Bull. Soc. math. France,
125, 1997, p. 249–267.

AMÉLIORATION D'UNE CONGRUENCE POUR CERTAINS ÉLÉMENTS DE STICKELBERGER QUADRATIQUES

PAR

Abdelmejid BAYAD et Gilles ROBERT (*)

Résumé. — Nous prouvons une relation de distribution additive, à coefficients racines de l'unité, entre fonctions elliptiques de seconde espèce (*cf.* § 4, th. 1). Cette relation, déjà notée par F.G. Frobenius [7], est de nature algébrique et nous permet d'améliorer (*cf.* § 5) les congruences pour les éléments de Stickelberger quadratiques de [3].

Abstract. — We improve (*cf.* § 5) on certain congruences for quadratic Stickelberger elements, as proved in [3]. For this we observe (*cf.* § 4, th. 1) the existence of a distribution relation – additive with coefficients roots of unity – between simple quotients, introduced in §§ 2–3, of the Klein function of [12] for distinct complex lattices. This distribution relation, first noted by F.G. Frobenius [7], has an algebraic nature.

Introduction

Les fonctions elliptiques de seconde espèce D, de diviseur $(\varphi) - (0)$ relativement à un réseau Λ pour (φ modulo Λ) un point de torsion non trivial dans $\mathbb{C}/\Lambda$, ont fait de nombreuses apparitions en théorie des nombres. L'ordre de (φ modulo Λ) sera noté p, et on observera que le réseau complexe Ω de périodes de la fonction D ci-dessus est alors l'unique sous-réseau de Λ tel que :

i) le point φ reste d'ordre p modulo Ω ;

(*) Texte reçu le 16 septembre 1996, accepté le 21 mars 1997.
A. Bayad, Université d'Évry, Département de Mathématiques, Bd. des Coquibus, 91025 Évry Cedex (France).
Email : bayad@lami.univ-evry.fr.
G. Robert, Université de Grenoble-I, Institut Fourier, UFR de Mathématiques, B.P. 74, 38402 St. Martin d'Hères Cedex (France).
Email : grobert@fourier.ujf-grenoble.fr.
Classification AMS : 11 G 05, 11 R 33.

ii) le quotient Λ/Ω est cyclique d'ordre p.

On désigne alors par E la courbe elliptique isomorphe à $\mathbb{C}/\Omega$ par le plongement de Weierstrass.

Quoique nous les regardions ici du seul point de vue complexe, les fonctions D sont algébriques en nature ; par exemple, pour définir l'accouplement de Weil, qui associe algébriquement à deux points de p-torsion de E une racine p-ième de l'unité, on fait appel à une fonction D du type ci-dessus, *cf. e.g.* D. Husemöller [9, chap. 12, p. 229].

Bien auparavant, elles ont été étudiées par Ch. Hermite [8] et G.F. Frobenius [7] ; ce dernier la note q. Dans les temps récents leur réapparition est liée à trois thèmes :

i) structure galoisienne et construction de bases d'entiers [5], [18] ;

ii) l'étude de résolvantes elliptiques, analogues aux sommes de Gauss : cette étude, pour certaines courbes elliptiques, a fourni des décompositions de leur discriminant à l'aide d'éléments de Stickelberger « quadratiques » *cf.* [3], [1] et [4] ;

iii) d'autres questions de nature plus variée *cf.* [10], [6], [11], et en particulier l'étude [2] par l'un des auteurs de la loi de réciprocité quadratique au-dessus d'un corps quadratique imaginaire.

Cette bibliographie ne prétend pas à l'exhaustivité ; pour $p \geq 3$, c'est S.P. Chan qui semble la première personne à les avoir reconsidéré et à en avoir étudié certaines valeurs particulières, *cf.* [5] déjà cité.

Un problème posé par leur usage récent est que faute de normalisation convenable, beaucoup de ces auteurs ont utilisé les quotients en deux valeurs particulières pour obtenir des quantités algébriques. Mais, *lorsque le corps de base peut être plongé dans* $\mathbb{C}$, une normalisation des fonctions D parfaitement canonique et algébrique existe : il suffit de demander au coefficient principal de son développement en série de Laurent, au voisinage du point $z = 0$, d'être égal à 1 ; *cf. e.g.* les commentaires que l'on trouve dans le § 1 de D. Kubert [11].

De notre point de vue, nous avons rencontré la nécessité de cette normalisation en tentant de comprendre le lien algébrique caché derrière les constructions analytiques des §§ 3 et 4 du texte déjà cité [3] de A. Bayad, W. Bley et Ph. Cassou-Noguès. Rappelons que celui-ci fait suite aux travaux [4] et [1] où d'abord Ph. Cassou-Noguès et M.J. Taylor explorent le cas $p = 2$ et où ensuite l'un des auteurs du présent travail, dans sa thèse, explore en partie le cas p premier quelconque.

Ceci nous a conduit à la preuve d'une relation de distribution additive, à coefficients racines de l'unité, satisfaite par ces fonctions D. *Celle-ci est*, à notre avis, *très belle.* Elle n'avait pas échappé à la sagacité de

F.G. Frobenius *cf. loc. cit.* [7, p. 91]. Grâce à elle on peut en particulier écrire les *résolvantes elliptiques*, telles qu'elles apparaissent dans [3], [1] ou [4], *comme une valeur particulière* d'une seule fonction elliptique D (de seconde espèce).

Le texte ci-dessous a donc un double objectif :

a) À partir des relations bien connues satisfaites par la fonction de Klein, *cf.* D. Kubert et S. Lang [12, chap. 2], donner une écriture *explicite* de la fonction D *normalisée*; contrairement à ses expressions [5] et [1] à l'aide des fonctions $\mathcal{P}$ et $\mathcal{P}'$ de Weierstrass, celle-ci est extrêmement simple, *cf.* ci-dessous § 2.

Puis prouver, dans la foulée, *la relation de distribution* que nous avons, après F.G. Frobenius, *redécouverte*. Les raisonnements restent élémentaires, *cf.* th. 1, § 4.

b) Utiliser cette relation de distribution dans le texte cité [3], qui nous avait servi de point de départ, *cf.* §5 ; plusieurs résultats de *loc. cit.* s'y trouvent nettement simplifiés, *cf.* th. 7 et 8. Dans ce paragraphe 5, nous renvoyons à [3] pour certaines notations un peu compliquées. En passant, on y améliore aussi un résultat de [4].

