A NEW FORMULATION OF THE EXPLICIT RECIPROCITY LAW

by

Gilles ROBERT

Max–Planck–Institut
für Mathematik
Gottfried–Claren–Str. 26
5300 Bonn 3
Federal Republic of Germany

MPI/89 – 12

A NEW FORMULATION OF THE EXPLICIT RECIPROCITY LAW

par Gilles ROBERT

SURVEY

Il s'agit ici en quelque sorte de la conclusion restée non écrite du § 6.8 consacré à la loi explicite de de réciprocité par G. Shimura dans son livre [2].

Soit N un entier, $N \geq 1$. Pour $f : z \longmapsto f(z)$ une fonction modulaire de niveau N dont les coefficients de Fourier à l'infini relatifs à $e^{2\pi i z/N}$ sont rationnels, on exprime la loi de réciprocité de loc. cit. p. 157 à l'aide de la fonction associeé π_f définie sur les triplets formés d'un réseau complexe $\underline{L}$, d'un sous–réseau L tel que $\underline{L}/L \simeq \mathbb{Z}/N$, et d'un point $\underline{w}_2$ de $\underline{L}$ dont le classe modulo L est un point de torsion d'ordre exact N dans $\mathbb{C}/L$. La formule que l'on trouve fait appel à l'action de l'inverse de l'idèle s du corps de multiplication complexe des réseaux L et $\underline{L}$ sur ceux–ci et sur la classe modulo L du point $\underline{w}_2$, d'ordre N dans $\mathbb{C}/L$.

Précisément, quand elle est définie la valeur $\pi_f(L,\underline{L},\underline{w}_2)$ appartient à la cloture abélienne K^{ab} de K, et on a

$$\pi_f(L,\underline{L},\underline{w}_2)^{[s,K^{ab}]} = \pi_f(s^{-1}L,s^{-1}\underline{L},s^{-1}\underline{w}_2)$$

où $s^{-1}\underline{w}_2$ désigne un représentant complexe de la classe modulo $s^{-1}L$ du point $s^{-1}(\underline{w}_2 \bmod L)$ d'ordre exact N dans $\mathbb{C}/s^{-1}L$, cf. th. infra. On notera que toute référence à un plongement particulier de K^x dans le groupe $G\ell_2^{>0}(\mathbb{Q})$ (dépendant du point quadratique imaginaire où est évalué f) a disparu de l'énoncé.

GREETINGS

They do not only go to the work [2] of G. Shimura, but also to S. Lang whose very useful book [1] has given us the possibility of understanding what the first named author did; particularly, his chapter 11 there was remarkably interesting (and his th. 5 loc. cit. gave us a prototype of our key proposition).

Let N be some integer, $N \geq 1$. Let L and $\underline{L}$ be two complex lattices satisfying i) $L \subset \underline{L}$ and ii) the quotient $\underline{L} / L$ is cyclic of order N . Choose a basis $(\underline{w}_1,\underline{w}_2)$ of $\underline{L}$, with $\mathrm{Im}(\underline{w}_2/\underline{w}_1) > 0$, such that $(w_1,w_2) = (\underline{w}_1, N\,\underline{w}_2)$ be a basis of L ; in particular $\underline{w}_2$ modulo L is a torsion point of exact order N in $\mathbb{C}/L$. If z is any complex number with $\mathrm{Im}(z) > 0$, let a matrix $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ of $G\ell_2^{>0}(\mathbb{R})$ act on z by

$$\gamma(z) = \frac{az + b}{cz + d}$$

so that $\mathrm{Im}(\gamma(z)) > 0$.

Suppose that L and $\underline{L}$ have complex multiplication by some imaginary quadratic field K . Let $\underline{q} : K^x \longrightarrow G\ell_2^{>0}(\mathbb{Q})$ be the normalized embedding with fixed point $\underline{w}_2/\underline{w}_1$ defined by

$$(1) \qquad \underline{q}(\mu)\begin{bmatrix} \underline{w}_2 \\ \underline{w}_1 \end{bmatrix} = \begin{bmatrix} \mu\,\underline{w}_2 \\ \mu\,\underline{w}_1 \end{bmatrix} , \quad \mu \in K^x ;$$

denote also $\underline{q}$ the associated embedding of $(K \otimes_{\mathbb{Q}} A_f)^{\times}$ inside $G\ell_2(A_f)$ where the latter term is the group $G\ell_2$ evaluated on the algebra of finite adèles A_f of $\mathbb{Q}$ and the former is the group of finite idèles of K . Adopt the analogous notation for the embedding $q : K^{\times} \longrightarrow G\ell_2^{>0}(\mathbb{Q})$ with fixed point w_2/w_1 associated in the same way with w_1 and w_2 in place of $\underline{w}_1$ and $\underline{w}_2$; for any finite idèle s of K , we have

$$q(s) = \begin{bmatrix} N & 0 \\ 0 & 1 \end{bmatrix} \underline{q}(s) \begin{bmatrix} N & 0 \\ 0 & 1 \end{bmatrix}^{-1} . \tag{2}$$

