MULTIPLICATION COMPLEXE ET LOIS DE RÉCIPROCITÉ: LE CAS DES FONCTIONS MODULAIRES ELLIPTIQUES

Gilles ROBERT

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

Federal Republic of Germany

MPI/89-44

MULTIPLICATION COMPLEXE

ET LOIS DE RÉCIPROCITÉ:

LE CAS DES FONCTIONS MODULAIRES ELLIPTIQUES

par Gilles ROBERT

le 22/6/89

Survey For N an integer ≥ 1, let $\mathcal{F}_N$ and $\mathcal{F}_N^0$ be the fields of modular elliptic functions defined as in the text below.

If s is an idèle of an imaginary quadratic field K, the way the Artin automorphism $[s,K]$ of the maximal abelian extension K^{ab} of K acts on the value $f(z)$ of a function f of $\mathcal{F}_N$ at a point z of K is known as the explicit reciprocity law, cf. [7] § 6.8 p. 157.

We give here, when f belongs to the $\mathbb{Q}$–rational model $\mathcal{F}_N^0$ of $\mathcal{F}_N$, an equivalent but direct description of this action. It mimics the way the automorphism $[s,K]$ acts on the modular invariant $\tilde{j}$, cf. formulas (1) and (2) of the introduction.

Two proofs of (2) are given: the direct one results from the study of these C.M. elliptic curves, which are defined with all their points of finite order on the field K^{ab}, cf. sections 3, 4; indeed, this study enables one to write identities analogous to (2) for a lot of functions (cf. also [4]) and especially for each of the well–known generators of $\mathcal{F}_N^0$ over $\mathbb{Q}$. The indirect one establishes by a thorough computation, when f belongs to $\mathcal{F}_N^0$, the

equivalence of (2) with the explicit reciprocity law, cf. sections 5, 6.

Introduction

Pour N entier ≥ 1, soit $\mathcal{F}_N$ (resp. $\mathcal{F}_N^0$) le corps des fonctions modulaires de niveau N à coefficents dans $\mathbb{Q}(e^{2\pi i/N})$ (resp. le sous–corps de $\mathcal{F}_N$ fixé par l'action du groupe $\left\{\begin{bmatrix} 1 & 0 \\ 0 & d \end{bmatrix} \in G\ell_2(\mathbb{Z}/N\mathbb{Z}) \mid d \in (\mathbb{Z}/N\mathbb{Z})^\times\right\}$) cf. n$^{\text{os}}$ 4, 5. On sait que

$$\mathcal{F}_N = \mathcal{F}_N^0(e^{2\pi i/N})$$

et que les corps des constantes de $\mathcal{F}_N^0$ et $\mathcal{F}_N$ sont respectivement $\mathbb{Q}$ et $\mathbb{Q}(e^{2\pi i/N})$, de sorte que $\mathcal{F}_N^0$ est un modèle $\mathbb{Q}$–rationnel du corps $\mathcal{F}_N$.

Soit K un corps quadratique imaginaire, et K^{ab} son extension abélienne maximale. La théorie du corps de classes global nous dit que la loi de réciprocité d'Artin

$$s \longmapsto [s,K]$$

est une surjection du groupe $K_{\mathbb{A}}^\times$ des idèles de K sur le groupe de Galois G_K des automorphismes de K^{ab}/K. Cet homomorphisme est continu si l'on munit ces groupes de leurs topologies naturelles, et son noyau peut être décrit.

L'action de l'automorphisme d'Artin $[s,K]$ de K^{ab}/K sur les valeurs $f(z)$ des fonctions f de $\mathcal{F}_N$ évaluées en un point z de K est décrite par la "loi de réciprocité explicite" de G. Shimura [7] § 6.8 p. 157 (cf. n^{o}5 th. 2, pour un rappel de celle–ci). On donne ici une description directe et équivalente de cette action pour les fonctions f de $\mathcal{F}_N^0$.

*

* *

Soit $\Gamma(N)$ le sous–groupe de congruence

$$\{\gamma \in S\ell_2(\mathbb{Z}) \mid \gamma \equiv I_2 (\mathrm{mod}\ N)\}$$

de niveau N de $S\ell_2(\mathbb{Z})$, que l'on fait agir sur le demi–plan de Poincaré $\mathfrak{H} = \{z \mid \mathrm{Im}\ z > 0\}$. On considère $\mathfrak{T}_N$ l'espace des triplets $(L, L_N, \dot{w})$ définis par les trois conditions suivantes:

i) L est un réseau complexe;

ii) L_N est un sur–réseau de L tel que L_N/L soit cyclique d'ordre N ;

iii) $\dot{w}$ est un élément de L/NL dont la classe modulo NL_N engendre L/NL_N (on sait d'après i) et ii) que ce quotient est cyclique d'ordre N).

Les espaces $\mathfrak{H}$ d'une part via la projection standard α , et $\mathfrak{T}_N$ d'autre part via une surjection ${}_N\beta$ définie dans le n^{o}1, sont tous deux des quotients de l'espace $\mathfrak{K}$ des bases positivement orientées de réseaux complexes. De plus ${}_N\beta$ induit en fait (cf. n^{o}1, lemme 1) un isomorphisme $\Gamma(N)\backslash\mathfrak{K} \xrightarrow{\sim} \mathfrak{T}_N$ qui permet de munir $\mathfrak{T}_N$ d'une structure d'espace analytique.

Rappelons aussi trois faits essentiellement classiques:

a) La projection

$$\pi_N : \mathfrak{T}_N \longrightarrow \Gamma(N)\backslash\mathfrak{H}$$

définie par $\pi_N = \alpha \circ {}_N\beta^{-1}$ est une fibration localement triviale de fibre $\mathbb{C}^\times$, pourvu que l'action de $\Gamma(N)$ sur $\mathfrak{H}$ soit sans points fixes i.e. $N \geq 3$.

b) Le groupe $K_{\mathbb{A}}^\times$ des idèles de K agit sur $\pi_N^{-1}(\Gamma(N)\backslash\mathfrak{H} \cap K)$ par

$$t : (L, L_N, \dot{w}) \longmapsto (tL, tL_N, t\dot{w})$$

c'est-à-dire par multiplication sur chacun des trois termes du triplet $(L, L_N, \dot{w})$, cf. n°2 lemme 2.

c) Si $N = 1$, on a $\mathcal{F}_N = \mathcal{F}_N^0 = \mathbb{Q}(j)$ où, en notant les éléments de $\mathfrak{T}_1$ par leur seul premier terme, l'invariant modulaire $\tilde{j} = \pi_1^* j$ vérifie

$$\tilde{j}(L)^{[s,K]} = \tilde{j}(s^{-1}L) \tag{1}$$

pour tout réseau L à multiplication complexe par K, cf. [6] § 5.4.