Pour cela dès le début, tant pour la fonction D que pour le point z_0, nos notations sont adaptées à celles utilisées dans [3].

Contenu.

Le paragraphe 1 contient quelques rappels ; le paragraphe 2 la définition et l'écriture explicite de la fonction D à l'aide de la fonction de Klein ; le paragraphe 3 est préparatoire ; la relation de distribution est prouvée dans le paragraphe 4 ; le paragraphe 5 simplifie certains résultats de [3].

Remerciements.

Nous remercions nos rapporteurs pour leurs commentaires et leurs critiques qui nous ont aidé à rendre plus pertinent ce travail.

1. Rappels

a) Soit $\mathbb{C}$ muni d'un réseau L ; si (w_1, w_2) désigne une base de L telle que $\mathrm{Im}(w_1/w_2) > 0$, on définit l'aire de L par

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

c'est un réel > 0 indépendant du choix de la base orientée (w_1, w_2) de L.

On définit alors la forme hermitienne

$$H_L(u,v) = \frac{\bar{u}v}{a(L)}, \quad (u,v) \in \mathbb{C} \times \mathbb{C},$$

et l'on pose $E_L = \operatorname{Im} H_L$ de sorte que

$$E_L(u,v) = \frac{1}{2i}\frac{\bar{u}v - \bar{v}u}{a(L)}, \quad (u,v) \in \mathbb{C} \times \mathbb{C}.$$

Notons que E_L est une forme $\mathbb{R}$-linéaire alternée ; ses valeurs sur $L \times L$ sont entières, et elle vaut -1 sur toutes les bases (w_1, w_2) de L telles que $\operatorname{Im}(w_1/w_2) > 0$.

On pose :

$$e(x) = \mathrm{e}^{2\pi i x}, \quad x \in \mathbb{C}.$$

Soit n un entier. Composant la restriction de E_L à $\frac{1}{n}L \times \frac{1}{n}L$ avec la fonction exponentielle

$$e(-nx) = \mathrm{e}(x)^{-n},$$

on en déduit une application bilinéaire alternée

$$e_n^L : \Big(\frac{1}{n}L/L\Big) \times \Big(\frac{1}{n}L/L\Big) \longrightarrow \boldsymbol{\mu}_n.$$

Il s'agit de la version analytique de l'accouplement de Weil, pour le tore complexe

$$E(\mathbb{C}) = \mathbb{C}/L,$$

cf. e.g. [13, chap. 18], [14, § 20] ou [9, chap. 12]. On a donc :

Définition 1. — Pour deux points λ et μ de $\frac{1}{n}L/L$, on note encore λ et μ des relèvements de ceux-ci dans $\frac{1}{n}L$, et on pose :

$$e_n^L(\lambda,\mu) = e\big(-nE_L(\lambda,\mu)\big) = e\Big(\frac{1}{n}E_L(n\lambda, -n\mu)\Big);$$

il s'agit d'une racine n-ième de l'unité, qui dépend de manière bilinéaire alternée du couple (λ, μ).

Remarque 2. — Pour $M \subset N$ deux réseaux complexes, on a :

$$a(N) = [N : M]^{-1} a(M)$$

et donc

$$E_N = [N : M] E_M$$

où $[N : M]$ désigne le nombre d'éléments de N/M.

b) On note ici $\mathcal{K}_L$ la fonction de Klein, étudiée par de nombreux auteurs au cours de ces dernières années notamment D. Kubert et S. Lang, *cf.* [12], [11] et [17].

Si $P(q)$, pour $|q| < 1$, désigne la valeur du produit infini convergent

$$\prod_{n=1}^{\infty}(1-q^n),$$

la fonction $\mathcal{K}_L(u)$ peut être définie *cf. e.g.* [16, § 1, p. 7–8], [20, chap. IV, formule (26)] et [12, chap. 2, § 1], par la série

$$\begin{aligned}(1)\qquad &\frac{2\pi}{w_2}e\Big(\frac{1}{8}\frac{w_1}{w_2}\Big)\Big[P\Big(e\Big(\frac{w_1}{w_2}\Big)\Big)\Big]^3\mathcal{K}_L(u)\\ &\quad = e\Big(\frac{u^2-u\bar{u}}{4ia(L)}\Big)\sum_{x\in\mathbb{Z}} e\Big[\frac{1}{2}\Big(x+\frac{1}{2}\Big)^2\frac{w_1}{w_2}+\Big(x+\frac{1}{2}\Big)\Big(\frac{u}{w_2}-\frac{1}{2}\Big)\Big],\end{aligned}$$

pour $u \in \mathbb{C}$ et (w_1, w_2) une base de L telle que $\mathrm{Im}(w_1/w_2) > 0$; elle est plus communément décrite par le produit infini

$$(2)\qquad \mathcal{K}_L(u) = u\,\mathrm{e}^{-\frac{1}{2}uu^*}\prod_{\substack{\ell\in L\\ \ell\neq 0}} \mathrm{e}^{\frac{u}{\ell}+\frac{1}{2}\left(\frac{u}{\ell}\right)^2}\Big(1-\frac{u}{\ell}\Big)$$

où, écrivant $u = a_1w_1 + a_2w_2$ avec $a_1, a_2 \in \mathbb{R}$, on note

$$u^* = a_1\eta_1 + a_2\eta_2$$

pour η_1 et η_2 les périodes de « deuxième espèce » associées aux périodes de « première espèce » w_1 et w_2. L'application $u \mapsto uu^*$ et donc d'après (2) la fonction $u \mapsto \mathcal{K}_L(u)$ ne dépend pas du choix de la base (w_1, w_2) de L, telle que $\mathrm{Im}(w_1/w_2) > 0$.

