"Concernant la relation de distribution satisfaite par la fonction φ associée à un réseau complexe"

par Gilles ROBERT

Max–Planck–Institut
für Mathematik
Gottfried–Claren–Straße 26
D–5300 Bonn 3

Federal Republic of Germany

MPI/88-67

À Isabelle

Introduction

Soit z une variable complexe et notons $E(z)$ l'exponentielle usuelle de $2\pi i z$, de sorte que

$$E(0) = 1 \quad \text{et} \quad \frac{d \log E(z)}{dz} = 2\pi i \ .$$

Le propos de ce texte est de prouver pour la fonction φ associée à une base d'un réseau complexe (que l'on définit précisément au début du n°1) la formule de distribution (15) du n°4. La fonction $\tilde{F}$ qui y apparait est elle–même définie par la formule (8) du n°3 complétée par la formule (14) du n°4.

La preuve en est élémentaire. On notera l'analogie du résultat (15) avec l'identité

$$(1 - E(nz)) = \prod_{j=1}^{n} (1 - E(z + \tfrac{j}{n}))$$

où n désigne un entier > 0 , et où les nombres rationnels j/n , $1 \leq j \leq n$, forment un système complet de représentants de $\mathbb{Z}$ modulo $\frac{1}{n}\mathbb{Z}$, ainsi qu'avec des formules de distribution comparables satisfaites, en caractéristique positive, par les fonctions exponentielles attachées aux modules de Drinfeld de rang quelconque. Toutefois, si comme d'habitude on note $\sin \pi z$ la fonction $\frac{1}{2i}(E(z/2) - E(-z/2))$, l'analogie la plus proche est donnée par l'identité suivante entre fonctions cyclotomiques

$$\frac{(2\sin \pi nz)^d}{2\sin \pi dnz} = \prod_{j=1}^{n} \frac{(2\sin \pi (z + \frac{j}{n}))^d}{2\sin \pi d(z + \frac{j}{n})}$$

où l'entier $d > 0$ est supposé impair.

Bien sûr, le cas où les réseaux possèdent des multiplications complexes nécessite un traitement particulier. Celui–ci n'est pas abordé dans ce texte, exception faite pour l'obervation du n°12 final. Les numéros 1 à 3 sont introductifs. Nos résultats sont énoncés au n°4, et prouvés au n°11. Le corps du travail est contenu dans les numéros 5 à 10.

Remerciements

Je tiens à témoigner ici de la confiance que m'ont faite, malgré mon absence apparente de travail, mes collègues de l'Institut Fourier auprès de l'Université de Grenoble. Certes, je me dois aussi de remercier la section mathématique du C.N.R.S. francais pour l'abri qu'il m'offre durant cette année (universitaire) 1988/89. Enfin, c'est avec un profond plaisir que je rend grâce au professeur F. Hirzebruch pour son acceuil cordial au M.P.I. de Bonn où ce travail a été conçu.

Pour conclure, je ne saurais trop citer MM. K. Rubin et E. de Shalit qui par leur travail ont, chacun de leur côté, relancé le mien (cf. aussi fin du n^{o}4 et début du n^{o}11). Plus obscure, mais non moins certaine est la part de R. Schertz [8].

1) Soit $L \subset \mathbb{C}$ un réseau complexe, et (w_1, w_2) une base de celui–ci, choisie de façon que $\mathrm{Im}(w_2/w_1) > 0$.

Lorsque t parcourt le plan complexe, on note $\varphi(t; w_1, w_2)$ la fonction définie par le produit infini

$$
\begin{aligned}
\varphi(t; w_1, w_2) &= i\, E\left(\frac{W}{12}\right) E\left(-\frac{T}{2}\right) E\left(\frac{T}{2}\left(\frac{T-\bar{T}}{W-\bar{W}}\right)\right) \\
&\times (1 - E(T)) \prod_{d=1}^{\infty} (1 - E(T + dW))(1 - E(-T + dW))
\end{aligned}
\tag{1}
$$

où l'on désigne par T (resp. W) le quotient t/w_1 (resp. w_2/w_1).

Il s'agit de la fonction φ classique associée à la base (w_1, w_2) de L ; ses zéros (simples) sont les points t de $\mathbb{Z}w_1 + \mathbb{Z}w_2 = L$. Ses valeurs, lorsque t représente un point de torsion du tore $\mathbb{C}/L$, sont des fonctions modulaires très remarquables cf. C.L. SIEGEL [10] et les références incluses, ainsi que plus récemment K. RAMACHANDRA [4], G. ROBERT [5], [6], H.M. STARK [11], D. KUBERT & S. LANG [3], R. SCHERTZ [8] et bien d'autres. Aussi, depuis G. FALTINGS [1] § 7, lemme p. 417, on sait que la restriction à $\mathbb{C}/L \times \{0\}$ de "la fonction de Green de $\mathbb{C}/L$ " (dont la définition peut être rendue précise, cf. loc. cit. § 3) coïncide avec le logarithme du module de φ .

En particulier la fonction

$$
|\varphi|(t; L) \overset{\mathrm{dfn}}{=} |\varphi(t; w_1, w_2)|
\tag{2}
$$

ne dépend pas du choix de la base (w_1, w_2) de L , et est une fonction périodique de t de réseau de période L . Il résulte des propriétés des fonctions de Green, ou bien de [5] prop. 1, que pour tout sous–réseau L' de L on a

particulières aux courbes elliptiques

$$(3) \qquad |\varphi|(t;L) = \prod_{j=1}^{[L:L']} |\varphi|(t+z_j;L')$$

où les nombres complexes z_j , $1 \leq j \leq [L:L']$, parcourent un système complet de représentants du quotient L/L' . Bien sûr, on désigne ici par $[L:L']$ l'indice de L' dans L . On retrouvera aussi l'identité (3) ci–dessus en appliquant les techniques du présent travail, cf. n^{o}8, remarque.

A vrai dire, pour u un point de L et si on pose $U = u/w_1$, on déduit immédiatement de (1) l'identité

$$(4) \qquad \varphi(t + u; w_1, w_2) = \epsilon_L(u)\, E\left[\frac{1}{2}\left[\frac{\bar{U}T - U\bar{T}}{W - \bar{W}}\right]\right] \varphi(t; w_1, w_2)$$

avec $\epsilon_L(u) = \begin{cases} 1 , \text{ si } u \in 2L \\ -1 , \text{ si } u \in L \setminus 2L \end{cases}$;

l'affirmation (2) en résulte.

Par ailleurs, il peut être prouvé cf. A. WEIL [12] Chap. VI que l'équation fonctionnelle (4) détermine φ à une constante non nulle près. Par suite φ est la seule fonction vérifiant (4) pour laquelle

$$\lim_{\substack{t\to 0\\ t\neq 0}} \varphi(t;\, w_1, w_2)/t = \eta^{(2)}(w_1, w_2) \quad , \tag{5}$$

où suivant l'identité (1) on a posé

$$\eta^{(2)}(w_1, w_2) = \frac{2\pi}{w_1}\, E(\frac{W}{12}) \prod_{d=1}^{\infty} (1-E(dW))^2 \quad .$$

2) Avant de poursuivre nous avons besoin de préciser deux autres faits concernant la fonction φ.

i) On peut écrire

$$\varphi(t;\, w_1,\, w_2) = \eta^{(2)}(w_1,\, w_2)K(t;\, L) \tag{6}$$

où la fonction de Klein $K(t;\, L)$ ne dépend que du nombre complexe t et du réseau $L = \mathbb{Z}w_1 + \mathbb{Z}w_2$, et non du choix d'une base particulière $(w_1,\, w_2)$ de L.

En effet, l'aire de $\mathbb{C}/L$ définie par

$$a(L) = (w_2\overline{w}_1 - w_1\overline{w}_2)/2i = |w_1|^2 \mathrm{Im}(W)$$

ne dépend pas du choix de la base $(w_1,\, w_2)$ de L. Or, cf. [12] loc. cit., le facteur

$$2\pi i \, \frac{\overline{U}T - U\overline{T}}{W - \overline{W}}$$

de (4) peut être re-écrit en fonction de $t = w_1T$ et $u = w_1U$ comme

$$H_L(u,t) - H_L(t,u)$$

avec $H_L(v,v') \overset{dfn}{=} \pi\,\overline{v}\,v'/a(L)$. Il s'ensuit que $K(t;\, L)$ est l'unique fonction vérifiant (4) pour laquelle

$$\lim_{\substack{t \to 0 \\ t \neq 0}} K(t; L)/t = 1 \ .$$

ii) La puissance 12–ième de $\eta^{(2)}$

$$\Delta(L) = \eta^{(2)}(w_1, w_2)^{12}$$

ne dépend également que du réseau L et non de la base particulière (w_1, w_2) de L .