<u>Il se trouve en fait</u> que l'écriture de l'identité (1) de c) est vraie, avec la définition de b), pour tout élément f de $\mathcal{F}_N^0$ regardé comme une fonction sur $\Gamma(N)\backslash\mathfrak{H}$ ceci <u>sans restriction sur l'entier</u> N.

Autrement dit, on démontre ici:

THÉORÈME

Soit $z \in K$ tel que $\mathrm{Im}\, z > 0$, et soit s un idèle de K.

Soit $f \in \mathcal{F}_N^0$ regardé comme une fonction sur $\Gamma(N)\backslash\mathfrak{H}$, et notons $\mathfrak{f} = \pi_N^* f$ l'image transposée de f par la projection π_N.

Alors, si f est définie en l'orbite $\Gamma(N) \cdot z$ de z sous $\Gamma(N)$ et si $\not{\!\!\rho} = (L, L_N, \dot{w})$ vérifie $\pi_N(\not{\!\!\rho}) = \Gamma(N) \cdot z$, on a

(2)
$$\mathfrak{f}(L, L_N, \dot{w})^{[s,K]} = \mathfrak{f}(s^{-1}L, s^{-1}L_N, s^{-1}\dot{w}) .$$

Ce théorème est bien sûr équivalent à la loi de réciprocité explicite pour $\mathcal{F}^0 = \bigcup_N \mathcal{F}_N^0$. On renvoit à la proposition clef du n^{o}6 pour une description précise de cette équivalence. On notera que si $\mathcal{F} = \bigcup_N \mathcal{F}_N$, on a

$$\mathcal{F} = \mathbb{Q}^{ab}\, \mathcal{F}^0$$

où $\mathbb{Q}^{ab}$ est l'extension abélienne maximale de $\mathbb{Q}$; d'une certaine façon, dans le cas de l'action des sous–groupes de congruence de $S\ell_2(\mathbb{Z})$ sur le demi–plan de Poincaré $\mathfrak{H}$, il nous semble avoir isolé dans ce travail une part de cette loi à caractère peut–être plus géométrique.

*

* *

Les n^{os} 3 et 4 sont consacrés à une preuve directe du théorème ci–dessus. En effet, on a $\mathcal{F}_N^0 = \mathbb{Q}(j, j_N, f^{(1)})$ où les images transposées par π_N des fonctions j, j_N et $f^{(1)}$ (regardées sur $\Gamma(N)\backslash\mathfrak{H}$) admettent au point $\not{\!\!\rho} = (L, L_N, \dot{w})$ de $\mathfrak{T}_N$ pour valeurs respectives

$$\tilde{j}(L),\ \tilde{j}(L_N)\ \text{ et }\ 2^5 3^4\,\frac{g_2(L)g_3(L)}{\Delta(L)}\ \ \wp(\iota(\not{a}),L)$$

avec $\tilde{j} = 2^6 3^3\, g_2^3/\Delta$. Ici $\wp$ est la fonction de Weierstrass de coefficients g_2 et g_3 et de discriminant non nul $\Delta = g_2^3 - 27g_3^2$, et $\iota(\not{a})$ est un représentant complexe du point $\dot{w}/N$ d'ordre N modulo L .

<u>Les trois fonctions</u> j, j_N <u>et</u> $f^{(1)}$ <u>vérifient la relation</u> (2): on le sait déjà pour j et j_N d'après (1).

La preuve que l'on en donne (cf. n°4) vaut pour ces trois fonctions, et résulte de l'existence de réseaux particuliers L à multiplication complexe par K et vérifiant les deux conditions ci–dessous (cf. n°3):

i) le modèle de Weierstrass de réseau de période L est défini sur la clôture abélienne K^{ab} de K ;

ii) les points d'ordre fini de ce modèle sont également définis sur K^{ab} .

En effet, de tels réseaux existent dans chaque classe d'homothétie de réseaux à multiplication complexe par K , cf. [7] § 7.8, p. 216.

Pour un tel réseau L , on définit une application continue $s \longmapsto \Lambda(s,L)$ du groupe des idèles de K à valeurs dans le groupe multiplicatif $F^{\times}$ d'un sous–corps convenable F de K^{ab} , de degré fini sur $\mathbb{Q}$. Cette application Λ ne dépend que de la classe d'isogénie de L (on donne deux preuves de ce résultat simple cf. n°3 lemme 4: l'une directe dans le n°3 est seulement esquissée, l'autre dans le n°4 résulte du théorème ci–dessus) de sorte qu'il s'agit d'un homomorphisme croisé pour l'action de G_K sur K^{ab} ;

par définition, elle controle l'action de $[s,K]$ sur les points de torsion de la courbe et par suite sur les formes et a fortiori les fonctions modulaires.

Cette fonction Λ a déjà été étudiée dans [1]. En particulier, pour F comme ci–dessus, son lien avec le caractère de Serre–Tate [5] associé à la variété abélienne, restriction des scalaires de F à K du modèle de Weierstrass en question, s'y trouve décrit.

*

* *

En bref, les éléments permettant de décrire la projection π_N ci–dessus sont rassemblés dans le n^{o}1 (la notation π_N n'est utilisée que dans l'introduction). Le n^{o}2 contient quelques considérations adéliques; en particulier, on vérifie b) mentionné plus haut et on énonce un résultat technique utilisé au n^{o}6. Le n^{o}3 décrit l'application Λ évoquée ci–dessus; on traite comme illustration le comportement du quotient $\Delta(L)/\Delta(L')$ évalué en deux réseaux commensurables L et L' lorsque ceux–ci possèdent des multiplications complexes. Le n^{o}4 contient la preuve par voie directe (th. 1) du théorème; en passant, on prouve que si une fonction f de $\mathcal{F}_N$ satisfait (2) en les points, où elle est définie, de deux corps quadratiques imaginaires distincts alors f appartient à $\mathcal{F}_N^0$. Le n^{o}5 contient (th. 2) un rappel de la loi de réciprocité explicite de G. Shimura pour $f \in \mathcal{F}_N$. Le n^{o}6 précise enfin (prop. clef) le lien entre le théorème et cette loi.

*

* *

<u>Remarque</u> Il nous semble que la théorie ci–dessus peut également être développée

pour les fonctions modulaires de Siegel à n variables; la fibre de l'analogue de π_N est alors de dimension complexe n^2 .