En fait, d'après (1), la fonction

$$(3)\qquad \theta_L : u \underset{\text{déf}}{\longmapsto} e\Big(\frac{1}{4i}H_L(u,u)\Big)\mathcal{K}_L(u)$$

est une fonction thêta associée au réseau L et est donc holomorphe ; son diviseur est $(0 \bmod L)$: seuls les points de L sont des zéros de cette fonction ; ceux-ci sont simples, *cf.* par exemple l'écriture (2).

Une autre écriture de θ_L peut être donnée, que nous citons pour future référence :

REMARQUE 3. — Posons $\tau = w_1/w_2$, $q = e(\tau)$ et $z^{1/2} = e(u/2w_2)$. Alors, on a :

$$\theta_L(u) = -\frac{w_2}{2\pi i}\frac{1}{[P(q)]^2} z^{-1/2}\, e\Big(\frac{1}{2(\tau-\overline{\tau})}\Big(\frac{u}{w_2}\Big)^2\Big)\theta_q(z)$$

avec *cf.* [1, chap. III, § 2],

$$\theta_q(z) = (1-z)\prod_{n\geq 1}(1-q^n z)(1-q^n z^{-1}).$$

De plus, on a :

PROPOSITION 4. — *Pour tout $\rho \in L$, on a :*

$$\mathcal{K}_L(u+\rho) = \chi_L(\rho) e\big(\tfrac{1}{2}E_L(\rho,u)\big)\mathcal{K}_L(u)$$

où l'on a posé

$$\chi_L(\rho) = \begin{cases} 1 & \textit{si } \rho \in 2L, \\ -1 & \textit{si } \rho \in L\setminus 2L. \end{cases}$$

REMARQUE 5. — Pour tous ρ et σ éléments de L, on a :

$$\chi_L(\rho+\sigma) = \chi_L(\rho)\chi_L(\sigma) e\big(\tfrac{1}{2}E_L(\rho,\sigma)\big),$$

de sorte que θ_L, *cf.* (3) ci-dessus, est une fonction thêta réduite de type (H_L, χ_L) au sens de A.Weil [19, chap. VI].

Enfin, la fonction $\mathcal{K}_L(u)$ admet u pour partie principale quand u tend vers 0 :

LEMME 6. — *On a* $\lim_{u\to 0}\mathcal{K}_L(u)/u = 1$.

2. Les fonctions D_Ω de poids p

On note $\Omega \subset \mathbb{C}$ le réseau des périodes complexes d'une courbe elliptique E et on fixe un isomorphisme

$$E(\mathbb{C}) \xrightarrow{\sim} \mathbb{C}/\Omega$$

par lequel nous identifions les deux membres.

Soit p un entier > 1. On note

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

un sous-groupe cyclique d'ordre p du groupe $E[p]$ des points de p-torsion de E, de générateur fixé ψ.

On désigne par φ un autre point de p-torsion de E, vérifiant $\varphi \notin \langle\psi\rangle$.

REMARQUE 1. — La condition ci-dessus $\varphi \notin \langle\psi\rangle$ suffit ; elle est moins stricte que celle implicite dans l'introduction, qui s'énoncerait « le couple (φ, ψ) est une base de $E[p]$ » ; lorsque p est premier, ces deux conditions sont équivalentes (c'est le cas du § 5, à partir de la remarque 4).

De ce fait, si l'ordre de φ est un diviseur strict de p, le réseau Ω ne coïncide pas avec le réseau de toutes les périodes de la fonction $D_\Omega(z; \varphi, \langle\psi\rangle)$ définie ci-dessous ; *cf. e.g.* § 4, cor. 2.

Le théorème d'Abel-Jacobi de la théorie des fonctions elliptiques, *cf. e.g.* [13], prouve alors l'existence d'une fonction non triviale

$$D_\Omega(z; \varphi, \langle\psi\rangle), \quad z \in \mathbb{C},$$

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

$$\sum_{\rho \in \langle\psi\rangle} (\varphi + \rho) - (\rho). \tag{1}$$

On normalise D_Ω en exigeant que

$$\lim_{z \to 0} z D_\Omega\big(z; \varphi, \langle\psi\rangle\big) = 1. \tag{2}$$

Il vient :

PROPOSITION 2. — *On a*

$$D_\Omega\big(z; \varphi, \langle\psi\rangle\big) = e\big(\tfrac{1}{2} E_\Lambda(z, -\varphi)\big) \frac{\mathcal{K}_\Lambda(z - \varphi)}{\mathcal{K}_\Lambda(z)\mathcal{K}_\Lambda(-\varphi)} \tag{3}$$

où $\mathcal{K}_\Lambda$ désigne la fonction de Klein associée au réseau $\Lambda = \Omega + \mathbb{Z}\psi$.

Démonstration. — Soit $\widetilde{D_\Omega}$ le m.d.d. de l'égalité (3) de la proposition. Il résulte des rappels sur la fonction de Klein (*cf.* § 1, formule (3)) et de l'égalité $E_\Lambda = \operatorname{Im} H_\Lambda$, que $\widetilde{D_\Omega}$ est proportionnel à la fonction méromorphe

$$z \longmapsto e\Big(\frac{1}{2i} H_\Lambda(\varphi, z)\Big) \theta_\Lambda(z - \varphi)/\theta_\Lambda(z);$$

de plus, d'après le § 1, prop. 4, on a :

$$\widetilde{D_\Omega}(z + \rho) = e\big(E_\Lambda(\rho, -\varphi)\big)\widetilde{D_\Omega}(z) \tag{4}$$

pour tout $\rho \in \Lambda$.

Or on a $E_\Lambda = pE_\Omega$ (*cf.* § 1, rem. 2), de sorte que

$$e\big(E_\Lambda(\rho,-\varphi)\big) = e(-pE_\Omega(\rho,\varphi)\big) = e_p^\Omega(\rho,\varphi) \tag{5}$$

où e_p^Ω est l'accouplement de Weil

$$\frac{1}{p}\Omega/\Omega \times \frac{1}{p}\Omega/\Omega \longrightarrow \boldsymbol{\mu}_p.$$

En particulier, si ρ appartient à Ω, l'identité (4) prouve que la fonction $\widetilde{D_\Omega}$ est invariante par translation par ρ : ainsi $z \mapsto \widetilde{D_\Omega}(z)$ est une fonction elliptique de réseau de périodes Ω.