Ce fait crucial est délicat à établir. Pour une preuve nous renvoyons à F. HIRZEBRUCH & D. ZAGIER [2] § 7; d'autres références peuvent y être trouvées.

Il s'ensuit que si $M \in SL_2(\mathbb{Z})$ est une matrice carrée à coefficients entiers de déterminant 1, et si l'on définit le couple $(\tilde{w}_1, \tilde{w}_2)$ par l'identité matricielle

$$\begin{bmatrix} \tilde{w}_2 \\ \tilde{w}_1 \end{bmatrix} = M \begin{bmatrix} w_2 \\ w_1 \end{bmatrix} \ ,$$

il existe une racine 12–ième de l'unité $\rho^{(2)}(M) \in \mu_{12}$ telle que

$$\eta^{(2)}(\tilde{w}_1, \tilde{w}_2) = \rho^{(2)}(M)\eta^{(2)}(w_1, w_2) \ . \tag{7}$$

En fait, on sait après Dedekind cf. [2] loc. cit. définir ~~un homomorphisme~~ une application de $SL_2(\mathbb{Z})$ dans le groupe μ_{24} des racines 24–ième de l'unité dont l'homomorphisme

$$\rho^{(2)} : SL_2(\mathbb{Z}) \longrightarrow \mu_{12}$$

est le carré.

3) Fixons pour tout le reste de ce texte une matrice $B \in G\ell_2^{>0}(\mathbb{Z})$ à coefficients entiers et de déterminant >0 . On suppose que ce dernier disons $\det(B)$, est impair. On définit le couple $(\underline{w}_1, \underline{w}_2)$ par l'identité matricielle

$$\begin{bmatrix} \underline{w}_2 \\ \underline{w}_1 \end{bmatrix} = B^{-1} \begin{bmatrix} w_2 \\ w_1 \end{bmatrix}$$

et on note $\underline{L}$ le réseau engendré par $\underline{w}_1$ et $\underline{w}_2$. Par définition, l'indice $[\underline{L}:L]$ du réseau L dans $\underline{L}$ est égal à $\det(B)$.

On considère alors la fonction

$$F^B_{w_1,w_2}(z) = \frac{\varphi(z;\ w_1,\ w_2)^{\det(B)}}{\varphi(z;\ \underline{w}_1,\ \underline{w}_2)} \; ; \tag{8}$$

d'après l'identité (6) du $n^o 2$, celle–ci peut encore être écrite

$$\frac{\eta^{(2)}(w_1,\ w_2)^{\det(B)}}{\eta^{(2)}(\underline{w}_1,\ \underline{w}_2)} \quad \frac{K(z;\ L)^{[\underline{L}:L]}}{K(z,\ \underline{L})} \; . \tag{9}$$

Le quotient des deux fonctions de Klein dont celle relative à L est élevée à la puissance $[\underline{L}:L]$ est, comme la fonction $F^B_{w_1,w_2}$ elle–même, une fonction méromorphe de la variable complexe z de réseau de période L . Cela tient à deux faits: i) comme $[\underline{L}:L]$ est impair, la racine de l'unité

$$\epsilon_L(u)^{[\underline{L}:L]} / \epsilon_{\underline{L}}(u) \, , \quad u \in L \; ,$$

vaut 1 ; de plus ii) on a

$$a(L) = [\underline{L}:L]\ a(\underline{L})$$

de sorte que $H_{\underline{L}} = [\underline{L}:L]\, H_L$, si bien que la puissance $[\underline{L}:L]$ de l'exponentielle qui apparait dans l'identité (4) pour L n'est autre, lorsque u appartient à L , que l'exponentielle qui apparait dans (4) pour $\underline{L}$. En fait, si les nombres complexes t_i , $1 \leq i \leq [\underline{L}:L]$, forment un système complet de représentants du quotient $\underline{L}/L$, le diviseur commun (non réduit) de ces fonctions est

$$\det(B)(0)_L - \sum_{i=1}^{[\underline{L}:L]} (t_i)_L \tag{10}$$

où $(t_i)_L$ désigne le point du tore $\mathbb{C}/L$ associé à t_i .

D'après l'identité (5) du n°1, on a

$$\lim_{\substack{z\to 0\\ z\neq 0}} F^B_{w_1,w_2}(z)/z^{\det(B)-1} = {\eta^{(2)}_{(w_1,w_2)}}^{\det(B)} / \eta^{(2)}_{(\underline{w}_1,\underline{w}_2)} \quad ; \tag{11}$$

de même, lorsque $z \longrightarrow t_i$ pour t_i point de $\underline{L}$ n'appartenant pas à L , on a

$$(12) \qquad \lim_{\substack{z \to t_i \\ z \neq t_i}} (z-t_i) F^{B}_{w_1, w_2}(z) = \epsilon_{\underline{L}}(t_i) \frac{\varphi(t_i\, ;\, w_1,\ w_2)^{\det(B)}}{\eta^{(2)}(\underline{w}_1,\ \underline{w}_2)}$$

avec $\epsilon_{\underline{L}}(t_i)$ égal à 1 ou –1 suivant que t_i appartient à $2\underline{L}$ ou non.

4) L'objet de ce texte est de prouver, pour chaque matrice $B \in G\ell_2^{>0}(\mathbb{Z})$ de déterminant premier à 6, l'existence d'un nombre complexe non nul $\rho(B)$ tel que les propriétés (a) et (b) ci–dessous soient vérifiées.

(a) Le quotient

$$\tilde{\eta}^{(2)}(L,\underline{L}) = \rho(B)^{-1}\eta^{(2)}(w_1, w_2)^{\det(B)}/\eta^{(2)}(\underline{w}_1, \underline{w}_2) \tag{13}$$

ne dépend que des réseaux L et $\underline{L}$ et non du choix d'une base de ceux–ci.

(b) Posons

$$\tilde{F}(z; L, \underline{L}) = \rho(B)^{-1}\, F^{B}_{w_1,w_2}(z) \ . \tag{14}$$

D'après l'identité (9) du n^{o}3, il résulte de (a) que, pour z fixé, ce quotient ne dépend aussi que des réseaux L et $\underline{L}$ et non du choix d'une base de ceux–ci.

Supposons l'existence de deux autres réseaux L' et $\underline{L}'$ tels que le diagramme ci–contre soit satisfait. Autrement dit, on demande i) les inclusions $L' \subset L \subset \underline{L}$ et $L' \subset \underline{L}' \subset \underline{L}$, ii) l'isomorphisme des quotients $\underline{L}/L$ et $\underline{L}'/L'$ d'une part et des quotients $\underline{L}/\underline{L}'$ et L/L' d'autre part, et iii) la disjonction linéaire de L et $\underline{L}'$ au–dessus de L', i.e. l'égalité

$$\begin{tikzcd}
 & \underline{L} \\
\underline{L}' \arrow[ur, dash, "/"] & \\
 & L \arrow[uu, dash, "//"'] \\
L' \arrow[uu, dash, "//"] \arrow[ur, dash, "/"] &
\end{tikzcd}$$

$$\underline{L}' \cap L = L' .$$

Vu la condition d'isomorphisme ii) ci–dessus, on sait qu'alors $\underline{L}$ est le plus petit réseau contenant à la fois $\underline{L}'$ et L .

Alors, chaque fois qu'une telle situation existe, on a l'égalité

$$\tilde{F}(z; L, \underline{L}) = \prod_{j=1}^{[L:L']} \tilde{F}(z + z_j; L', \underline{L}') \tag{15}$$

où les nombres complexes z_j , $1 \leq j \leq [L:L']$, parcourent un système complet de représentants du quotient L/L' .

Remarque 1. Ces conditions sont très fortes. En effet, désignons par Π une matrice de passage de L à L' . En appliquant ces conditions aux matrices $\Pi = n\,\mathrm{Id}$ avec n entier >0 , premier à $\det(B)$, on voit que l'unicité de $\rho(B)$ est assurée.

En effet, soit $\rho'(B)$ un autre nombre complexe non vul vérifiant (a) et (b). Soit ρ son quotient par $\rho(B)$. Alors, d'après (15) il est clair que ρ vérifie les identités

$$\rho^{n^2} = \rho ,$$

pour tout entier $n > 0$, premier à $\det(B)$. Celles–ci imposent $\rho = 1$.