Remerciements

Citons d'abord S. Lang dont le livre [2] bien connu nous a ouvert le passage pour comprendre au moins un peu l'ouvrage cité [7] de G. Shimura; est–il nécessaire de préciser qu'un résultat mis en valeur par le premier nommé (loc. cit. Chap. 11, th. 5) fut un prototype pour la proposition clef de notre n°6 ?

Aussi, ils vont à tous les membres du M.P.I. de Bonn et à mes collègues qui y établissent une ambiance si chaleureuse, particulièrement à Don Zagier qui a eu la gentillesse de s'intéresser à des versions préalables de ce texte et la profondeur de vue nécessaire pour nous aider à sortir de l'impasse où nous nous débations alors.

1) Soit $\mathfrak{K}$ l'ensemble des bases positivement orientées de réseaux complexes, sur lesquelles on fait agir $\mathbb{C}^\times$ par homothétie de sorte que l'application

$$\alpha : (w_1,w_2) \longmapsto w_2/w_1$$

définit une bijection de $\mathfrak{K}/\mathbb{C}^\times$ sur le demi–plan de Poincaré $\mathfrak{H} = \{z \mid \operatorname{Im} z > 0\}$.

Le groupe $G\ell_2^{>0}(\mathbb{R})$ des matrices $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ à coefficients réels et de déterminant > 0 agit à gauche sur $\mathfrak{K}$, en appliquant la base (w_1,w_2) sur la base $(w_1',w_2') = \gamma(w_1,w_2)$ définie par l'identité matricielle

$$\begin{bmatrix} w_2' \\ w_1' \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} w_2 \\ w_1 \end{bmatrix} .$$

Ainsi $\mathfrak{K}$ est un espace principal homogène (= torseur) sur $G\ell_2^{>0}(\mathbb{R})$. L'action correspondante de γ sur $\mathfrak{H}$ est donnée par

$$\gamma : z \longmapsto \gamma(z) = az + b/cz + d \ , \ \ z \in \mathfrak{H} \ .$$

Pour N entier ≥ 1 , soit

$$\Gamma(N) = \{\gamma \in S\ell_2(\mathbb{Z}) \mid \gamma \equiv I_2 (\text{mod } N)\}$$

le sous–groupe de congruence de niveau N du groupe modulaire $S\ell_2(\mathbb{Z})$. On définit $\mathfrak{T}_N$ comme l'ensemble des triplets $(L, L_N, \dot{w})$ vérifiant les trois conditions énumérées dans l'introduction.

Soit ${}_N\beta$ l'application qui à chaque élément (w_1, w_2) de $\mathfrak{K}$ associe l'élément $(L, L_N, \dot{w})$ de $\mathfrak{T}_N$ ainsi défini: le réseau L (resp. L_N) est engendré par (w_1, w_2) (resp. $(w_1/N, w_2)$) et le point $\dot{w}$ désigne la classe de w_2 modulo NL .

On a:

<u>Lemme</u> 1 <u>L'application</u> ${}_N\beta : \mathfrak{K} \longrightarrow \mathfrak{T}_N$ <u>définit une bijection de</u> $\Gamma(N)\backslash\mathfrak{K}$ <u>sur</u> $\mathfrak{T}_N$.

<u>Preuve</u>: Ce résultat est bien connu: puisque l'action de $G\ell_2^{>0}(\mathbb{R})$ sur $\mathfrak{K}$ est transitive, soit $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ dans ce groupe tel que (w_1, w_2) et $(w_1', w_2') = \gamma(w_1, w_2)$ aient même image $(L, L_N, \dot{w})$ par ${}_N\beta$. On trouve qu'il en est ainsi si et seulement si i) les

matrices γ et $\begin{bmatrix} N & 0 \\ 0 & 1 \end{bmatrix} \gamma \begin{bmatrix} N & 0 \\ 0 & 1 \end{bmatrix}^{-1}$ laissent respectivement stables les réseaux L et NL_N, d'où $\gamma \in S\ell_2(\mathbb{Z})$ avec $c \equiv 0 (\mathrm{mod}\ N)$, et ii) la matrice γ vérifie la congruence $\gamma(w_1,w_2) \equiv (w_1',w_2)\ (\mathrm{mod}\ NL)$ d'où $(a,b) \equiv (1,0)\ (\mathrm{mod}\ N)$.

D'autre part, tous les points de $\mathfrak{T}_N$ sont atteints par ${}_N\beta$: pour trouver un antécédent à $(L,L_N,\dot{w})$, on procède en deux étapes.

a) On relève d'abord $\dot{w}$ en un point primitif w_2 de L tel que w_2 modulo NL soit $\dot{w}$. On regarde alors w_2 dans L_N ; comme $\dot{w}$ est d'ordre exact N cf. définition de $\mathfrak{T}_N$ condition iii), on trouve que w_2 est aussi un point primitif de L_N.

b) Ceci permet de trouver w_1, avec $\mathrm{Im}(w_2/w_1) > 0$, tel que $(w_1/N,w_2)$ soit une base de L_N. Alors (w_1,w_2) est une base de L, de sorte que l'on a bien

$$ {}_N\beta(w_1,w_2) = (L,L_N,\dot{w}) \ . $$

<u>Corollaire</u> <u>Les applications</u> $\alpha : \mathfrak{K} \longrightarrow \mathfrak{H}$ et ${}_N\beta : \mathfrak{K} \longrightarrow \mathfrak{T}_N$ <u>définissent une bijection des fonctions sur</u> $\mathfrak{H}$ <u>invariantes par</u> $\Gamma(N)$ <u>sur les fonctions sur</u> $\mathfrak{T}_N$ <u>invariantes par homothétie</u>.

On peut dresser la table de correspondance suivante:

fonction sur $\mathfrak{H}$ invariante par $\Gamma(N)$	fonction sur $\mathfrak{T}_N$ invariante par homothétie
ne dépend pas de l'action des matrices $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ de $S\ell_2(\mathbb{Z})$ vérifiant respectivement:	
$c \equiv 0 (\text{mod } N)$	ne dépend pas de $\dot{w}$
$a \equiv 1 (\text{mod } N)$ et $c \equiv 0 (\text{mod } N)$	ne dépend que de la classe de $\dot{w}$ modulo NL_N
$a \equiv 1 (\text{mod } N)$ et $b \equiv 0 (\text{mod } N)$	ne dépend pas de L_N