De plus, son diviseur modulo Ω est bien le diviseur (1) demandé pour la fonction

$$z \longmapsto D_\Omega\big(z;\varphi,\langle\psi\rangle\big).$$

Enfin, comme $\lim\limits_{z\to 0} \mathcal{K}_\Lambda(z)/z = 1$, *cf.* § 1, lemme 6, on a

$$\lim_{z\to 0} z\widetilde{D_\Omega}(z) = 1$$

ce qui complète la preuve de l'identité (3), et donc de la proposition 2.

Corollaire 3. — *On a :*

i) $D_\Omega\big(-z;-\varphi,\langle\psi\rangle\big) + D_\Omega\big(z;\varphi,\langle\psi\rangle\big) = 0$;

ii) $D_\Omega\big(z;\varphi+\psi,\langle\psi\rangle\big) = D_\Omega\big(z;\varphi,\langle\psi\rangle\big)$.

Les relations (4) et (5) assurent également :

Proposition 4. — *Pour tout $\rho \in \langle\psi\rangle$, on a :*

$$\frac{D_\Omega\big(z+\rho;\varphi,\langle\psi\rangle\big)}{D_\Omega\big(z;\varphi,\langle\psi\rangle\big)} = e_p^\Omega(\rho,\varphi).$$

Par ailleurs, vu la formule explicite en termes de $\mathcal{K}_\Lambda$ donnée dans [12, chap. 2, § 6, p. 51–52] pour la différence

$$\mathcal{P}_\Lambda(z) - \mathcal{P}_\Lambda(\varphi),$$

où $\mathcal{P}_\Lambda$ désigne la fonction $\mathcal{P}$ de Weierstrass du réseau $\Lambda = \Omega + \mathbb{Z}\psi$, on a aussi :

COROLLAIRE 5. — *Si* $\Lambda = \Omega + \mathbb{Z}\psi$, *on a :*

$$D_\Omega\big(z;\varphi,\langle\psi\rangle\big)D_\Omega\big(z;-\varphi,\langle\psi\rangle\big) = \mathcal{P}_\Lambda(z) - \mathcal{P}_\Lambda(\varphi).$$

Autrement dit, la fonction $D_\Omega\big(z;\varphi,\langle\psi\rangle\big)$ est une sorte de racine carrée — tordue par un groupe cyclique $\langle\psi\rangle = \Lambda/\Omega$ d'ordre multiple de celui de φ, mais tel que $\varphi \notin \langle\psi\rangle$ — de la fonction

$$\mathcal{P}_\Lambda(z) - \mathcal{P}_\Lambda(\varphi);$$

une première apparition de cette propriété a déjà été notée dans [4, § IV, haut des p. 330 et 332], *cf.* aussi [1, chap. II, cor. 2.27].

En forçant un peu le trait, on pourrait aussi dire que le corollaire 5 ci-dessus dit qu'il existe entre les fonctions D_Ω et $\mathcal{P}_\Lambda$ une relation analogue à celle existant entre une somme de Gauss et le nombre entier produit de celle-ci et de sa conjuguée.

3. Les fonctions D_Ω de poids ℓp

Considérons maintenant un entier $\ell > 1$, premier à p. Soit

$$\langle\alpha\rangle \subset E[\ell]$$

un sous-groupe cyclique d'ordre ℓ du groupe $E[\ell]$ des points de ℓ-torsion de E, de générateur fixé α. Le groupe

$$\langle\alpha\rangle \oplus \langle\psi\rangle \subset E[\ell p]$$

est donc cyclique, d'ordre ℓp.

Par ailleurs, soit

$$\gamma \in E[\ell]$$

un autre point de ℓ-torsion de E, arbitraire. On note aussi α et γ des relèvements de ces points dans $\mathbb{C}$.

Posons

$$z_0(\varphi,\gamma) = \Big[\frac{1}{\ell}\Big]_p\varphi - \Big[\frac{1}{p}\Big]_\ell\gamma$$

où $\Big[\frac{1}{\ell}\Big]_p$ (resp. $\Big[\frac{1}{p}\Big]_\ell$) désigne l'inverse de ℓ dans $\mathbb{Z}/p\mathbb{Z}$ (resp. de p dans $\mathbb{Z}/\ell\mathbb{Z}$). Clairement $z_0(\varphi,\gamma)$ est un point de $E[\ell p]$, mais il n'appartient pas à $\langle\alpha\rangle \oplus \langle\psi\rangle$ puisque φ n'appartient pas à $\langle\psi\rangle$.

La construction précédente peut donc être appliquée au groupe cyclique $\langle\alpha\rangle\oplus\langle\psi\rangle\subset E[\ell p]$ d'ordre ℓp, et au point $z_0(\varphi,\gamma)$ de ℓp-torsion de E. Soit

$$D_\Omega\big(z;z_0(\varphi,\gamma),\langle\alpha\rangle\oplus\langle\psi\rangle\big)$$

la fonction obtenue : d'après le § 2, prop. 2, on a la formule explicite

$$\begin{aligned}(1)\qquad & D_\Omega\big(z;z_0(\varphi,\gamma),\langle\alpha\rangle\oplus\langle\psi\rangle\big)\\ &\qquad = e\big(\tfrac12 E_\Sigma(z,-z_0(\varphi,\gamma))\big)\frac{\mathcal{K}_\Sigma(z-z_0(\varphi,,\gamma))}{\mathcal{K}_\Sigma(z)\mathcal{K}_\Sigma(-z_0(\varphi,\gamma))}\end{aligned}$$

où apparaît cette fois-ci la fonction de Klein $\mathcal{K}_\Sigma$ relative au réseau $\Sigma=\Omega+\mathbb{Z}\alpha+\mathbb{Z}\psi$. Or, on a :

LEMME. — *Il vient :*

i) $e^\Omega_{\ell p}\big(\psi,z_0(\varphi,\gamma)\big)=e^\Omega_p(\psi,\varphi)$;

ii) $e^\Omega_{\ell p}\big(\alpha,z_0(\varphi,\gamma)\big)=e^\Omega_\ell(\gamma,\alpha)$.

Démonstration. — Simple calcul à partir des formules définissant les divers termes.