(c) Il résulte de l'unicité prouvée ci–dessus que l'on a pour toutes matrices B , $D \in Gl_2^{>0}(\mathbb{Z})$, de déterminant premier à 6, la formule de multiplicativité

$$\rho(BD) = \rho(B)^{\det(D)}\rho(D) . \tag{16}$$

En effet, celle–ci résulte de l'identité

$$F^{BD}_{w_1,w_2} = (F^{B}_{w_1,w_2})^{\det(B)}\, F^{D}_{\underline{w}_1,\underline{w}_2} \tag{17}$$

entre fonctions méromorphes.

(d) En fait, on verra au n°11, remarque, que $\rho(B)$ est une racine 12–ième de l'unité; on en donnera alors un moyen de calcul.

(e) D'ailleurs, lorsque $B \in SL_2(\mathbb{Z})$, la relation (a) impose l'égalité

$$\rho(B) = \rho^{(2)}(B) \tag{18}$$

où $\rho^{(2)}(B)$ est la racine 12–ième de l'unité définie par l'identité (7) du n°2.

<u>Remarque</u> 2. Réciproquement, ce dernier fait (e) joint à la formule de multiplicativité (16) de (c) assure la véracité de (a).

En effet, pour M et N éléments de $SL_2(\mathbb{Z})$, on a d'après (16) l'égalité

$$\rho(MBN)/\rho(B) = \rho(M)^{\det(B)}\rho(N) \ ;$$

or, lorsque l'on passe des bases respectives (w_1, w_2) et $(\underline{w}_1, \underline{w}_2)$ des réseaux L et $\underline{L}$ aux bases respectives $(\tilde{w}_1, \tilde{w}_2)$ et $(\tilde{\underline{w}}_1, \tilde{\underline{w}}_2)$ des mêmes réseaux, celles–ci étant définies par les identités matricielles

$$\begin{bmatrix} \tilde{\underline{w}}_2 \\ \tilde{\underline{w}}_1 \end{bmatrix} = (\mathrm{MBN})^{-1}\begin{bmatrix} \tilde{w}_2 \\ \tilde{w}_1 \end{bmatrix} , \quad \begin{bmatrix} \tilde{w}_2 \\ \tilde{w}_1 \end{bmatrix} = \mathrm{M}\begin{bmatrix} w_2 \\ w_1 \end{bmatrix} \quad \text{et} \quad \begin{bmatrix} \tilde{\underline{w}}_2 \\ \tilde{\underline{w}}_1 \end{bmatrix} = \mathrm{N}^{-1}\begin{bmatrix} \underline{w}_2 \\ \underline{w}_1 \end{bmatrix} ,$$

on constate que la définition (7) du n$^{\mathrm{o}}$2 pour l'invariant $\rho^{(2)}$ impose au quotient $\eta^{(2)}(w_1, w_2)^{\det(B)}/\eta^{(2)}(\underline{w}_1, \underline{w}_2)$ le facteur $\rho^{(2)}(\mathrm{M})^{\det(B)}\rho^{(2)}(\mathrm{N})$. On conclut par l'égalité (18) de (e).

Nota. La puissance 12–ième de l'identité (15) ci–dessus est "presque" connue. Certes, lorsque les quatre réseaux possèdent des multiplications complexes par l'anneau des entiers d'un même corps quadratique imaginaire, elle résulte de la relation de distribution prouvée dans le livre [9] de Ehud de SHALIT, § 2.3 p. 50 (la relation citée est valable même si det(B) n'est pas premier à 6).

Les assertions de ce numéro seront prouvées au n$^{\mathrm{o}}$11. Les numéros intermédiaires 5 à 10 sont employés à rigidifier la situation évoquée plus haut, puis à en tirer certaines conséquences. Enfin, le n$^{\mathrm{o}}$12 prouve, dans le cas de multiplication complexe, une relation particulière satisfaite par $\tilde{\eta}^{(2)}(\mathrm{L},\underline{\mathrm{L}})$.

5) Soient donc $\underline{L}$, $\underline{L}'$, L' et L quatre réseaux définis comme dans le n^{o}4 (b), et soit (w_1, w_2) une base de L telle que $\mathrm{Im}(w_2/w_1) > 0$. On impose B comme matrice de passage de $\underline{L}$ à L d'une part, et de $\underline{L}'$ à L' d'autre part. De plus, on choisit la matrice de passage Π de L à L' de façon que les identités matricielles ci–dessous, où $(\underline{w}_1, \underline{w}_2)$, $(\underline{w}'_1, \underline{w}'_2)$ et (w'_1, w'_2) sont respectivement des bases de $\underline{L}$, $\underline{L}'$ et L' , soient vérifiées

$$\begin{bmatrix} \underline{w}'_2 \\ \underline{w}'_1 \end{bmatrix} = B^{-1} \begin{bmatrix} w'_2 \\ w'_1 \end{bmatrix} , \quad \begin{bmatrix} w'_2 \\ w'_1 \end{bmatrix} = \Pi \begin{bmatrix} w_2 \\ w_1 \end{bmatrix} \quad \text{et} \quad \begin{bmatrix} w_2 \\ w_1 \end{bmatrix} = B \begin{bmatrix} \underline{w}_2 \\ \underline{w}_1 \end{bmatrix} .$$

D'un coté,il existe donc:

i) deux matrices U et V de $Sl_2(\mathbb{Z})$ telles que la matrice $U \Pi V$ fasse passer de la base $(\underline{w}_1, \underline{w}_2)$ de $\underline{L}$ à la base $(\underline{w}'_1, \underline{w}'_2)$ de $\underline{L}'$; autrement dit, on suppose que l'identité

$$(19) \qquad B^{-1} \Pi B = U \Pi V , \ U \text{ et } V \in Sl_2(\mathbb{Z}) ,$$

est vérifiée par la matrice Π (la matrice B étant supposée donnée). D'autre part, on rappelle que:

ii) les réseaux $\underline{L}'$ et L sont supposés linéairement disjoints au–dessus de L' ; autrement dit, on suppose l'égalité

$$\underline{L}' \cap L = L' ;$$

si l'identité (19) ci–dessus est vraie, cette dernière condition est certainement satisfaite dès que les déterminants respectifs det(B) et det(Π) des matrices B et Π sont premiers entre eux.

Définition. On appelle $\mathscr{A}_B$ l'ensemble des matrices Π qui satisfont aux deux conditions i) et ii) ci-dessus.

Nota. L'ensemble $\mathscr{A}_B \subset G\ell_2^{>0}(\mathbb{Z})$ n'est pas stable par multiplication. Cependant, soit n un entier $\neq 0$ premier à $\det(B)$; alors, on a

$$n \, \mathrm{Id} \in \mathscr{A}_B ,$$

et le produit $n\Pi$ d'une telle matrice avec un élément Π de $\mathscr{A}_B$ appartient encore à $\mathscr{A}_B$.

On a la remarque suivante:

Lemme. Soit $\Pi \in \mathscr{A}_B$; on note $z_j \in \mathbb{C}$, $1 \leq j \leq \det \Pi$ un système complet de représentants du quotient L/L'. Alors, il existe une constante non nulle

$$C = C_{w_1,w_2}(\Pi,B)$$

telle que l'on ait l'égalité

$$F^B_{w_1,w_2}(z) = C \prod_{j=1}^{\det(\Pi)} F^B_{w'_1,w'_2}(z + z_j) \tag{20}$$

entre fonctions méromorphes de la variable z.

Preuve: Comme il s'agit de comparer deux fonctions méromorphes admettant le réseau de périodes $L' \subset L$, il suffit de comparer leurs diviseurs relativement à L'.

Pour le membre de gauche de (20), son diviseur relativement à L s'écrit

$$\det(B)\,(0)_L - \sum_{i=1}^{\det(B)} (t_i)_L$$

où les $t_i \in \mathbb{C}$, $1 \leq i \leq \det(B)$, parcourent un système complet de représentants de $\underline{L}/L$ cf. identité (10) du n°3. Relativement à L', ce diviseur peut donc être re–écrit

$$\det(B) \sum_{j=1}^{\det(\Pi)} (z_j)_{L'} - \sum_{i=1}^{\det(B)} \sum_{j=1}^{\det(\Pi)} (t_i + z_j)_{L'} .$$

Par ailleurs, pour le membre de droite de (20) le diviseur de son j–ième terme s'écrit

$$\det(B)\,(z_j)_{L'} - \sum_{i=1}^{\det(B)} (t_i' + z_j)_{L'}$$

où les $t_i' \in \mathbb{C}$, $1 \leq i \leq \det(B)$, parcourent un système complet de représentants de $\underline{L}'/L'$.

