UNE RELATION DE DISTRIBUTION ADDITIVE SATISFAITE PAR UNE FAMILLE DE FONCTIONS ELLIPTIQUES

par Abelmejid BAYAD et Gilles ROBERT

À André Weil,

avec admiration et émerveillement.

Introduction

Soient ℓ et p des entiers > 1, premiers entre eux. On note $\Omega \subset \mathbb{C}$ le réseau des périodes complexes d'une courbe elliptique E, de sorte que la paramétrisation de Weierstrass fournit un isomorphisme

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

par lequel nous identifions un point de $E(\mathbb{C})$ à la classe modulo Ω d'un nombre complexe.

On décrit ici, dans ce cadre complexe une relation de distribution satisfaite par les fonctions elliptiques de diviseur

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

d'une part, et celles de diviseur

$$\sum_{\rho \in \langle \alpha \rangle \oplus \langle \psi \rangle} \big(z_0(\varphi, \gamma) + \rho\big) - (\rho) \tag{2}$$

d'autre part, où $\langle \psi \rangle \subset E[p]$ (resp. $\langle \alpha \rangle \subset E[\ell]$) désigne un sous-groupe cyclique d'ordre p (resp. ℓ) de $E(\mathbb{C}) \simeq \mathbb{C}/\Omega$ tandis que φ (resp. γ) désigne un autre point de E d'ordre p (resp. ℓ).

On a posé ci-dessus

$$z_0(\varphi, \gamma) = \left[\frac{1}{\ell}\right]_p \varphi - \left[\frac{1}{p}\right]_\ell \gamma \tag{3}$$

où $\left[\frac{1}{\ell}\right]_p$ (resp. $\left[\frac{1}{p}\right]_\ell$) désigne l'inverse de ℓ dans $\mathbb{Z}/p\mathbb{Z}$ (resp. de p dans $\mathbb{Z}/\ell\mathbb{Z}$) de sorte que $z_0(\varphi, \gamma)$ est un point de E d'ordre ℓp ; ainsi, comme ℓ et p sont premiers entre eux et le groupe $\langle \alpha \rangle \oplus \langle \psi \rangle$ cyclique d'ordre ℓp, les fonctions elliptiques de diviseur (2) sont un cas particulier — après changement de p en ℓp — des fonctions de diviseur (1).

L'expression cf. § 3, th. 1 que nous trouvons de la fonction de diviseur (2) comme combinaison linéaire, à coefficients des racines de l'unité, des translatés par les éléments du groupe $\langle \alpha \rangle$ de la fonction de diviseur (1) — et que nous désignons improprement sous le nom de relation de distribution — est extrêmement suggestive. En particulier, le résultat fondamental de ce travail reste vrai sur un produit de courbes elliptiques (munies de la polarisation somme directe) : cela se déduit aisément à partir du th. 1 du § 3 par un produit.

Notons enfin que c'est en tant que *résolvantes elliptiques* (analogue à une somme de Gauss) que les fonctions de diviseur (2) sont d'abord apparues dans la thèse [1] de l'un des auteurs de cette note — ainsi que dans le travail commun [2] de celui-ci avec W. Bley et Ph. Cassou-Noguès — et pour le cas particulier $p = 2$ dans l'article [3] dû à la collaboration de Ph. Cassou-Noguès et M.J. Taylor. Mais, pour les temps modernes, la première personne à avoir reconsidéré les fonctions elliptiques de diviseur (1) pour p premier quelconque et à en avoir étudié certaines valeurs particulières a été S.P. Chan [4].

Notre résultat original est énoncé dans le § 3 ; les deux types de fonctions mentionnées ci-dessus font l'objet des §§ 1 et 2 ; quant au § 0, il contient quelques rappels concernant la fonction de Klein, et l'accouplement de Weil de points d'ordre fini de E. Une simplification des résultats de [2] est donnée en Appendice ; on y améliore aussi légèrement un résultat de [3].

0. 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

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

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

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

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 $\mathrm{Im}(w_1/w_2) > 0$.

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

$$e(-nx) = e(x)^{-n} \overset{\text{dfn}}{=} e^{-2\pi i n x},$$

on en déduit une application bilinéaire alternée

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

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. [8], chap. 18, [9], § 20 ou [1], chap. II, § 1 ; on en trouve aussi une mention dans [5], chap. II, §§ 4.13 et 6.2. 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. [7], [6] et [12].

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. [11], § 1, pp. 7–8, [14], chap. IV, formule (26) et [7], chap. 2, § 1, par la série

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

pour (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

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

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

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

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).

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*

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

où l'on a posé

$$\chi_L(\rho) = \begin{cases} 1 & \text{si } \rho \in 2L \\ -1 & \text{si } \rho \in L \smallsetminus 2L \end{cases}$$

Remarque 5. — *Pour tous ρ et σ éléments de L, on a*

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

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* [13], chap. VI.

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

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

1. Les fonctions D_Ω de poids p

Reprenant les notations de l'introduction, 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 $\varphi \notin \langle\psi\rangle$.