Par conséquent le paragraphe 2, prop. 5, assure les identités

$$(2)\qquad \begin{cases} D_\Omega\big(z+\psi;z_0(\varphi,\gamma),\langle\alpha\rangle\oplus\langle\psi\rangle\big)\\ \qquad\qquad = e^\Omega_p(\psi,\varphi)D_\Omega\big(z;z_0(\varphi,\gamma),\langle\alpha\rangle\oplus\langle\psi\rangle\big);\\ D_\Omega\big(z+\alpha;z_0(\varphi,\gamma),\langle\alpha\rangle\oplus\langle\psi\rangle\big)\\ \qquad\qquad = e^\Omega_\ell(\gamma,\alpha)D_\Omega\big(z;z_0(\varphi,\gamma),\langle\alpha\rangle\oplus\langle\psi\rangle\big).\end{cases}$$

4. La relation de distribution satisfaite par les fonctions D_Ω

Nous pouvons maintenant énoncer notre résultat principal (dû à G.F. Frobenius [7, p. 91]) :

THÉORÈME 1. — *Soit p un entier >1. On note $\langle\psi\rangle\subset E[p]$ un sous-groupe cyclique d'ordre p de E, et $\varphi\in E[p]$ un point de p-torsion de E tel que $\varphi\notin\langle\psi\rangle$.*

Soit aussi ℓ un entier >1, premier à p. On note $\langle\alpha\rangle\subset E[\ell]$ un sous-groupe cyclique d'ordre ℓ de E.

Alors, pour tout point $\gamma\in E[\ell]$ de ℓ-torsion de E, on a :

$$\sum_{t\in\langle\alpha\rangle} D_\Omega\big(z+t;\varphi,\langle\psi\rangle\big)e^\Omega_\ell(\gamma,t)^{-1}=D_\Omega\Big(z;\Big[\frac1\ell\Big]_p\varphi-\Big[\frac1p\Big]_\ell\gamma,\langle\alpha\rangle\oplus\langle\psi\rangle\Big)$$

où $e^\Omega_\ell : E[\ell]\times E[\ell]\to\boldsymbol{\mu}_\ell$ désigne l'accouplement de Weil.

Démonstration. — D'après le § 2, prop. 4 et le lemme du § 3, le membre de droite comme le membre de gauche admettent les multiplicateurs $e_p^\Omega(\psi,\varphi)$ quand z devient $z+\psi$ et $e_\ell^\Omega(\gamma,\alpha)$ quand z devient $z+\alpha$; or le dénominateur des pôles de chacune de ces deux fonctions est

$$\sum_{\rho\in\langle\alpha\rangle\oplus\langle\psi\rangle}(\rho)$$

relativement au réseau Ω.

Il s'ensuit que leur quotient est une fonction périodique pour le réseau de périodes

$$\Sigma=\Omega+\mathbb{Z}\alpha+\mathbb{Z}\psi,$$

et que relativement à ce réseau Σ son ordre est au plus 1. Ceci n'est possible que si elle est constante.

Or, abrégeant en m.d.g.(z) (resp. m.d.d.(z)) le membre de gauche (resp. droite) de l'identité à prouver, la normalisation de D_Ω *cf.* § 2, identité (2) impose

$$\lim_{z\to 0} z \text{ m.d.g.}(z)=1=\lim_{z\to 0} z \text{ m.d.d.}(z).$$

Donc les deux membres coïncident, et le théorème est démontré.

Prenant pour γ l'origine 0 de $E(\mathbb{C})\simeq\mathbb{C}/\Omega$, on en déduit :

Corollaire 2. — *On a la relation de distribution*

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

où le second membre pourrait encore être écrit $D_{\mathcal{L}}\Big(z;\Big[\frac{1}{\ell}\Big]_p\varphi,\langle\psi\rangle\Big)$ *avec* $\mathcal{L}=\Omega+\mathbb{Z}\alpha$, *cf.* § 2, *prop.* 2.

Vu la relation d'antisymétrie

$$z_0(\varphi,\gamma)+z_0(\gamma,\varphi)=0,$$

on déduit également du théorème 1 la relation suivante liant les valeurs des fonctions $D_\Omega\big(z;\varphi,\langle\psi\rangle\big)$ et $D_\Omega(z;\gamma,\langle\alpha\rangle)$, obtenue en tenant compte du cor. 3, i) du § 2.

Corollaire 3. — *Supposons que* γ *n'est pas dans* $\langle\alpha\rangle$ *et* φ *n'est pas dans* $\langle\psi\rangle$. *Alors, on a* :

$$\sum_{t\in\langle\alpha\rangle} D_\Omega\big(z+t;\varphi,\langle\psi\rangle\big)e_\ell^\Omega(\gamma,t)^{-1} + \sum_{q\in\langle\psi\rangle} D_\Omega\big(-z+q;\gamma,\langle\alpha\rangle\big)e_p^\Omega(\varphi,q)^{-1}=0.$$

On a aussi :

LEMME 4. — *On suppose que le groupe* $\langle\gamma\rangle \subset E[\ell]$ *engendré par* γ *est d'ordre* ℓ, *et que l'on a* :

$$\langle\alpha\rangle \cap \langle\gamma\rangle = \{0\};$$

autrement dit, on demande que le couple (α,γ) *soit une base de* $E[\ell]$ *sur* $\mathbb{Z}/\ell\mathbb{Z}$.

Alors, lorsque s *décrit le groupe* $\langle\gamma\rangle$, *le* $\mathbb{C}$*-espace vectoriel engendré par les fonctions*

$$D_\Omega\big(z; z_0(\varphi,s), \langle\alpha\rangle \oplus \langle\psi\rangle\big),$$

où $z_0(\varphi,s) = \Big[\dfrac{1}{\ell}\Big]_p \varphi - \Big[\dfrac{1}{p}\Big]_\ell s$, *est de dimension* ℓ.

Démonstration. — Cela résulte directement de l'étude des fonctions thêta sur $\mathbb{C}/\Omega$, *cf. e.g.* [19, chap. VI, n$^{\text{o}}$ 7] ou [15, chap. II, prop. 1.3], ou bien peut-être vu de la manière suivante.