2) Soit $\mathbb{A} = \mathbb{A}_f \times \mathbb{R}$ la décomposition de l'algèbre $\mathbb{A}$ des adèles de $\mathbb{Q}$ en partie finie et infinie. Si $\hat{\mathbb{Z}}$ désigne la complétion de l'anneau des entiers rationnels $\mathbb{Z}$ pour la topologie des sous–groupes d'indice fini, on a

$$\mathbb{A}_f = \hat{\mathbb{Z}} \otimes \mathbb{Q} \quad .$$

Soit K un corps quadratique imaginaire, et L un réseau à multiplication complexe par K. On sait que l'algèbre $K_{\mathbb{A}}$ des adèles de K s'identifie canoniquement à $\mathbb{A} \otimes K$. De plus, pour tout idèle t de K, le produit tL de L par (la partie finie de) l'idèle t

est un autre réseau à multiplication complexe par K caractérisé par les identités

$$\mathbb{Z}_p \otimes (tL) \overset{\mathrm{dfn}}{=} t_p(\mathbb{Z}_p \otimes L)\ ,\ p \text{ premier}\ ,$$

lues dans $\mathbb{Q}_p \otimes L$, où t_p désigne la p–partie de l'idèle $t \in (\mathbb{A} \otimes K)^{\times}$.

En fait, l'action $L \longmapsto tL$ avec $t \in K_{\mathbb{A}}^{\times}$ est transitive sur l'ensemble des réseaux commensurables à L dont l'ordre

$$\mathcal{O} = \{\lambda \in \mathbb{C} \mid \lambda L \subset L\}$$

est un sous–anneau de l'anneau des entiers de K <u>a priori</u> fixé.

De plus, pour tous réseaux L_0 et L_1 commensurables à L tels que $L_0 \subset L_1$, la multiplication par l'idèle t définit des isomorphismes de groupes

$$(3) \qquad t : L_1/L_0 \xrightarrow{\sim} tL_1/tL_0$$

du quotient du réseau L_1 par L_0 sur le quotient du réseau tL_1 par tL_0, <u>qui sont compatibles entre eux</u>: si L_1' et L_0' vérifient respectivement $L_1' \supset L_1$ et $L_0' \subset L_0$, alors l'isomorphisme

$$(3') \qquad t : L_1'/L_0' \xrightarrow{\sim} tL_1'/tL_0'$$

induit par restriction et projection l'isomorphisme (3) ci–dessus.

En effet, pour L fixé, la limite projective de ces quotients est un espace principal homogène (= torseur) sur le groupe $A_f \otimes K$.

En particulier, on a:

Lemme 2 Si le point $(L, L_N, \dot{w})$ appartient à $\mathcal{T}_N$ et si L possède des multiplications complexes par K , alors pour tout idèle t de K le point

$$(tL, tL_N, t\dot{w})$$

appartient aussi à $\mathcal{T}_N$.

D'une façon comparable, on a:

Lemme 3 Soit (w_1, w_2) un point de $\mathfrak{R}$ et L le réseau complexe qu'il engendre. Si le quotient w_2/w_1 appartient au corps quadratique imaginaire K , alors pour tout idèle t de K , le couple (tw_1, tw_2) d'éléments de $A_f \otimes L$ forme une base du module $\hat{\mathbb{Z}} \otimes tL$ sur l'anneau $\hat{\mathbb{Z}}$.

3) Soit K un corps quadratique imaginaire, et K^{ab} l'extension abélienne maximale de K . Ici vient le fait principal, cf. [7] § 7.8 p. 216: pour toute courbe elliptique E définie sur $\mathbb{C}$ et à multiplication complexe par K , il existe une forme différentielle invariante $\omega \neq 0$ dont le réseau des périodes L vérifie les deux conditions:

i) le modèle de Weierstrass de (E, ω)

$$y^2 = 4x^3 - g_2(L)x - g_3(L)\ , \quad \omega = dx/y\ ,$$

associé à L est défini sur K^{ab} ;

ii) les points d'ordre fini de ce modèle sont également définis sur K^{ab} .

Précisons que l'énoncé cité de G. Shimura est bien plus général: il s'applique mutatis mutandis à toutes les variétés abéliennes définies sur $\mathbb{C}$, pourvu qu'elles aient beaucoup de multiplications complexes. Il fait appel au théorème principal de la multiplication complexe des variétés abéliennes, cf. [6] 1.5; pour une bonne version du théorème cité cf. [7] § 4.

Dans notre situation particulière, il est facile de traduire i) comme suit: on demande que les coefficients $g_2(L)$ et $g_3(L)$ de l'équation différentielle satisfaite par la fonction $\wp(z,L)$ de Weierstrass appartiennent à K^{ab} . Il est plus délicat de traduire ii); si l'on fixe pour corps de définition de E un corps de nombres contenu dans K^{ab} , comme c'est toujours possible d'après i), on peut le faire en termes du caractère de Serre–Tate relatif à la variété abélienne obtenue par restriction des scalaires à K de la courbe elliptique E . Nous adoptons ici un point de vue légèrement différent, cf. [1] § 4 p. 199:

Soit s un idèle de K , et $[s,K]$ l'automorphisme de K^{ab}/K associé à s par la loi de réciprocité d'Artin. D'après le théorème principal de la multiplication complexe des courbes elliptiques cf. [7] § 5.3 (déjà employé pour prouver l'existence d'une forme différentielle invariante $\omega \neq 0$ convenable) il existe un élément $\Lambda(s,L)$ de K^{ab} caractérisé par les identités suivantes

$$\wp(\rho,L)^{[s,K]} = \Lambda(s,L)^{-2}\, \wp(s^{-1}\rho,s^{-1}L) \quad , \tag{4}$$

$$\wp'(\rho,L)^{[s,K]} = \Lambda(s,L)^{-3}\, \wp'(s^{-1}\rho,s^{-1}L) \quad , \tag{5}$$

vérifiées par tout nombre complexe ρ dont la classe modulo L est un point de torsion

$\neq 0$ de $\mathbb{C}/L$, et où $s^{-1}\rho$ désigne un représentant de la classe $s^{-1}(\rho \text{ modulo } L)$ bien définie modulo $s^{-1}L$ d'après le n°2.