L'égalité des deux diviseurs sera donc établie si l'on s'assure que les nombres t_i', $1 \leq i \leq \det(B)$, forment un système complet de représentants de $\underline{L}/L$. Vu l'inclusion $\underline{L}' \subset \underline{L}$, il suffit pour cela de vérifier que la différence $t_k' - t_\ell'$ de deux quelconques d'entre eux ne peut appartenir à L que si $k = \ell$. Or si $t_k' - t_\ell'$ appartient à L, comme cette différence appartient déjà à $\underline{L}'$, il résulte de la disjonction linéaire de $\underline{L}'$ et L au–dessus de L' que $t_k' - t_\ell'$ appartient à L' ; d'où l'égalité demandée.

On a aussi l'observation élémentaire:

<u>Remarque</u>. On suppose les matrices B et Π fixées. <u>Alors, la constante</u> $C_{w_1,w_2}(\Pi,B)$ <u>ne dépend que du quotient</u> $W = w_2/w_1$ <u>des deux nombres complexes</u> w_1 <u>et</u> w_2 (supposés tels que $\operatorname{Im} W > 0$).

En effet, pour tout nombre complexe $\lambda \neq 0$, on a

$$\varphi(\lambda z;\, \lambda w_1,\, \lambda w_2) = \varphi(z;\, w_1,\, w_2)$$

et par suite $F^B_{\lambda w_1,\lambda w_2}(\lambda z) = F^B_{w_1,w_2}(z)$.

6) Plus généralement, pour chaque couple (w_1, w_2) de nombres complexes tels que $\operatorname{Im} W > 0$, fixons une fonction

$$F_{w_1,w_2} : z \longmapsto F_{w_1,w_2}(z)$$

à valeurs complexes, non identiquement nulle, périodique de réseau de périodes $L = \mathbb{Z}w_1 + \mathbb{Z}w_2$.

Je précise que je demande seulement à la fonction F_{w_1,w_2} d'être définie sur une partie <u>non vide</u> de $\mathbb{C}$, invariante sous les translations de L, et d'être <u>non nulle</u> en au moins un point.

On dira que l'ensemble des fonctions F_{w_1,w_2} <u>est</u> (faiblement) <u>multiplicatif</u> s'il existe une famille $\mathscr{A}$ de matrices, éléments de $G\ell_2^{>0}(\mathbb{Z})$, telle que les trois propriétés i), ii) et iii) ci–dessous soient satisfaites:

i) Il existe un entier $d_{\mathscr{A}} \geq 1$ ne dépendant que de $\mathscr{A}$, tel que la matrice $n\,\mathrm{Id}$, avec n entier >0, appartient à $\mathscr{A}$ dès que n est premier à $d_{\mathscr{A}}$.

ii) Pour toute matrice $\Pi \in \mathscr{A}$, <u>il existe une constante complexe</u> (non nulle) $C_{w_1,w_2}(\Pi)$ telle que

$$(21) \qquad F_{w_1,w_2}(z) = C_{w_1,w_2}(\Pi) \prod_{j=1}^{\det(\Pi)} F_{w_1',w_2'}(z + z_j)$$

où le couple (w_1', w_2') est défini par l'identité matricielle

$$\begin{bmatrix} w_2' \\ w_1' \end{bmatrix} = \Pi \begin{bmatrix} w_2 \\ w_1 \end{bmatrix} .$$

Ici comme précédemment, pour L' le réseau engendré par w_1' et w_2', on suppose que les nombres complexes z_j, $1 \leq j \leq \det(\Pi)$, forment un système complet de représentants du quotient L/L'.

iii) Si $\Pi \in \mathscr{A}$ et $n\,\mathrm{Id} \in \mathscr{A}$, avec n entier > 0 premier à $d_{\mathscr{A}}$, alors le produit $n\Pi$ des matrices $n\,\mathrm{Id}$ et Π de $\mathscr{A}$ appartient aussi à $\mathscr{A}$.

Ecrivons alors la relation (21) pour la matrice $n\Pi$ de $\mathscr{A}$ des deux facons suivantes: d'une part en faisant d'abord Π puis $n\,\mathrm{Id}$, et d'autre part en faisant $n\,\mathrm{Id}$ puis Π. On trouve que la constante $C_{w_1,w_2}(n\,\Pi)$ est identique à l'un et à l'autre des deux produits ci–dessous

$$C_{w_1,w_2}(\Pi)\, C_{w_1',w_2'}(n\,\mathrm{Id})^{\det(\Pi)} = C_{w_1,w_2}(n\,\mathrm{Id})\, C_{nw_1,nw_2}(\Pi)^{n^2}$$

dont l'égalité est ainsi démontrée.

<u>Hypothèse</u>. Pour chaque élément Π de $\mathscr{A}$, on suppose désormais que, lorsque les paramètres complexes w_1 et w_2 varient, la constante $C_{w_1,w_2}(\Pi)$ ne dépend que de la valeur du quotient w_2/w_1.

La relation ci–dessus se re–écrit alors:

(22) $$C_{w_1,w_2}(\Pi)^{n^2-1} = C_{w'_1,w'_2}(n\ \mathrm{Id})^{\det(\Pi)}/C_{w_1,w_2}(n\ \mathrm{Id})$$

où (w'_1,w'_2) est défini par $\begin{bmatrix} w'_2 \\ w'_1 \end{bmatrix} = \Pi \begin{bmatrix} w_2 \\ w_1 \end{bmatrix}$.

Appliquons ceci à $C_{w_1,w_2}(\Pi,B)$, la matrice B étant fixée. On trouve que l'ensemble des fonctions

$$(w_1, w_2) \longmapsto F^B_{w_1,w_2}$$

est faiblement multiplicatif; en effet, il résulte du n°5 que $\mathscr{A} \overset{dfn}{=} \mathscr{A}_B$ vérifie les conditions i), ii) et iii) ci–dessus, l'entier $d_{\mathscr{A}}$ pouvant être choisi égal à $\det(B)$.

Comme d'après la remarque à la fin du n°5, la constante $C_{w_1,w_2}(\Pi,B)$ vérifie l'hypothèse encadrée ci–dessus on peut lui appliquer la relation (22). On en déduit donc:

<u>Remarque</u>. Si, pour un entier $n \geq 2$ premier à $\det(B)$, les constantes $C_{w_1,w_2}(n\ \mathrm{Id},B)$ et $C_{w'_1,w'_2}(n\ \mathrm{Id},B)$ <u>sont des racines de l'unité</u>, alors il en va de même de la constante $C_{w_1,w_2}(\Pi,B)$.

7) Soit n un entier ≥ 2 fixé. L'étape suivante consiste à évaluer le produit

$$\prod_{(i,j)\in J} \varphi(iw_1/n + jw_2/n; w_1, w_2)$$

pour $J = \{(i,j) \mid 0 \leq i, j \leq n-1 , (i,j) \neq (0,0)\}$; on utilise pour cela le produit infini convergent donné par la formule (1).

On notera d'abord que le produit

$$\prod_{1\leq i\leq n-1} (1 - E(i/n)) ,$$

égal à la limite quand $X \longrightarrow 1$ du quotient $(1 - X^n)/(1 - X)$, vaut n . D'autre part le produit

$$\prod_{i=0}^{n-1} \prod_{j=1}^{n-1} (1 - E(i/n + jW/n)) ,$$

égal à $\prod_{1\leq j\leq n-1} (1 - E(jW))$, est précisément l'inverse du produit

$$\prod_{(i,j)\in J} \prod_{d\geq 1} (1 - E(i/n + (j + dn)W/n)) \tag{23}$$

$$(1 - E(-i/n + (-j + dn)W/n)) .$$

En effet, ce dernier produit, s'il était pris sur tous les entiers i et j compris entre 0 et n–1 , serait égal au produit

$$\prod_{j=0}^{n-1} \prod_{d=1}^{\infty} (1 - E((j + dn)W))(1 - E((-j + dn)W))$$

soit après changement d'indices

$$\prod_{j'=0}^{n-1} (1 - E(j'W)) \prod_{d' \geq n} (1 - E(d'W))^2 \ .$$

Mais le terme correspondant à $(i,j) = (0,0)$ vaut

$$\prod_{d \geq 1} (1 - E(dW))^2$$

de sorte que le produit (23) vaut en fait

$$1/\prod_{j'=0}^{n-1} (1 - E(j'W)) \ .$$

Reste à évaluer le produit correspondant aux quatre premiers termes de (1). Commençons par l'exponentielle de la forme quadratique $\frac{T}{2}\left[\frac{T-\overline{T}}{W-\overline{W}}\right]$. Comme pour $T = i/n + jW/n$ on a $(T - \overline{T})/(W - \overline{W}) = j/n$, on trouve à sommer

$$\frac{1}{2} \sum_{0 \leq i,j \leq n-1} \left(\frac{1}{n} + \frac{i}{n}W\right)\frac{i}{n}$$

$$= \frac{1}{2} \sum_{0 \leq i,j \leq n-1} \frac{ij}{n^2} + \frac{1}{2} \sum_{0 \leq j \leq n-1} \frac{j^2}{n} W \ .$$

La première somme du membre de droite vaut aussi

$$\frac{1}{2}\Big(\sum_{0\le i\le n-1}\frac{i}{n}\Big)\Big(\sum_{0\le j\le n-1}\frac{j}{n}\Big),$$

soit $\frac{1}{8}(n-1)^2$; quand à la seconde vu l'identité

$$\sum_{0\le j\le n-1} j^2 = \frac{(n-1)n(2n-1)}{6},$$

elle vaut $(n-1)(2n-1)W/12$. En tout, on trouve donc

a) $\quad E(\frac{1}{8}(n-1)^2 + (n-1)(2n-1)\frac{W}{12})$.

