elliptique E à multiplication complexe par $\mathfrak{o}$, définie sur une extension finie arbitraire F de K. Dans les parties II et III, nous nous bornons aux courbes E/F vérifiant les propriétés équivalentes (4. 1). Le lecteur intéressé par nos résultats principaux pourra assimiler nos notations et conventions en lisant le § 4, puis se reporter immédiatement aux §§ 7 et 9: les résultats des §§ 1, 2, 5 et 6 interviennent dans les démonstrations des théorèmes principaux. Le § 8 est une annexe du § 7 qui étudie le cas où la courbe E descend à un sous-corps réel F^+ de F, avec $[F: F^+] = 2$. Enfin les §§ 3 et 10, qui peuvent être négligés dans une première lecture, présentent des propriétés d'intégralité de certains nombres dont nous avons prouvé l'algébricité; nous espérons qu'ils pourront être utiles pour des calculs numériques.

*) Ajouté sur epreuves: Elliptic curves with complex multiplication and the conjecture of Birch and Swinnerton-Dyer; à paraître dans Inventiones Math.

Première partie: Des séries d'Eisenstein

> Es ist hier sehr unwesentlich, zu bemerken, daß $\Sigma \frac{1}{\alpha m+\beta n}$ bei einem gewissen Arrangement der Glieder den Werth *Null* hat; man muss aber deshalb nicht glauben, daß diese Reihe stets den Werth Null hätte.
>
> *Gotthold Eisenstein*, Genaue Untersuchung..., J. reine angew. Math. **35** (1847), 172, Fußnote.

§ 1. Rappels

Pour introduire les séries d'Eisenstein dont nous aurons besoin, nous allons adopter ici le point de vue et les méthodes de Kronecker exposés par Weil dans [26], ch. VIII.

Dans tout ce paragraphe, nous noterons L un réseau du plan complexe. On définit comme suit un invariant de L: Soit (u, v) une base quelconque de L sur $\mathbb{Z}$ telle que $\mathrm{Im}(v/u) > 0$. Alors le réel $\dfrac{\bar{u}v - u\bar{v}}{2\pi i}$ est strictement positif et indépendant de la base choisie; nous le noterons $A(L)$. Considérons alors la famille suivante d'homomorphismes du groupe additif $\mathbb{C}$ dans le groupe multiplicatif des nombres complexes de module 1, paramétrée par la variable complexe z_0:

$$\chi(z, z_0, L) = \exp\{A(L)^{-1}(\bar{z}_0 z - z_0 \bar{z})\}.$$

Alors, pour chaque entier $k \geqq 0$, on définit des fonctions holomorphes dans le domaine $\mathrm{Re}(s) > 1 + \dfrac{k}{2}$ par

$$\textbf{(1. 0)} \qquad H_k(z, z_0, s, L) = \sum{}' \chi(z, z_0, L) \frac{(\bar{z}+\bar{\omega})^k}{|z+\omega|^{2s}},$$

la somme étant étendue à tous les $\omega \in L$ sauf $-z$, si $z \in L$. Ce sont les doubles séries de Kronecker notées K dans [26], VIII, § 12.

(1. 1) Théorème. (i) *La fonction $s \mapsto \Gamma(s)\, H_k(z, z_0, s, L)$ peut être prolongée dans tout le plan complexe en une fonction méromorphe, qui est en fait partout holomorphe, sauf dans les deux cas*:

(a) $k = 0$ *et* $z \in L$,

(b) $k = 0$ *et* $z_0 \in L$.

Dans le cas (a), *la fonction a un pôle simple en $s = 0$ dont le résidu est $-\chi(-z, z_0, L)$; dans le cas* (b), *elle a un pôle simple en $s = 1$, dont le résidu est $A(L)^{-1}$ si $z_0 = 0$.*

(ii) *On a de plus l'équation fonctionnelle*

$$\Gamma(s)\, H_k(z, z_0, s, L) = A(L)^{k+1-2s}\Gamma(k+1-s)\, \chi(-z, z_0, L)\, H_k(z_0, z, k+1-s, L).$$

Pour la démonstration, voir [26], VIII, § 13.

La fonction $z \mapsto H_k(z, z_0, s, L)$ est paire ou impaire selon que k est pair ou impair; elle est de plus périodique par rapport à L.

Par (1. 0), ces faits sont clairs pour $\mathrm{Re}(s) > 1 + \frac{k}{2}$; ils s'en déduisent par prolongement analytique dans le cas général.

Nous sommes maintenant en mesure d'introduire les *séries d'Eisenstein*. Soient i et j deux entiers tels que $j > i \geqq 0$ et soit $z \in \mathbb{C} \setminus L$. On pose $E^*_{i,j}(z, L) = H_{i+j}(z, 0, j, L)$ et, pour simplifier, $E^*_k(z, L) = E^*_{0,k}(z, L)$, si k est un entier $\geqq 1$. Pour $j \geqq i+3$, on trouve donc la formule explicite:

$$E^*_{i,j}(z, L) = \sum_{\omega \in L} \frac{(\bar{z} + \bar{\omega})^i}{(z+\omega)^j};$$

et pour $k \geqq 3$:

$$E^*_k(z, L) = \sum_{\omega \in L} (z+\omega)^{-k}.$$

Le théorème (1. 1) n'est nécessaire à la définition des $E^*_{i,j}$ que si $j - i$ vaut 1 ou 2.

Le résultat suivant est contenu dans [26], VIII, § 14:

(1. 2) Proposition. (i) *Pour* $k > 1$, $E^*_k(z, L)$ *est une fonction holomorphe de* z, *pour* $z \in \mathbb{C} \setminus L$.

(ii) $$\frac{\partial}{\partial \bar{z}} E^*_1(z, L) = \frac{-1}{A(L)}.$$

De plus, les propriétés des fonctions H_k montrent que les fonctions $E^*_{i,j}$ sont périodiques par rapport à L, et paires ou impaires selon la parité de $i+j$.

La proposition suivante nous permettra de ramener l'étude des fonctions $E^*_{i,j}$ à celle des E^*_k. C'est une variante de la formule (11) de [26], VI, § 4, mieux adaptée à l'étude des propriétés d'intégralité. Sa démonstration est tout à fait analogue à celle de Weil.

(1. 3) Proposition. *Pour tout couple d'entiers* (i, j) *tel que* $j > i \geqq 0$, *il existe un polynôme* $\Phi_{i,j}$ *à* $i+j$ *indéterminés, de degré* $i+1$, *à coefficients dans* $\mathbb{Z}$, *tel que, pour tout* $z \in \mathbb{C} \setminus L$, *on ait*:

$$E^*_{i,j}(z, L) = \frac{(A(L)/2)^i}{(j-1)!} \Phi_{i,j}(0!\, E^*_1(z, L), \ldots, (i+j-1)!\, E^*_{i+j}(z, L)).$$

(1. 4) Remarque. De la définition se déduisent aussitôt les propriétés d'homogénéité des séries d'Eisenstein: Pour tout $\lambda \in \mathbb{C}^*$, on a

$$E^*_{i,j}(\lambda z, \lambda L) = \bar{\lambda}^{(i+j)} |\lambda|^{-2j} E^*_{i,j}(z, L) = \frac{\bar{\lambda}^i}{\lambda^j} E^*_{i,j}(z, L);$$

$$E^*_k(\lambda z, \lambda L) = \lambda^{-k} E^*_k(z, L).$$

De plus, il est évident que $A(\lambda L) = |\lambda|^2 A(L)$; nous en déduisons que

$$\Phi_{i,j}(\lambda X_1, \lambda^2 X_2, \ldots, \lambda^{i+j} X_{i+j}) = \lambda^{i+j} \Phi_{i,j}(X_1, \ldots, X_{i+j}),$$

où les $\Phi_{i,j}$ sont les polynômes définis dans la proposition (1. 3).

Un point de vue bien connu, celui de Weierstrass, est d'associer à un réseau L des fonctions méromorphes dans le plan complexe, mais pas nécessairement périodiques. Rappelons des définitions de ces fonctions classiques:

$$\sigma(z, L) = z \prod_{\omega \in L \setminus \{0\}} \left(1 - \frac{z}{\omega}\right) \exp\left\{\frac{z}{\omega} + \frac{1}{2}\left(\frac{z}{\omega}\right)^2\right\};$$

$$\zeta(z, L) = \frac{d}{dz} \log \sigma(z, L);$$

$$\wp(z, L) = -\frac{d}{dz} \zeta(z, L).$$

Nous notons enfin $s_2(L) = \lim\limits_{\substack{s \to 0 \\ s > 0}} \sum\limits_{\omega \in L \setminus \{0\}} \omega^{-2} |\omega|^{-2s}$.

Voici le lien entre les points de vue de Kronecker-Eisenstein et de Weierstrass.

(1. 5) Proposition. *Pour tout* $z \in \mathbb{C} \setminus L$, *on a*

$$E_1^*(z, L) = \zeta(z, L) - z s_2(L) - \bar{z} A(L)^{-1},$$
$$E_2^*(z, L) = \wp(z, L) + s_2(L),$$
$$E_k^*(z, L) = \frac{(-1)^k}{(k-1)!} \wp^{(k-2)}(z, L), \quad \textit{pour tout} \quad k \geqq 3.$$

Démonstration (cf. [6], p. 242—243). On emprunte d'abord à [2], formule (3. 4), la définition, pour $z \in \mathbb{C} \setminus L$:

$$\Psi(z, s, L) = \frac{\bar{z}}{|z|^{2s}} + \sum_{\omega \in L \setminus \{0\}} \left\{\frac{\bar{z} + \bar{\omega}}{|z + \omega|^{2s}} - \frac{\bar{\omega}}{|\omega|^{2s}}\left(1 - \frac{sz}{\omega} - \frac{(s-1)\bar{z}}{\bar{\omega}}\right)\right\}.$$

Cette série converge pour $\mathrm{Re}(s) > \frac{1}{2}$ et, pour $s \to 1$, tend vers $\zeta(z, L)$ uniformément en z. Pour $\mathrm{Re}(s) > \frac{3}{2}$, la convergence absolue permet de réordonner le membre de droite et d'écrire

$$\Psi(z, s, L) = H_1(z, 0, s, L) + sz \sum \omega^{-2} |\omega|^{2-2s} + (s-1)\bar{z} H_0(0, 0, s, L);$$

car $\sum \bar{\omega} |\omega|^{-2s} = 0$. Pour $s \to 1$, ceci donne (compte tenu du théorème (1. 1)) la première partie de la proposition. Les autres en découlent par dérivation par rapport à z, grâce aux propriétés différentielles des séries d'Eisenstein, voir [26], VIII, § 14, formule (34).

La proposition que nous venons de démontrer nous permet de déterminer immédiatement la «pseudo-période» $\eta(\omega, L) = \zeta(z + \omega, L) - \zeta(z, L)$ de la fonction ζ de Weierstrass, associée à l'élément ω de L.

(1. 6) Corollaire. *Pour tout $\omega \in L$, on a*

$$\eta(\omega, L) = \omega s_2(L) + \bar{\omega} A(L)^{-1}.$$

Selon G. Robert (cf. [14]; [15], § 0), nous nous inspirons maintenant de (1. 5) pour trouver une fonction analogue à la fonction σ de Weierstrass, mais qui soit reliée aux séries d'Eisenstein et par ailleurs rationnelle en $\wp$. Nous simplifions légèrement les formules de Robert, ce qui semble convenable dans le cas du présent travail, et posons d'abord

$$\theta(z, L) = \exp\left\{-s_2(L)\frac{z^2}{2}\right\}\sigma(z, L).$$

Un calcul naïf à partir de (1. 5) et des relations différentielles entre les E_k^* ([26], VIII, § 14) montre alors le

(1. 7) Corollaire. *Pour tout $\rho \in \mathbb{C} \setminus L$, on a le développement de Taylor*

$$\frac{d}{dz}\log\theta(z+\rho, L) = \bar{\rho} A(L)^{-1} + \sum_{k=1}^{\infty} (-1)^{k-1} E_k^*(\rho, L) z^{k-1}.$$

D'autre part, en vertu de la formule bien connue (cf. par exemple [12], **18**, § 1)

$$\sigma(z+\omega, L) = \pm\sigma(z, L)\exp\left\{\eta(\omega, L)\left(z+\frac{\omega}{2}\right)\right\},$$

pour tout $\omega \in L$ (où le signe est $+$ ou $-$ selon que ω est ou non dans $2L$) nous déduisons immédiatement de (1. 6):

(1. 8) Lemme. *Pour tout $\omega \in L$, on a*

$$\theta(z+\omega, L) = \pm\theta(z, L)\exp\left\{\bar{\omega}\left(z+\frac{\omega}{2}\right)A(L)^{-1}\right\}.$$

Afin de fabriquer une fonction périodique, on se sert d'un réseau auxiliaire $\mathfrak{L} \supset L$, et on pose

$$\Theta^*(z, L, \mathfrak{L}) = \frac{\theta^2(z, L)^{[\mathfrak{L}:L]}}{\theta^2(z, \mathfrak{L})},$$

où $[\mathfrak{L}: L]$ est l'indice de L dans $\mathfrak{L}$.

Nous avons alors le

(1. 9) Théorème. *La fonction $\Theta^*(z, L, \mathfrak{L})$ est périodique par rapport au réseau L. On a l'identité*

$$\Theta^*(z, L, \mathfrak{L}) = \prod_l (\wp(z, L) - \wp(l, L))^{-1},$$

où le produit est pris sur un système quelconque de représentants des classes non nulles de $\mathfrak{L}$ modulo L.

Démonstration. La périodicité résulte du lemme (1. 8) L'identité explicite est alors un exercice de comparaison de diviseurs et d'estimation quand $z \to 0$, que nous laissons au lecteur.

§ 2. Algébricité de valeurs spéciales des séries d'Eisenstein. I

Notre but est d'étudier certains objets attachés à une courbe elliptique à multiplication complexe: la voici donc. Soit E une courbe elliptique définie sur une extension finie F de $\mathbb{Q}$, telle que $\mathrm{End}_F E$ soit isomorphe à l'anneau des entiers $\mathfrak{o}$ d'un corps quadratique imaginaire K. Nous fixons une identification de $\mathrm{End}_F E$ avec $\mathfrak{o}$, ce qui détermine l'action de K sur l'espace tangent de E à l'origine, donc un plongement de K dans F. Notons

$$\tilde{\psi}: F_{\mathbb{A}}^* \longrightarrow K^*$$

le (quasi-) caractère sur les idèles de F attaché à E/F selon [18], Thm. 10. Il vaut $N_{F/K}$ sur les idèles principaux. L'homomorphisme

$$\tilde{\psi} \otimes N^{-1}_{F\otimes R/K\otimes R}: F_{\mathbb{A}}^* \longrightarrow (K\otimes \mathbb{R})^*$$

est donc trivial sur F^* et on en déduit (via les deux plongements différents de K dans $\mathbb{C}$) les deux *Grössencharaktere* complexes conjugués de E/F.

Nous fixons une fois pour toutes un modèle de Weierstrass de E sur F:

(2. 0) $$y^2 = 4x^3 - g_2 x - g_3; \quad g_2, g_3 \in F.$$

Ceci revient à choisir une forme différentielle de première espèce $\omega \left(= \dfrac{dx}{y}\right.$ en termes des coordonnées de (2. 0)$\left.\right)$ de E définie sur F.

Afin de disposer aussi du point de vue analytique complexe, fixons désormais un plongement de F (donc aussi de K!) dans $\mathbb{C}$. Ceci nous permet d'abord de distinguer un Grössencharakter $\psi: F_{\mathbb{A}}^* \to \mathbb{C}^*$ parmi les deux caractères complexes conjugués déduits de $\tilde{\psi}$. Nous interpréterons souvent ψ comme caractère de Hecke, défini sur les idéaux de F premiers à l'ensemble S des places de F où E a mauvaise réduction.

D'autre part, le plongement $F \hookrightarrow \mathbb{C}$ permet d'attacher à (E, ω) un réseau L du plan complexe; il est caractérisé par $g_2(L) = g_2$ et $g_3(L) = g_3$. Grâce à la multiplication complexe, le réseau s'écrit $L = \Omega\mathfrak{a}$, où $\Omega \in \mathbb{C}^*$, et $\mathfrak{a}$ un idéal fractionnaire de K. Nous fixons $\mathfrak{a}$ (ce qui détermine Ω à une racine de l'unité dans K près); mais les résultats des §§ 2 et 3 sont indépendants du choix de Ω et de $\mathfrak{a}$. On a l'isomorphisme de Weierstrass $\xi: \mathbb{C}/L \to E(\mathbb{C})$ donné par $\xi(z, L) = (\wp(z, L), \wp'(z, L))$. Notons qu'après tous ces choix, un élément α de $\mathfrak{o}$, vu comme endomorphisme de E, envoie $\xi(z, L)$ sur $\xi(\alpha z, L)$.