Comme $g_2(L)$ et $g_3(L)$ sont des polynômes symétriques à coefficients rationnels de degrés respectifs 2 et 3 en les valeurs de $\mathcal{P}$ en les représentants des points de 2–torsion non nuls de $\mathbb{C}/L$, il résulte de (4) que g_2 et g_3 satisfont l'identité

$$(6) \qquad g_i(L)^{[s,K]} = \Lambda(s,L)^{-2i} g_i(s^{-1}L) \ , \ i \in \{2,3\} \ ;$$

en particulier, le discriminant $\Delta = g_2^3 - 27g_3^2$ de la courbe E vérifie

$$(7) \qquad \Delta(L)^{[s,K]} = \Lambda(s,L)^{-12} \Delta(s^{-1}L) \ .$$

Notons $\mathcal{L}$ l'ensemble des réseaux commensurables à un tel réseau L . Clairement, chaque élément de $\mathcal{L}$ vérifie aussi les propriétés i) et ii) ci–dessus. De plus, on a:

Lemme 4 Soient L et L′ deux éléments de $\mathcal{L}$. Alors, pour tout idèle s de K , on a

$$\Lambda(s,L) = \Lambda(s,L') \ .$$

Nota Comparer avec l'affirmation qui dit que sur un corps de nombres fixé, le Grössencharakter ne dépend que de la classe d'isogénie de la courbe.

Première preuve du lemme 4:

Une seconde preuve sera donnée au n° suivant. Voici une esquisse de preuve directe: sans restriction de généralité, on peut supposer $L \subset L'$, de sorte que l'égalité

$\Lambda(s,L) = \Lambda(s,L')$ résulte des relations de distribution satisfaites par les fonctions $\wp$ d'une part et $\wp'$ d'autre part.

Corollaire Soit L un réseau à multiplications complexes par K, et L' un réseau commensurable à L. Alors, pour tout idèle s de K on a

$$(\Delta(L)/\Delta(L'))^{[s,K]} = \Delta(s^{-1}L)/\Delta(s^{-1}L') \ .$$

Preuve La fonction $\Delta(L)/\Delta(L')$ est invariante par homothéties. On peut donc supposer sans restreindre la généralité que L vérifie les propriétés i) et ii) ci–dessus. Il s'ensuit que L' les vérifie aussi, et il suffit pour prouver le corollaire de combiner le lemme 4 à l'identité (7) satisfaite par Δ pour le réseau L d'une part et L' d'autre part.

Remarque Il résulte du lemme 4 ci–dessus que l'application $s \longmapsto \Lambda(s,L)$ est un homomorphisme croisé pour l'action de G_K sur K^{ab}, i.e. vérifie

$$\Lambda(st,L) = \Lambda(s,L)^{[t,K]}\Lambda(t,L)$$

pour tous idèles s et t de K.

Il s'agit d'une application continue de $K_{\mathbb{A}}^{\times}$ dans $\mathbb{C}^{\times}$; son image est contenue dans un sous–corps de degré fini de K^{ab}.

Pour tout ceci, cf. [1] § 4.

Nota Une version plus grossière de Λ, à savoir Λ^e où e désigne le nombre d'automorphismes du réseau L, se trouve aussi décrite dans G. Robert [3].

4) Pour N entier ≥ 1, soit donc $\mathcal{F}_N$ le corps des fonctions $f : z \longmapsto f(z)$ définies sur le demi–plan de Poincaré $\mathfrak{H}$, et qui satisfont les trois propriétés bien connues ci–dessous:

i) f est méromorphe sur $\mathfrak{H}$;

ii) f est invariante par l'action sur $\mathfrak{H}$ du sous–groupe de congruence $\Gamma(N)$ de $S\ell_2(\mathbb{Z})$;

iii) f est méromorphe aux pointes de $\Gamma(N)$, et ses coefficients de Fourier appartiennent au corps $\mathbb{Q}(e^{2\pi i/N})$.

On désigne par $\mathcal{F}^0$ le sous–corps de $\mathcal{F}_N$ des fontions modulaires f qui vérifient de plus:

iv) les coefficients de Fourier de f à l'infini, relativement à $e^{2\pi i\, z/N}$, sont rationnels.

Cette définition coïncide avec celle donnée dans l'introduction, cf. n°5.

On sait que $\mathcal{F}_N = \mathcal{F}_N^0(e^{2\pi i/N})$, et les corps de constantes de $\mathcal{F}_N^0$ et $\mathcal{F}_N$ sont respectivement $\mathbb{Q}$ et $\mathbb{Q}(e^{2\pi i/N})$; on pose

$$\mathcal{F}^0 = \bigcup_N \mathcal{F}_N^0 \quad \text{et} \quad \mathcal{F} = \bigcup_N \mathcal{F}_N$$

où N parcourt tous les entiers ≥ 1 .

On déduit de l'existence de $\Lambda(s,L)$ le résultat suivant:

THÉORÈME 1 <u>Soit</u> $f \in \mathcal{F}_N$, <u>et soit</u> K <u>un corps quadratique imaginaire.</u> <u>Considérons les propriétés</u> i) <u>et</u> $\text{ii})_K$ <u>suivantes:</u>

i) $f \in \mathcal{F}_N^0$;

$\mathrm{ii})_K$ <u>pour tout point</u> $\wp = (L, L_N, \dot{w})$ <u>de</u> $\mathfrak{T}_N$ <u>, tel que le réseau</u> L <u>possède des multiplications complexes par</u> K <u>et que la fonction</u> $\mathfrak{f}$ <u>sur</u> $\mathfrak{T}_N$ (<u>image par</u> ${}_N\beta_* \circ \alpha^*$ <u>de la fonction</u> f <u>sur</u> $\mathfrak{H}$) <u>soit bien définie en</u> $\wp$ <u>, on a</u>

$$\mathfrak{f}(L, L_N, \dot{w})^{[s,K]} = \mathfrak{f}(s^{-1}L, s^{-1}L_N, s^{-1}\dot{w}) \ , \quad s \in K_A^\times \ ,$$

<u>où le symbole</u> $[s,K]$ <u>agit comme automorphisme sur l'élément</u> $\mathfrak{f}(L, L_N, \dot{w})$ <u>de</u> K^{ab} .

<u>Alors, on a les implications</u>:

$$\mathrm{i}) \Rightarrow \mathrm{ii})_K \quad \text{et} \quad (\mathrm{ii})_K \, , \mathrm{ii})_{K'} \, , K \neq K') \Rightarrow \mathrm{i}) \, .$$

<u>Preuve</u>: <u>$\mathrm{i}) \Rightarrow \mathrm{ii})_K$</u>

On sait que le corps $\mathcal{F}_N^0$ est engendré sur le corps des rationnels par trois fonctions j, j_N et $f^{(1)}$ sur $\mathfrak{H}$ décrites ci–dessous cf. e.g. [7] § 6.2 p. 140, et il s'agit de voir que chacune d'elles vérifie $\mathrm{ii})_K$.