D'autre part, le troisième terme $E(-T/2)$ fournit

$$-\frac{1}{2}\sum_{0\le i\le n-1} i - \frac{1}{2}\sum_{0\le j\le n-1} jW ,$$

d'où

b) $\quad E(-\frac{n(n-1)}{4} - \frac{n(n-1)}{4}W)$.

Pour les deux premiers termes ils fournissent

c) $\quad E(\frac{n^2-1}{4} + \frac{n^2-1}{12}W)$.

Développons le produit de a), b) et c): on vérifie facilement que le coefficient de W vaut 0 . Quant aux termes constants, ils fournissent $E((n^2-1)/8)$. On a ainsi prouvé:

Lemme. Soit n un entier ≥ 2 fixé. Alors, le produit

$$\prod_{(i,j)\in J} \varphi(iw_1/n + jw_2/n;\, w_1,\, w_2)$$

est indépendant du choix de la base (w_1, w_2) (telle que $\mathrm{Im}(w_2/w_1) > 0$) du réseau $L = \mathbb{Z}w_1 + \mathbb{Z}w_2$; il vaut

$$n\, E(\tfrac{n^2-1}{8})\ .$$

8) Appliquons ce lemme (du n^{o}7) au calcul de $C_{w_1,w_2}(n\ \mathrm{Id}, B)$. On a:

Proposition. Soit n un entier ≥ 2 premier à $\det(B)$. Alors, il existe une racine de l'unité

$$\zeta_n(B; w_1, w_2) \in \mu_{2n}$$

d'ordre un diviseur de $2n$ telle que

$$C_{w_1,w_2}(n\ \mathrm{Id}, B) = \zeta_n(B; w_1, w_2)/E((\frac{n^2-1}{8})(\det(B) - 1)) \quad ;$$

en particulier $C_{w_1,w_2}(n\ \mathrm{Id}, B)$ est une racine de l'unité.

Avant de prouver ce résultat, énonçons quelques unes de ses conséquences:

Corollaire 1. Pour toute valeur de la matrice B (supposée de déterminant impair) la constante

$$C_{w_1,w_2}(2\ \mathrm{Id}, B)$$

est une racine 4–ième de l'unité.

Joignant ce résultat à la remarque de la fin du n^{o}6, on obtient:

Corollaire 2. Pour tout B comme ci–dessus et tout Π élément de $\mathscr{A}_B$, la constante

$$C_{w_1,w_2}(\Pi, B)$$

est une racine de l'unité.

Il s'ensuit:

Corollaire 3. La constante $C_{w_1,w_2}(\Pi, B)$ ne dépend pas des valeurs de w_1 et w_2.

Preuve: Puisque la fonction

$$(w_1, w_2) \longmapsto C_{w_1,w_2}(\Pi, B)$$

a été définie (cf. n°5, lemme) comme quotient de fonctions continues non nulles en le paramètre w_2/w_1 sa valeur, contrainte à être une racine de l'unité, est nécessairement constante.

Il nous reste à prouver la proposition:

Preuve de la proposition: Pour comparer les fonctions

$$F^B_{w_1,w_2}(z) \text{ et } \prod_{0\leq i,j\leq n-1} F^B_{nw_1,nw_2}(z + iw_1 + jw_2) \ ,$$

il suffit de voir si le quotient de chacune d'elles par $z^{\det(B)-1}$ possède la même limite (non nulle) quand $z \longrightarrow 0$. Or, la première limite vaut

$$\eta^{(2)}(w_1, w_2)^{\det(B)} / \eta^{(2)}(\underline{w}_1, \underline{w}_2) \ ;$$

quand à la seconde elle est égale au produit

$$\frac{\eta^{(2)}(nw_1, nw_2)^{\det(B)}}{\eta^{(2)}(n\underline{w}_1, n\underline{w}_2)} \prod_{(i,j)\in J} \frac{\varphi(iw_1 + jw_2;\ nw_1,\ nw_2)^{\det(B)}}{\varphi(iw_1 + jw_2;\ n\underline{w}_1,\ n\underline{w}_2)} \ .$$

Mais alors, d'après le lemme du n°7 appliqué au réseau nL , on a

$$\eta^{(2)}(nw_1, nw_2) \prod_{(i,j)\in J} \varphi(iw_1 + jw_2; nw_1, nw_2) = E\left(\frac{n^2-1}{8}\right) \eta^{(2)}(w_1, w_2) \ ; \tag{24}$$

en effet, on sait a priori que $\eta^{(2)}(nw_1, nw_2) = \frac{1}{n}\, \eta^{(2)}(w_1, w_2)$. D'autre part, la formule (4) du n°1 assure l'égalité

$$\prod_{(i,j)\in J} \varphi(iw_1 + jw_2; n\underline{w}_1, n\underline{w}_2) = \zeta_n \prod_{(i',j')\in J} \varphi(i'\underline{w}_1 + j'\underline{w}_2; n\underline{w}_1, n\underline{w}_2) \ ,$$

où $\zeta_n \overset{\mathrm{dfn}}{=} \zeta_n(B; w_1, w_2)$ est une certaine racine 2n–ième de l'unité: en effet, comme n est premier à det(B) , les éléments $iw_1 + jw_2$, $0 \leq i, j \leq n-1$, fournissent bien un système complet de représentants du quotient $\underline{L}/n\underline{L}$. En appliquant alors le lemme du n°7 au réseau $n\underline{L}$, on trouve

$$\eta^{(2)}(n\underline{w}_1, n\underline{w}_2) \prod_{(i,j)\in J} \varphi(iw_1 + jw_2; n\underline{w}_1, n\underline{w}_2) = \zeta_n E\left(\frac{n^2-1}{8}\right) \eta^{(2)}(\underline{w}_1, \underline{w}_2) \ . \tag{25}$$

Elevant (24) à la puissance det(B) et divisant le tout par (25), on obtient après simplification

$$C_{w_1,w_2}(n\,\mathrm{Id}, B) = \zeta_n(B; w_1, w_2)/E((\tfrac{n^2-1}{8})(\det(B)-1)) \ .$$

La proposition est démontrée.

Remarque. On peut aussi déduire du lemme du n^{o}7 la stricte multiplicativité des fonctions $|\varphi|(t, L)$, i.e. l'identité (3) du n^{o}1.

Voici une esquisse de la preuve. Pour w_1, w_2 des nombres complexes tels que $\mathrm{Im}\ W > 0$, considérons l'application

$$(w_1, w_2) \longmapsto F_{w_1,w_2}(t) = |\varphi|(t, L)$$

avec $L = \mathbb{Z}w_1 + \mathbb{Z}w_2$. On vérifie d'abord que les fonctions $|\varphi|(t, L)$ sont faiblement multiplicatives; commes les constantes associées par ailleurs réelles >0, disons $|C|_{w_1,w_2}(\Pi)$, satisfont à l'hypothèse encadrée du n^{o}6 la relation (22) assure qu'elles vérifient l'identité

$$|C|_{w_1,w_2}(\Pi)^{n^2-1} = |C|_{w'_1,w'_2}(n\,\mathrm{Id})^{\det(\Pi)}/|C|_{w_1,w_2}(n\,\mathrm{Id}) \tag{26}$$

pour tout $\Pi \in G\ell_2^{>0}(\mathbb{Z})$ et tout entier $n > 0$. Mais, d'après le lemme du n^{o}7, on a

$$|C|_{w_1,w_2}(n\,\mathrm{Id}) = 1$$

quelques que soient les nombres complexes w_1 et w_2, et l'entier $n > 0$. Vu (26) la stricte multiplicativité des fonctions $|\varphi|(t, L)$ en résulte.