Le théorème d'Abel-Jacobi de la théorie des fonctions elliptiques cf. e.g. [8] prouve alors l'existence d'une fonction non triviale

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

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

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

Il vient :

Proposition 1. — *On a*

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

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. § 0, formule (3)) et de l'égalité $E_\Lambda = \operatorname{Im} H_\Lambda$, que $\widetilde{D_\Omega}$ est proportionnel à la fonction méromorphe

$$z \longmapsto \theta_\Lambda(z-\varphi)/\theta_\Lambda(z)\ ;$$

de plus, d'après le § 0, prop. 3, 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. § 0 rmq. 2), de sorte que

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

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 $\rho \in \Omega$, 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. § 0, 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 1.

Corollaire 2. — *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 3. — *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 [7], chap. 2, § 6, pp. 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 4. — *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 $\langle\psi\rangle$ 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 le cas $p = 2\ell$) dans [3], § IV, haut des pp.330 et 332, cf. aussi [1], chap. II, corollaire 2.27.

En forçant un peu le trait, on pourrait aussi dire que le corollaire 4 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.

2. 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 comme dans l'introduction

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

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

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 § 1, prop. 1, on a la formule explicite

$$(1) \qquad D_\Omega\big(z; z_0(\varphi,\gamma), \langle\alpha\rangle \oplus \langle\psi\rangle\big) = e\Big(\frac{1}{2}E_\Sigma\big(z, -z_0(\varphi,\gamma)\big)\Big)\frac{\mathcal{K}_\Sigma(z - z_0(\varphi,\gamma))}{\mathcal{K}_\Sigma(z)\mathcal{K}_\Sigma(-z_0(\varphi,\gamma))}$$

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 § 1, prop. 4, assure les identités

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

3. La relation de distribution satisfaite par les fonctions D_Ω

Nous pouvons maintenant énoncer notre résultat principal :

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

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

où $e_\ell^\Omega : E[\ell]\times E[\ell] \longrightarrow \boldsymbol{\mu}_\ell$ désigne l'accouplement de Weil.

Démonstration. — D'après le § 1, prop. 3 et le lemme du § 2, le m.d.d. comme le m.d.g. 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. § 1 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 $D_\Gamma\Big(z;\Big[\frac{1}{\ell}\Big]_p\varphi,\langle\psi\rangle\Big)$ avec $\Gamma = \Omega + \mathbb{Z}\alpha$, cf. § 1 prop. 1.

Vu la relation d'antisymétrie

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

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

COROLLAIRE 3. — *Supposons que $\gamma\notin\langle\alpha\rangle$ et $\varphi\notin\langle\psi\rangle$. 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 $z_0(\gamma,s)=\left[\frac{1}{\ell}\right]_p\varphi-\left[\frac{1}{p}\right]_\ell s$, est de dimension ℓ.

Démonstration. — Cela résulte directement de l'étude des fonctions thêta sur $\mathbb{C}/\Omega$, cf. e.g. [13], chap. VI, n^{o}7 ou [10], chap. II, prop. 1.3, ou bien peut-être vu de la manière suivante :

Vu le lemme du § 2 et la prop. 4 du § 1, 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 Van der Monde 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

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

Bibliographie

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

[2] A. Bayad, W. Bley, Ph. Cassou-Noguès. — *Sommes arithmétiques et éléments de Stickelberger*, à paraître au J. of Algebra.

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

[4] Shih-Ping Chan. — *Modular functions, elliptic functions and Galois module structure*, J. Reine Angew. Math. **375** (1987), 67–82.

[5] E. de Shalit. — *Iwasawa theory of elliptic curves with complex multiplication*, (Perspective in math., vol. 3), Academic Press, 1987.

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

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

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

[9] D. Mumford. — *Abelian varieties*, (Tata institute of fundamental research, Bombay, vol. 5), Oxford Univ. Press, 1970.

[10] D. Mumford. — *Tata lectures on theta I*, (Progress in math., vol. 28), Birkhäuser, 1983.

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

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

[13] A. Weil. — *Variétés kählériennes*, (Publication de l'institut de math. de l'univ. de Nancago, VI), Hermann, Paris, 1958.

[14] A. Weil. — *Elliptic functions according to Eisenstein and Kronecker*, (Ergeb. der Math. 88), Springer-Verlag, 1976.

Appendice

Application à l'élément de Stickelberger quadratique de [2]

Fixons un modèle de Weierstrass

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

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

On note $F = \mathbb{Q}\big(g_2(\Omega), g_3(\Omega)\big)$ le corps de définition de ce modèle $\left(E, \frac{dx}{y}\right)$ 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. § 1. 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 § 1, 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 1. — *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* $\langle\psi\rangle = \Lambda/\Omega$*.*

N.B. 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 § 2, 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* $\gamma \notin \langle\alpha\rangle$. On note Γ le réseau $\Omega + \mathbb{Z}\alpha$.