Enfin, pour un idéal entier $\mathfrak{g} \neq \mathfrak{o}$ de K, nous écrivons

$$E_{\mathfrak{g}} = \{\xi(z, L) : z \in \mathfrak{g}^{-1}L\} \subset \mathbb{P}_2(\mathbb{C})$$

le groupe des points de $\mathfrak{g}$-torsion de E sur $\mathbb{C}$. Si l'on rajoute à F les coordonnées de tous les points de $E_{\mathfrak{g}}$, on obtient l'extension abélienne finie $F(E_{\mathfrak{g}})$ de F, qui est non ramifiée en dehors des places de F divisant $\mathfrak{g}$ et de l'ensemble S des mauvaises places: [5], chap. 2. Pour tout idéal entier $\mathfrak{b}$ de F, premier à $\mathfrak{g}$ et à S, nous noterons $\sigma_{\mathfrak{b}}$ le symbole d'Artin de $\mathfrak{b}$ pour l'extension $F(E_{\mathfrak{g}})/F$. Soit ρ un élément de $\mathfrak{g}^{-1}L \setminus L$. On a donc $\xi(\rho, L) \in E_{\mathfrak{g}}$. Alors ψ est caractérisé par la formule

$$\xi(\rho, L)^{\sigma_{\mathfrak{b}}} = \xi(\psi(\mathfrak{b})\rho, L),$$

valable pour tout idéal $\mathfrak{b}$ comme ci-dessus.

Avec ces notations, le résultat principal de ce paragraphe est le théorème suivant:

(2. 1) Théorème. *Soit $k \geqq 1$ un entier. Alors*

(i) $E_k^*(\rho, L)$ *appartient à* $F(E_\mathfrak{g})$.

(ii) $E_k^*(\rho, L)^{\sigma_\mathfrak{b}} = E_k^*(\psi(\mathfrak{b})\rho, L)$.

Démonstration. (i) Dans la formule explicite du théorème (1. 9), les $\wp(l, L)$ n'interviennent que par leurs polynômes symétriques élémentaires. Nous voyons donc que $\Theta^*(z, L, \Omega)$ est, pour tout réseau Ω contenant L, une fonction rationnelle en $\wp(z, L)$ à coefficients dans F. D'après le théorème d'addition des fonctions $\wp$ de Weierstrass, $\Theta^*(z+\rho, L, \Omega)$ est donc rationnelle en $\wp(z, L)$ et $\wp'(z, L)$, à coefficients dans $F(E_\mathfrak{g})$. Le développement en z de $\wp(z, L)$ ayant des coefficients dans $\mathbb{Q}(g_2, g_3) \subset F$, nous en déduisons que les coefficients a_k du développement

$$\frac{d}{dz} \log \Theta^*(z+\rho, L, \Omega) = 2 \sum_{k=1}^{\infty} a_k z^{k-1}$$

se trouvent dans $F(E_\mathfrak{g})$. Or, d'après (1. 7), nous avons

$$a_1 = [\Omega : L]\,\{E_1^*(\rho, L) + \bar{\rho} A(L)^{-1}\} - E_1^*(\rho, \Omega) - \bar{\rho} A(\Omega)^{-1};$$

$$a_k = (-1)^{k-1}\,\{[\Omega : L]\, E_k^*(\rho, L) - E_k^*(\rho, \Omega)\}, \quad \text{pour} \quad k \geqq 2.$$

Choisissons maintenant $\Omega = \alpha^{-1} L$, où $\alpha \in \mathfrak{o}$, $\alpha \equiv 1 \bmod \mathfrak{g}$. Alors $\alpha\rho \equiv \rho \bmod L$ et, compte tenu des propriétés d'homogénéité (1. 4), nous avons, pour tout $k \geqq 1$,

$$a_k = (-1)^{k-1}\,(N\alpha - \alpha^k)\, E_k^*(\rho, L).$$

En prenant $\alpha \notin \mathbb{Z}$, $(N\alpha - \alpha^k)$ est non nul même pour $k=2$. Nous concluons donc que $E_k^*(\rho, L)$ est dans $F(E_\mathfrak{g})$ pour tout $k \geqq 1$.

(ii) Nous savons que $\xi(\rho, L)^{\sigma_\mathfrak{b}} = \xi(\psi(\mathfrak{b})\rho, L)$. Le symbole d'Artin de $\mathfrak{b}$ agit donc sur la fonction $\Theta^*(z+\rho, L, \Omega)$, rationnelle en $\wp(z, L)$ et $\wp'(z, L)$, par

$$(\Theta^*(z+\rho, L, \Omega))^{\sigma_\mathfrak{b}} = \Theta^*(z+\psi(\mathfrak{b})\rho, L, \Omega).$$

Et il opère de la même façon sur le développement en série de $\dfrac{d}{dz} \log \Theta^*(z+\rho, L, \Omega)$, en agissant sur les coefficients. L'expression explicite de ces coefficients, donnée plus haut, permet alors de conclure.

(2. 2) Remarques. 1) De (1. 5) et (2. 1), on déduit que $s_2(L)$ appartient à F.

2) Pour $k \geqq 3$, le théorème est évident; car alors $E_k^*(z, L)$ appartient à $F(\wp(z, L), \wp'(z, L))$ d'après la proposition (1. 5).

(2. 3) Corollaire[1]**).** *Soient* $\mathfrak{g}$ *et* ρ *comme dans* (2. 1). *Pour tout couple d'entiers* (i, j) *tel que* $j > i \geqq 0$, *nous avons*

$$\left(\frac{\Omega\bar{\Omega}}{2\pi i}\right)^{-i} E_{i,j}^*(\rho, L) \in F(E_\mathfrak{g}).$$

[1]) Dans tout cet article, le symbole «i» désigne l'unité imaginaire si et seulement s'il est immédiatement précédé du symbole «π».

De plus, si $\mathfrak{b}$ *est un idéal entier de* F *premier à* $\mathfrak{g}$ *et à* S,

$$\left\{\left(\frac{\Omega\bar{\Omega}}{2\pi i}\right)^{-i} E^*_{i,j}(\rho, L)\right\}^{\sigma_\mathfrak{b}} = \left(\frac{\Omega\bar{\Omega}}{2\pi i}\right)^{-i} E^*_{i,j}(\psi(\mathfrak{b})\rho, L).$$

Démonstration. Rappelons que $L = \Omega\mathfrak{a}$, donc que $\frac{2\pi i}{\Omega\bar{\Omega}} \cdot A(L)$ appartient à $K \subset F$. Le corollaire (2. 3) se déduit immédiatement de (2. 1) et (1. 3).

§ 3. Intégralité des valeurs spéciales des séries d'Eisenstein

Nous gardons les notations du paragraphe précédent et supposons en outre pour simplifier que $\xi(\rho, L)$ est un point de $\mathfrak{g}$-division primitif de $E(\mathbb{C})$, c'est-à-dire qu'il n'est pas un point de $\mathfrak{g}'$-division pour un diviseur propre $\mathfrak{g}'$ de $\mathfrak{g}$.

Un problème naturel est de chercher des dénominateurs explicites (ou, au moins, une majoration de ces dénominateurs) pour les $E^*_k(\rho, L)$ étudiés au § 2 et de généraliser ces résultats aux valeurs $E^*_{i,j}(\rho, L)$. Nous avons essayé alternativement deux méthodes:

Soit trouver, en chaque place, un dénominateur local par une méthode analogue à celle de Coates-Wiles (voir [6], [7]) ou G. Robert ([15]), c'est-à-dire en étudiant les propriétés d'intégralité locale d'un développement, en série de t, de $z\frac{d}{dz}\log\Theta^*(z, L)$ — ou plus précisément d'une variante de Θ^* (voir [15]) —, où $t = -2\wp(z)/\wp'(z)$ est le paramètre local à l'infini de la courbe E.

Soit utiliser directement un résultat de Cassels sur l'intégralité de $\xi(\rho, L)$, comme le fait Damerell dans [8].

Nous n'avons pas réussi à tirer de la première méthode des résultats pour les places divisant l'idéal $\mathfrak{g}$. Nous nous bornerons donc ici à donner un aperçu de la seconde méthode.

Nous supposerons dans la suite de ce paragraphe que le modèle (2. 0) *a été choisi de sorte que*

(3. 0) $$g_2 \quad et \quad g_3 \in 4\mathfrak{o}_F.$$

Notons g le plus petit entier rationnel positif contenu dans $\mathfrak{g}$: alors $\xi(\rho, L)$ est un élément d'ordre g dans le groupe $E(\bar{\mathbb{Q}})$. Nous utilisons alors le théorème IV de [3]:

(3. 1) Théorème. *Les nombres* $\wp(\rho, L)$ *et* $\frac{1}{2}\wp'(\rho, L)$ *sont des entiers algébriques, sauf si* $g = p^k$ *pour un nombre premier* $p \geqq 3$. *Dans ce dernier cas, il existe un idéal entier* $\mathfrak{t}$ *de* $F(E_\mathfrak{g})$ *tel que* $\mathfrak{t}^2\wp(\rho, L)$ *et* $\frac{1}{2}\mathfrak{t}^3\wp'(\rho, L)$ *soient entiers et que*

$$\mathfrak{t}^{(p-1)p^{k-1}} | p \quad si \quad p \neq 3;$$
$$\mathfrak{t}^{8\cdot 3^{2k-2}} | 3 \quad si \quad p = 3.$$

(3. 2) Corollaire. *Le nombre* $g^{5/4} E_1^*(\rho, L)$ *est un entier algébrique.*

La démonstration est celle du lemme 7. 2 de [8] où la fonction $E_1^*(., L)$ est notée h.

Nous supposons alors, pour toute la suite de ce paragraphe, que g a au moins deux diviseurs premiers rationnels distincts. Rappelons aussi que l'hypothèse (3. 0) est toujours valable.

(3. 3) Corollaire. *Le nombre* $\sqrt{d_K}\, E_2^*(\rho, L)$, *où* d_K *est le discriminant du corps K, est un entier algébrique.*

Cela résulte du lemme 7. 5 de [8]. En fait, la formule (4. 4) de [8] et notre proposition (1. 5) montrent que le «φ» de Damerell est ici $-s_2(L)$.

(3. 4) Corollaire. *Soit k un entier* $\geqq 3$. *Alors* $(k-1)!\, E_k^*(\rho, L)$ *est un entier algébrique.*

La démonstration se déduit de (3. 1) et (1. 5).

Nous sommes maintenant en mesure d'établir les résultats généraux relatifs aux $E_{i,j}^*$ pour $i > 0$.

(3. 5) Proposition. *Soient g et* ρ *comme ci-dessus. Soit* (i, j) *un couple d'entiers tels que* $0 < i < j$.

(a) *Si* $j \neq i+2$, *alors* $\left(\dfrac{4\pi i\, g^{5/4}}{\Omega\bar{\Omega}\, N\mathfrak{a}}\right)^i (j-1)!\, E_{i,j}^*(\rho, L)$ *est un entier algébrique.*

(b) *Si* $j = i+2$, *alors* $\sqrt{d_K}\left(\dfrac{4\pi i\, g^{5/4}}{\Omega\bar{\Omega}\, N\mathfrak{a}}\right)^i (j-1)!\, E_{i,j}^*(\rho, L)$ *est un entier algébrique.*

Démonstration. Rappelons d'abord que $L = \Omega\mathfrak{a}$, donc que

$$\frac{1}{2} A(L) = \frac{1}{4\pi i}\, \Omega\bar{\Omega}\, N\mathfrak{a}\, \sqrt{d_K}.$$

Nous utilisons naturellement la proposition (1. 3). Un terme générique de $\Phi_{i,j}(X_1, \ldots, X_{i+j})$ est de la forme $\lambda_{(\mu)} X_1^{\mu_1} \cdots X_{i+j}^{\mu_{i+j}}$. D'après les propriétés de $\Phi_{i,j}$ (voir aussi (1. 4)), nous en déduisons que $\sum \mu_k \leqq i+1$. En particulier $\mu_1 = i+1$ (et donc $\mu_k = 0$ pour $k > 1$) n'est possible que si $i+1 = i+j$, donc $j = 1$ et $i = 0$, cas traité dans le corollaire (3. 2) et exclu ici. Donc X_1 intervient au plus à la puissance i. De même $\mu_2 = i+1$ entraîne $2(i+1) = i+j$, soit $j = i+2$. Ces remarques, jointes aux corollaires (3. 2), (3. 3) et (3. 4) achèvent la démonstration.

(3. 6) Remarque. Les résultats obtenus par cette variante de la méthode de [8] sont bien sûr analogues à ceux de Damerell. Remarquons que nous obtenons toutefois, grâce à la proposition (1. 3), un résultat plus précis dans le cas $j = i+2 \geqq 2$ (cas «$s_0 = 1$» dans [8]) que Damerell n'élucide pas totalement.

Deuxième partie: Des courbes elliptiques dont les points de torsion engendrent des extensions abéliennes de K

Τρεῖς γραμμὰς ἐπὶ πέντε τομαῖς εὑρὼν ∪ ∪ — ∪
Περσεὺς τῶν δ' ἕνεκεν δαίμονας ἱλάσατο.

Proclus, In Eucl. I, ed. Friedl. 112

§ 4. Théorie algébrique

Nous introduisons maintenant la classe des courbes elliptiques pour lesquelles nous pourrons aboutir à des résultats précis concernant la rationalité des valeurs spéciales de la série L d'une puissance de leur Grössencharakter.

Soit, comme dans le § 2, E/F une courbe elliptique à multiplication complexe par l'anneau des entiers $\mathfrak{o}$ de K, la courbe aussi bien que sa multiplication complexe étant définies sur l'extension finie F du corps quadratique imaginaire K. Le sous-corps K, identifié à $\mathbb{Q} \otimes \mathrm{End}_F E$, agit linéairement sur F, vu comme espace tangent de E en 0. On continue à noter ψ le Grössencharakter complexe de E sur F (relatif à un plongement $K \subset F \hookrightarrow \mathbb{C}$). De plus, pour un nombre premier rationnel l, notons

$$\rho_l(E)\colon G(\bar{F}/F) \longrightarrow \mathrm{Aut}\left(V_l(E)\right)$$

la représentation l-adique attachée à E/F. Voir, par exemple, [16] ou [10], §§ 7 et 8.

Nous allons aussi considérer la variété abélienne B sur K, qui se déduit de E par restriction de scalaires de F à K, au sens d'A. Weil; cf. [24] et [10], § 15. Un peu plus précisément, c'est une variété abélienne B de dimension $n = [F\colon K]$ définie sur K, munie d'un isomorphisme défini sur F:

$$B \cong_{/F} \prod_{\sigma \in G} E^{\sigma}.$$

Ici, G désigne l'ensemble des plongements $F \hookrightarrow \bar{K}$ sur K. (Nous supposerons en fait bientôt que F/K est galoisienne, et même que G est abélien). On voit facilement que, pour tout l, la représentation l-adique attachée à B,

$$\rho_l(B)\colon G(\bar{K}/K) \longrightarrow \mathrm{Aut}\left(V_l(B)\right),$$

n'est autre que la représentation induite, par rapport à $G(\bar{\mathbb{Q}}/F) \hookrightarrow G(\bar{\mathbb{Q}}/K)$, par la représentation l-adique de E, $\mathrm{Ind}_{F/K}\left(\rho_l(E)\right)$.

Enfin, nous appellerons E_{tors} le sous-groupe de torsion de $E(\bar{\mathbb{Q}})$ ou, ce qui revient au même, de $E(\mathbb{C})$; donc $F(E_{\mathrm{tors}})$ est l'extension abélienne de F engendrée par les coordonnées de tous les points de division de la courbe E.

Nous sommes alors en mesure de formuler le théorème caractérisant les courbes elliptiques qui nous intéresseront par la suite.

(4. 1) Théorème. *Les hypothèses suivantes sur E/F sont équivalentes.*

(i) *$F(E_{\mathrm{tors}})$ est une extension abélienne de K.*

(ii) *Pour tout nombre premier l, la représentation induite $\mathrm{Ind}_{F/K}\left(\rho_l(E)\right)$ est une représentation abélienne, c'est-à-dire à image commutative ou encore qui se factorise par $G(K^{ab}/K)$.*

(iii) *Il existe un l, tel que* $\mathrm{Ind}_{F/K}(\rho_l(E))$ *est abélienne.*

(iv) *La variété abélienne B est à multiplication complexe sur K, dans le sens précis que*

$$\mathrm{End}_K B \underset{\mathbb{Z}}{\otimes} \mathbb{Q} = \mathrm{End}_K B \underset{\mathfrak{o}}{\otimes} K \cong \prod_{i=1}^{r} T_i,$$

où chaque T_i $(i=1,\ldots,r)$ *est un corps de type CM contenant K, tels que*

$$\sum_{i=1}^{r} [T_i : K] = n = [F : K].$$

(v) *L'extension F/K est abélienne et il existe un Grössencharakter* φ *de K, tel que* $\psi = \varphi \circ N_{F/K}$ *(où N désigne la norme).*

Démonstration. L'équivalence de (i) et (v) est un cas particulier de [19], Thm. 7.44.

L'équivalence entre (i) et (ii) est un exercice facile que nous laissons au lecteur.

L'équivalence de (ii) et (iii) se déduit aussitôt de [16]; voir en particulier III, 2.3.

Il est bien connu que (iv) implique (ii). Pour déduire (iv) de (ii), nous utilisons le lemme suivant (nous savons déjà que (ii) implique (v)!).

(4.2) Lemme. *Si E/F vérifie la condition* (4.1), (v), *alors toutes les courbes conjuguées* E^σ, *pour* $\sigma \in G$, *sont isogènes entre elles sur F.*

Démonstration. Le Grössencharakter de E^σ n'est autre que ψ^σ, donc ψ. Or, ψ est un invariant de la classe de F-isogénie de E. Pour plus de détails, voir [10], § 9.