For any finite idèle t of K and any sublattice L_0 of L , let tL_0 be the complex lattice defined by multiplication by the idèle t . Recall that this action defines an isomorphism

$$t : (\mathbb{C}/L_0)_{\mathrm{tors}} \longrightarrow (\mathbb{C}/tL_0)_{\mathrm{tors}} \tag{3}$$

of the group of torsion points of $\mathbb{C}/L_0$ inside the group of torsion points of $\mathbb{C}/tL_0$.

We have the following lemma:

<u>LEMMA</u> <u>For any sublattice</u> L_0 <u>of</u> L <u>and any finite idèle</u> t <u>of</u> K , <u>we have</u>

$$\underline{q}(t) \begin{bmatrix} \underline{w}_2 \\ \underline{w}_1 \end{bmatrix} \underset{tL_0}{\equiv} \begin{bmatrix} t\,(\underline{w}_2 \bmod L_0) \\ t\,(\underline{w}_1 \bmod L_0) \end{bmatrix} \tag{4}$$

<u>where on both lines the congruence is to be readed modulo the complex lattice</u> tL_0 .

PROOF: For p a prime, let t_p be the p–component of t and denote by $L_{0,p}$ the tensor product $L_0 \otimes \mathbb{Z}_p$ inside $L_0 \otimes \mathbb{Q}_p$. Then the right hand side of (4) satisfy by definition the congruence

$$\begin{bmatrix} t_p\,(\underline{w}_2 \bmod L_{0,p}) \\ t_p\,(\underline{w}_1 \bmod L_{0,p}) \end{bmatrix} \underset{t_pL_{0,p}}{\equiv} \begin{bmatrix} t_p & \underline{w}_2 \\ t_p & \underline{w}_1 \end{bmatrix}$$

where on both lines the congruence is to be readed modulo the lattice $t_pL_{0,p}$. But, we have the matrix equality

$$\begin{bmatrix} t_p & \underline{w}_2 \\ t_p & \underline{w}_1 \end{bmatrix} = \underline{q}(t_p)\begin{bmatrix} \underline{w}_2 \\ \underline{w}_1 \end{bmatrix}\ ,\ t_p \in K \otimes_{\mathbb{Q}} \mathbb{Q}_p\ ,$$

where $\underline{q}(t_p)$ belongs to $G\ell_2(K \otimes_{\mathbb{Q}} \mathbb{Q}_p)$. Hence we have the congruence (4) with a p added everywhere; as p is arbitrary, the lemma is proved.

Let U be the subgroup of $G\ell_2(A_f)$ defined by

$$U = \prod_{p\ \text{prime}} G\ell_2(\mathbb{Z}_p)\,.$$

Also, denote by $U_N = \prod_p U_{N,p}$, $\nabla = \prod_p \nabla_p$ and $\Delta = \prod_p \Delta_p$ the subgroups of U defined by the conditions

$$U_{N,p} = \begin{cases} G\ell_2(\mathbb{Z}_p)\ , & \text{if } p \nmid N \\[2ex] I_2 + NM_2(\mathbb{Z}_p)\ , & \text{if } p \mid N \end{cases}\ ,$$

$$\nabla_p = \begin{cases} 1 & , \text{ if } p \nmid N \\ \left\{ \begin{bmatrix} 1 & b_p \\ 0 & d_p \end{bmatrix} \middle| \; b_p \in \mathbb{Z}_p ,\; d_p \in \mathbb{Z}_p^{\times} \right\} & , \text{ if } p \mid N \end{cases} ,$$

$$\Delta_p = \begin{cases} 1 & , \text{ if } p \nmid N \\ \left\{ \begin{bmatrix} 1 & 0 \\ 0 & d_p \end{bmatrix} \middle| \; d_p \in \mathbb{Z}_p^{\times} \right\} & , \text{ if } p \mid N \end{cases} .$$