Introduisons les images transposées de celles–ci J, J_N et $F^{(1)}$ par α dont les valeurs au point (w_1, w_2) de $\mathfrak{K}$ sont respectivement données par les quotients

$$J(w_1, w_2) = \tilde{\mathfrak{j}}(L) \, , \ J_N(w_1, w_2) = \tilde{\mathfrak{j}}(L_N) \ ,$$

$$F(w_1, w_2) = 2^5 3^4 \, \frac{g_2(L) g_3(L)}{\Delta(L)} \ \wp(w_2/N, L) \ ,$$

où $\tilde{\mathfrak{j}}$ est l'invariant modulaire $12^3 \, g_2^3/\Delta$ et $(L, L_N, w_2 \text{ modulo } NL) = {}_N\beta(w_1, w_2)$.

Le réseau L , s'il possède des multiplications complexes par K , peut être choisi de façon à vérifier les propriétés i) et ii) du n^{o}3 sans altérer les valeurs de ces trois fonctions J, J_N et $F^{(1)}$ invariantes par homothétie.

Le réseau L_N vérifie alors ces mêmes propriétés de sorte que les relations (4), (6) et (7) fournissent une description de l'action de l'automorphisme d'Artin $[s,K]$, pour s idèle de K , sur chacun de ces trois quotients.

Mais, à nouveau vu la stabilité des trois fonctions par homothétie, la règle de transformation de j, j_N et $f^{(1)}$ est bien donnée par ii)$_K$: le facteur $\Lambda(s,L)$ (resp. $\Lambda(s,L_N)$) pour j et $f^{(1)}$ (resp. j_N) apparait avec l'exposant 0 .

<u>(ii)$_K$, ii)$_{K'}$, $K \neq K'$) $\Rightarrow$ i)</u>

Réciproquement, soit f un élément de $\mathcal{F}_N$ vérifiant ii)$_K$ et ii)$_{K'}$, avec $K \neq K'$. Vu l'action des automorphismes de K^{ab}/K sur le corps des constantes de $\mathcal{F}_N$, il est clair d'après ii)$_K$ que f est un élément de l'extension $K\,\mathcal{F}_N^0$ de $\mathcal{F}_N^0$ par le corps K . Ecrivons alors f comme une somme

$$(8) \qquad f = g + \sqrt{-d_K}\, h$$

où g et h sont deux éléments de $\mathcal{F}_N^0$ et $-d_K < 0$ est le discriminant du corps K . Choisissons un idèle s' de K' , tel que l'automorphisme $[s',K']$ ne fixe pas l'élément $\sqrt{-d_K}$ de K'^{ab} , ce qui est possible puisque $K \neq K'$. Comme, d'après ce qui vient d'être prouvé, les fonctions f, g et h vérifient ii)$_{K'}$, on déduit de (8) en faisant agir $[s',K']$ sur la valeur de

$$\tilde{f} = \tilde{g} + \sqrt{-d_K}\,\tilde{h}$$

en le point $\not{p}' = (L', L'_N, \dot{w}')$ de $\mathfrak{T}_N$, tel que L' possède des multiplications complexes par K' et que les fonctions $\tilde{f}$, $\tilde{g}$ et $\tilde{h}$ respectivement associées à f, g et h soient bien définies en $\not{p}'$, l'égalité

$$2\,\tilde{h}(\not{p}') = 0 \; .$$

Comme l'ensemble des points de K' est dense dans $\mathfrak{H}$, on en déduit bien $h = 0$.

Le théorème est démontré.

Notons que le lemme 4 du n°3 n'a pas été utilisé dans la preuve ci–dessus du th. 1; on a donc:

Seconde preuve du lemme 4:

Par homogénéité le lemme 4 est clair si $L' = rL$ avec r entier rationnel; il suffit donc pour chaque entier $N \geq 1$ de prouver que le quotient

$$(9) \qquad \Lambda(s,L)/\Lambda(s,L_N)$$

vaut 1, chaque fois que L_N est un sur–réseau de L tel que L_N/L soit cyclique d'ordre N.

Mais, définissons alors une fonction P (resp. P') sur $\mathfrak{R}$ invariante par homothétie en posant

$$P(w_1,w_2) = \wp(w_2/N,L)/\wp(w_2/N,L_N)$$

$$\text{(resp. } P'(w_1,w_2) = \wp'(w_2/N,L)\ \wp'(w_2/N,L_N)\ )$$

où $(L,L_N,w_2$ modulo $NL)$ est l'image de (w_1,w_2) par ${}_N\beta$. On vérifie sans difficultés que les images directes des deux fonctions P et P′ par α appartiennent à $\mathcal{F}_N^0$; en effet, le développement à l'infini relativement à $e^{2\pi i z/N}$ avec $z = w_2/w_1$ des formes modulaires images directes respectives de $\left[\frac{2\pi}{w_1}\right]^2 \wp(w_2/N,L)$ et $\left[\frac{2N\pi}{w_1}\right]^2 \wp(w_2/N,L_N)$ par α est à coefficients de Fourier rationnels cf. e.g. [6] § 6.2 p. 141.

Par suite, l'implication i) $\Rightarrow$ ii)$_K$ du th. 1 assure que le carré (resp. le cube) du quotient (9) vaut 1.

5) D'après G. Shimura [7] Chap. 6, la partie positive du groupe $G\ell_2$ évalué sur les adèles $\mathbf{A}$ de $\mathbb{Q}$, i.e. le produit

$$G\ell_2^{>0}(\mathbf{A}) = G\ell_2(\mathbf{A}_f) \times G\ell_2^{>0}(\mathbb{R})$$

agit sur le corps $\mathcal{F}$ des fonctions modulaires arithmétiques. On note cette action

$$f \longmapsto f^\eta\ ,\quad \eta \in G\ell_2^{>0}(\mathbf{A})\ ,$$

de sorte que $f^{\eta\eta'} = (f^\eta)^{\eta'}$; il s'agit d'un homomorphisme surjectif de $G\ell_2^{>0}(\mathbf{A})$ sur le groupe des automorphismes du corps $\mathcal{F}$, continu si l'on munit ces groupes de leurs topologies naturelles; son noyau peut être décrit, cf. [7] § 6.6 p. 150.