Comme $B \cong \prod_{\sigma \in G} E^\sigma$ sur F, on trouve que

$$\mathrm{End}_F B \cong \prod_{(\sigma', \sigma)} \mathrm{Hom}_F(E^{\sigma'}, E^\sigma)$$

est un anneau de «matrices», de rang n^2 sur $\mathfrak{o}$. L'anneau $\mathrm{End}_K B$ étant formé des «matrices» invariantes par l'action de G, lesquelles sont déterminées précisément par les coefficients de leur première ligne, on déduit donc de (4.2) que

(4.3) $\mathrm{End}_K B \cong \prod_{\sigma \in G} \mathrm{Hom}_F(E, E^\sigma)$ *est de rang n sur* $\mathfrak{o}$.

Posons maintenant, pour un premier l, $K_l = K \otimes_{\mathbb{Q}} \mathbb{Q}_l$. Dans $\mathrm{End}_{K_l}(V_l(B)) = M(n, K_l)$, considérons l'image $\mathfrak{T}$ de l'algèbre de groupe $K_l[G(\bar{K}/K)]$ par $\rho_l(B)$. D'après (ii), $\mathfrak{T}$ est commutative. Or, G étant un quotient de $\mathrm{Gal}(\bar{K}/K)$, $\mathfrak{T}$ contient n «matrices de permutation» qui sont linéairement indépendantes sur K_l. Donc $\dim_{K_l} \mathfrak{T} = n$ et $\mathfrak{T}$ est son propre commutant. D'autre part, la sous-algèbre $K_l \otimes_{\mathfrak{o}} \mathrm{End}_K B$ de $\mathrm{End}_{K_l}(V_l(B))$ est aussi de rang n sur K_l, d'après (4.3), et commute avec $\mathfrak{T}$. On trouve donc bien que

$$K_l \otimes_{\mathfrak{o}} \mathrm{End}_K B \cong \mathfrak{T}.$$

(Notons que ceci démontre la *conjecture de Tate* pour les $\rho_l(B)$.)

$\mathfrak{T}$ étant semi-simple, on en déduit aussitôt (iv). Ceci achève la démonstration du théorème (4.1).

(4. 4) Remarque. Il est évident que les n choix possibles du caractère φ satisfaisant à la condition (v) de (4. 1) se déduisent de l'un d'eux en le multipliant par χ, pour χ décrivant le groupe $\hat{G}$ des caractères de G, interprétés comme caractères de Dirichlet de K.

(4. 5) Exemples. 1) La classe des exemples concrets les plus étudiés de courbes satisfaisant les conditions de (4. 1) sont les «$\mathbb{Q}$-courbes» de Gross [10] (considérées sur le corps de classes de Hilbert de K), dans le cas où K a un discriminant d_K premier. (Dans le cas général, une «$\mathbb{Q}$-courbe» n'est pas nécessairement du type (4. 1).)

2) D'autre part, les courbes caractérisées par le théorème (4. 1) sont «génériques» dans le sens (assez faible) suivant: Chaque courbe elliptique à multiplication complexe par $\mathfrak{o}$, définie sur un corps de nombres, a un modèle sur $\bar{\mathbb{Q}}$ qui descend à une courbe E/F vérifiant les conditions de (4. 1), pour une certaine extension abélienne F de K. Cela est démontré par Shimura [19], p. 216, qui remarque aussi que, dans sa construction, F peut être choisi comme le corps de classes de Hilbert de K, si $d_K \not\equiv 1 \bmod 3$.

Supposons désormais que E sur F satisfait les conditions équivalentes du théorème (4. 1). *On fixe un Grössencharakter φ vérifiant la condition* (v) *de* (4. 1).

Notons, comme au début du § 2, $\tilde{\psi}$ le caractère de Serre-Tate attaché à E/F. De même, fixons une fois pour toutes l'identification $K \otimes_{\mathbb{Q}} \mathrm{End}_K B = T := \prod_{i=1}^{r} T_i$ et appelons $\tilde{\varphi}\colon K_{\mathbf{A}}^* \to T^*$ le caractère de Serre-Tate attaché à B/K. Il donne le plongement diagonal $K^* \xrightarrow{d} T^*$ sur les idèles principaux et, pour chaque $\varepsilon \in \mathrm{Hom}_K(T, \mathbb{C})$, on déduit de $\tilde{\varphi} \otimes d_\infty^{-1}\colon K_{\mathbf{A}}^* \to (T \otimes \mathbb{R})^*$ un caractère complexe $\varphi_\varepsilon\colon K_{\mathbf{A}}^* \to \mathbb{C}^*$ trivial sur K^*, qui prend ses valeurs dans $\varepsilon(T)$ ($= T_i$, pour un $i = 1, \ldots, r$) sur les idéaux entiers de K premiers à son conducteur. Nous allons démontrer que les φ_ε sont précisément les caractères $\varphi\chi$, pour χ décrivant $\hat{G}$ — cf. (4. 4).

Ecrivons $\mathfrak{f}$ le p.p.c.m. du conducteur de $\tilde{\varphi}$ et du conducteur de l'extension abélienne F/K. *Dans tout le reste du papier, nous travaillerons avec un idéal entier fixé* $\mathfrak{g}$ *de K, qui est divisible par* $\mathfrak{f}$. *Nous notons alors* $\mathfrak{a}$ *un idéal entier de K qui est premier à* $\mathfrak{g}$. Dans ce paragraphe, nous considérons $\mathfrak{a}$ comme donné par un idèle a dont l'idéal associé est $\mathfrak{a}$ et tel que $a_v \equiv 1 \bmod \mathfrak{g}\mathfrak{o}_v$, si $v|\mathfrak{g}$, et $a_v = 1$, si $v|\infty$.

Alors le caractère $\tilde{\varphi}$ est caractérisé par la relation:

(4. 6) $\tilde{\varphi}(\mathfrak{a})(P) = P^{\sigma_\mathfrak{a}}$, *pour tout point de* $\mathfrak{g}$*-division P de B.*

Ici, $\tilde{\varphi}(\mathfrak{a}) = \tilde{\varphi}(a)$ est considéré comme élément de $\mathrm{End}_K B$, et σ_a est le symbole d'Artin de a sur K^{ab}/K. En fait, (4. 6) montre que l'on n'utilise que l'automorphisme $\sigma_\mathfrak{a}$ du corps des rayons modulo $\mathfrak{g}$ de K. Plus précisément:

(4. 7) Lemme. *Les corps $F(E_\mathfrak{g}^\sigma)$ obtenus en ajoutant à F les coordonnées des points de* $\mathfrak{g}$*-division de E^σ sont tous égaux, pour σ décrivant G, au corps des rayons modulo* $\mathfrak{g}$ *de K.*

Démonstration. On peut supposer que $\sigma=1$. Le fait que $F(E_{\mathfrak{g}})$ contienne le corps des rayons se déduit par exemple de [19], Ex. 5. 10 (p. 124). Inversement, F est certainement contenu dans le corps des rayons mod $\mathfrak{g}$, par hypothèse sur $\mathfrak{g}$. Soit $a \in K_{\mathbf{A}}^*$ un idèle ayant ses composantes $a_v=1$ aux places à l'infini, $a_v \equiv 1 \bmod \mathfrak{g}\mathfrak{o}_v$, pour v divisant $\mathfrak{g}$, et $a_v \in \mathfrak{o}_v^*$ pour toute autre place finie v de K. Il s'agit de démontrer que son symbole d'Artin σ_a agit trivialement sur les points de $\mathfrak{g}$-division de E. Or, cela résulte immédiatement de (4. 6).

Avec les notations précédentes, nous trouvons:

(4. 8) Lemme. (i) $\tilde{\psi} = \tilde{\varphi} \circ N_{F/K}$.

(ii) *La K-algèbre T est engendrée par les valeurs de $\tilde{\varphi}$ sur les idéaux entiers de K premiers à* $\mathfrak{g}$.

(iii) $\{\varphi_\varepsilon : \varepsilon \in \mathrm{Hom}_K(T, \mathbb{C})\} = \{\varphi\chi : \chi \in \hat{G}\}$.

Démonstration. (i) est une conséquence immédiate de (4. 6) et de la relation analogue pour l'action de $\tilde{\psi}$ sur les points de $\mathfrak{g}$-division de E.

En choisissant dans (4. 6) des idéaux $\mathfrak{a}$ dont les symboles d'Artin recouvrent le groupe G, on démontre (ii) à l'aide de (4. 3).

(iii) se déduit immédiatement de (i), de (ii) et de (4. 4).

Notons que, d'après (4. 8), les corps T_i tels que $T = \prod T_i$ correspondent aux orbites sous $\mathrm{Aut}_K(\mathbb{C})$ de $\{\varphi\chi : \chi \in \hat{G}\}$.

De plus, on voit aisément que l'idéal $\mathfrak{f}$ s'écrit aussi comme le p.p.c.m. du conducteur de φ et du conducteur de F/K — p.p.c.m. qui est indépendant du choix de φ d'après (4. 4).

Nous aurons besoin par la suite de quelques propriétés élémentaires du caractère complexe φ. Appelons $K(\varphi)$ son corps de valeurs — d'après (4. 8), c'est un des corps T_i de (4. 1), (iv). On note $\mathfrak{o}_M$ l'anneau des entiers d'un corps de nombres M.

(4. 9) Lemme. *Soient* $\mathfrak{a}$ *et* $\mathfrak{b}$ *des idéaux entiers de K premiers à* $\mathfrak{g}$, *tels que* $\sigma_{\mathfrak{b}}$ *induit l'identité sur F. Alors*

(i) $\varphi(\mathfrak{b})$ *appartient à* K^*.

(ii) $\varphi(\mathfrak{a}) \cdot \mathfrak{o}_{K(\varphi)} = \mathfrak{a} \cdot \mathfrak{o}_{K(\varphi)}$ *et* $\varphi(\mathfrak{b})\mathfrak{o} = \mathfrak{b}$.

(iii) $\varphi\bar{\varphi} = N_{K/\mathbb{Q}}$.

Démonstration. (i) D'après (4. 6), $\tilde{\varphi}(\mathfrak{b})$ induit un élément de $\mathrm{End}_F B = \mathfrak{o}$. Donc $\varphi(\mathfrak{b}) = \tilde{\varphi}(\mathfrak{b}) \in K \hookrightarrow \mathbb{C}$. (ii) et (iii) sont clairement vrais pour une puissance convenable de $\mathfrak{a}$ (engendrée par un élément $\equiv 1 \bmod \mathfrak{g}$). Ils sont donc valables en général, car on peut extraire des racines de façon unique dans les idéaux et les réels positifs.

Il est amusant de remarquer que (iii) redémontre le fait que les T_i sont des corps de type *CM*.

Reprenons maintenant quelques conventions du § 2. D'abord nous conservons ω, la forme différentielle de première espèce de E définie sur F qui correspond au modèle de Weierstrass (2. 0) de E/F. Pour alléger un peu l'écriture, nous supposerons que le plongement de F dans $\mathbb{C}$ est choisi de telle façon que l'invariant $\mathbf{j}$ algébrique de la courbe E sur F s'identifie à l'invariant analytique complexe $\mathbf{j}(\mathfrak{o})$. Le réseau L du plan complexe, qui correspond alors à (E, ω), s'écrit donc $L = \Omega\mathfrak{o}$, avec un $\Omega \in \mathbb{C}^*$ qui est bien déterminé à une (racine de 1') unité dans K près. Nous fixons désormais (arbitrairement) Ω. Nous continuons à écrire $\xi(., L)\colon \mathbb{C}/L \to E(\mathbb{C})$ l'isomorphisme de Weierstrass.

En appliquant σ_a ($\mathfrak{a}$ et a comme avant (4. 6)) aux coefficients $g_2(\omega)$, $g_3(\omega)$ du modèle de Weierstrass (2. 0), on obtient un modèle $(E^{\mathfrak{a}}, \omega^{\mathfrak{a}})$ sur F de la courbe $E^{\mathfrak{a}}$, conjuguée de E par $\sigma_{\mathfrak{a}|F}$. Comme $\mathbf{j}(\mathfrak{o})^{\sigma_{\mathfrak{a}}} = \mathbf{j}(\mathfrak{a}^{-1}\mathfrak{o})$, le réseau $L_{\mathfrak{a}}$, qui correspond (toujours par rapport au même plongement fixé $F \hookrightarrow \mathbb{C}$) à $(E^{\mathfrak{a}}, \omega^{\mathfrak{a}})$, est de la forme

$$L = \Omega_{\mathfrak{a}}\mathfrak{a}^{-1}, \quad \text{avec un} \quad \Omega_{\mathfrak{a}} \in \mathbb{C}^*.$$

En particulier, $\Omega_{\mathfrak{a}}$ dépend de $\mathfrak{a}$ et pas seulement de $\sigma_{\mathfrak{a}}$. L'isomorphisme de Weierstrass attaché à $E^{\mathfrak{a}}$ s'écrit donc $\xi(., L_{\mathfrak{a}})\colon \mathbb{C}/L_{\mathfrak{a}} \to E^{\mathfrak{a}}(\mathbb{C})$. Nous allons montrer que, Ω étant fixé, les $\Omega_{\mathfrak{a}}$ peuvent être déterminés sans ambiguité.

L'endomorphisme $\tilde{\varphi}(\mathfrak{a})$ de $\mathrm{End}_K B$ induit — selon (4. 3) et (4. 6) — une isogénie de E à $E^{\mathfrak{a}}$ définie sur F, notée encore $\tilde{\varphi}(\mathfrak{a})$. L'image réciproque («*pullback*») $\tilde{\varphi}(\mathfrak{a})^*(\omega^{\mathfrak{a}})$ est donc une forme différentielle non nulle de E définie sur F. On peut alors poser la

Définition. Nous appelons $\Lambda(\mathfrak{a})$ l'élément de F^* qui satisfait $\Lambda(\mathfrak{a})\omega = \tilde{\varphi}(\mathfrak{a})^*(\omega^{\mathfrak{a}})$.

(4. 10) Proposition. (i) *Pour tout idéal* $\mathfrak{a}$ *comme précédemment, l'application* $\mathfrak{a} \mapsto \Lambda(\mathfrak{a})$, *définie sur les idéaux entiers de K premiers à* $\mathfrak{g}$ *et à valeurs dans* F^*, *est caractérisée par la commutativité du diagramme suivant*:

$$\begin{array}{ccc} E & \xleftarrow{\xi(\cdot, L)} & \mathbb{C}/L \\ \Big\downarrow{\scriptstyle \tilde{\varphi}(\mathfrak{a})} & & \Big\downarrow{\scriptstyle \cdot\Lambda(\mathfrak{a})} \\ E^{\mathfrak{a}} & \xleftarrow{\xi(\cdot, L_{\mathfrak{a}})} & \mathbb{C}/L_{\mathfrak{a}} \end{array}$$

(ii) *Pour tout* $\mathfrak{a}$, $L_{\mathfrak{a}} = \Lambda(\mathfrak{a})\,\Omega\mathfrak{a}^{-1}$.

(iii) *Pour tout* $\rho \in \mathfrak{g}^{-1}L \smallsetminus L$, *on trouve que*

$$\xi(\rho, L)^{\sigma_{\mathfrak{a}}} = \xi(\Lambda(\mathfrak{a})\,\rho, L_{\mathfrak{a}}).$$

(iv) Λ *est un homomorphisme croisé par l'action de Galois à travers le quotient* G; *c'est-à-dire que, pour* $\mathfrak{a}$ *et* $\mathfrak{b}$ *deux idéaux entiers premiers à* $\mathfrak{g}$, *on a*

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

(v) *Les applications* Λ, *pour des idéaux* $\mathfrak{g}$ *différents, sont compatibles entre elles de façon évidente.*

(vi) *L'application Λ dépend du choix initial de la forme ω: la forme $\omega' = \alpha\omega$, pour $\alpha \in F^*$, conduit à l'application Λ' telle que, pour tout* $\mathfrak{a}$:

$$\Lambda'(\mathfrak{a}) = \Lambda(\mathfrak{a}) \cdot \alpha^{(\sigma_\mathfrak{a} - 1)}.$$

La traduction, en termes d'idèles, de la proposition (4. 10) donne un 1-cocycle continu Λ: $K_\mathbf{A}^* \to F^*$, qui induit l'identité sur K^* (ici, $K_\mathbf{A}^*$ agit sur F^* par le quotient G). D'après (vi), sa classe dans $H^1(K_\mathbf{A}^*, F^*)$ est indépendante de ω. — Signalons aussi que des constantes analogues aux $\Lambda(\mathfrak{a})$, mais pour des courbes plus générales, se trouvent déjà dans [15], App. D. e. Voir également [10], § 21. 1 et [11]. — Enfin, les parties (i), (ii) et (iii) de (4. 10) représentent une version explicite du «*théorème principal de la multiplication complexe*» pour notre classe de courbes elliptiques — cf. [19], Thm. 5. 4.

Démonstration. (i) se déduit directement de la définition. — D'après ce que nous savons de $\tilde{\varphi}$, on voit que le noyau de l'isogénie $\tilde{\varphi}(\mathfrak{a}) \in \mathrm{Hom}(E, E^\mathfrak{a})$ est isomorphe à $\mathfrak{a}^{-1}/\mathfrak{o}$. Compte tenu de (i), ceci implique (ii). — (iii) se déduit immédiatement de (i) et de (4. 6). — (iv) résulte par un calcul standard de la multiplicativité de $\tilde{\varphi}$ et de (i). — (v) et (vi) sont évidents.