9) Au vu du corollaire 3 du n^{o}8, adoptons la définition suivante:

Définition. On pose

$$C(\Pi, B) = C_{w_1,w_2}(\Pi, B)$$

pour un choix arbitraire des valeurs des paramètres complexes w_1 et w_2, tels que $\mathrm{Im}(w_2/w_1) > 0$.

Suivons alors l'un et l'autre diagrammes ci–dessous.

I)
$$\begin{tikzcd}
\underline{L}'' \arrow[d, "B"] \arrow[r, dash] & \underline{L}' \arrow[d, "B"] \arrow[r, dash] & \underline{L} \arrow[d, "B"] \\
L'' & L' \arrow[l, "Q"'] & L \arrow[l, "\Pi"']
\end{tikzcd}$$

II)
$$\begin{tikzcd}
\underline{\underline{L}}' \arrow[d, "D"'] \arrow[r, dash] & \underline{\underline{L}} \arrow[d, "D"] \\
\underline{L}' \arrow[d, "B"'] & \underline{L} \arrow[l, "B^{-1}\Pi B"'] \arrow[d, "B"] \\
L' & L \arrow[l, "\Pi"']
\end{tikzcd}$$

Dans le cas de I, on trouve la formule

$$C(Q\Pi, B) = C(Q, B)^{\det(\Pi)} C(\Pi, B) \tag{27}$$

pourvu que les trois termes aient un sens, c'est–à–dire que Π, Q et $Q\Pi$ appartiennent à $\mathscr{O}_B$. Dans le cas de II, on trouve la formule

$$C(\Pi, BD) = C(\Pi, B)^{\det(D)} C(B^{-1}\Pi B, D) \tag{28}$$

pourvu que les deux termes du membre de droite aient un sens, c'est–à–dire que Π (resp. $B^{-1}\Pi B$) appartienne à $\mathscr{A}_B$ (resp. $\mathscr{A}_D$).

Tandis que la première formule résulte d'un calcul direct à partir de la définition de $C_{w_1,w_2}(\Pi, B)$ ($n^o 5$, égalité (20)), la dernière formule résulte de l'égalité (17) entre fonctions méromorphes, déjà utilisée au $n^o 4$. Dans ce numéro et le suivant, ces formules vont nous permettre d'obtenir de précieux renseignements sur $C(\Pi, B)$. Appliquons d'abord (27); on trouve:

Fait 1. i) La constante $C(\Pi, B)$ est une racine 12–ième de l'unité.

ii) De plus, si $(\det(B), 6) = 1$, alors on a

$$C(\Pi, B) = \zeta(B)^{\det(\Pi)-1} \tag{29}$$

où $\zeta(B)$ est la racine 12–ième de l'unité définie par

$$\zeta(B) = C(2\,\mathrm{Id}, B)^3 / C(3\,\mathrm{Id}, B) \ . \tag{30}$$

Preuve: En écrivant 2Π comme le produit de $2\,\mathrm{Id}$ et de Π de deux manières différentes, et en appliquant la formule (27) on trouve

$$C(\Pi, B)^3 = C(2\,\mathrm{Id}, B)^{\det(\Pi)-1} \ .$$

Or, on sait déjà par le corollaire 1 du n°8 que $C(2\,\mathrm{Id}, B)$ est une racine 4–ième de l'unité, d'où i).

Si de plus $(\det(B), 3) = 1$, alors on vérifie de même par la formule (27) l'identité

$$C(\Pi, B)^8 = C(3\,\mathrm{Id}, B)^{\det(\Pi)-1}$$

et il résulte de la proposition du n°8 que $C(3\,\mathrm{Id}, B)$ est une racine 6–ième de l'unité.

Il s'ensuit que $\zeta(B) = C(2\,\mathrm{Id}, B)^3/C(3\,\mathrm{Id}, B)$ est bien une racine 12–ième de l'unité dont la puissance $\deg(\Pi) - 1$ est égale à $C(\Pi, B)$, d'où ii).

Ce résultat est complété par:

Fait 2. Si $B \in SL_2(\mathbb{Z})$ alors, pour la définition (30) de $\zeta(B)$, on a

$$\zeta(B) = 1/\rho^{(2)}(B)$$

où $\rho^{(2)}(B)$ est la racine 12–ième de l'unité définie par la formule (7) du n°2 .

Preuve. Il suffit de prouver l'identité

$$C(\Pi, B) = \rho^{(2)}(B)^{1-\deg(\Pi)} \quad . \tag{31}$$

En effet, appliquée aux termes du quotient définissant $\zeta(B)$, celle–ci assure bien le fait 2.

Or, pour calculer le membre de gauche de (31), il s'agit de comparer d'une part

$$\eta^{(2)}(w_1, w_2)/\eta^{(2)}(\underline{w}_1, \underline{w}_2)$$

et d'autre part

$$[\eta^{(2)}(w'_1, w'_2)/\eta^{(2)}(\underline{w}'_1, \underline{w}'_2)]^{\deg(\Pi)} \quad ;$$

en effet, les fonctions de Klein ne dépendant que du réseau L (resp. L') n'apparaissent pas dans les expressions respectives ci–dessus de $F^B_{w_1,w_2}$ et du produit des $F^B_{w'_1,w'_2}$, qui proviennent l'une et l'autre de l'identité (9) du n°3. Bien sûr, les bases $(\underline{w}_1, \underline{w}_2)$, $(\underline{w}'_1, \underline{w}'_2)$ et (w'_1, w'_2) sont définies par la base (w_1, w_2) comme au début du n°5. Comme B est la matrice de passage, d'une part de $(\underline{w}_1, \underline{w}_2)$ à (w_1, w_2) et d'autre part de $(\underline{w}'_1, \underline{w}'_2)$ à (w'_1, w'_2) , les deux expressions en question sont respectivement égales d'après la formule (7) du n°2 à $\rho^{(2)}(B)$ et $\rho^{(2)}(B)^{\det(\Pi)}$, d'où l'identité (31).

10) Pour pouvoir utiliser efficacement la formule (28) du n^{o}9, énoncons d'abord le lemme bien connu suivant:

Lemme. Soient n et p deux entiers ≥ 1. On suppose n impair. Alors, on a

$$C\left(\begin{bmatrix} 1 & 0 \\ 0 & p \end{bmatrix}, \begin{bmatrix} n & 0 \\ 0 & 1 \end{bmatrix}\right) = 1 \ .$$

Preuve: Ce lemme est bien connu. Rappelons sa preuve: il s'agit de comparer les deux fonctions de la variable complexe z

$$\varphi(z;\, w_1/p,\, w_2)^n / \varphi(z;\, w_1/p,\, w_2/n)$$

d'une part, et

$$\prod_{j=0}^{p-1} \varphi(z + j\tfrac{w_1}{p};\, w_1,\, w_2)^n / \varphi(z + j\tfrac{w_1}{p};\, w_1,\, w_2/n)$$

d'autre part. Comme elles ont même diviseur, il suffit de voir si le quotient de chacune de ces deux fonctions par z^{n-1} possède la même limite (non nulle) quand $z \longrightarrow 0$.

Autrement dit, on veut comparer

$$\eta^{(2)}(w_1/p,\, w_2)^n / \eta^{(2)}(w_1/p,\, w_2/n)$$

d'une part, et

$$\frac{\eta^{(2)}(w_1,\ w_2)^n}{\eta^{(2)}(w_1,\ w_2/n)} \prod_{j=1}^{p-1} \frac{\varphi(jw_1/p;\ w_1,\ w_2)^n}{\varphi(jw_1/p;\ w_1,\ w_2/n)}$$

d'autre part. Pour cela, il suffit de vérifier l'identité, indépendante des valeurs de w_1 et w_2,

$$\eta^{(2)}(w_1, w_2) \prod_{j=1}^{p-1} \varphi(jw_1/p; w_1, w_2) = \eta^{(2)}(w_1/p, w_2) \ . \tag{32}$$

La vérification de cette dernière identité est immédiate: il suffit de se reporter au développement en produit (1) de $\varphi(t; w_1, w_2)$. En effet i) la forme quadratique $\frac{T}{2}\left(\frac{T - \overline{T}}{W - \overline{W}}\right)$ vaut zéro sur les points $T = j/p$, $1 \leq j \leq p-1$, considérés; de plus ii) la somme $-\frac{1}{2} \sum_{j=1}^{p-1} \frac{j}{p} = -\frac{p-1}{4}$ provenant de $E(-T/2)$ annihile exactement le coefficient $(i)^{p-1} = E(\frac{p-1}{4})$ qui provient du premier terme du développement en produit de $\varphi(t; w_1, w_2)$, et enfin iii) le facteur p supplémentaire dans le membre de droite de (32) tient à ce que

$$\prod_{j=1}^{p-1} (1 - E(j/p)) = \lim_{x \longrightarrow 1} \frac{1 - x^p}{1 - x} = p \ .$$

De ce fait, il reste à comparer d'un coté

$$\prod_{d \geq 1} (1 - E(dW))^2 \prod_{j=1}^{p-1} \prod_{d \geq 1} (1 - E(\tfrac{j}{p} + dW))^2$$

et de l'autre

$$\prod_{d\geq 1}(1-E(pdW))^2 \ ;$$

leur égalité résulte de

$$(1-E(dW))\prod_{j=1}^{p-1}(1-E(\tfrac{j}{p}+dW)) = (1-E(pdW))$$

déjà mentionnée dans l'introduction.