Posons

$$U = \prod_{p \text{ premier}} G\ell_2(\mathbb{Z}_p) \times G\ell_2^{>0}(\mathbb{R}) \ ,$$

et

$$U_N = \prod_{p \text{ premier}} U_{N,p} \times G\ell_2^{>0}(\mathbb{R}) \ ,$$

avec

$$U_{N,p} = \{\gamma \in G\ell_2(\mathbb{Z}_p) \mid \gamma \equiv I_2 (\mathrm{mod}\ N)\} \ .$$

Le groupe U est un sous–groupe ouvert de $G\ell_2^{>0}(A)$, et le groupe U_N un sous–groupe ouvert de U ; on sait que le corps $\mathcal{F}_N$ est le plus grand sous–corps de $\mathcal{F}$ sur lequel U_N agit trivialement. De plus, si

$$\Delta = \prod_{p \text{ premier}} \Delta_p \times \{1\}$$

avec

$$\Delta_p = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & d_p \end{bmatrix} \in G\ell_2(\mathbb{Z}_p) \mid d_p \in \mathbb{Z}_p^{\times} \right\} \ ,$$

le corps $\mathcal{F}_N^0$ défini dans le n$^{\text{o}}$4 est le plus grand sous–corps de $\mathcal{F}$ sur lequel le groupe $\Delta\, U_N$ agit trivialement: on retrouve ainsi la définition de $\mathcal{F}_N^0$ de l'introduction; pour tout ceci, cf. [6] chap. 6.

Si z désigne un élément d'un corps quadratique imaginaire K , avec $\mathrm{Im}\, z > 0$, on définit un plongement q de $K^{\times}$ dans le groupe $G\ell_2^{>0}(\mathbb{Q})$, des matrices à coefficients rationnels et de déterminant > 0 , par l'égalité matricielle

$$(10) \qquad q(\mu)\begin{bmatrix} z \\ 1 \end{bmatrix} = \begin{bmatrix} \mu z \\ \mu \end{bmatrix}, \quad \mu \in K^{\times} .$$

Ce plongement peut être prolongé en un plongement que l'on note encore q , du groupe $K_{\mathbb{A}}^{\times} = (\mathbb{A} \otimes K)^{\times}$ des idèles de K dans le groupe $G\ell_2^{>0}(\mathbb{A})$.

D'après G. Shimura [7] § 6.8 p. 157, la loi de réciprocité explicite pour $\mathcal{F} = \bigcup_N \mathcal{F}_N$ s'énonce:

THÉORÈME 2 <u>Soit</u> z <u>un élément d'un corps quadratique imaginaire</u> K , <u>avec</u> $\mathrm{Im}\, z > 0$, <u>et supposons la fonction modulaire</u> f <u>définie au point</u> z .

<u>Alors si, pour un entier</u> $N \geq 1$ <u>convenable la fonction</u> f <u>appartient au corps</u> $\mathcal{F}_N$ <u>défini au n°4, le nombre</u> $f(z)$ <u>appartient à</u> K^{ab} <u>et, pour tout idèle</u> s <u>de</u> K , <u>on a</u>

$$f(z)^{[s,K]} = f^{q(s^{-1})}(z)$$

<u>où</u> q <u>désigne le plongement de</u> $K_{\mathbb{A}}^{\times}$ <u>dans</u> $G\ell_2^{>0}(\mathbb{A})$ <u>défini par le point</u> z , <u>cf. identité</u> (10) <u>ci-dessus</u>.

6) On prouve dans ce numéro le résultat suivant:

PROPOSITION CLEF <u>Soit</u> (w_1,w_2) <u>un point de</u> $\mathfrak{R}$ <u>d'image par</u> ${}_N\beta$ <u>le point</u> $(L,L_N,\dot{w})$ <u>de</u> $\mathfrak{T}_N$. <u>On suppose que</u> L <u>est à multiplication complexe par</u> K , <u>et soit</u> s

un idèle de K .

Soit (u_1,u_2) un point de $\mathfrak{K}$ d'image par ${}_N\beta$ le point $(s^{-1}L, s^{-1}L_N, s^{-1}\dot{w})$ de $\mathfrak{T}_N$, cf. n°2. On définit l'élément η de $G\ell_2^{>0}(\mathbb{Q})$ par l'égalité matricielle

$$(11) \qquad \begin{bmatrix} u_2 \\ u_1 \end{bmatrix} = \eta \begin{bmatrix} w_2 \\ w_1 \end{bmatrix} .$$

Alors, si q désigne l'adélisation du plongement de $K^\times$ dans $G\ell_2^{>0}(\mathbb{Q})$ (de point fixe $z = w_2/w_1$) défini par l'identité (10) du n°5, on a

$$\eta\, q(s) \in \Delta\, U_N .$$

Corollaire Pour le sous-corps $\mathcal{F}_N^0$ de $\mathcal{F}_N$, le th. 2 du n°5 (loi de réciprocité explicite de G. Shimura) et l'assertion i) ⇒ ii)$_K$ du th. 1 du n°4 sont équivalentes.

Preuve: Soit η comme dans la prop. clef. Comme l'orbite de $(L,L_N,\dot{w})$ (resp. de $(s^{-1}L, s^{-1}L_N, s^{-1}\dot{w})$) par homothéties correspond via $\alpha \circ {}_N\beta^{-1}$ à l'orbite de $z = w_2/w_1$ (resp. $\eta(z) = u_2/u_1$) par $\Gamma(N)$, il est clair que l'assertion ii)$_K$ du th. 1 est vraie si et seulement si l'on peut prouver l'égalité

$$f(z)^{[s,K]} = f(\eta(z)) .$$

Or, soit $\theta = (\eta\, q(s))^{-1}$. Alors, par la loi de réciprocité (th. 2) on a

$$f(z)^{[s,K]} = f^{q(s^{-1})}(z) = f^{\theta\eta}(z) .$$

Mais, comme dans [7] § 6.8, p. 163, il vient

$$f^{\theta\eta}(z) = f^{\theta}(\eta(z)) = f(\eta(z))$$

puisque l'élément θ de $\Delta\, U_N$ laisse invariant l'élément f de $\mathcal{F}_N^0$: d'où l'implication $i) \Rightarrow ii)_K$ (th. 1).

L'argument ci–dessus étant réversible, le corollaire est démontré.

<u>Preuve de la proposition clef</u>:

Soit $(\underline{w}_1, \underline{w}_2)$ la base (w_1, Nw_2) de NL_N ; de même, soit $(\underline{u}_1, \underline{u}_2)$ la base (u_1, Nu_2) de $s^{-1}NL_N$. On désigne par q (resp. $\underline{q}$) l'adélisation du plongement de $K^\times$ dans $G\ell_2^{>0}(\mathbb{Q})$ associé au point w_2/w_1 (resp. $\underline{w}_2/\underline{w}_1$) de K. Ce dernier, qui appartient aussi à $\mathfrak{H}$, est fixé par l'action de chacun des éléments de $q(K^\times)$ (resp. $\underline{q}(K^\times)$) de sorte que l'on a

$$\underline{q}(s) = \begin{bmatrix} N & 0 \\ 0 & 1 \end{bmatrix} q(s) \begin{bmatrix} N & 0 \\ 0 & 1 \end{bmatrix}^{-1} \tag{12}$$

pour tout idèle s de K.