Nous allons maintenant considérer le produit tensoriel $T \otimes_K F$ muni de l'action de $G = G(F/K)$ qui est naturelle sur F et triviale sur T.

(4. 11) Corollaire. (i) *Pour un idéal entier $\mathfrak{a}$ de K premier à $\mathfrak{g}$, l'élément*

$$\Phi(\mathfrak{a}) = \tilde{\varphi}(\mathfrak{a})\ \Lambda(\mathfrak{a})^{-1} \quad \textit{de} \quad (T \otimes_K F)^*$$

ne dépend que de la restriction $\sigma_{\mathfrak{a}|F} \in G$.

(ii) *L'application Φ: $G \to (T \otimes_K F)^*$, qui résulte de* (i), *est un* 1*-cocycle, c'est-à-dire que, pour $\sigma, \tau \in G$, on a $\Phi(\sigma\tau) = \Phi(\sigma)\ \Phi(\tau)^\sigma$.*

Démonstration. Si $\sigma_\mathfrak{a}$ fixe F (a fortiori $\mathfrak{a}$ est donc un idéal principal de K), $\tilde{\varphi}(\mathfrak{a})$ appartient à $K \hookrightarrow \mathbb{C}$ et donne l'endomorphisme de E qui envoie $\xi(\rho, L)$ sur $\xi(\tilde{\varphi}(\mathfrak{a})\,\rho, L)$. Compte tenu de (4. 10), (iii), on en déduit aussitôt (i), et (ii) est alors immédiat.

Notons en passant que si le modèle ω de départ est un modèle de Weierstrass minimal de E/F, les valeurs de Φ sont des unités de $\mathrm{End}_K B \otimes_\mathfrak{o} \mathfrak{o}_F$ — voir (10. 4) et la fin de [11].

Enfin, mentionnons tout de suite que le groupe de cohomologie $H^1(G, (T \otimes_K F)^*)$ est trivial. La même démonstration que pour $H^1(G, F^*)$ — «Hilbert 90» — marche aussi dans ce cas plus général. On trouve donc le

(4. 12) Lemme. *Il existe un $x \in (T \otimes_K F)^*$ tel que, pour tout $\sigma \in G$, $\Phi(\sigma) = x^{\sigma - 1}$. Cet élément x est bien déterminé à multiplication par T^* près.*

§ 5. Les fonctions L partielles

La démonstration de la formule suivante est parfaitement analogue à celle de la décomposition en produit de fonctions L (de caractères de Dirichlet) de la fonction zêta d'un corps de nombres abélien — voir par exemple, [25], XIII-10.

Avec les notations de (4. 4), *on a pour tout* $k \geqq 1$:

(5. 0) $$L(\psi^k, s) = \prod_{\chi \in \hat{G}} L(\varphi^k \chi, s).$$

Suivant N. Arthaud [1], on va s'inspirer encore une fois de la théorie analytique classique des nombres algébriques, en introduisant des séries L partielles relatives à notre situation.

Ici, et pour les trois paragraphes à venir, il sera très convenable de considérer des fonctions L éventuellement non primitives: nous gardons notre «Erklärungsmodul» $\mathfrak{g}$, fixé au § 4, qui est divisible par les conducteurs de φ et de l'extension F/K, et nous considérons (pour k un entier positif quelconque) les fonctions

$$L_{\mathfrak{g}}(\varphi^k, s) = \prod_{\mathfrak{p} \nmid \mathfrak{g}} (1 - \varphi^k(\mathfrak{p}) N\mathfrak{p}^{-s})^{-1}, \qquad \left(\mathrm{Re}(s) > 1 + \frac{k}{2}\right)$$

où $\mathfrak{p}$ décrit les idéaux premiers de K qui ne divisent pas $\mathfrak{g}$. Et de même

$$L_{\mathfrak{g}}(\psi^k, s) = \prod_{\mathfrak{P} \nmid \mathfrak{g}} (1 - \psi^k(\mathfrak{P}) N\mathfrak{P}^{-s})^{-1}, \qquad \left(\mathrm{Re}(s) > 1 + \frac{k}{2}\right)$$

où $\mathfrak{P}$ décrit les idéaux premiers de F qui ne divisent pas $\mathfrak{g}\mathfrak{o}_F$.

(5. 1) Convention. Nous supprimons l'indice $\mathfrak{g}$, pour alléger l'écriture (sauf s'il y a risque de confusion) et désignons donc par L les fonctions $L_{\mathfrak{g}}$ écrites ci-dessus.

Lue selon cette convention, la formule (5. 0) reste, bien sûr, vraie et est en fait plus simple à démontrer!

Définition. On garde les hypothèses faites au § 4. Pour k un entier positif, $\sigma \in G = G(F/K)$ et pour s avec $\mathrm{Re}(s) > 1 + \frac{k}{2}$, on définit la série L partielle de φ^k, relative à l'automorphisme σ de F/K, par

$$L(\varphi^k, \sigma, s) = \sum_{\sigma_{\mathfrak{a}} = \sigma} (\varphi^k(\mathfrak{a}) N\mathfrak{a}^{-s}),$$

la somme étant étendue à tous les idéaux entiers $\mathfrak{a}$ de K, premiers à $\mathfrak{g}$, dont le symbole d'Artin $\sigma_{\mathfrak{a}}$ induit σ sur F.

On a trivialement (grâce à (5. 1)),

(5. 2) $$L(\varphi^k, s) = \sum_{\sigma \in G} L(\varphi^k, \sigma, s).$$

En plus, (5. 0) donne

(5. 3) $$L(\psi^k, s) = \prod_{\chi \in \hat{G}} \sum_{\sigma \in G} \chi(\sigma)\, L(\varphi^k, \sigma, s).$$

Or, il nous sera très utile de transformer (5. 3) au moyen d'une formule bien connue — dite de Frobenius et due à Dedekind, voir [13], **3** § 6 — comme suit:

(5. 4) Lemme. $L(\psi^k, s) = \pm \det_{\sigma,\tau\in G}\big(L(\varphi^k, \sigma\tau, s)\big)$, *le signe étant celui de la permutation* $\tau \mapsto \tau^{-1}$ *de* G.

La proposition fondamentale suivante établit le lien entre la première et la deuxième partie de ce papier. Elle donne la décomposition des séries L partielles que nous venons d'introduire en somme de séries de Kronecker, définies au § 1. Cette décomposition fait intervenir le caractère φ ainsi que son conjugué complexe $\bar{\varphi}$ (pour lequel toutes les formules précédentes sont naturellement valables, par changement du plongement de K dans $\mathbb{C}$). En fait, nous serons amenés à étudier d'abord les fonctions L attachées aux caractères $\bar{\varphi}$ et $\bar{\psi}$, selon nos normalisations. Mais nous gardons pourtant le plongement fixé!

(5. 5) Proposition. *Soient* $\mathfrak{a}$ *un idéal entier de* K *premier à* $\mathfrak{g}$ *et* $\mathfrak{B}$ *un système d'idéaux entiers de* K, *premiers à* $\mathfrak{g}$, *tels que les symboles d'Artin* $\sigma_{\mathfrak{b}}$, *pour* $\mathfrak{b}\in\mathfrak{B}$, *décrivent (sans répétition) le groupe de Galois de* $F(E_{\mathfrak{g}})$ *sur* F. *Soit* $\rho\in\Omega K^*\subset\mathbb{C}^*$ *tel que l'idéal* $\rho\Omega^{-1}\mathfrak{o}$ *soit égal à* $\mathfrak{g}^{-1}\mathfrak{h}$, *avec un idéal entier* $\mathfrak{h}$ *de* K, **premier** *à* $\mathfrak{g}$.

Alors on a, pour tout entier positif k, *et tout* s *avec* $\mathrm{Re}(s) > 1+\frac{k}{2}$ *(dans les notations du* § 1):

$$\frac{\varphi^k(\mathfrak{a}\mathfrak{h})}{N(\mathfrak{a}\mathfrak{h})^{k-s}}\,\frac{\overline{(\Lambda(\mathfrak{a})\rho)^k}}{|\Lambda(\mathfrak{a})\rho|^{2s}}\,L(\bar{\varphi}^k, \sigma_{\mathfrak{a}\mathfrak{h}}, s) = \sum_{\mathfrak{b}\in\mathfrak{B}} H_k(\varphi(\mathfrak{b})\,\Lambda(\mathfrak{a})\,\rho, 0, s, L_{\mathfrak{a}}).$$

(5. 6) Remarque. Le théorème (1. 1) montre donc que les séries L partielles ont un prolongement analytique en des fonctions L partielles, holomorphes dans tout le plan complexe. La formule de la proposition, aussi bien que les formules (5. 2), (5. 3), (5. 4) restent évidemment vraies pour tout $s\in\mathbb{C}$. — Signalons aussi que les hypothèses de la proposition font de $\xi(\Lambda(\mathfrak{a})\rho, L_{\mathfrak{a}})$ un point de $\mathfrak{g}$-division *primitif* de $E^{\mathfrak{a}}$.

Démonstration de (5. 5). Rappelons (4. 10) que $L_{\mathfrak{a}} = \Lambda(\mathfrak{a})\,\Omega\mathfrak{a}^{-1}$. En faisant sortir $\Lambda(\mathfrak{a})\rho$ de la définition (1. 0), appliquée aux arguments en question, on obtient donc

$$\sum_{\mathfrak{b}\in\mathfrak{B}} H_k(\varphi(\mathfrak{b})\,\Lambda(\mathfrak{a})\,\rho, 0, s, L_{\mathfrak{a}}) = \frac{\overline{(\Lambda(\mathfrak{a})\rho)^k}}{|\Lambda(\mathfrak{a})\rho|^{2s}} \sum_{\mathfrak{b}\in\mathfrak{B}} \sum_{\alpha\in(\mathfrak{a}\mathfrak{h})^{-1}\mathfrak{g}} \frac{\overline{(\varphi(\mathfrak{b})+\alpha)^k}}{|\varphi(\mathfrak{b})+\alpha|^{2s}}.$$

On utilise alors le lemme (4. 9) et on voit aussitôt qu'il reste à démontrer l'identité

$$L(\bar{\varphi}^k, \sigma_{\mathfrak{a}\mathfrak{h}}, s) = \sum_{\mathfrak{b}\in\mathfrak{B}} \sum_{\alpha} \frac{\bar{\varphi}^k(\mathfrak{a}\mathfrak{h}(\varphi(\mathfrak{b})+\alpha))}{N(\mathfrak{a}\mathfrak{h}(\varphi(\mathfrak{b})+\alpha))^s},$$

où α décrit toujours le réseau $(\mathfrak{a}\mathfrak{h})^{-1}\mathfrak{g}$.

Ceci est un exercice classique de théorie du corps de classes dont la résolution ne présentera guère d'obstacles au lecteur.

Un coup d'oeil au corollaire (2. 3) nous indique tout de suite quelle forme définitive il faut donner à la décomposition des valeurs spéciales des fonctions L partielles en celles des séries d'Eisenstein:

(5. 7) Corollaire. *Gardons les notations de la proposition* (5. 5). *Soit de plus* j *un entier avec* $\frac{k}{2} < j \leqq k$. *Alors on a l'identité*

$$\left(\frac{2\pi i}{N(\mathfrak{h})}\right)^{k-j} \frac{\varphi^k(\mathfrak{ah})}{(\Lambda(\mathfrak{a})\rho)^k} L(\bar{\varphi}^k, \sigma_{\mathfrak{ah}}, j) = \sum_{\mathfrak{b} \in \mathfrak{B}} \mathfrak{E}_{j,k}(\mathfrak{a}, \mathfrak{b}),$$

où l'on écrit, avec les notations introduites au § 1:

$$\mathfrak{E}_{j,k}(\mathfrak{a}, \mathfrak{b}) = \left(\frac{2\pi i N\mathfrak{a}}{|\Lambda(\mathfrak{a})\rho|^2}\right)^{k-j} E^*_{k-j,j}(\varphi(\mathfrak{b})\,\Lambda(\mathfrak{a})\,\rho, L_{\mathfrak{a}}).$$

Le corollaire se déduit immédiatement de (5. 5) et (5. 6).

Le but du prochain paragraphe sera de présenter toutes les belles propriétés dont jouissent les $\mathfrak{E}_{j,k}(\mathfrak{a}, \mathfrak{b})\ldots$

§ 6. Algébricité de valeurs spéciales des séries d'Eisenstein. II

Dans les deux théorèmes de ce paragraphe, les notations sont celles de (5. 5) et (5. 7). En particulier, on garde les hypothèses et notations introduites au § 4.

(6. 1) Théorème. *Soient* $\mathfrak{a}$ *et* $\mathfrak{b}$ *deux idéaux entiers de* K *premiers à* $\mathfrak{g}$, *tels que* $\sigma_{\mathfrak{b}}$ *induise l'identité sur* F. *Alors*

(i) $\mathfrak{E}_{j,k}(\mathfrak{a}, \mathfrak{b})$ *appartient à* $F(E_{\mathfrak{g}})$.

(ii) $\mathfrak{E}_{j,k}(\mathfrak{a}, \mathfrak{b}) = \mathfrak{E}_{j,k}(\mathfrak{o}, \mathfrak{b})^{\sigma_{\mathfrak{a}}}$.

(iii) $\mathfrak{E}_{j,k}(\mathfrak{a}, \mathfrak{b}) = \mathfrak{E}_{j,k}(\mathfrak{a}, \mathfrak{o})^{\sigma_{\mathfrak{b}}}$.

On peut déduire les énoncés (i) et (iii) du corollaire (2. 3). Mais nous allons déduire tout le théorème (6. 1) du cas particulier suivant à l'aide de la proposition (1. 3).

(6. 2) Théorème. *Dans les notations précédentes on trouve pour les séries d'Eisenstein* E^*_k $(k \geqq 1)$ *introduites au* § 1:

(i) $E^*_k(\varphi(\mathfrak{b})\,\Lambda(\mathfrak{a})\,\rho, L_{\mathfrak{a}}) \in F(E_{\mathfrak{g}})$

(ii) $E^*_k(\varphi(\mathfrak{b})\,\Lambda(\mathfrak{a})\,\rho, L_{\mathfrak{a}}) = E^*_k(\varphi(\mathfrak{b})\,\rho, L)^{\sigma_{\mathfrak{a}}}$

(iii) $E^*_k(\varphi(\mathfrak{b})\,\Lambda(\mathfrak{a})\,\rho, L_{\mathfrak{a}}) = E^*_k(\Lambda(\mathfrak{a})\,\rho, L_{\mathfrak{a}})^{\sigma_{\mathfrak{b}}}$.

Notons d'abord que (6. 1) est effectivement impliqué par (6. 2). En fait, l'invariant $A(L_{\mathfrak{a}})$, qu'il faut calculer pour appliquer la proposition (1. 3), vaut bien

$$A(\Lambda(\mathfrak{a})\,\Omega\mathfrak{a}^{-1}) = \frac{1}{2\pi i} |\Lambda(\mathfrak{a})\Omega|^2\, N\mathfrak{a}^{-1} \sqrt{d_K},$$

où d_K est le discriminant de K. Or, $\sqrt{d_K}$ et $\rho\Omega^{-1}$ sont dans K^*, et on peut aussi, en appliquant (1. 3), négliger tous les facteurs rationnels.

Démonstration du théorème (6. 2). Compte tenu de (4. 7), la partie (i) se déduit tout de suite du premier énoncé du théorème (2. 1), appliqué à la courbe $E^{\mathfrak{a}}$. De même, pour déduire la partie (iii) du deuxième énoncé de (2. 1), il suffit de prendre un idéal $\tilde{\mathfrak{b}}$ de F premier à $\mathfrak{g}$, tel que $\sigma_{\mathfrak{b}}$ induit $(\tilde{\mathfrak{b}}, F(E_{\mathfrak{g}})/F)$; car alors on a $\varphi(\mathfrak{b})\rho \equiv \psi(\tilde{\mathfrak{b}})\rho \bmod L$, d'après (4. 7). — Ou bien, on peut refaire la démonstration de (2. 1), en remplaçant ψ par φ, au moyen de (4. 6).

Reste donc à démontrer (ii). Il faut pour cela pasticher la démonstration du théorème (2. 1) et se servir encore de la fonction Θ^* étudiée au § 1. Nous pouvons évidemment supprimer $\varphi(\mathfrak{b})$, ce qui simplifie l'écriture. En utilisant les mêmes constructions que dans la démonstration de (2. 1), on est réduit à démontrer que

$$\textbf{(6. 3)} \qquad \Theta^*(z+\rho, L, \Omega)^{\sigma_{\mathfrak{a}}} = \Theta^*\big(z+\Lambda(\mathfrak{a})\rho, L_{\mathfrak{a}}, \Lambda(\mathfrak{a})\mathfrak{a}^{-1}\Omega\big),$$

pour un réseau convenable $\Omega \supset L$ du plan complexe. Dans (6. 3), $\sigma_{\mathfrak{a}}$ agit sur $\Theta^*(z+\rho)$ en tant que série de Laurent en z à coefficients dans $F(E_{\mathfrak{g}})$. Cela revient au même de considérer l'action sur $\Theta^*(z+\rho)$ en tant que fonction rationnelle en $\wp(z, L)$ et $\wp'(z, L)$ à coefficients dans $F(E_{\mathfrak{g}})$, *pourvu que* l'on fasse agir $\sigma_{\mathfrak{a}}$ aussi sur les coefficients des développements en z de $\wp$ et $\wp'$. Comme ceux-ci appartiennent à $\mathbb{Q}(g_2(L), g_3(L))$, $\sigma_{\mathfrak{a}}$ transforme $\wp(z, L)$ en $\wp(z, L_{\mathfrak{a}})$, et de même pour la dérivée, d'après la définition de $L_{\mathfrak{a}}$.