Fix some finite idèle s of K , and let $s^{-1}L$ and $s^{-1}\underline{L}$ be the complex lattices image of respectively L and $\underline{L}$ by multiplication by the idèle s^{-1} . By the isomorphism (3), the class

$$\underline{u}_2 \bmod s^{-1}L \overset{\mathrm{dfn}}{=} s^{-1}(\underline{w}_2 \bmod L) \tag{5}$$

is a torsion point of exact order N in $\mathbb{C}/s^{-1}L$. Let us choose some complex representative $\underline{u}_2$ of it. We have $\underline{u}_2 \in s^{-1}\underline{L}$, so that by the noted property we can find some other element $\underline{u}_1 \in s^{-1}\underline{L}$, such that $(\underline{u}_1,\underline{u}_2)$ be a basis of $s^{-1}\underline{L}$ with $\mathrm{Im}(\underline{u}_2/\underline{u}_1) > 0$ and $(u_1,u_2) = (\underline{u}_1,N\underline{u}_2)$ be a basis of $s^{-1}L$. Hence our choices define a matrix

$$\eta \in G\ell_2^{>0}(\mathbb{Q}) ,$$

with rational coefficients and positive determinant, such that

$$\text{a)}\quad \begin{bmatrix} \underline{u}_2 \\ \underline{u}_1 \end{bmatrix} = \eta \begin{bmatrix} \underline{w}_2 \\ \underline{w}_1 \end{bmatrix}, \qquad\qquad \text{b)}\quad \begin{bmatrix} u_2 \\ u_1 \end{bmatrix} = \begin{bmatrix} N & 0 \\ 0 & 1 \end{bmatrix} \eta \begin{bmatrix} N & 0 \\ 0 & 1 \end{bmatrix}^{-1} \begin{bmatrix} w_2 \\ w_1 \end{bmatrix}.$$

By equation a), we have $\eta\, \underline{q}(s) \in U$ and by equation b) we have $\begin{bmatrix} N & 0 \\ 0 & 1 \end{bmatrix} \eta \begin{bmatrix} N & 0 \\ 0 & 1 \end{bmatrix}^{-1} q(s) \in U$. But by (2) this can be rewritten as $\begin{bmatrix} N & 0 \\ 0 & 1 \end{bmatrix} \eta\, \underline{q}(s) \begin{bmatrix} N & 0 \\ 0 & 1 \end{bmatrix}^{-1}$, so that

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

Moreover by the lemma and the equation (5) we have the congruence

$$\begin{bmatrix} \underline{u}_2 \\ \underline{u}_1 \end{bmatrix} \underset{s^{-1}L}{\equiv} \begin{bmatrix} s^{-1}\,(\,\underline{w}_2 \mod L\,) \\ s^{-1}\,(\,\underline{w}_1 \mod L\,) \end{bmatrix} \underset{s^{-1}L}{\equiv} \underline{q}(s^{-1}) \begin{bmatrix} \underline{w}_2 \\ \underline{w}_1 \end{bmatrix} ;$$

hence by the above definition a) of η

$$(\eta\, \underline{q}(s)) \begin{bmatrix} \underline{u}_2 \\ \underline{u}_1 \end{bmatrix} \underset{s^{-1}L}{\equiv} \begin{bmatrix} \underline{u}_2 \\ \underline{u}_1 \end{bmatrix} ;$$

this proves that the left upper coefficient of $\eta\, \underline{q}(s)$ is congruent to 1 modulo N . These two facts imply that

$$\eta\, \underline{q}(s) \in \nabla\, U_N = U_N \nabla .$$

Yet, let $\Gamma_1(N)$ be the group

$$\left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}) \,|\, a \equiv d \equiv 1 (\text{mod } N) \,,\ c \equiv 0 (\text{mod } N) \right\}$$

and put $\eta' = \gamma\,\eta$ for some γ in $\Gamma_1(N)$. Modify both basis $(\underline{u}_1,\underline{u}_2)$ and (u_1,u_2) by putting

$$\begin{bmatrix} \underline{u}'_2 \\ \underline{u}'_1 \end{bmatrix} = \gamma \begin{bmatrix} \underline{u}_2 \\ \underline{u}_1 \end{bmatrix} \,,\quad \begin{bmatrix} u'_2 \\ u'_1 \end{bmatrix} = \begin{bmatrix} N & 0 \\ 0 & 1 \end{bmatrix} \gamma \begin{bmatrix} N & 0 \\ 0 & 1 \end{bmatrix}^{-1} \begin{bmatrix} u_2 \\ u_1 \end{bmatrix}$$

so that the pairs $(\underline{u}'_1,\underline{u}'_2)$ and $(u'_1,u'_2) = (\underline{u}'_1, N\,\underline{u}'_2)$ are always positively oriented basis of respectively $s^{-1}\underline{L}$ and $s^{-1}L$. Note that, if we write $\underline{u}'_1, \underline{u}'_2, u'_1, u'_2$ and η' in place of $\underline{u}_1, \underline{u}_2, u_1, u_2$ and η, the above relations a) and b) as well as the equation (5) are satisfied by the new quantities. We thus have $\eta' \in \nabla\, U_N$; as

$$\nabla\, U_N = \Gamma_1(N) \,\Delta\, U_N \,,$$

we have proved:

PROPOSITION Let L and $\underline{L}$ be two complex lattices as above. Suppose given a basis $(\underline{w}_1,\underline{w}_2)$ of $\underline{L}$, with $\text{Im}(\underline{w}_2/\underline{w}_1) > 0$, such that $(\underline{w}_1, N\,\underline{w}_2)$ be a basis of L, and assume that L and $\underline{L}$ have complex multiplication by some imaginary quadratic field K.

Let s be some finite idèle of K. Then, one can find a basis $(\underline{u}_1,\underline{u}_2)$ of $s^{-1}\underline{L}$, with $\text{Im}(\underline{u}_2/\underline{u}_1) > 0$, such that

i) $(\underline{u}_1, N\,\underline{u}_2)$ is a basis of $s^{-1}L$,

ii) $\underline{u}_2 \bmod s^{-1}\underline{L} = s^{-1}(\underline{w}_2 \bmod \underline{L})$,

iii) the matrix $\eta \in G\ell_2^{>0}(\mathbb{Q})$ such that

(6)
$$\begin{bmatrix} \underline{u}_2 \\ \underline{u}_1 \end{bmatrix} = \eta \begin{bmatrix} \underline{w}_2 \\ \underline{w}_1 \end{bmatrix}$$

<u>does satisfy</u> $\eta\, \underline{q}(s) \in \Delta\, U_N = U_N \Delta$, <u>where</u> $\underline{q}$ <u>is the adelisation of the embedding of</u> K^x <u>inside</u> $G\ell_2^{>0}(\mathbb{Q})$ (<u>with fixed point</u> $\underline{w}_2/\underline{w}_1$) <u>defined by</u> (1).

<u>REMARK</u> If, for the same finite idèle s of K , another basis $(\underline{u}'_1, \underline{u}'_2)$ of $s^{-1}\underline{L}$, with $\mathrm{Im}(\underline{u}'_2/\underline{u}'_1) > 0$, also satisfy the conditions i), ii) and iii) of the proposition, then for the corresponding matrix $\eta' \in G\ell_2^{>0}(\mathbb{Q})$ we have $\eta' = \gamma\,\eta$ with γ element of

$$SL_2(\mathbb{Z}) \cap \Delta\, U_N = \{\delta \in SL_2(\mathbb{Z}) \,|\, \delta \equiv I_2 (\mathrm{mod}\ N)\} .$$

*

*   *

Let now $f : z \longmapsto f(z)$ be some modular function of level N , defined over the Poincaré half plane $\{z \,|\, \mathrm{Im}(z) > 0\}$, and invariant under the action of $\Gamma_1(N)$. As usual, associate to f a function π_f on the triples $(L, \underline{L}, \underline{w}_2)$ where the complex lattices L and $\underline{L}$ satisfy i) $L \subset \underline{L}$ and ii) $\underline{L}/L \simeq \mathbb{Z}/N$, and where the point $\underline{w}_2$ satisfy iii) $\underline{w}_2 \in \underline{L}$ and iv) the class of $\underline{w}_2$ modulo L is of exact order N in $\mathbb{C}/L$. Recall how to define π_f : the above conditions on $\underline{w}_2$ imply the existence of a second point $\underline{w}_1$ of $\underline{L}$ such that i) $(\underline{w}_1, \underline{w}_2)$ be a basis of $\underline{L}$, with $\mathrm{Im}(\underline{w}_2/\underline{w}_1) > 0$, and ii) $(\underline{w}_1, N\,\underline{w}_2)$ be a basis of L ; then put

$$\pi_f(L, \underline{L}, \underline{w}_2) \overset{\mathrm{dfn}}{=} f(\underline{w}_2/\underline{w}_1) .$$

The invariance condition on the function f implies that the above definition is meaningfull.