Par ailleurs, l'identité (10) du n°5 qui définit le plongement q associé au point $z = w_2/w_1$, possède d'après le lemme 3 du n°2 la version adélisée suivante:

<u>Lemme</u> 5 <u>Pour tout idèle</u> t <u>de</u> K, <u>la base</u> (tw_1, tw_2) <u>sur</u> $\hat{\mathbb{Z}}$ <u>du module</u> $\hat{\mathbb{Z}} \otimes tL$ <u>vérifie l'identité matricielle</u>

$$\begin{bmatrix} tw_2 \\ tw_1 \end{bmatrix} = q(t) \begin{bmatrix} w_2 \\ w_1 \end{bmatrix}, \quad t \in K_A^{\times} ,$$

dont les coefficients appartiennent a priori à $A_f \otimes L$.

On déduit de ces deux faits les conclusions suivantes α) et β) concernant le produit $\eta\, q(s)$ (en un mot, on reproduit ici les étapes de la preuve du lemme 1, première partie):

α) D'après (11) l'image (u_1,u_2) de (w_1,w_2) par η , et d'après le lemme 5 l'image $(s^{-1}w_1, s^{-1}w_2)$ de (w_1,w_2) par $q(s^{-1})$, forment chacune une base de $\hat{\mathbb{Z}} \otimes s^{-1}L$ sur $\hat{\mathbb{Z}}$. Par suite, comme la partie finie de U est $G\ell_2(\hat{\mathbb{Z}})$, on a $\eta\, q(s) \in U$.

De plus, si $\underline{\eta} \overset{\mathrm{dfn}}{=} \begin{bmatrix} N & 0 \\ 0 & 1 \end{bmatrix} \eta \begin{bmatrix} N & 0 \\ 0 & 1 \end{bmatrix}^{-1}$, l'image de $(\underline{w}_1,\underline{w}_2)$ par $\underline{\eta}$ est $(\underline{u}_1,\underline{u}_2)$ .En appliquant le lemme 5 ci–dessus à $\underline{q}(s^{-1})$, on en déduit de même que $\underline{\eta}\, \underline{q}(s) \in U$. Mais d'après (12) ce dernier terme peut–être re–écrit $\begin{bmatrix} N & 0 \\ 0 & 1 \end{bmatrix} \eta\, q(s) \begin{bmatrix} N & 0 \\ 0 & 1 \end{bmatrix}^{-1}$ de sorte que

$$\eta\, q(s) \in \begin{bmatrix} N & 0 \\ 0 & 1 \end{bmatrix}^{-1} U \begin{bmatrix} N & 0 \\ 0 & 1 \end{bmatrix} \cap U .$$

β) Posons $\dot{u}_i = u_i (\mathrm{mod}\ s^{-1}NL)$ et $\dot{w}_i = w_i (\mathrm{mod}\ NL)$, $i \in \{1,2\}$; on a donc $\dot{w}_2 \overset{\mathrm{dfn}}{=} \dot{w}$. D'après le lemme 5 ci–dessus, on a l'égalité matricielle

$$\begin{bmatrix} s^{-1}w_2 \\ s^{-1}w_1 \end{bmatrix} = q(s^{-1}) \begin{bmatrix} w_2 \\ w_1 \end{bmatrix} ,$$

d'où d'après l'identité $\dot{u}_2 = s^{-1}\dot{w}_2$ la congruence

$$\begin{bmatrix} \dot{u}_2 \\ s^{-1}\dot{w}_1 \end{bmatrix} \equiv q(s^{-1}) \begin{bmatrix} w_2 \\ w_1 \end{bmatrix}$$

modulo $\hat{\mathbb{Z}} \otimes s^{-1}NL$. Comme $(u_1,u_2) = \eta(w_1,w_2)$, on en déduit donc l'égalité matricielle

$$(\eta\, q(s)) \begin{bmatrix} \dot{u}_2 \\ s^{-1}\dot{w}_1 \end{bmatrix} = \begin{bmatrix} \dot{u}_2 \\ \dot{u}_1 \end{bmatrix}$$

à coefficients dans $s^{-1}L/s^{-1}NL$; autrement dit, si s_p désigne la p–composante de l'idèle s, la ligne supérieure de $\eta\, q(s_p)$ est congrue à $(1,0)$ modulo N pour tout p premier.

Comme α) assure que pour tout p premier le coefficient inférieur gauche de $\eta\, q(s_p)$ est congru à 0 modulo N, les faits α) et β) prouvent que

$$\eta\, q(s) \in \Delta\, U_N = U_N\, \Delta\ .$$

<u>Remarque</u> Pour p premier, posons $L_p = \mathbb{Z}_p \otimes L$. Alors, le coefficient inférieur droit de $\eta\, q(s_p)$, congru modulo N au produit $\det(\eta)\det(q(s_p))$, est donc congru au quotient des indices (définis par comparaison à un réseau contenant à la fois L et $s^{-1}L$, resp. L_p et $s_p^{-1}L_p$)

$$[L : s^{-1}L] / [L_p : s_p^{-1}L_p]$$

modulo N. Comme $[L : s^{-1}L]$ est le produit sur tous les nombres premiers p de la puissance de p définie par $[L_p : s_p^{-1}L_p]$, ce quotient est bien un élément de $\mathbb{Z}_p^\times$.

Bibliography

[1] C. GOLDSTEIN & N. SCHAPPACHER, Séries d'Eisenstein et fonctions L de courbes elliptiques à multiplication complexe, Journ. f.r.u. and. Math. 327 (1981) 184–218.

[2] S. LANG, Elliptic functions, Ed: Addisson–Wesley, 1973.

[3] G. ROBERT, Sur le corps de définition de certaines courbes elliptiques à multiplications complexes, Sém. Th. Nombres de Bordeaux (1983/84) exposé n^{o}8 (16 déc. 1983).

[4] G. ROBERT, Elliptic units, en cours de rédaction (juin 1989).

[5] J–P. SERRE & J. TATE, Good reduction of abelian varieties, Ann. of Math. 88 (1968) 492–517.

[6] G. SHIMURA, On the field of definition for a field of automorphic functions II, Ann. of Math. 81 (1965) 160–189.

[7] G. SHIMURA, Introduction to the arithmetic theory of automorphic functions, Ed: Iwanami Shoten et P.U.P., 1971.

[8] G. SHIMURA, On canonical models of arithmetic quotients of bounded symmetric domains I, Ann. of Math. 91 (1970) 144–222.