Pour vérifier (6. 3), on se ramène, grâce à (4. 10), (iii), à la formule simplifiée

$$\textbf{(6. 4)} \qquad \Theta^*(z, L, \Omega)^{\sigma_{\mathfrak{a}}} = \Theta^*\big(z, L_{\mathfrak{a}}, \Lambda(\mathfrak{a})\mathfrak{a}^{-1}\Omega\big),$$

pour des réseaux $\Omega \supset L$ convenables.

Rappelons alors la formule explicite pour Θ^* du théorème (1. 9)! En passant par un module $\mathfrak{g}'$ qui est aussi divisible par $[\Omega : L]$, on déduit de (4. 10), (iii) et (v) que

$$\textbf{(6. 5)} \qquad \Theta^*(z, L, \Omega)^{\sigma_{\mathfrak{a}}} = \prod_{l} \big(\wp(z, L_{\mathfrak{a}}) - \wp\big(\Lambda(\mathfrak{a})l, L_{\mathfrak{a}}\big)\big)^{-1},$$

pour tous les réseaux Ω contenant L, tels que $[\Omega : L]$ soit premier à $\mathfrak{a}$. Ici, l décrit toujours un système de représentants non triviaux de Ω modulo L. Mais, comme $\mathfrak{a}$ est premier à $[\Omega : L]$, les $\Lambda(\mathfrak{a})l$ décrivent donc un système de représentants non triviaux de $\Lambda(\mathfrak{a})\mathfrak{a}^{-1}\Omega$ modulo $L_{\mathfrak{a}}$, ce qui démontre — grâce à (1. 9) — la formule (6. 4) pour tout reseau Ω, tel que $[\Omega : L]$ soit premier à $\mathfrak{a}$. Reste à signaler que la construction du réseau auxiliaire $\Omega = \alpha^{-1}L$ dans la démonstration du théorème (2. 1) ne présente aucune difficulté, si l'on impose que α soit premier à $\mathfrak{a}$.

(6. 6) Remarques. 1) Pour tout $\mathfrak{a}$, les invariants $s_2(L_{\mathfrak{a}})$ (introduits avant la proposition (1. 5)) appartiennent à F, d'après (2. 2). En plus, (6. 2) et (1. 5) montrent qu'ils sont reliés par $s_2(L)^{\sigma_{\mathfrak{a}}} = s_2(L_{\mathfrak{a}})$.

2) Comme dans (2. 2), on note que le théorème (6. 2) se voit sans l'intermédiaire de la fonction Θ^*, si k n'est pas 1 ou 2.

§ 7. Rationalité des $L(\bar{\psi}^k, j)$ et la conjecture de Birch et Swinnerton-Dyer

Rappelons nos données. E est une courbe elliptique définie sur le corps de nombres F, telle que $\mathrm{End}_F E = \mathfrak{o}$, l'anneau des entiers de $K \hookrightarrow F \hookrightarrow \mathbb{C}$. Nous supposons que E/F satisfait les conditions équivalentes de (4.1). En particulier, F/K est abélienne. Nous avons fixé au § 4 un idéal $\mathfrak{g}$ de $\mathfrak{o}$ tel que — en particulier — F est contenu dans le corps des rayons mod $\mathfrak{g}$ de K. Enfin, ψ désigne le Grössencharakter de E/F.

Nous avons fixé une forme différentielle $\omega \in H^0(E, \Omega^1_{/F})$ et choisi le plongement $F \hookrightarrow \mathbb{C}$ de sorte que le réseau $L \subset \mathbb{C}$ correspondant à (E, ω) s'écrit $L = \Omega\mathfrak{o}$, $\Omega \in \mathbb{C}^*$. Le nombre Ω est donc une période de ω. Plus généralement, grâce à la multiplication complexe, l'homologie rationnelle $H_1(E(\mathbb{C}), \mathbb{Q})$ est un espace vectoriel de dimension un sur K. Si γ en est une base, alors $\Omega^{-1} \int_\gamma \omega$ appartient à K^*.

(7. 0) Posons $n = [F : K]$, et choisissons un système $\mathfrak{A}$ de n idéaux entiers de K premiers à $\mathfrak{g}$, dont les symboles d'Artin $\sigma_\mathfrak{a}$, $\mathfrak{a} \in \mathfrak{A}$, recouvrent le groupe de Galois G de F sur K. Pour chaque $\mathfrak{a} \in \mathfrak{A}$, $\sigma_\mathfrak{a}$ transforme ω en une forme $\omega^\mathfrak{a}$ sur la courbe conjuguée $E^\mathfrak{a}$. Nous avons introduit (4.10) des invariants $\Lambda(\mathfrak{a}) \in F^*$ tels que $(\Lambda(\mathfrak{a})\Omega)^{-1} \int_\gamma \omega^\mathfrak{a}$ appartient à K^*, pour chaque élément non trivial γ de $H_1(E^\mathfrak{a}(\mathbb{C}), \mathbb{Q})$.

Nous nous donnons enfin deux entiers positifs, j et k, tels que $k/2 < j \leqq k$.

Avec ces notations, voici la première version de notre résultat de rationalité à propos de $L(\bar{\psi}^k, j)$:

(7. 1) Théorème. *Le nombre*

$$L^*(\bar{\psi}^k, j) = (2\pi i)^{n(k-j)} \cdot \prod_{\mathfrak{a} \in \mathfrak{A}} (\Lambda(\mathfrak{a})\Omega)^{-k} \cdot L(\bar{\psi}^k, j)$$

appartient à F. De plus, pour $\sigma \in G$, on a

$$L^*(\bar{\psi}^k, j)^\sigma = \mathrm{sgn}(\sigma)\, L^*(\bar{\psi}^k, j),$$

où $\mathrm{sgn}(\sigma)$ *est le signe de la permutation $\tau \mapsto \tau\sigma$ de l'ensemble G.*

Démonstration. Montrons d'abord comment on déduit de (5. 4), que $L^*(\bar{\psi}^k, j)$ est égal, à un facteur dans K^* près, au déterminant

$$D = \det_{\mathfrak{a}_1, \mathfrak{a}_2 \in \mathfrak{A}} \left((2\pi i)^{k-j} \varphi^k(\mathfrak{a}_1\mathfrak{a}_2\mathfrak{h}) \, (\Lambda(\mathfrak{a}_1)\rho)^{-k} L(\bar{\varphi}^k, \sigma_{\mathfrak{a}_1\mathfrak{a}_2\mathfrak{h}}, j) \right).$$

Compte tenu que $\rho\Omega^{-1} \in K^*$, il s'agit de montrer que $\varphi(\mathfrak{h}^n) \prod_{\mathfrak{a} \in \mathfrak{A}} \varphi(\mathfrak{a}^2)$ appartient à K^*. Mais c'est évident, car φ prend ses valeurs dans K^* sur le noyau du symbole d'Artin relatif à F/K, voir (4. 9).

Nous sommes donc ramenés à démontrer (7. 1) avec le déterminant D à la place de $L^*(\bar{\psi}^k, j)$. D'après (6. 1), (5. 7) et la partie (iv) de la proposition (4. 10), ce déterminant s'écrit

$$D = \det_{\mathfrak{a}_1, \mathfrak{a}_2 \in \mathfrak{A}} \left(\{\Lambda(\mathfrak{a}_2)^k \, [(2\pi i)^{k-j} \varphi^k(\mathfrak{h}) \rho^{-k} L(\bar{\varphi}^k, \sigma_\mathfrak{h}, j)]^{\sigma_{\mathfrak{a}_2}}\}^{\sigma_{\mathfrak{a}_1}} \right).$$

Le théorème est alors évident.

Le théorème (7.1) mérite quelques *commentaires* et *corollaires*:

D'abord, il faut signaler au lecteur soucieux de ne pas oublier la convention (5.1) que celle-ci est tout-à-fait inutile pour tous nos *énoncés* de rationalité (sinon pour leurs *démonstrations*). Dans le cas présent, les facteurs d'Euler supprimés appartiennent en effet à K^*.

Notons F_{pair} le corps fixe du sous-groupe des éléments de G dont le signe vaut $+1$. Pour la plupart des cas, F_{pair} sera donc égal à K. Plus précisément, on voit aisément que F_{pair} est différent de K si et seulement si la partie 2-primaire du groupe G est cyclique (et non-triviale). En tout cas, F_{pair} est une extension au plus quadratique de K, contenue dans F, qui peut être caractérisée comme étant l'unique corps de définition minimal de toutes les formes différentielles $\bigwedge_{\sigma \in G} \eta^\sigma$ sur la variété abélienne B (voir le § 4), où η décrit les formes différentielles non nulles de degré un de E sur F.

Le théorème (7.1) montre que les $L^*(\bar{\psi}^k, j)$ sont toujours dans F_{pair}. Plus exactement, si $L^*(\bar{\psi}^k, j) \neq 0$, $L^*(\bar{\psi}^k, j)$ engendre F_{pair} sur K et on peut écrire $L^*(\bar{\psi}^k, j) = \sqrt{\alpha}$, avec $\alpha \in K^*$. Dans ce cas, les $L^*(\bar{\psi}^k, j)$ sont en fait, comme le montre la démonstration de (7.1), des exemples de déterminants classiques:

Soient en effet $f_1, \ldots, f_n$ une K-base de F et posons

$$\delta = \det_{\substack{1 \leqq i \leqq n \\ \tau \in G}} (f_i^\tau).$$

Alors on a aussi évidemment $\delta^\sigma = \operatorname{sgn}(\sigma)\delta$, pour tout $\sigma \in G$. Donc δ engendre F_{pair} sur K et on peut résumer (7.1) comme ceci:

(7.2) Variante. *Pour tout δ comme ci-dessus, le nombre*

$$\delta L^*(\bar{\psi}^k, j) = (2\pi i)^{n(k-j)}\, \delta \prod_{\mathfrak{a} \in \mathfrak{A}} (\Lambda(\mathfrak{a})\Omega)^{-k} \cdot L(\bar{\psi}^k, j)$$

appartient à K.

Indiquons maintenant comment on peut réinterpréter le produit $\delta \prod (\Lambda(\mathfrak{a})\Omega)$ en termes de la variété abélienne B, restriction de scalaires de E par rapport à F/K.

Soient $\eta_1, \ldots, \eta_n$ une base du K-espace vectoriel $H^0(B, \Omega^1_{/K})$ des formes différentielles de première espèce de B définies sur K, et soit $\omega \in H^0(E, \Omega^1_{/F})$ la forme différentielle fixée de E sur F. Compte tenu de la décomposition de B sur F, chaque η_i, pour $i = 1, \ldots, n$, induit $f_i\omega$ sur E, pour un certain élément $f_i \in F^*$. De plus, comme les η_i sont rationnelles sur K, elles induisent $f_i^\sigma \omega^\sigma$ sur E^σ, pour tout $\sigma \in G$. Les η_i formant une base, on trouve bien que $\delta = \det(f_i^\tau)$ n'est pas nul.

D'autre part, choisissons, en considérant B comme variété abélienne à multiplication complexe par K, une K-base $\{\gamma_\sigma : \sigma \in G\}$ de l'homologie rationnelle

$$H_1(B(\mathbb{C}), \mathbb{Q}) = \bigoplus_\sigma H_1(E^\sigma(\mathbb{C}), \mathbb{Q}),$$

telle que pour chaque σ, γ_σ soit concentré sur E^σ. Appelons alors Ω_B le déterminant de la matrice de périodes

$$\left(\int_{\gamma_\sigma} \eta_i\right)_{\substack{1 \leqq i \leqq n \\ \sigma \in G}}.$$

A un élément dans K^* près, Ω_B ne dépend pas des choix de bases et on voit tout de suite que (à un élément dans K^* près) Ω_B vaut $\delta \prod_{\mathfrak{a} \in \mathfrak{A}} (\Lambda(\mathfrak{a})\Omega)$. De manière un peu plus conceptuelle, on considère l'accouplement d'intégration

$$H_1(B(\mathbb{C}), \mathbb{Q}) \times H^0(B, \Omega^1_{/K}) \xrightarrow{\int} \mathbb{C}.$$

L'action de K par la multiplication complexe étant bien normalisée — voir les débuts des §§ 2, 4 —, on trouve que $\int$ est K-bilinéaire, *et Ω_B donne la classe du déterminant de $\int$ dans $\mathbb{C}^*/K^*$.*

En somme, nous avons démontré cette deuxième variante du théorème (7.1):

(7. 3) Variante. *Le nombre*

$$(2\pi i)^{n(k-j)}\, \Omega_B^{-k}\, L(\bar{\psi}^k, j)$$

appartient à F_{pair}. Si l'exposant k est impair, il appartient même à K.

(7. 4) Remarques sur les périodes utilisées. 1) Pour $k=j=1$, Ω_B est essentiellement la période qu'il faut construire pour $L(\bar{\psi}, 1)$ dans le cadre de Deligne [9]. La différence entre les énoncés (7. 2) et (7. 3) indique clairement que l'expression $\delta \prod_{\mathfrak{a} \in \mathfrak{A}} (\Lambda(\mathfrak{a})\Omega)$, calculée sur F, se comporte mieux que Ω_B par passage aux puissances k-ièmes. Voir le § 9 pour plus de détails.

2) Le produit $\prod_{\mathfrak{a} \in \mathfrak{A}} |\Lambda(\mathfrak{a})\Omega|^2$ est donné explicitement par la formule de Chowla et Selberg — voir par exemple, [10], § 21.

3) On voit facilement que, pour tout $\sigma \in G$, $[\prod_{\mathfrak{a} \in \mathfrak{A}} \Lambda(\mathfrak{a})]^{\sigma - 1}$ appartient à K^*. Par conséquent, $\prod \Lambda(\mathfrak{a})$ est contenu dans une sous-extension de F/K de degré divisant $\text{card}(\mathfrak{o}^*)$. Par exemple, si $\mathfrak{o}^* = \{\pm 1\}$ et n est impair, $\prod (\Lambda(\mathfrak{a})\Omega)$ peut être remplacé — en ce qui concerne les questions de rationalité — par Ω^n. En général, les nombres algébriques dont nous étudions les propriétés d'intégralité au § 10, se trouvent dans une extension de petit degré de K.

4) Enfin, notons que toutes les périodes intervenant dans ce paragraphe sont des nombres transcendants, car Ω est transcendant: [23], Th. 3. 3. 1.

Revenons maintenant à la variante (7. 2), valable pour tout k. On en tire

$$\textbf{(7. 5)} \qquad \delta L^*(\bar{\psi}^k, j) \cdot \overline{\delta L^*(\bar{\psi}^k, j)} = N_{K/\mathbb{Q}}(\delta L^*(\bar{\psi}^k, j)) \in \mathbb{Q}.$$

Ici, le choix du plongement de F dans $\mathbb{C}$ n'intervient qu'implicitement, dans la définition de $L^*(\bar{\psi}^k, j)$. Posons maintenant

$$L^*(\psi^k, j) = (-2\pi i)^{n(k-j)} \prod_{\mathfrak{a} \in \mathfrak{A}} \overline{(\Lambda(\mathfrak{a})\Omega)^{-k}} \cdot L(\psi^k, j) = \overline{L^*(\bar{\psi}^k, j)}.$$

On peut naturellement récrire $N(\delta L^*(\bar{\psi}^k, j))$ comme $(\delta\bar{\delta})\, L^*(\psi^k, j)\, L^*(\bar{\psi}^k, j)$. Notons que cette nouvelle expression dépend visiblement du plongement de F dans $\mathbb{C}$. Toutefois, un changement du plongement multiplie $\delta\bar{\delta}$ au plus par -1. Rappelons alors le rôle classique des déterminants δ: D'après [17], III, §§ 2, 3, il existe un idéal $\mathfrak{b}$ de K, dépendant du choix des f_i définissant δ, tel que (noter que $\delta^2 \in K^*$!):

$$\delta^2 \mathfrak{o} = \mathfrak{d}_{F/K} \mathfrak{b}^2,$$

où $\mathfrak{d}_{F/K}$ est l'idéal discriminant de F sur K.

Nous venons donc d'établir le corollaire suivant du théorème (7.1):

(7. 6) Corollaire. *Soient* $\mathfrak{d}_{F/K}$ *le discriminant de* F *sur* K, *et* $N\mathfrak{d}_{F/K} = \mathrm{card}(\mathfrak{o}/\mathfrak{d}_{F/K})$ *sa norme absolue. Soit* $L^*(\psi^k, j)$ *comme dans* (7. 5), *et* $L^*(\bar{\psi}^k, j)$ *comme dans* (7. 1). *Alors pour tout choix de la racine* $\sqrt{N\mathfrak{d}_{F/K}}$, *le nombre*

$$\sqrt{N\mathfrak{d}_{F/K}}\, L^*(\psi^k, j)\, L^*(\bar{\psi}^k, j)$$

est rationnel.