DÉFINITION 2. — *On forme le produit bien défini*

$$A_p\big(\gamma, \langle\alpha\rangle\big) \overset{\text{dfn}}{=} \prod_{\langle\psi\rangle\subset E[p]} \prod_{\varphi\in E[p]\smallsetminus\langle\psi\rangle} D_\Omega\Big(\gamma; \Big[\frac{1}{\ell}\Big]_p \varphi - \Big[\frac{1}{p}\Big]_\ell \gamma, \langle\alpha\rangle \oplus \langle\psi\rangle\Big),$$

où φ *parcourt les points de* $E[p] \smallsetminus \langle\psi\rangle$ *tandis que* $\langle\psi\rangle$ *décrit les sous-groupes cycliques d'ordre* p *de* $E[p]$.

Il résulte de la proposition 1 ci-dessus qu'il s'agit d'un élément de

$$F\big(\gamma \bmod \Gamma, \langle\alpha\rangle\big) \subset F\big(E[\ell]\big).$$

Supposons maintenant, comme dans [2] cf. aussi [1] et [3], que les hypothèses suivantes sont satisfaites :

i) le point de paramètre complexe α est rationnel sur F ;

ii) 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

$$F\big(\gamma \bmod \Gamma, \langle\alpha\rangle\big) = F\big(E[\ell]\big)$$

et les degrés respectifs sont les suivants

$$\big[F(\zeta_\ell) : F\big] = \ell - 1,$$
$$\big[F\big(E[\ell]\big) : F(\zeta_\ell)\big] \big| \ell.$$

Enfin, comme dans [2] faisons l'hypothèse :

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

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

$$n_p = \frac{p^2(p-1)^2(p+1)}{12} ;$$

pour p premier impair, le quotient $n_p/p(p-1)$ est donc entier.

LEMME 3. — *La quantité*

$$A_p\big(\gamma, \langle\alpha\rangle\big)^{p(p-1)}$$

coïncide, au facteur $p^{p^2(p-1)}\Delta(\Omega)^{n_p}$ *près, avec la résolvante elliptique introduite dans* [2], § 2 *(et notée* $\widetilde{T}_p(P,Q)$ *dans loc. cit.).*

Démonstration. — Calcul élémentaire, à partir de l'expression du dénominateur donnée dans [2] ; on utilise les formules de multiplicativité des fonctions de Klein, cf. e.g. [6].

On a alors un énoncé analogue à la prop. 2.4 de [2]. Compte tenu de la proposition 1 ci-dessus, pour obtenir le point *ii)* (resp. *iii)*) on applique la prop. 4 du § 1 précisée par le lemme du § 2 (resp. le cor. 2 i) du § 1) ; les calculs nécessaires au point *v)* sont ceux de [2] ; on trouve :

Proposition 4. — *Soient* p *premier et* ℓ *premier* ≥ 5*, avec* $(\ell, p(p+1)) = 1$*. Posons* $N = F(\zeta_\ell + \zeta_\ell^{-1})$.

Alors, on a :

i) $A_p(\gamma, \langle\alpha\rangle) \in F(E[\ell])$ *;*

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

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

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

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

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

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

iv) suivant la parité de p*, l'idéal* $\big(A_p(\gamma, \langle\alpha\rangle)\big)$ *est un idéal ambige pour* $F\big(E[\ell]\big)/N$ *(resp.* $F\big(E[\ell]\big)/F(\zeta_\ell)\big)$ *;*

v) si $p \geq 3$*, l'élément de Stickelberger quadratique défini par* $A_p(\gamma, \langle\alpha\rangle)^\ell$ *est le quotient par* $p(p-1)$ *de celui, correspondant à la même valeur de* p*, décrit dans [2],* § *1.*

D'autre part pour $p = 2$, d'après le lemme 3 ci-dessus, le produit par $2^4\Delta(\Omega)$ de la résolvante $\widetilde{T}_2(P,Q)$ de [2] coïncide avec l'élément $A_2(\gamma, \langle\alpha\rangle)^2$, dont la puissance ℓ-ième appartient à N. De plus d'après la proposition 4 ci-dessus, et ceci améliore légèrement un résultat de [3], on a

$$A_2(\gamma, \langle\alpha\rangle)^\ell \in F(\zeta_\ell).$$

L'élément de Stickelberger quadratique défini dans $\mathbb{Q}[\Gamma]$, avec $\Gamma = \mathrm{Gal}(N/F)$, par $A_2(\gamma, \langle\alpha\rangle)^{2\ell}$ est donc le même que celui, correspondant à la valeur $p = 2$, décrit dans

[2], § 1 ; mais, l'élément de Stickelberger associé à $A_2(\gamma, \langle\alpha\rangle)^\ell$ appartient quant à lui à l'algèbre de groupe $\mathbb{Q}[\widetilde{\Gamma}]$, avec $\widetilde{\Gamma} = \mathrm{Gal}\big(F(\zeta_\ell)/F\big)$; nous laissons son calcul comme exercice au lecteur.

– ◇ –

Université de Grenoble I
Institut Fourier
Laboratoire de Mathématiques
associé au CNRS (URA 188)
B.P. 74
38402 ST MARTIN D'HÈRES Cedex (France)

(6 novembre 1995)