Corollaire. Soit n un entier impair ≥ 1, et soient a et b des entiers dont le produit est ≥ 1. Alors, si les entiers a et n sont étrangers, on a

$$C(\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}, \begin{bmatrix} n & 0 \\ 0 & 1 \end{bmatrix}) = 1 \ .$$

Preuve: On développe de deux facons différentes la matrice $\begin{bmatrix} a & 0 \\ 0 & 2b \end{bmatrix}$ comme produit des matrices $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$ et $\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$, et on applique la formule (27): vu le lemme ci–dessus l'identité du corollaire suit.

On en déduit:

Fait 3. Soit n un entier ≥ 1, et soient c et d des entiers (impairs) tels que $cd \geq 1$.

Alors, si l'on suppose n étranger à cd, on a

$$C(n\,\mathrm{Id}, \begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix}) = 1 \ .$$

<u>Preuve</u>: Vu le fait 2 appliqué à $B = -\mathrm{Id}$ et la formule (28) du n°9, on peut supposer que les entiers c et d sont positifs.

De plus, vu le corollaire ci–dessus, on peut aussi supposer que $c = 1$. Or, on a

$$\begin{bmatrix} 1 & 0 \\ 0 & d \end{bmatrix} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} d & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

et d'après le fait 2

$$C(n\,\mathrm{Id}, \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}) = (-1)^{1-n^2} \ .$$

Comme $n\,\mathrm{Id}$ commute avec toutes les matrices de $G\ell_2^{>0}(\mathbb{Z})$, la formule (28) s'applique: pour passer de $C(n\,\mathrm{Id}, \begin{bmatrix} d & 0 \\ 0 & 1 \end{bmatrix})$ à $C(n\,\mathrm{Id}, \begin{bmatrix} 1 & 0 \\ 0 & d \end{bmatrix})$ le fait 2 fournit un facteur

$$(-1)^{(1-n^2)(1-d)} \ ,$$

identiquement égal à 1 vu l'hypothèse de primarité faite entre n et d .

11) Nous voici à même de prouver les assertions proposées dans le n^o4.

Nota. L'idée clef de ce numéro a déjà été publiée par K. RUBIN (il s'agit, dans son travail sur le groupe de Tate–Shafarevitch [7], d'un appendice consacré aux "unités elliptiques"); celui–ci l'attribue à E. de SHALIT, cf. loc. cit. § 12 p. 554. Dans l'appendice cité, les réseaux L et $\underline{L}$ sont supposés à multiplications complexes par l'anneau des entiers d'un corps quadratique imaginaire, de nombre de classes 1.

Soit f un entier ≥ 1. Si $(6f, \det(B)) = 1$, on pose

$$\rho(B) = C(6f\,\mathrm{Id}, B) \;;$$

il résulte donc de l'identité (28) du n^o9 que la formule (16) de multiplicativité du n^o4, à savoir

$$\rho(BD) = \rho(B)^{\det(D)}\rho(D) \;,$$

est satisfaite par toutes les matrices B et D de déterminant premier à 6f.

On prouve dans ce numéro que l'invariant $\rho(B)$ introduit ci–dessus satisfait les assertions (a) et (b) du n^o4. L'affirmation d'unicité qui en résulte (cf. n^o4, remarque 1) assure que $\rho(B)$ est indépendant du choix de l'entier f.

Prouvons d'abord (a): comme 12 divise $(6f)^2 = \det(6f\,\mathrm{Id})$, il résulte des faits 1 et 2 du n^o9 que, si $B \in SL_2(\mathbb{Z})$, alors on a

$$\rho(B) = \rho^{(2)}(B) \;;$$

autrement dit, l'égalité (18) de (e) est satisfaite.

Comme nous l'avons alors fait voir (n^o4, remarque 2), puisqu'il satisfait aussi la formule (16) de (c), ceci assure que l'invaraint $\rho(B)$ vérifie la propriété (a).

Remarque. Ces deux identités (16) et (18), jointes au fait 3 du n^o10, rendent possible le calcul de la racine 12–ième de l'unité $\rho(B)$. Voici le résultat:

On cherche deux matrices M et N de $Sl_2(\mathbb{Z})$ telles que

$$MBN = \begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix} ,$$

avec c et d entiers, de sorte que $(6f, cd) = 1$. Il résulte alors des faits cités que l'on a

$$1/\rho(B) = \rho^{(2)}(M)^{\det(B)}\rho^{(2)}(N) \;,$$

formule qui établit directement l'indépendance de $\rho(B)$ vis–à–vis du choix de f.

Reste à prouver (b): on pose

$$\tilde{F}^B_{w_1,w_2}(z) = \rho(B)^{-1}F^B_{w_1,w_2}(z) \;.$$

La fonction $(w_1, w_2) \longmapsto \tilde{F}^B_{w_1,w_2}$ satisfait aux conditions du n^o6: en effet, pour les fonctions $\tilde{F}^B_{w_1,w_2}$ qui sont de ce fait faiblement multiplicatives, la famille $\mathscr{S} = \mathscr{S}_B$ des matrices introduites dans le n^o5 vérifie les conditions i), ii) et iii) du n^o6; comme précédemment, pour $d_{\mathscr{A}}$ on peut choisir l'entier det(B) .

Soit $\tilde{C}(\Pi, B)$ la constante qui apparait dans la formule (21) du n°6 relative aux fonctions $\tilde{F}^B_{w_1,w_2}$: comme on a

$$\tilde{C}(\Pi, B) = C(\Pi, B)\rho(B)^{\det(\Pi)-1} , \tag{33}$$

il s'agit d'une racine 12–ième de l'unité indépendante du choix des paramètres complexes w_1 et w_2 . A fortiori, cette constante satisfait donc l'hypothèse encadrée du n°6, et par suite on peut lui appliquer la formule (22) du dit numéro; cette dernière s'écrit dans notre cas

$$\tilde{C}(\Pi, B)^{n^2-1} = \tilde{C}(n\,\mathrm{Id}, B)^{\det(\Pi)-1} \tag{34}$$

pour tout entier $n > 0$ premier à det(B) , et tout $\Pi \in \mathscr{A}_B$.

Or, pour $n = 6f$, on a d'après (33)

$$\begin{aligned} &\tilde{C}(6f\,\mathrm{Id}, B) \\ &= C(6f\,\mathrm{Id}, B)\rho(B)^{\det(6f\,\mathrm{Id})-1} \\ &= C(6f\,\mathrm{Id}, B)^{36\,f^2} = 1 . \end{aligned}$$

Par suite, comme $\tilde{C}(\Pi, B) \in \mu_{12}$, on déduit de (34) pour $n = 6f$ l'égalité

$$\tilde{C}(\Pi, B) = 1$$

pour tout $\Pi \in \mathscr{A}_B$; l'assertion (b) est prouvée.

12) Soit K un corps quadratique imaginaire, et revenons sur les hypothèses du n^{o}4 en imposant de plus aux réseaux L et $\underline{L}$ les deux conditions suivantes:

i) On suppose que les réseaux L et $\underline{L}$ possèdent des multiplications complexes par l'anneau des entiers $\mathcal{O}_K$ de K ; on note $\mathfrak{b}$ l'unique idéal de $\mathcal{O}_K$ tel que

$$L = \mathfrak{b}\,\underline{L} \ .$$

Cela impose en particulier au déterminant de la matrice de passage $\det(B) = N\mathfrak{b}$, déjà supposé premier à 6, la restriction d'être la norme d'un idéal entier (non nul) de K . En particulier, si μ_K désigne le groupe des unités de $\mathcal{O}_K$ et $w(K)$ son ordre, la différence

$$\det(B) - 1$$

est un multiple de $w(K)$.

ii) On suppose de plus que les sommes

$$g_2(L) = 60 \sum_{n,m}{}' \ (nw_1 + nw_2)^{-4}$$

et

$$g_3(L) = 140 \sum_{n,m}{}' \ (nw_1 + nw_2)^{-6} \ ,$$

où (w_1, w_2) désigne une base de L telle que $\mathrm{Im}(w_2/w_1) > 0$, et où la somme est prise sur les points (n,m) de $\mathbb{Z} \times \mathbb{Z}$ exception faite du point $(n,m) = (0,0)$, appartiennent au corps de classes de Hilbert H de K .