Vu le lemme du § 3 et la prop. 5 du § 2, les pôles de

$$D_\Omega\big(z; z_0(\varphi,s), \langle\alpha\rangle \oplus \langle\psi\rangle\big)$$

en les points t de $\langle\alpha\rangle$ forment, pour chaque s dans $\langle\gamma\rangle$, un vecteur de valeur

$$\big(e_\ell^\Omega(s,t), t \in \langle\alpha\rangle\big) \in \mathbb{C}^\ell;$$

or, lorsque s décrit $\langle\gamma\rangle$ ces ℓ vecteurs — et à plus forte raison les fonctions dont ils sont les pôles — sont $\mathbb{C}$-linéairement indépendants (puisque la matrice de Vandermonde qu'ils composent est inversible).

Le lemme 4 ci-dessus permet alors d'inverser formellement les formules du théorème 1, on a donc :

COROLLAIRE 5. — *On suppose que* (α,γ) *est une base de* $E[\ell]$ *sur* $\mathbb{Z}/\ell\mathbb{Z}$.

Alors, pour tout $t \in \langle\alpha\rangle$, *on a* :

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

5. Simplification de l'élément de Stickelberger quadratique de [3]

Dans ce paragraphe, grâce au théorème 1 du § 4, nous débarassons l'élément de Stickelberger $\theta_2(p)$ introduit dans [3] de son facteur inutile $(p^3 - p^2)$, *lui rendant sa forme naturelle.* Ceci nous permet de réviser les principaux résultats obtenus dans [3].

Remarque 1. — *La forme exacte de* $\theta_2(p)$ *est donnée dans* [3, § 1], nous ne souhaitons pas la reproduire ici ; *l'élément simplifié*

$$\tilde{\theta}_2(p) = \frac{1}{p^3 - p^2}\, \theta_2(p) \in \mathbb{Q}[\Gamma]$$

vérifie la congruence

$$\tilde{\theta}_2(p) \equiv \frac{p^2-1}{\ell} \sum_{t=1}^{(\ell-1)/2} t^2 \sigma_t^{-1} \pmod{\mathbb{Z}[\Gamma]}$$

où les notations sont précisées ci-dessous, cf. substitutions 1, 2 *et* 3*.*

Nous ne précisons pas non plus la définition exacte *de la résolvante elliptique à laquelle se réfère le lemme* 5, *ni* la définition précise *du facteur* $\mathcal{D}_{E/F,\mathrm{reg}}$ *de* $\mathcal{D}_{E/F}$*, pour lesquelles nous prions le lecteur de se reporter à* [3]*.*

Il s'agit pour nous de donner ici dans ce paragraphe le mouvement général de la simplification, *et non ces détails plus secondaires.*

On fixe donc un modèle de Weierstrass

$$\text{(1)} \qquad \Big(E, \frac{\mathrm{d}x}{y}\Big) \begin{cases} y^2 = 4x^3 - g_2(\Omega)x - g_3(\Omega), \\ g_k(\Omega) \ = \ d_k \displaystyle\sum_{\rho\in\Omega,\rho\neq 0} \rho^{-2k}, \quad k \in \{2,3\}, \end{cases}$$

de la courbe elliptique E, avec $d_2 = 60$ et $d_3 = 140$, de façon à ce que le réseau $\Omega \subset \mathbb{C}$ soit formé des périodes complexes de $\big(E, \frac{1}{y}\,\mathrm{d}x\big)$.

On note

$$F = \mathbb{Q}\big(g_2(\Omega), g_3(\Omega)\big)$$

le corps de définition de ce modèle $\big(E, \frac{1}{y}\,\mathrm{d}x\big)$ et pour tout automorphisme $\sigma \in \mathrm{Aut}(\mathbb{C}/F)$ de $\mathbb{C}$ fixant F notons

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

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

Soit p un entier > 1, et soient $\langle\psi\rangle$ un sous-groupe cyclique de $E[p]$ d'ordre p, et $\varphi \in E[p]$ un point de p-torsion de E tel que $\varphi \notin \langle\psi\rangle$, *cf.* § 2. On note Λ le réseau $\Omega + \mathbb{Z}\psi$.

Alors vu *l'algébricité* et *l'unicité* de la définition de la fonction elliptique $z \mapsto D_\Omega\big(z;\varphi,\langle\psi\rangle\big)$ sur $\mathbb{C}/\Omega$ prouvée dans le paragraphe 2, à partir de seulement i) *le sous-groupe cyclique* $\langle\psi\rangle = \Lambda/\Omega$ *d'ordre* p et ii) *le point non trivial* (φ modulo Λ) *de* p*-torsion*, on obtient le résultat ci-dessous ; on peut aussi faire appel à [1, chap. 4, § 3].

PROPOSITION 2. — *On a :*

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

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

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

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

NOTA BENE. — Le corps $F\big(\varphi \bmod \Lambda, \langle\psi\rangle\big)$ ne contient pas nécessairement de racine primitive p-ième de l'unité.

D'autre part, comme dans le § 3, pour ℓ un entier > 1 sans facteur commun avec p, soient $\langle\alpha\rangle$ un sous-groupe cyclique de $E[\ell]$ d'ordre ℓ, et $\gamma \in E[\ell]$ un point de ℓ-torsion de E. *On suppose ici que* γ *n'est pas dans* $\langle\alpha\rangle$. On note $\mathcal{L}$ le réseau $\Omega + \mathbb{Z}\alpha$.

Plutôt que le produit de résolvantes de [3, § 2, p. 149–150], introduisons :

DÉFINITION 3. — On forme le produit bien défini

$$(2)\quad A_{p,\Omega}\big(\gamma,\langle\alpha\rangle\big) \overset{\text{def}}{=\!=} \frac{1}{p}\prod_{\langle\psi\rangle\subset E[p]}\ \prod_{\varphi \bmod \langle\psi\rangle} D_\Omega\Big(\gamma;\Big[\frac{1}{\ell}\Big]_p\varphi - \Big[\frac{1}{p}\Big]_\ell\gamma, \langle\alpha\rangle\oplus\langle\psi\rangle\Big),$$

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

Il résulte de la proposition 2 ci-dessus qu'il s'agit d'un élément de

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

REMARQUE 4. — Vu le théorème 1 du § 4, chacun des termes

$$D_\Omega(\gamma; z_0(\varphi,\gamma), \langle\alpha\rangle \oplus \langle\psi\rangle)$$

de (2), avec $z_0(\varphi,\gamma) = \left[\dfrac{1}{\ell}\right]_p \varphi - \left[\dfrac{1}{p}\right]_\ell \gamma$, y a valeur d'une résolvante.