Also, note that π_f does not depend of the choice of $\underline{w}_2$ if and only if f is invariant under the action of the bigger group

$$\Gamma_0(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}) \mid c \equiv 0 (\mathrm{mod}\ N) \right\} .$$

We have:

THEOREM Let f be a modular function of level N, and suppose that its Fourier coefficients at ∞ relative to $e^{2\pi i z/N}$ are rational (which necessarily implies the invariance of f under $\Gamma_1(N)$).

Let $(L,\underline{L},\underline{w}_2)$ be a triple as above. Assume that L and $\underline{L}$ have complex multiplication by an imaginary quadratic field K, and that π_f is well defined on the triple $(L,\underline{L},\underline{w}_2)$.

Then, the element $\pi_f(L,\underline{L},\underline{w}_2)$ belongs to the abelian closure K^{ab} of K, and for any (finite) idèle s of K we have

$$\pi_f(L,\underline{L},\underline{w}_2)^{[s,K^{ab}]} = \pi_f(s^{-1}L, s^{-1}\underline{L}, s^{-1}\underline{w}_2)$$

where $[s,K^{ab}]$ denotes the Artin automorphism of K^{ab}/K associated to s, and $s^{-1}\underline{w}_2$ is any number of $s^{-1}\underline{L}$ whose class modulo $s^{-1}L$ coincides with the point $s^{-1}(\underline{w}_2 \bmod L)$ of exact order N in $\mathbb{C}/s^{-1}L$.

PROOF: First note that the modular function f is invariant under the subgroup ΔU_N of $G\ell_2(A_f)$.

Then, let $(\underline{w}_1,\underline{w}_2)$ with $\mathrm{Im}(\underline{w}_2/\underline{w}_1) > 0$ be a basis of $\underline{L}$ such that $(\underline{w}_1, N\,\underline{w}_2)$ be a basis of L. By the above proposition, we can choose $(\underline{u}_1,\underline{u}_2)$ with $\mathrm{Im}(\underline{u}_2/\underline{u}_1) > 0$ a basis of $s^{-1}\underline{L}$ satisfying conditions i), ii) and iii) of it; hence by iii), the matrix η of $G\ell_2^{>0}(\mathbb{Q})$ defined by the identity (6) is such that the product $\eta\,\underline{q}(s)$ belongs to ΔU_N. Put $t = (\eta\,\underline{q}(s))^{-1}$.

As we can, suppose f to be defined at $z = \underline{w}_2/\underline{w}_1$. Then, by the conditions i) and ii) of the proposition, the assertion of the theorem would result of the equality

$$f(z)^{[s,K^{ab}]} = f(\eta\,(z)) . \tag{7}$$

But, noting exponentially the action τ of $G\ell_2(A_f)$ on f, the explicit reciprocity law of G. Shimura of [2] § 6.8 p. 157 says that the left hand side of (7) is equal to

$$f^{\tau(\underline{q}(s^{-1}))}(z) = f^{\tau(t\eta)}(z) ,$$

and we have as in loc. cit. p. 163

$$f^{\tau(t\eta)}(z) = f^{\tau(t)}(\eta(z)) = f(\eta(z)) .$$

The theorem is proved.

NOTA Let $\mathcal{F}_0$ be the field of all modular functions f as in the theorem, where the integer N takes any convenient value.

Then, for $\mathcal{F}$ the field of all modular functions whose Fourier coefficients belong to the abelian closure $\mathbb{Q}^{ab}$ of $\mathbb{Q}$, we have

$$\mathcal{F} = \mathbb{Q}^{ab} \mathcal{F}_0$$

as is noted in [2] Exercise 6.26 p. 152.

It is for the elements of the field $\mathcal{F}$ that G. Shimura did first state his explicit reciprocity law.

[1] S. LANG, Elliptic Functions (1973) Ed: Addison–Wesley.

[2] G. SHIMURA, Introduction to the arithmetic theory of automorphic functions (1971) Ed: Iwanami Shoten and P.U.P.

Errata (31 mars 1989)

p. 8, l. –8, suppress: "and invariant under the action of $\Gamma_1(N)$"

p. 9, first two lines, add more precisely:

"The fact that the function f be invariant under the action of

$$\left\{\begin{bmatrix} 1 & 0 \\ c & 1 \end{bmatrix} \middle| c \equiv 0 \pmod{N}\right\} \subset \left\{\delta \in SL_2(\mathbb{Z}) \mid \delta \equiv I_2 \pmod{N}\right\}$$

implies that the above definition is meaningful."

p. 9, inside THEOREM, suppress: "(which necessarily implies the invariance of f under $\Gamma_1(N)$)"

p. 10, l. 1, write: "First note that by hypothesis the modular function f ....."