Il n'est pas besoin de rappeler ici que $g_2(L)$ et $g_3(L)$ sont les constantes qui apparaissent dans l'équation différentielle

$$\wp'^2 = 4\,\wp^3 - g_2\,\wp - g_3$$

satisfaite par la fonction $\wp(z,L)$ de Weierstrass, caractérisée par le fait que $(0)_L$ est son seul pôle (double) sur $\mathbb{C}/L$ et que l'on a

$$\lim_{z \longrightarrow 0} \left(\wp(z, L) - \frac{1}{z^2} \right) = 0 \ .$$

Comme on le sait, le déterminant $\Delta(L)$ de L défini au n°2 comme la puissance 12–ième de $\eta^{(2)}(w_1, w_2)$ s'exprime aussi rationellement en fonction de g_2 et g_3 par

$$\Delta(L) = g_2(L)^3 - 27\,g_3(L)^2 \ .$$

L'hypothèse i) assure que $H = K(j(L))$, où l'invariant modulaire

$$j(L) = 12^3\,g_2(L)^3/\Delta(L)$$

ne dépend que de la classe d'homothétie du réseau L .

On a alors:

<u>Proposition</u>. <u>Sous les hypothèses précédentes, le quotient</u>

$$\tilde{\eta}^{(2)}(L, \underline{L})$$

défini par l'identité (13) du n^{o}4 appartient à H .

Preuve: Vu l'identité (9) du n^{o}3, on a

$$\tilde{F}(z; L, \underline{L}) = \tilde{\eta}^{(2)}(L, \underline{L})K(z; L)^{\det(B)}/K(z; \underline{L}) \tag{35}$$

où le membre de gauche est défini par la formule (14) du n^{o}4.

Soit $\mathfrak{f}$ un idéal entier (non nul) de K , $\mathfrak{f} \neq \mathcal{O}_K$, et notons $\wp^{(w/2)}(z, L)$ la puissance w(K)/2–ième de $\wp(z, L)$. Aussi, disons d'un point z de $\mathbb{C}$ qu'il est un point "primitif de $\mathfrak{f}$–division" du tore $\mathbb{C}/L$ si l'on a l'égalité

$$\{\lambda \in \mathcal{O}_K \mid \lambda z \in L\} = \mathfrak{f} .$$

On sait que, si z est un tel point primitif de $\mathfrak{f}$–division du tore $\mathbb{C}/L$, alors sous l'hypothèse ii) ci–dessus le corps

$$H(\wp^{(w/2)}(z, L))$$

est le corps de classes $H_{\mathfrak{f}}$ de rayon modulo $\mathfrak{f}$ de K .

Or, vu l'hypothèse i), on peut écrire

$$(36)\qquad K(z,L)^{\det(B)}/K(z,\underline{L}) = \left[\frac{1}{\wp^{(w/2)}(z,L)}\right]^{\frac{\det(B)-1}{w(K)}}$$

$$\prod_{\substack{\mu_K\lambda\subset\underline{L}/L\\ \lambda\neq 0}} (1 - \wp^{(w/2)}(\lambda,L)/\,\wp^{(w/2)}(z,L))^{-1}\ ,$$

où le produit est pris sur les points non nuls de $\underline{L}/L$ modulo l'action transitive du groupe μ_K sur ceux–ci.

Par suite, lorsque λ parcourt les points non nuls de $\underline{L}/L$ modulo μ_K , les coefficients $\wp^{(w/2)}(\lambda, L)$ du membre de droite de (36) sont permutés par le groupe de Galois $\mathrm{Gal}(H_{\mathfrak{b}}/H)$. Ainsi, si l'on regarde le membre de droite de (36) comme une fraction rationnelle en $1/\wp^{(w/2)}(z, L)$ les coefficients de son développement appartiennent à H .

Soient alors $\mathfrak{f}_1$ et $\mathfrak{f}_2$ deux idéaux entiers de K , premiers à $6\mathfrak{b}$, étrangers entre eux, et distincts de $\mathcal{O}_K$. Soient de plus z_i des points primitifs de $\mathfrak{f}_i$–division du tore $\mathbb{C}/L$, $i = 1, 2$. Appliquons l'identité (15) du n°4 à la matrice $\Pi = 2\,\mathrm{Id}$ (resp. $3\,\mathrm{Id}$); pour prouver la proposition, il suffit de voir qu'en évaluant les deux membres de (15) en z_1 , puis en z_2 , on trouve via la formule (35) ci–dessus le fait que

$$\tilde{\eta}^{(2)}(L,\underline{L})^3\ \ (\text{resp. } \tilde{\eta}^{(2)}(L,\underline{L})^8)$$

appartient à $H = H_{\mathfrak{f}_1} \cap H_{\mathfrak{f}_2}$.

Or, sous l'hypothèse ii), le groupe de Galois $\mathrm{Gal}(H_{2\mathfrak{f}_i}/H_{\mathfrak{f}_i})$ permute les nombres

$$\wp^{(w/2)}(z_i + \omega, 2L)\ ,$$

lorsque ω parcourt un système complet de représentants de $L/2L$. De même, le groupe de Galois $\mathrm{Gal}(H_{3f_i}/H_{f_i})$ permute les nombres

$$\wp^{(w/2)}(z_i + \underline{\omega}, 3L)$$

lorsque $\underline{\omega}$ parcourt un système complet de représentants de $L/3L$. Bien sûr, ceci est vrai pour $i = 1$ comme pour $i = 2$. Vu l'identité

$$\tilde{\eta}^{(2)}(L', \underline{L}') = (\tfrac{1}{n})^{\det(B) - 1}\, \tilde{\eta}^{(2)}(L, \underline{L})$$

valable dès que $\Pi = n\,\mathrm{Id}$, avec n entier $\neq 0$ premier à $\det(B)$, on trouve bien le fait précédent et par suite l'assertion de la proposition.

Remarque. La proposition ci–dessus peut etre considérée comme une description explicite de la racine 12–ième de

$$\Delta(L)^{N(\mathfrak{b})}/\Delta(\mathfrak{b}^{-1}L)$$

dans $H^{\times}$, lorsque l'idéal entier $\mathfrak{b}$ de $\mathcal{O}_K$ est premier à 6, dont l'existence sous les hypothèses précédentes résulte de G. ROBERT [6] appendice A, p. 349.

Bibliographie

[1] G. FALTINGS, Calculus on arithmetic surfaces, Ann. of Math. 119 (1984) 387–424

[2] F. HIRZEBRUCH, D. ZAGIER, The Atiyah–Singer Theorem and Elementary Number Theory, Math. Lectures Series 3 (1974) Ed: Publish or Perish, Berkeley

[3] D. KUBERT, S. LANG, Modular Units, Grundleh. der math. Wiss. 244 (1981) Ed: Springer–Verlag

[4] K. RAMACHANDRA, Some Applications of Kronecker's limit formulas, Ann. of Math. 80 (1964) 104–148

[5] G. ROBERT, Unités elliptiques, Bull. Soc. math. France Mémoire 36 (1973) 77 p.

[6] G. ROBERT, Nombres de Hurwitz et unités elliptiques, Ann. sc. E.N.S. (4) 11 (1978) 297–389

[7] K. RUBIN, Tate–Shafarevich groups and L–functions of elliptic curves with complex multiplication, Inv. math. 89 (1987) 527–559

[8] R. SCHERTZ, Niedere Potenzen elliptischer Einheiten, Proc. Int. Conf. on Class Numbers and Fundamental Units (Japan, June 1986, Katata) 67–88

[9] E. de SHALIT, Iwasawa Theory of Elliptic Curves with Complex Multiplication, Perspectives in math. 3 (1987) Ed: Academic Press

[10] C.L. SIEGEL, Lectures notes on advanced analytic number theory, Tata Inst. of Fund. Research (1961) Bombay

[11] H.M. STARK, L–Functions at $s = 1$, IV, First Derivatives at $s = 0$, Advances in Math. 35 (1980) 197–235

[12] A. WEIL, Introduction à l'étude des variétés kählériennes (1957) Ed: Hermann, Paris