Supposons maintenant, comme dans [3] (*cf.* aussi [1] et [4]), que les hypothèses suivantes sont satisfaites :

(H_1) *Le point de paramètre complexe α est rationnel sur F.*

(H_2) *On a $F \cap \mathbb{Q}(\zeta_\ell) = \mathbb{Q}$, où ζ_ℓ désigne une racine primitive ℓ-ième de l'unité.*

Alors si l'ordre de γ est ℓ, on a :

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

et les degrés respectifs sont les suivants

$$\big[F(\zeta_\ell) : F\big] = \mathrm{card}(\mathbb{Z}/\ell\mathbb{Z})^\times, \quad \big[F\big(E[\ell]\big) : F(\zeta_\ell)\big] \mid \ell.$$

Enfin, comme dans [3], faisons l'hypothèse :

(H_3) *Les nombres ℓ et p sont premiers, et de plus $(\ell, p(p+1)) = 1$ et $\ell \geq 5$; on suppose aussi $[F : \mathbb{Q}]$ fini.*

Soit $\Delta(\Omega) = g_2(\Omega)^3 - 27 g_3(\Omega)^2$ le discriminant du modèle de Weierstrass (1), réseau de périodes Ω, de E et posons

$$n_p = \tfrac{1}{12} p^2 (p-1)^2 (p+1), \quad \widetilde{n}_p = \tfrac{1}{12}(p-1)(p+1).$$

Le calcul clef est alors le suivant :

LEMME 5. — *Soient P et Q les points de $E[\ell]$ de paramètres complexes α et γ, et notons $\widetilde{T}_p(P,Q)$ la résolvante elliptique de* [3, déf. 2.3] ; *on a*

$$A_{p,\Omega}\big(\gamma, \langle\alpha\rangle\big)^{p^2(p-1)} = \Delta(\Omega)^{n_p} \widetilde{T}_p(P,Q). \tag{3}$$

Ainsi $A_{p,\Omega}(\gamma, \langle\alpha\rangle)$ est une racine $(p^3 - p^2)$-ième du produit de la résolvante $\widetilde{T}_p(P,Q)$ de [3] *par une puissance convenable de $\Delta(\Omega)$.*

Démonstration. — Calcul sans difficulté, à partir de l'expression du dénominateur donnée dans [3] *loc. cit.* ; on utilise les formules de multiplicativité des fonctions de Klein, *cf. e.g.* [11].

Or, pour $A_{p,\Omega}(\gamma, \langle\alpha\rangle)$, on a alors un énoncé analogue à la proposition 2.4 de [3]. Compte tenu de la proposition 2 ci-dessus, pour obtenir le point ii) (resp. iii)), on applique les formules de transformation de $\mathcal{K}_\Lambda$, avec $\Lambda = \Omega + \mathbb{Z}\psi$, soit la prop. 4 du § 1 précisée par le lemme du § 3 (resp. le cor. 3 i) du § 2) ; on trouve :

PROPOSITION 6. — *Soient p et ℓ premiers, avec $(\ell, p(p+1)) = 1$ et $\ell \geq 5$. Posons $N = F(\zeta_\ell + \zeta_\ell^{-1})$. Alors, on a :*

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

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

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

avec $(a_\sigma, b_\sigma) \in (\mathbb{Z}/\ell\mathbb{Z})^2$, $a_\sigma \neq 0$, il vient :

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

iii) *on a $A_{p,\Omega}(-\gamma, \langle\alpha\rangle) = \varepsilon(p) A_{p,\Omega}(\gamma, \langle\alpha\rangle)$ avec $\varepsilon(p) = +1$ (resp. -1) si $p \geq 3$ (resp. $p = 2$), et donc il vient :*

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

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

Dans les théorèmes 1.1 et 1.2 de [3], remplaçons alors :

SUBSTITUTION 1. — *La résolvante elliptique $\widetilde{T}_p(P, Q)$ par $A_{p,\Omega}(\gamma, \langle\alpha\rangle)$.*

SUBSTITUTION 2. — *Le discriminant minimal $\mathcal{D}_{E/F}$ de la courbe E/F (dont (1) est un modèle) par le quotient*

$$\mathcal{D}_{E/F}/\big(\Delta(\Omega)\big).$$

L'idéal $\mathcal{D}_{E/F}/(\Lambda(\Omega))$, contrairement à $\mathcal{D}_{E/F}$, dépend de Ω, *i.e.* du modèle choisi ; de plus *c'est la puissance 12-ième d'un idéal de F* puisque par définition, en une place finie $\mathfrak{p}$ de F, la valuation $\mathfrak{p}$-adique de $\mathcal{D}_{E/F}$ est l'entier $v_\mathfrak{p}(\mathcal{D}_{E/F})$ compris entre 0 et 11 tel que

$$v_\mathfrak{p}\big(\mathcal{D}_{E/F}\big) \equiv v_\mathfrak{p}\big(\Delta(\Omega)\big) \pmod{12}.$$

C'est ce fait, pour $p \in \{2, 3\}$, qui assure que le membre de droite de l'identité (8) ci-dessous est bien un idéal de F.

Pour t premier à ℓ, notons σ_t l'automorphisme de N sur F qui applique ζ_ℓ sur ζ_ℓ^t, de sorte que $\Gamma = \mathrm{Gal}(N/F)$ est donné par

$$\Gamma = \big\{\sigma_t,\ 1 \leq t \leq \tfrac{1}{2}(\ell - 1)\big\},$$

et soit $\mathbb{Q}[\Gamma]$ l'algèbre associée au groupe Γ.