(7. 7) Remarque. Il est clair que $N\mathfrak{d}_{F/K}$ est un carré dans $\mathbb{Q}^*$ si et seulement si (par rapport à n'importe quel plongement de F dans $\mathbb{C}$) $\bar{\delta}$ est dans F et que l'on a, pour tout $\sigma \in G$, $(\bar{\delta})^\sigma = \mathrm{sgn}(\sigma)\bar{\delta}$ — autrement dit, si F_{pair} est un corps de type CM.

A titre d'exemple, si F est le corps de classes de Hilbert de K, on a $\mathfrak{d}_{F/K} = \mathfrak{o}$, donc $N\mathfrak{d}_{F/K} = 1^2$. En effet, quand, dans ce dernier cas, $F_{\mathrm{pair}} \neq K$ (c'est-à-dire, d_K est divisible par exactement deux premiers rationnels distincts) on trouve que F_{pair} est de type CM.

Dans le cas général, $N\mathfrak{d}_{F/K}$ est un carré notamment si $F_{\mathrm{pair}} = K$ ou si F lui même est un corps de type CM. Cette dérnière condition équivaut à $F \subset \mathbb{Q}^{ab}$; mais comme F contient forcément le corps de classes de Hilbert de K, elle ne peut avoir lieu que si le groupe de classes d'idéaux de K est d'exposant 2: voir [10], § 5.

(7. 8) Corollaire. *Soit* $L(E/F, s)$ *la fonction L de Hasse-Weil de la courbe elliptique* E *sur* F. *Alors, avec les notations précédentes,*

$$\sqrt{N\mathfrak{d}_{F/K}} \prod_{\mathfrak{a} \in \mathfrak{A}} |\Lambda(\mathfrak{a})\Omega|^{-2}\, L(E/F, 1)$$

est un nombre rationnel: l'énoncé de rationalité contenu dans la conjecture de Birch et Swinnerton-Dyer pour E *sur* F *est vrai.*

Démonstration. On a la formule clé (voir par exemple [19], Th. 7. 42):

$$L(E/F, s) = L(\psi, s)\, L(\bar{\psi}, s).$$

Bien entendu, cette formule n'est vraie que si nous abandonnons pour un moment notre convention (5. 1), et écrivons des séries L primitives à droite. Mais les facteurs d'Euler (en nombre fini) qui s'y glissent sont tous dans K^* et se regroupent par paires de conjugués complexes. Pour les questions de rationalité, on peut donc les négliger. La première assertion du corollaire (7. 8) se déduit alors immédiatement du cas $j = k = 1$ de (7. 6).

Supposons maintenant que $L(E/F, 1) \neq 0$, et écrivons la conjecture de Birch et Swinnerton-Dyer pour E sur F dans ce cas (cf. [5], Chap. 1):

$$\sqrt{|d_F|} \prod_{v \in S} m_v^{-1} \cdot L(E/F, 1) = \mathrm{card}(Ш)\, \mathrm{card}\,(E(F)_{\mathrm{tors}})^{-2}.$$

Ici, $d_F \in \mathbb{Q}^*$ est le discriminant de F sur $\mathbb{Q}$; S est un ensemble fini convenable de places de F contenant les places à l'infini; m_v la mesure de Tamagawa de E sur F_v, convenablement normalisée; Ш désigne le groupe de Tate-Chafarévitch de E sur F, que l'on suppose conjecturalement fini; et $E(F)_{\mathrm{tors}}$ est le groupe fini des points de division de E qui sont rationnels sur F. Tout ce qu'il nous faut savoir des m_v, pour v à distance finie, est que $m_v \in \mathbb{Q}^*$. L'énoncé de rationalité pour $L(E/F, 1)$ contenu dans la con-

jecture de Birch et Swinnerton-Dyer pour E sur F est donc le suivant:

$$\sqrt{|d_F|} \prod_{v|\infty} m_v^{-1} \cdot L(E/F, 1) \in \mathbb{Q}.$$

Cette conjecture est d'ailleurs triviale, si $L(E/F, 1) = 0$.

Pour évaluer les m_v pour les places v à l'infini, rappelons que nous avons fixé un modèle ω de E sur F. (Notons en passant qu'un changement du modèle laisse invariante la conjecture de Birch et Swinnerton-Dyer grâce au «principe de Tamagawa», mais multiplie le produit $\prod_{v|\infty} m_v$ par la norme à K d'un élément de F^*). Comme les places v à l'infini de F correspondent aux différents plongements $F \hookrightarrow \mathbb{C}$ sur K, on peut associer à chaque v un $\mathfrak{a} \in \mathfrak{A}$ tel que

$$m_v = \int_{E(F_v)} |\omega_v| \, d\mu_v = |\Lambda(\mathfrak{a})\Omega|^2 \, N\mathfrak{a}^{-1} \sqrt{|d_K|},$$

cf. [5], Chap. 1, et aussi la démonstration de (6.1). La formule bien connue $d_F = N\mathfrak{d}_{F/K} \cdot d_K^n$ montre alors l'équivalence entre la conjecture de rationalité déduite de la conjecture de Birch et Swinnerton-Dyer et le résultat de rationalité établi dans la première partie du corollaire (7.8).

(7.9) Remarque. Jusqu'ici nous n'avons considéré que les valeurs de $L(\bar{\psi}^k, s)$ aux points entiers de la moitié droite de la bande critique, $0 < \mathrm{Re}(s) < k+1$, de cette fonction. On se sert alors de l'équation fonctionnelle de $L(\bar{\psi}^k, s)$ pour rabattre les résultats de la droite sur la moitié gauche de la bande critique. C'est ainsi que l'on obtient finalement (en partant par exemple de [25], VII-7) le résultat suivant:

Soient $j, k \in \mathbb{Z}$ *tels que* $0 < j \leqq \dfrac{k+1}{2}$; *soit* $\mathfrak{A}$ *un ensemble d'idéaux comme dans* (7.0) *et* δ *comme dans* (7.2). *Alors le nombre*

$$(2\pi i)^{n(k-j)} \delta \prod_{\mathfrak{a} \in \mathfrak{A}} \overline{(\Lambda(\mathfrak{a})\Omega)}^{-k} \cdot \tau(\psi^k) \cdot L(\bar{\psi}^k, j)$$

appartient à K. Ici, $\tau(\psi^k) = \prod_v \sum_x \psi_v^{-k}(x) \exp\left(2\pi i \, \lambda\left(\mathrm{Tr}\left(\frac{x}{y}\right)\right)\right)$, où v décrit les places de F divisant le conducteur $\mathfrak{f}_k$ de ψ^k et x les unités de l'anneau de valuation complété $\mathfrak{o}_v$ de v, prises modulo $(1 + \mathfrak{f}_k \mathfrak{o}_v)$; ψ_v est la composante en v du caractère ψ sur les idèles de F; $\lambda : \mathbb{Q}_p \to \mathbb{Q}_p/\mathbb{Z}_p \to \mathbb{Q}/\mathbb{Z} \to \mathbb{R}/\mathbb{Z}$ est l'application naturelle; enfin, y engendre l'idéal $(\mathfrak{D}\mathfrak{f}_k)\mathfrak{o}_v$, $\mathfrak{D}$ étant la différente de F sur $\mathbb{Q}$.

Si k *est impair*, on peut comparer ce résultat pour $j = \dfrac{k+1}{2}$ à (7.2), et on obtient la relation amusante:

$$\prod_{\mathfrak{a} \in \mathfrak{A}} \left\{ \frac{\overline{(\Lambda(\mathfrak{a})\Omega)}}{\Lambda(\mathfrak{a})\Omega} \right\}^k \in \tau(\psi^k) K^*,$$

pourvu que $L\left(\bar{\psi}^k, \dfrac{k+1}{2}\right) \neq 0$. Dans ce cas, (7.2) est donc vrai pour tout $j = 1, \ldots, k$.

Troisième partie: Compléments

. . . .

Non missura cutem nisi plena cruoris hirudo.

Q. Horatius F., Ep. ad Pis., finis.

§ 8. Descente à un sous-corps réel

Nous gardons les hypothèses et notations du § 4, et supposons en outre que le conjugué complexe $\bar{F}$ du corps F est égal à F. Autrement dit, nous supposons F galoisien sur $\mathbb{Q}$. Notons $\tau \in \mathrm{Gal}(F/\mathbb{Q})$ la conjugaison complexe induite par le plongement fixé de F dans $\mathbb{C}$, et F^+ le corps fixe de τ. On a donc $[F: F^+]=2$.

Ce paragraphe sera consacré à l'étude du cas où la courbe E descend à F^+, c'est-à-dire que nous supposons qu'il existe une courbe elliptique E^+ définie sur F^+ qui, sur F, devient isomorphe à la courbe E. Nous supposons en fait que la forme différentielle ω de E sur F (fixée dès le § 4!) est définie sur F^+.

Dans ce paragraphe, la convention (5.1) *n'est pas en vigueur: toutes les fonctions L considérées seront primitives.*

L'existence de E^+ équivaut à $\psi(\bar{\mathfrak{a}})=\bar{\psi}(\mathfrak{a})$, pour tout idéal $\mathfrak{a}$ de $\mathfrak{o}$ premier à $\mathfrak{g}$ — car au § 4 on a plongé F dans $\mathbb{C}$ de sorte que $\mathbf{j}(E)=\mathbf{j}(\mathfrak{o})=\overline{\mathbf{j}(\mathfrak{o})}=\mathbf{j}(E)^{\tau}$. (Cf. [10], § 10). En particulier, on voit que

(8. 0) $\qquad L(\psi^k, s)=L(\bar{\psi}^k, s) \in \mathbb{R}$, *pour tout* $k \geqq 1$ *et* $s \in \mathbb{R}$.

Nous allons définir: une période $\Omega^+ \in \mathbb{R}^*$; des constantes $\Lambda^+(\mathfrak{a}) \in F^*$, $\mathfrak{a} \in \mathfrak{A}$, pour un certain type d'ensemble $\mathfrak{A}$ comme dans (7. 0); et un déterminant δ^+ (du type δ introduit au § 7), tels qu'un énoncé analogue à (7. 2) sera vrai, avec K remplacé par $\mathbb{Q}$. Ces quantités ne seront bien déterminées qu'à un facteur dans $\mathbb{Q}^*$ près. Dans ce sens, nos constructions semblent *ad hoc*. Quoi qu'il en soit, elles nous permettront de démontrer directement l'énoncé de rationalité contenu dans la conjecture de Birch et Swinnerton-Dyer pour E^+ sur F^+.

Au § 4, la période Ω a été définie (à $\mathfrak{o}^*$ près) par la relation $L=\Omega\mathfrak{o}$, où L correspond à (E, ω). Comme E descend à F^+, on a $\bar{L}=L$. Par conséquent, $\bar{\Omega}\Omega^{-1}$ appartient à $\mathfrak{o}^*$. On construit facilement un élément α_0 de K^* tel que $\Omega^+=\Omega\alpha_0$ soit réel. On récrit alors:

$$L=\Omega^+(\alpha_0\mathfrak{o})^{-1}.$$

Nous construisons maintenant un ensemble $\mathfrak{A}$ (comme dans (7. 0), mais adapté à notre situation), et pour tout $\mathfrak{a} \in \mathfrak{A}$, une constante $\Lambda^+(\mathfrak{a})$.

Soit v une place réelle de F^+ et w l'unique place (complexe) de F au-dessus de v. Choisissons un idéal entier $\mathfrak{a}$ de K premier à $\mathfrak{g}$ (qui fera partie de notre ensemble $\mathfrak{A}$) tel que l'élément de $G=G(F/K)$ défini par le symbole d'Artin $\sigma_{\mathfrak{a}}$ corresponde à w. L'invariant modulaire $\mathbf{j}(\mathfrak{a}^{-1})$ est alors réel et on trouve un $\zeta \in K^*$ tel que $\bar{\mathfrak{a}}\mathfrak{a}^{-1}=\zeta\mathfrak{o}$. Il vient $\zeta\bar{\zeta}=1$ et, par «Hilbert 90», $\zeta=\beta_{\mathfrak{a}}^{1-\tau}$, pour un $\beta_{\mathfrak{a}} \in K^*$. Comme E descend à F^+, le réseau $L=\Lambda(\mathfrak{a})\Omega\mathfrak{a}^{-1}$ est invariant par conjugaison complexe. On en déduit la relation $\overline{(\Lambda(\mathfrak{a})\beta_{\mathfrak{a}})}\,(\Lambda(\mathfrak{a})\beta_{\mathfrak{a}})^{-1} \in \mathfrak{o}^*$. En somme, on voit qu'il existe un élément $\alpha_{\mathfrak{a}}$ de K^* tel que l'on peut récrire

$$L_{\mathfrak{a}}=\Lambda^+(\mathfrak{a})\,\Omega^+(\alpha_{\mathfrak{a}}\mathfrak{a})^{-1},$$

avec $\Lambda^+(\mathfrak{a})=\Lambda(\mathfrak{a})\,\alpha_{\mathfrak{a}}\alpha_{\mathfrak{o}}^{-1}$ appartenant à $(F^+)^*$.

Si, au contraire, v est une place complexe de F^+, il y a deux places, w et w', de F au-dessus de v. Si σ, σ' sont les éléments de G correspondant à w, w', on a, dans $G(F/\mathbb{Q})$, $\tau\sigma\tau = \sigma'$, de sorte que, *restreint à* F^+, σ' est le conjugué complexe de σ. Choisissons comme élément de $\mathfrak{A}$ donnant σ, un idéal $\mathfrak{a}$ tel que $\bar{\mathfrak{a}}$ soit encore premier à $\mathfrak{g}$. L'automorphisme σ' est alors induit par $\sigma_{\bar{\mathfrak{a}}}$, et nous prenons $\bar{\mathfrak{a}}$ comme l'élément de $\mathfrak{A}$ correspondant à σ'. Comme E descend à F^+, on a $\overline{L_{\mathfrak{a}}} = L_{\bar{\mathfrak{a}}}$, donc $\overline{\Lambda(\mathfrak{a})}\,\Lambda(\bar{\mathfrak{a}})^{-1} \in \mathfrak{o}^*$, et nous pouvons choisir un $\alpha_{\mathfrak{a}} = \alpha_{\bar{\mathfrak{a}}}$ dans K^* tel que, si l'on pose

$$\Lambda^+(\mathfrak{a}) = \Lambda(\mathfrak{a})\,\alpha_{\mathfrak{a}}\alpha_{\mathfrak{o}}^{-1}; \quad \Lambda^+(\bar{\mathfrak{a}}) = \Lambda(\bar{\mathfrak{a}})\,\alpha_{\bar{\mathfrak{a}}}\alpha_{\mathfrak{o}}^{-1},$$

on ait

$$L_{\mathfrak{a}} = \Lambda^+(\mathfrak{a})\,\Omega^+(\alpha_{\mathfrak{a}}\mathfrak{a})^{-1}; \quad L_{\bar{\mathfrak{a}}} = \Lambda^+(\bar{\mathfrak{a}})\,\Omega^+(\alpha_{\bar{\mathfrak{a}}}\bar{\mathfrak{a}})^{-1},$$

et

$$\overline{\Lambda^+(\mathfrak{a})} = \Lambda^+(\bar{\mathfrak{a}}).$$

Ecrivons $n = [F^+ : \mathbb{Q}] = r_1 + 2r_2$, où r_1 (resp. r_2) est le nombre des places réelles (resp. complexes) de F^+. Notons d_M le discriminant (sur $\mathbb{Q}$) d'un corps de nombres M. Enfin, donnons-nous, comme d'habitude, deux entiers positifs, j et k, tels que $k/2 < j \leqq k$. Avec ces notations, nous posons:

$$L^+(\psi^k, j) = \left(\frac{2\pi i}{\sqrt{d_K}}\right)^{n(k-j)} \prod_{\mathfrak{a} \in \mathfrak{A}} \left(\Lambda^+(\mathfrak{a})\,\Omega^+\right)^{-k} \cdot L(\psi^k, j).$$

Alors, d'après (7.1) et (8.0), $L^+(\psi^k, j)$ appartient à F^+. En fait, on a le

(8.1) Théorème. *Le nombre*

$$\sqrt{(|d_K|^{-r_2}\,|d_{F^+}|)} \cdot L^+(\psi^k, j)$$

est rationnel.

Démonstration. Soient $f_1, \ldots, f_n$ une base de l'anneau des entiers de F^+ sur $\mathbb{Z}$, et G^+ l'ensemble des plongements de F^+ dans $\mathbb{C}$. Posons

$$\delta^+ = \det_{\substack{1 \leqq i \leqq n \\ t \in G^+}} (f_i^t) \in F.$$

D'après la description des places à l'infini de F^+ que nous avons donnée, on voit immédiatement que

$$(\delta^+)^\tau = (-1)^{r_2}\delta^+.$$

Par conséquent, le nombre $(\sqrt{d_K})^{-r_2}\delta^+$ appartient à F^+. Mais, au signe près, ce nombre est bien $(|d_K|^{-r_2}\,|d_{F^+}|)^{1/2}$. Or, $\delta^+ = \det_{\substack{1 \leqq i \leqq n \\ \sigma \in G}} (f_i^\sigma)$. Ceci permet de déduire (8.1) de (7.2).