Dans [3, th. 1.1 et 1.2], changeons aussi :

Substitution 3. — *Les exposants* $\theta_2(p)$ *et* n_p *par*

$$\widetilde{n}_p = \frac{1}{p^3 - p^2}\, n_p = \frac{(p-1)(p+1)}{12} \in \frac{1}{12}\mathbb{Z}, \tag{4}$$

$$\tilde{\theta}_2(p) = \frac{1}{p^3 - p^2}\, \theta_2(p) \in \mathbb{Q}[\Gamma]. \tag{5}$$

Le facteur $(p^3 - p^2)$ n'intervient pas dans le passage concerné de [3, § 1], d'où la congruence

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

de sorte que l'élément de Stickelberger $\tilde{\theta}_2(p)$ peut encore être dit quadratique, et que

$$\ell\tilde{\theta}_2(p) \in \mathbb{Z}[\Gamma]. \tag{7}$$

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

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

lorsque les diviseurs de $\mathfrak{a}\mathfrak{b}^{-1}$ divisent ℓ. Alors on déduit de la proposition 6 et du lemme 5 ci-dessus, les exposants $12\,\widetilde{n}_p$ et $\ell\tilde{\theta}_2(p)$ restant entiers d'après (4) et (7), que le théorème 1.1 de [3] implique :

Théorème 7.

1) *Pour* $p \geq 3$, *l'identité* (*factorisation dans* N *de l'idéal* $\big(\widetilde{T}_p(P, Q)\big)^\ell$ *à l'aide de* $\ell\theta_2(p)$, *aux diviseurs de* ℓ *près*) *du* th. 1.1 de [3] *est encore vraie après que les substitutions* 1 *à* 3 *aient été faites.*

2) *Pour* $p = 2$, *d'une part le carré des deux membres de l'identité — après substitutions* 1 *à* 3 *— coïncident bien.*

De plus, la nouvelle identité est vraie (*aux diviseurs de* ℓ *près*), *à condition de regarder son membre de droite comme un idéal de* $F(\zeta_\ell)$ (*et non plus de* N).

Alors le passage à la norme, qui dans [3] lie le théorème 1.2 au théorème 1.1, permet ici de déduire du théorème 7 ci-dessus le résultat suivant :

Théorème 8. — *Sous les hypothèses* (H_1) *à* (H_3) *précédentes, on a :*

$$\Big(\prod_{t=1}^{(\ell-1)/2} A_{p,\Omega}(t\gamma, \langle\alpha\rangle)\Big) \equiv \big((\Delta(\Omega))\mathcal{D}_{E/F}^{-1}\big)^{\frac{\ell-1}{2}\tilde{n}_p} \mathcal{D}_{E/F,\mathrm{reg}}^{\frac{(\ell+1)(\ell-1)}{2}\tilde{n}_p} \pmod{\ell}. \tag{8}$$

Le facteur $\mathcal{D}_{E/F,\mathrm{reg}}$ de $\mathcal{D}_{E/F}$ est défini dans [3, § 1, rem. p. 148] ; en fait ces deux idéaux coïncident souvent ; or, le théorème 1.2 de [3] est énoncé sous l'hypothèse

$$\mathcal{D}_{E/F,\mathrm{reg}} \equiv \mathcal{D}_{E/F} \pmod{\ell},$$

et l'identité du théorème 8 est alors une racine (p^3-p^2)-ième de l'identité de ce théorème là.

BIBLIOGRAPHIE

[1] Bayad (A.). — *Résolvantes elliptiques et éléments de Stickelberger*, Université de Bordeaux I, thèse soutenue le 24 avril 1992.

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

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

[4] Cassou-Noguès (Ph.), Taylor (M.J.). — *Un élément de Stickelberger quadratique*, J. Number Th., t. **37** (3), 1991, p. 307–342.

[5] Shih-Ping Chan. — *Modular functions, elliptic functions and Galois module structure*, J. Reine angew. Math., t. **375**, 1987, p. 67–82.

[6] Egami (Sh.). — *An elliptic analogue of the multiple Dedekind sums*, Comp. Math., t. **99**, 1995, p. 99–103.

[7] Frobenius (F.G.). — *Über die elliptischen Functionen zweiter Art*, Ges. Abhand. b. II, p. 81–96 ; J. reine angew. Math., t. **93**, 1882, p. 53–68.

[8] Hermite (Ch.). — *Sur quelques applications des fonctions elliptiques*, *Œuvres*, t. III, p. 266 ; C. R. Acad. Sci. Paris, t. **85–94**, 1877—1882.

[9] Husemöller (D.). — *Elliptic curves*, Graduate texts in Math. **111**, Springer-Verlag, 1986.

[10] Ito (H.). — *On a product related to the cubic Gauss sums*, J. reine angew. Math., t. **395**, 1989, p. 202–213.

[11] Kubert (D.). — *Product formulae on elliptic curves*, Invent. Math., t. **117**, 1994, p. 227–273.

[12] Kubert (D.), Lang (S.). — *Modular units*, Grundlehren der math. Wiss. **244**. — Springer-Verlag, 1981.

[13] Lang (S.). — *Elliptic functions.* — Addison-Wesley, 1973.
[14] Mumford (D.). — *Abelian varieties.* — Tata Institute of fundamental Research, Bombay, vol. **5**, Oxford Univ. Press, 1970.
[15] Mumford (D.). — *Tata lectures on theta I*, Progress in Math., vol. **28**, Birkhäuser, 1983.
[16] Robert (G.). — *Unités elliptiques*, Bull. Soc. Math. France, Mémoire **36**, 1973.
[17] Robert (G.). — *Concernant la relation de distribution satisfaite par la fonction φ associée à un réseau complexe*, Invent. Math., t. **100**, 1990, p. 231–257.
[18] Srivastav (A.), Taylor (M.J.). — *Elliptic curves with complex multiplication and Galois module structure*, Inv. Math., t. **99**, 1990, p. 165–184.
[19] Weil (A.). — *Variétés kählériennes*, Publication de l'Institut de Math. de l'Université de Nancago, VI, Hermann, Paris, 1958.
[20] Weil (A.). — *Elliptic functions according to Eisenstein and Kronecker*, Ergeb. der Math. **88**, Springer-Verlag, 1976.