(8.2) Corollaire. *Soit $L(E^+/F^+, s)$ la fonction L de Hasse-Weil de la courbe elliptique E^+ sur F^+. Alors, avec les notations précédentes,*

$$\sqrt{|d_{F^+}|} \cdot \left[|d_K|^{\frac{r_2}{2}} \prod_{\mathfrak{a} \in \mathfrak{A}} \left(\Lambda^+(\mathfrak{a})\,\Omega^+\right)\right]^{-1} \cdot L(E^+/F^+, 1)$$

est un nombre rationnel: L'énoncé de rationalité contenu dans la conjecture de Birch et Swinnerton-Dyer pour E^+ sur F^+ est vrai.

Démonstration. Nos raisonnements seront analogues à ceux de la démonstration du corollaire (7. 8). D'abord, on a l'identité de fonctions L (voir [12], **10**, § 4):

$$L(E^+/F^+, s) = L(\psi, s).$$

D'où le premier énoncé de (8. 2). On cherche à démontrer — cf. la démonstration de (7. 8) —:

$$\sqrt{|d_{F^+}|} \cdot \Big(\prod_{v|\infty} m_v^+\Big)^{-1} \cdot L(E^+/F^+, 1) \in \mathbb{Q},$$

où, cette fois-ci, le produit est pris sur les places v à l'infini de F^+, et m_v^+ est la mesure de Tamagawa de E^+ en v.

Il s'agit donc de vérifier que le terme entre crochets dans la formule de (8. 2) vaut, à un rationnel non nul près, $\prod_{v|\infty} m_v^+$. — Ceci se déduit facilement de la description des places v et des réseaux correspondants que nous avons donnée; cf. [5], Chap. 1, pour des formules explicites des m_v^+.

§ 9. Rationalité des $L(\bar{\varphi}^k, j)$ et la conjecture de Deligne

Pour énoncer le résultat de rationalité relatif aux nombres $L(\bar{\varphi}^k, j)$, nous adopterons un nouveau point de vue, qui est analogue à [9], 2.2. et qui prolonge les données du § 4; nous aurons donc besoin de notations adéquates.

Soit $k \geqq 1$ un entier. Notons $T(k)$ la sous-K-algèbre de $T = \mathrm{End}_K B$ — cf. (4. 1) — engendrée par l'image de $\tilde{\varphi}^k$, la puissance k-ième du caractère de Serre-Tate attaché à la variété abélienne $B = R_{F/K}E$ sur K. Posons $J = \mathrm{Hom}_K(T(k), \mathbb{C})$. Pour $\varepsilon \in J$, écrivons φ_ε^k le caractère à valeurs dans le corps

$$T(k)_\varepsilon = \varepsilon\big(T(k)\big) \subset \mathbb{C}$$

qui se déduit de $\tilde{\varphi}^k \otimes (\mathrm{diag})_\infty^{-1}$ par ε. Si φ est le caractère de K fixé au § 4, φ_ε^k s'écrit sous la forme $\varphi_\varepsilon^k = (\varphi\chi)^k$, pour un $\chi \in \hat{G}$ — cf. (4. 8). Choisissons un x comme dans le lemme (4. 12) et tel que $x^k \in \big(T(k) \otimes_K F\big)^*$. On note alors x_ε^k la ε-composante de x^k dans

$$\big(T(k) \otimes_K F\big)^* \hookrightarrow \big(T(k) \otimes_K \mathbb{C}\big)^* = \mathbb{C}^{*J}.$$

Ici, le plongement de F dans $\mathbb{C}$ est celui fixé au § 4.

Enfin, si X est un anneau, Y un sous-ensemble de X, et que a, b appartiennent à X, alors nous écrirons

$$\ll a \underset{Y}{\sim} b \gg$$

pour signaler qu'il existe un c dans Y tel que $a = b \cdot c$. Bien entendu, cette relation n'est pas, en général, symétrique.

(9. 1) Théorème. *Soient j un entier avec $k/2 < j \leqq k$ et Ω la période de E fixée au § 4. Alors dans $T(k) \otimes_K \mathbb{C}$, on a:*

$$\big(L(\bar{\varphi}_\varepsilon^k, j)\big)_{\varepsilon \in J} \underset{T(k)}{\sim} (2\pi i)^{j-k} (x\Omega)^k.$$

Notons que, comme dans les deux paragraphes précédents, nos résultats s'appliquent aux fonctions L primitives. Mais dans la démonstration suivante, on suppose la convention (5.1), ce qui supprime quelques facteurs d'Euler appartenant à $T(k)^*$.

Démonstration. D'après (4.12), (5.2) et (5.7), on trouve pour un ensemble $\mathfrak{A}$ comme dans (7.0):

$$\left((2\pi i)^{k-j}(x_\varepsilon^k \Omega^k)^{-1} L(\bar{\varphi}_\varepsilon^k, j)\right)_{\varepsilon\in J} \underset{T(k)}{\sim} \sum_{\substack{\mathfrak{a}\in\mathfrak{A}\\ \mathfrak{b}\in\mathfrak{B}}} \left\{\frac{\mathfrak{E}_{j,k}(\mathfrak{a},\mathfrak{b})}{(x^{\sigma_\mathfrak{a}})_\varepsilon^k}\right\}_{\varepsilon\in J}.$$

Il est facile de voir — cf. la démonstration de (6.2), (iii) — que les $\mathfrak{E}_{j,k}(\mathfrak{a},\mathfrak{b})$ ne dépendent pas de ε. Leur comportement sous l'action de $\mathrm{Aut}_K(\mathbb{C})$ est décrit dans (6.1). Mais les mêmes formules sont vraies pour les termes de la somme à droite, pourvu qu'on les considère comme éléments de $T\otimes_K \mathbb{C}$ et que l'on munisse T de l'action triviale de $\mathrm{Aut}_K(\mathbb{C})$. Le théorème s'en déduit immédiatement.

(9.2) Remarque. On peut redémontrer le cas $k=j=1$ du théorème (7.1) — sous la forme (7.2) — à partir de (9.1) et (5.0). En fait, grâce au lemme (4.8), il suffit de démontrer que

$$\prod_{\varepsilon\in J} x_\varepsilon \underset{K^*}{\sim} \delta \prod_{\mathfrak{a}\in\mathfrak{A}} \Lambda(\mathfrak{a}).$$

(Le produit des x_ε est effectivement bien déterminé à K^* près!) — Nous laissons au lecteur le soin de déduire cette relation de (4.10)—(4.12).

(9.3) Corollaire. *Soient* $0<\frac{k}{2}<j\leqq k$. *La conjecture de Deligne*: [9], 2.8, *est vraie pour le motif* $R_{K/\mathbb{Q}}(H_1(B)^{\otimes k})(j-k)$, *à coefficients dans* T.

Avant d'entamer la démonstration de ce corollaire, signalons que, strictement parlant, nos motifs ne rentrent pas dans le cadre de [9], dans la mesure où l'algèbre des coefficients ne sera pas toujours un corps. Evidemment, ceci n'est pas une véritable extension du cadre de Deligne, car on peut toujours décomposer B, à K-isogénie près, en produit de r variétés abéliennes de type CM sur K.

Les motifs considérés dans (9.3) sont à coefficients dans T. Pour la démonstration de (9.3), nous posons donc, *indépendemment de* k, $J=\mathrm{Hom}_K(T,\mathbb{C})$.

Dans le reste de ce paragraphe, une référence du type $\langle\cdots\rangle$ *renvoie au paragraphe indiqué de l'article* [9].

Selon $\langle 8.1\rangle$ et $\langle 8.3\rangle$, on a $M(\varphi^{-k})=H_1(B)^{\otimes k}$ (à cause de la préférence pour le Frobenius géométrique). Par conséquent — voir $\langle 2.2\rangle$ —, on a pour tout ε dans J:

$$L(\varepsilon, R_{K/\mathbb{Q}}(H_1(B)^{\otimes k}), s)=L(\varepsilon, H_1(B)^{\otimes k}, s)=L(\varphi_\varepsilon^{-k}, s)=L(\bar{\varphi}_\varepsilon^k, s+k).$$

D'après $\langle 3.1.2\rangle$, on trouve donc bien

$$L(R_{K/\mathbb{Q}}(H_1(B)^{\otimes k})(j-k))=(L(\bar{\varphi}_\varepsilon^k, j))_{\varepsilon\in J}.$$

Compte tenu de $\langle 5.1.8\rangle$ (où l'on pose $d^+=d^-=1$, selon $\langle 8.15\rangle$) et de notre théorème (9.1), le corollaire (9.3) équivaut à:

(9.4) $$c^\pm(R_{K/\mathbb{Q}}(H_1(B)^{\otimes k})) \underset{T^*}{\sim} ((x\Omega)^k, \overline{(x\Omega)^k}) \in (T\otimes_{\mathbb{Q}}\mathbb{C})^*.$$

(Le lecteur vérifiera aisément, en utilisant ⟨8.1⟩ et ⟨8.2⟩, que toutes les valeurs considérées sont critiques au sens de ⟨2.3⟩.)

Nous déduirons (9.4) de la proposition ⟨8.16⟩. Traduisons les notations utilisées par Deligne: Le poids w du motif $H_1(B)^{\otimes k}$ est $-k$. Pour $\sigma: K \hookrightarrow \mathbb{C}$ et $\tau \in \mathrm{Hom}_{\mathbb{Q}}(T, \mathbb{C})$, on trouve, d'après ⟨8.2⟩, que $n(\sigma, \tau)$ vaut $-k$ ou 0 selon que τ induit σ où $\bar{\sigma}$. Calculons maintenant la période $p'(\sigma, \tau)$ — définie en ⟨8.7⟩ — pour $n(\sigma, \tau) = -k$. Il suffit de faire ce calcul, si σ est notre plongement préféré de K dans $\mathbb{C}$; donc $\tau \in J$.

Posons

$$\eta_\tau = \coprod_{\alpha \in G} (x^\alpha)_\tau (\omega^\alpha) \in H^0(B, \Omega^1),$$

où ω est la forme différentielle de E/F choisi au § 4. Alors η_τ est défini sur le corps T_τ. Un calcul immédiat, utilisant (4.10)—(4.12), montre que, pour un idéal entier $\mathfrak{a}$ de K premier à $\mathfrak{g}$, on a

$$\tilde{\varphi}(\mathfrak{a})^* (\eta_\tau) = \varphi_\tau(\mathfrak{a}) \cdot \eta_\tau.$$

Donc η_τ est un vecteur propre pour l'action de T. En outre, on trouve facilement, pour chaque $\gamma \in H_1(B(\mathbb{C}), \mathbb{Z})$, que l'élément

$$\left(\int_\gamma \eta_\varepsilon\right)_{\varepsilon \in J} (x\Omega)^{-1} \quad \text{de} \quad (T \otimes_K \mathbb{C})^*$$

est une combinaison linéaire à coefficients dans K (non tous nuls) des $\tilde{\varphi}(\mathfrak{a}) \in T$, $\mathfrak{a}$ décrivant un ensemble $\mathfrak{A}$ comme dans (7.0). Donc

$$\left(\int_\gamma \eta_\varepsilon\right)_{\varepsilon \in J} \underset{T^*}{\sim} x\Omega.$$

En partant de ce cas particulier, et compte tenu des compatibilités avec les puissances tensorielles de toutes les constructions en jeu, on déduit finalement de ⟨8.7⟩ que

$$p'(\sigma, \tau) \underset{T^*}{\sim} (x\Omega)^{-k} \in (T \otimes_K \mathbb{C})^*.$$

Ceci démontre (9.4) pour c^+, grâce à ⟨8.16⟩; car les facteurs D_τ dans cette proposition sont négligeables dans le cas présent, selon ⟨8.17⟩.

Or, on peut déduire de ⟨8.15⟩, que la formule de ⟨8.16⟩ donne c^- aussi bien que c^+ (à ceci près que le facteur D_τ se multiplie par $(-1)^{[k:Q]/2} \in E^*$). On a en effet $H^+_{DR} = H^-_{DR}$ pour les motifs considérés en ⟨8.15⟩ (cf. ⟨1.7⟩).

Ceci achève la démonstration de (9.3).

(9.5) Remarque. Pour $k > 1$, la conjecture de Deligne que nous venons de démontrer est, en apparence, plus faible que notre théorème (9.1), si $T(k) \neq T$. Nous n'avons pas essayé d'expliciter un motif M_k, à coefficients dans $T(k)$, qui donne $H_1(B)^{\otimes k}$ par extension de l'algèbre des coefficients, ⟨2.1⟩. Un tel motif M_k existe conjecturalement, ⟨8.1⟩, (i), et la conjecture ⟨2.8⟩ pour $R_{K/\mathbb{Q}} M_k$ équivaudrait à (9.1) — cf. ⟨2.10⟩.

(9. 6) Remarque. Soit j tel que $0<j\leqq\frac{k+1}{2}$. Comme dans (7. 9), on trouve au moyen de l'équation fonctionnelle que

$$\left(\tau(\bar{\varphi}_\varepsilon^k)\, L(\varphi_\varepsilon^k, j),\ \tau(\varphi_\varepsilon^k)\, L(\bar{\varphi}_\varepsilon^k, j)\right)_{\varepsilon\in J} \underset{T(k)}{\sim} (2\pi i)^{j-k}\cdot\left((x\Omega)^k, \overline{(x\Omega)^k}\right)$$

dans $T(k)\otimes_{\mathbb{Q}}\mathbb{C}$, où $\tau(\varphi_\varepsilon^k)$, la somme de Gauss intervenant dans l'équation fonctionnelle de $L(\varphi_\varepsilon^k, s)$, s'obtient à partir de la formule pour $\tau(\psi^k)$ donnée en (7. 9) par substitution formelle de φ_ε à ψ.

Si k est impair et $L\left(\varphi_\varepsilon^k, \frac{k+1}{2}\right)\neq 0$, pour tout $\varepsilon\in J$, alors une comparaison du résultat ci-dessus avec (9. 1) donne:

$$\left(\frac{\overline{x\Omega}}{x\Omega}\right)^k \underset{T(k)^*}{\sim} \left(\tau(\varphi_\varepsilon^k)\right)_{\varepsilon\in J}.$$

Dans ce cas, (9. 1) est donc valable pour tout $j=1,\ldots,k$.

Notons en passant que l'on a l'équivalence

$$L(\varphi_\varepsilon^k, j)=0 \Leftrightarrow L(\varphi_{\varepsilon'}^k, j)=0,$$

pour tout $j=1,\ldots,k$, *pourvu que* ε et ε' soient dans le même orbite de J sous l'action de $\mathrm{Aut}_K(\mathbb{C})$. Cela se déduit des résultats de Shimura [22]; cf. ⟨2. 7⟩, ii.

(9. 7) Proposition. *Soient $j, k\in\mathbb{Z}$ avec $0<k/2<j\leqq k$. Le théorème* (7. 1) *équivaut à la conjecture de Deligne pour le motif*

$$R_{F/\mathbb{Q}}\left(H_1(E)^{\otimes k}\right)(j-k), \quad \textit{à coefficients dans } K.$$

(9. 8) Remarque. Le corollaire (9. 3) permet alors, grâce à ⟨2. 11⟩, de déduire (7. 1) de (9. 1) en passant par le formalisme de Deligne. (Cf. (9. 2)). Aussi, la compatibilité avec la conjecture de Birch et Swinnerton-Dyer (7. 8) se déduit maintenant de ⟨4⟩.

Démonstration de (9. 7). Elle est analogue à celle de (9. 3), ce qui nous permettra d'être brefs. On se ramène (en utilisant la variante (7. 2)) à l'assertion:

$$\textbf{(9. 9)} \qquad c^{\pm}\left(R_{F/\mathbb{Q}}\left(H_1(E)^{\otimes k}\right)\right) \underset{K^*}{\sim} \left(\delta\prod\left(\Lambda(\mathfrak{a})\Omega\right)^k, \bar{\delta}\prod\overline{\left(\Lambda(\mathfrak{a})\Omega\right)^k}\right).$$

Signalons que le cas $k=1$ de (9. 9) peut être vérifié directement sur la définition des $c^{\pm}$ en écrivant $\delta\prod\left(\Lambda(\mathfrak{a})\Omega\right)$ plutôt comme Ω_B, cf. (7. 3).

Pour le cas général, nous nous servirons de la proposition ⟨8. 16⟩. En effet, si τ est notre plongement préféré de K dans $\mathbb{C}$, et σ un prolongement de τ à F (qui s'identifie donc à un idéal $\mathfrak{a}$ de $\mathfrak{A}$), on trouvera $n(\sigma,\tau)=-k$, et

$$p'(\sigma,\tau) \underset{F^*}{\sim} \left(\int_{\gamma_\sigma}\omega^\sigma\right)^{-k} \underset{K^*}{\sim} \left(\Lambda(\mathfrak{a})\Omega\right)^{-k},$$

où $\gamma_\sigma\in H_1\left(E^\sigma(\mathbb{C}),\mathbb{Z}\right)$ est arbitraire, et ω notre modèle de E/F. En prenant le produit sur les σ, l'expression sera bien déterminée à K^* près.

Finalement, c'est un exercice facile à partir de ⟨8. 15⟩ (cf. aussi ⟨8. 17⟩) de montrer que $D_\tau \underset{K^*}{\sim} \delta^{-1} \underset{K^*}{\sim} \delta$ dans cette application de ⟨8. 16⟩.

§ 10. Intégralité des valeurs spéciales de fonctions L

Nous voulons appliquer ici les résultats du paragraphe 3 et trouver des dénominateurs explicites pour certains des nombres algébriques introduits dans la deuxième partie de ce papier.

Les notations sont celles des paragraphes précédents. Rappelons que pour toute extension algébrique M de $\mathbb{Q}$, $\mathfrak{o}_M$ désigne l'anneau des entiers de M. Nous reprenons alors l'hypothèse:

(3. 0) $$g_2, g_3 \in 4\mathfrak{o}_F,$$

où g_2 et g_3 sont les constantes du modèle de Weierstrass (2. 0) de la courbe E/F. Nous noterons $\mathfrak{f}$ l'idéal entier de K qui est le p.p.c.m. des conducteurs des caractères φ et du conducteur de l'extension abélienne F/K; nous désignerons par f le plus petit entier strictement positif contenu dans $\mathfrak{f}$. En particulier, tout idéal $\mathfrak{g}$ considéré jusqu'à présent, est divisible par $\mathfrak{f}$: mais nous n'utiliserons dans ce paragraphe que des idéaux $\mathfrak{g}$ vérifiant de plus les hypothèses supplémentaires suivantes:

(10. 0) $\mathfrak{g}$ *est divisible par au moins deux nombres premiers rationnels distincts;* $\mathfrak{g}\mathfrak{f}^{-1}$ *est sans facteurs carrés.*

Nous allons naturellement utiliser la décomposition (5. 7) des séries L partielles en séries d'Eisenstein: les coefficients figurant dans (5. 7) introduisent des dénominateurs que nous allons étudier immédiatement.

Pour tout idéal $\mathfrak{g}$ comme ci-dessus, nous avons:

(10. 1) $$\frac{\Omega}{\rho} \in K^* \quad \text{et} \quad \frac{\Omega}{\rho}\mathfrak{o} = \frac{\mathfrak{g}}{\mathfrak{h}},$$

où ρ est attaché à $\mathfrak{g}$ comme dans la proposition (5. 5) et où $\mathfrak{h}$ est un idéal entier de K *premier à* $\mathfrak{g}$.

Pour tout idéal entier $\mathfrak{a}$ de K premier à $\mathfrak{g}$, l'invariant $\Lambda(\mathfrak{a})$ introduit en (4. 10) vérifie:

$$\Lambda(\mathfrak{a})^{12}\mathfrak{o}_F = \Delta(L)^{(1-\sigma_{\mathfrak{a}})}\mathfrak{a}^{12}\mathfrak{o}_F,$$

où L est le réseau complexe attaché au modèle de Weierstrass choisi. Cette propriété résulte de [12], **12** § 2 et de l'homogénéité de Δ. Nous ferons désormais l'**hypothèse** fondamentale suivante:

(10. 2) *Il existe un modèle de Weierstrass de* E/F *tel que, si* L *désigne le réseau associé à ce modèle, l'idéal* $\Delta(L)\mathfrak{o}_F$ *soit invariant sous l'action de* $\mathrm{Gal}(F/K)$.

(10. 3) Remarques. i) Si (10. 2) est vérifiée, il est trivialement possible de trouver un modèle de Weierstrass de E/F satisfaisant à (10. 2) et (3. 0) simultanément. Nous choisissons un tel modèle pour toute la suite de ce paragraphe.

ii) Si la courbe E/F a un modèle de Weierstrass minimal, l'hypothèse (10. 2) est vérifiée: soit en effet $\mathfrak{L}$ le réseau associé à ce modèle minimal. D'après [11] (2. 1), $\Delta(\mathfrak{L})\mathfrak{o}_F$ dépend uniquement du Grössencharakter ψ, qui est ici le même pour toutes les courbes conjuguées E^a; donc:

$$\Delta(\mathfrak{L}_a)\mathfrak{o}_F = \Delta(\mathfrak{L})\mathfrak{o}_F,$$

et (10. 2) est vérifiée.

On trouvera dans [11] la construction de modèles minimaux de Weierstrass pour certaines «$\mathbb{Q}$-courbes». Nous ne connaissons pas pour l'instant de courbes satisfaisant aux conditions de (4.1), mais pas à l'hypothèse (10.2): en fait, nous ne connaissons pas d'exemples de courbes satisfaisant (4.1), mais n'ayant pas d'équation minimale de Weierstrass.

Sous l'hypothèse (10.2) nous avons donc:

(10.4) $$\Lambda(\mathfrak{a})\,\mathfrak{o}_F = \mathfrak{a}\,\mathfrak{o}_F.$$

Rappelons maintenant que, pour tout Grössencharakter α de K, nous notons $K(\alpha)$ le corps des valeurs de α. D'après (4.9), tout idéal entier $\mathfrak{a}$ de K, premier au conducteur de φ, vérifie:

(10.5) $$\varphi(\mathfrak{a})\cdot \mathfrak{o}_{K(\varphi)} = \mathfrak{a}\,\mathfrak{o}_{K(\varphi)}.$$

Nous sommes maintenant en mesure d'expliciter les résultats annoncés. Nous rappelons que n est le degré de F sur K; nous notons $\tilde{F}$ le corps obtenu en rajoutant à F une racine quatrième de f et le groupe des racines quatrièmes de l'unité. (D'après (7.4), 3, on peut effectivement remplacer, dans ce qui suit, $\tilde{F}$ par une extension «très petite» de K.) D'autre part, nous abandonnons la convention (5.1) et notons précisément $L_{\mathfrak{f}}$ (resp. $L_{\mathfrak{g}}$) la fonction L (non nécessairement primitive) relative à des caractères modulo $\mathfrak{f}$ (resp. $\mathfrak{g}$). Nous avons alors:

(10.6) Proposition. $f^{\frac{5}{4}n}\Omega^{-n}L_{\mathfrak{f}}(\bar{\psi}, 1) \in \mathfrak{f}^{-n}\mathfrak{o}_{\tilde{F}}$.

Démonstration. Les corollaires (3.2) et (5.7), *appliqués à* $\mathfrak{f}$, montrent que, pour tout idéal $\mathfrak{a}$ entier de K, premier à $\mathfrak{f}$:

$$f^{\frac{5}{4}}\frac{\varphi(\mathfrak{a}\mathfrak{b})}{(\Lambda(\mathfrak{a})\rho)}L(\bar{\varphi}, \sigma_{\mathfrak{a}\mathfrak{b}}, 1)$$

est un entier algébrique. Notons que, ici, $\rho \in \mathfrak{f}^{-1}L \smallsetminus L$ est tel que (10.1) s'applique avec $\mathfrak{g}$ remplacé par $\mathfrak{f}$. Nous déduisons alors de (10.4) et de (10.5) que

$$\det_{\mathfrak{a}_1, \mathfrak{a}_2 \in \mathfrak{A}}\left(f^{5/4}\Omega^{-1}L(\bar{\varphi}, \sigma_{\mathfrak{a}_1\mathfrak{a}_2\mathfrak{b}}, 1)\right) \in \mathfrak{f}^{-n}\mathfrak{o}_{\tilde{F}},$$

pour un ensemble $\mathfrak{A}$ comme dans (7.0). D'après (5.4), ceci est exactement le résultat souhaité.

Nous aurons besoin pour la suite de définir un nouvel invariant.

(10.7) Définition. Soit k un entier $\geqq 1$ et soit S l'ensemble des places de K divisant $\mathfrak{f}$. Nous notons $\mathfrak{w}_k(E/F)$ le plus grand idéal entier $\mathfrak{h}$ de K (au sens de la divisibilité) tel que:

i) Les diviseurs premiers de $\mathfrak{h}$ appartiennent à S.

ii) $$G\big(F(E_{\mathfrak{h}})/F\big)^k = 1.$$

Remarquons que cet idéal est l'analogue de la S-partie de l'invariant cyclotomique introduit dans [4], page 293.

Une autre façon de formuler cette définition est donnée par le lemme suivant:

(10.8) Lemme. *L'idéal* $\mathfrak{w}_k(E/F)$ *est le p.g.c.d. de l'ensemble*

$$\{\psi^k(\mathfrak{P}) - 1;\ \ \mathfrak{P} \text{ idéal premier de } F,\ \ \mathfrak{P} \nmid \mathfrak{f}\}.$$

Démonstration. Par définition de $\mathfrak{w}_k(E/F)$, $\mathfrak{p}^e$ divise $\mathfrak{w}_k(E/F)$ (pour un entier $e \geqq 1$ et un idéal premier $\mathfrak{p}$ de S) si et seulement si $\sigma^k = 1$ pour tout élément $\sigma \in G(F(E_{\mathfrak{p}^e})/F)$; donc, par la loi de réciprocité d'Artin, si et seulement si $(\mathfrak{P}, F(E_{\mathfrak{p}^e})/F)^k = 1$, pour tout idéal premier $\mathfrak{P}$ de F ne divisant pas $\mathfrak{f}$. Notons que ce symbole d'Artin $(\mathfrak{P}, F(E_{\mathfrak{p}^e})/F)$ est bien défini puisque $\mathfrak{p} \in S$. Or, l'action du symbole d'Artin $(\mathfrak{P}, F(E_{\mathfrak{p}^e})/F)$ sur un point $\xi(\rho, L)$ de $\mathfrak{p}^e$-torsion est donnée par

$$\xi(\rho, L)^{(\mathfrak{P}, F(E_{\mathfrak{p}^e})/F)} = \xi(\psi(\mathfrak{P})\rho, L);$$

donc $\mathfrak{p}^e$ divise $\mathfrak{w}_k(E/F)$ si et seulement si $\psi^k(\mathfrak{P})$ est congru à 1 modulo $\mathfrak{p}^e$, i.e. si et seulement si $\mathfrak{p}^e$ divise $\psi^k(\mathfrak{P}) - 1$, pour tout idéal premier $\mathfrak{P}$ de F, ne divisant pas $\mathfrak{f}$.

Nous avons alors le résultat suivant:

(10. 9) Proposition. *Sous les hypothèses* (3. 0) *et* (10. 2),

$$(\sqrt{d_K})^n \Omega^{-2n} L_{\mathfrak{f}}(\bar{\psi}^2, 2) \in \mathfrak{w}_2^{-1}(E/F)\mathfrak{f}^{-2n}\mathfrak{o}_F.$$

Démonstration. Pour tout idéal $\mathfrak{g}$ vérifiant (10. 0), nous avons, grâce à (3. 3) et (5. 7) que

$$\sqrt{d_K}\frac{\varphi^2(\mathfrak{ab})}{(\Lambda(\mathfrak{a})\rho)^2} L(\bar{\varphi}^2, \sigma_{\mathfrak{ab}}, 2)$$

est un entier algébrique; ici ρ vérifie (10. 1). Donc, comme dans la démonstration de (10. 6),

$$(\sqrt{d_K})^n \Omega^{-2n} L_{\mathfrak{g}}(\bar{\psi}^2, 2) \in \mathfrak{g}^{-2n}\mathfrak{o}_F.$$

Or

$$L_{\mathfrak{f}}(\bar{\psi}^2, 2) = \prod_{\substack{\mathfrak{P}|\mathfrak{g} \\ \mathfrak{P}\nmid\mathfrak{f}}} \left(\frac{\psi^2(\mathfrak{P})}{\psi^2(\mathfrak{P}) - 1}\right) \cdot L_{\mathfrak{g}}(\bar{\psi}^2, 2).$$

D'autre part, puisque $\frac{\mathfrak{g}}{\mathfrak{f}}$ est sans facteurs carrés $\prod_{\substack{\mathfrak{P}|\mathfrak{g} \\ \mathfrak{P}\nmid\mathfrak{f}}} \psi^2(\mathfrak{P})$ engendre $\left(\frac{\mathfrak{g}}{\mathfrak{f}}\right)^{2n}$.

Donc, pour tout $\mathfrak{g}$ vérifiant (10. 0),

$$\prod_{\substack{\mathfrak{P}|\mathfrak{g} \\ \mathfrak{P}\nmid\mathfrak{f}}} (\psi^2(\mathfrak{P}) - 1) \sqrt{d_K^n}\, \Omega^{-2n} L_{\mathfrak{f}}(\bar{\psi}^2, 2) \in \mathfrak{f}^{-2n}\mathfrak{o}_F,$$

ce qui conduit clairement, par le lemme (10. 8), au résultat annoncé.

Des démonstrations tout à fait analogues à celles des propositions (10. 6) et (10. 9) conduisent, en utilisant cette fois le corollaire (3. 4), puis la proposition (3. 5), aux résultats suivants:

(10. 10) Proposition. *Soit* $k \geqq 3$. *Alors*

$$(k-1)!^n \Omega^{-kn} L_{\mathfrak{f}}(\bar{\psi}^k, k) \in \mathfrak{w}_k^{-1}(E/F)\mathfrak{f}^{-kn}\mathfrak{o}_F.$$

(10.11) Proposition. *Soit* (j, k) *un couple d'entiers tel que* $0 < \frac{k}{2} < j < k$.

a) *Si* $2j \neq k+2$, *on a*

$$(j-1)!^n \left\{4\pi i \frac{f^{5/4}}{N\mathfrak{f}}\right\}^{n(k-j)} \Omega^{-kn} L_{\mathfrak{f}}(\bar{\psi}^k, j) \in \mathfrak{w}_k^{-1}(E/F)\mathfrak{f}^{-kn}\mathfrak{o}_F.$$

b) *Si* $2j=k+2$, *on a*

$$(j-1)!^n \sqrt{d_K^n} \left\{4\pi i \frac{f^{5/4}}{N\mathfrak{f}}\right\}^{n(k-j)} \Omega^{-kn} L_{\mathfrak{f}}(\bar{\psi}^k, j) \in \mathfrak{w}_k^{-1}(E/F)\mathfrak{f}^{-kn}\mathfrak{o}_{\mathfrak{F}}.$$

(10.12) Remarque. Quand l'idéal $\mathfrak{f}$ est déjà divisible par deux premiers rationnels distincts, on peut prendre $\mathfrak{f}=\mathfrak{g}$ dans (10. 0), ce qui permet de supprimer les idéaux $\mathfrak{w}_k(E/F)$ dans les énoncés (10. 9), (10. 10) et (10. 11).

Références

[1] *N. Arthaud*, On Birch and Swinnerton-Dyer's conjecture for elliptic curves with complex multiplication. I, Compos. Math. **37** (1978), 209—232; II, Ph. D. thesis, Stanford University 1978.

[2] *B. J. Birch* et *H. P. F. Swinnerton-Dyer*, Notes on elliptic curves. II, J. reine angew. Math. **218** (1965), 79—108.

[3] *J. W. S. Cassels*, A note on the division values of $\wp(u)$, Proc. Cambr. Phil. Soc. **45** (1949), 167—172.

[4] *J. Coates*, p-adic L-functions and Iwasawa's theory, dans: A. Fröhlich (ed.), Algebraic Number Fields (Proceedings), New York-London 1977.

[5] *J. Coates*, Arithmetic on elliptic curves with complex multiplication, Hermann Weyl lectures, I.A.S. Princeton (1979); à paraître dans Ann. Math. Studies.

[6] *J. Coates* et *A. Wiles*, On the conjecture of Birch and Swinnerton-Dyer, Inventiones Math. **39** (1977), 223—251.

[7] *J. Coates* et *A. Wiles*, On p-adic L-functions and elliptic units, J. Austr. Math. Soc. **26** (1978), 1—25.

[8] *R. M. Damerell*, L-functions of elliptic curves with complex multiplication. I, Acta Arithm. **17** (1970), 287—301; II, Acta Arithm. **19** (1971), 311—317.

[9] *P. Deligne*, Valeurs de fonctions L et périodes d'intégrales, dans: Proceedings of Symposia in Pure Mathematics (AMS) **33** (1979), part 2, 313—346.

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

[11] *B. Gross*, Minimal models for elliptic curves with complex multiplication, à paraître.

[12] *S. Lang*, Elliptic functions, Reading, Mass. 1973.

[13] *S. Lang*, Cyclotomic Fields. I, Berlin-Heidelberg-New York 1978.

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

[15] *G. Robert*, Nombres de Hurwitz et unités elliptiques, Ann. Sci. E.N.S. (4e sér.) **11** (1978), 297—389.

[16] *J. P. Serre*, Abelian l-adic representations and elliptic curves, New York-Amsterdam 1968.

[17] *J. P. Serre*, Corps Locaux, 2e éd., Paris 1968.

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

[19] *G. Shimura*, Introduction to the arithmetic theory of automorphic functions, Princeton 1971.

[20] *G. Shimura*, On some arithmetic properties of modular forms of one and several variables, Ann. of Math. **102** (1975), 491—515.

[21] *G. Shimura*, The special values of the zeta functions associated with cusp forms, Comm. on Pure and Appl. Math. **29** (1976), 783—804.

[22] *G. Shimura*, On the periods of modular forms, Math. Ann. **229** (1977), 211—221.

[23] *M. Waldschmidt*, Nombres transcendants et groupes algébriques, Astérisque **69/70** (1979).

[24] *A. Weil*, Adeles and algebraic groups, Princeton 1961.

[25] *A. Weil*, Basic number theory, 3rd ed., Berlin-Heidelberg-New York 1974.

[26] *A. Weil*, Elliptic Functions according to Eisenstein and Kronecker, Berlin-Heidelberg-New York 1976.

Mathématiques, Bât. 425, Université de Paris-Sud, Centre d'Orsay, F-91405 Orsay, Cédex

Mathematisches Institut der Universität Göttingen, Bunsenstr. 3—5, D-3400 Göttingen

Eingegangen 29. Januar 1981