LEILA SCHNEPS

Fonctions L p-adiques et construction explicite de certains groupes comme groupes de Galois

Thèses d'Orsay, 1990

<http://www.numdam.org/item?id=BJHTUP11_1990__0277__P0_0>

ORSAY
n° d'ordre : 63869

UNIVERSITE DE PARIS-SUD

CENTRE D'ORSAY

THESE

présentée

Pour obtenir

Le TITRE de DOCTEUR EN SCIENCE

PAR

Mademoiselle Leila Schneps

SUJET : Fonctions L p-adiques, et Construction explicite de groupes de Galois

soutenue le 15 Janvier 1990 devant la Commission d'examen

MM. BEAUVILLE Président

HENNIART

HUBBARD

MESTRE

BARSKY

Je tiens à remercier tout d'abord John Coates qui m'a proposé le problème de la nullité de l'invariant-μ des fonctions L p-adiques et également celui de la construction explicite de fonctions L p-adiques dans un cas où ça n'avait pas encore été fait, les extensions des corps quadratiques imaginaires non nécéssairement abéliennes sur $\mathbf{Q}$. Je remercie aussi Pierre Colmez qui a abordé ce deuxième problème avec moi.

J'aimerais exprimer la plus vive reconnaissance à Jean-François Mestre pour toutes les conversations mathématiques et autre que j'ai eu avec lui et qui m'ont orientée dans la direction des groupes de Galois, ainsi qu'à Jean-Pierre Serre qui m'a donné de son temps pour améliorer la rédaction de la note que je lui ai soumise.

Je remercie également le Max-Planck Institut für Mathematik pour son hospitalité et son soutien financier pendant la préparation d'une grande partie de ce travail.

Finalement, je remercie sincèrement M. Arnaud Beauville pour avoir accepté de présider le jury de soutenance, ainsi que MM. Jean-François Mestre, John Hubbard et Daniel Barsky qui en font partie, et particulièrement Guy Henniart pour avoir joué le rôle parfois ingrat de directeur de thèse.

SCHNEPS, Leila

Titre de la thèse: Fonctions L p-adiques, et Construction explicite de certains groupes comme groupes de Galois

Code matière AMS: 14K07, 11F67, 11F85, 12F10

Mots clefs: Elliptic curves, Special values of L-functions, p-adic theory, Galois theory

Résumé: Cette thèse consiste en un ensemble de travaux réunis autour de deux thèmes principaux: les fonctions L p-adiques et la construction explicite de certains groupes comme groupes de Galois.

Abstract: This thesis consists of a collection of articles on two different themes: p-adic L-functions and explicit construction of certain groups as Galois groups.

Table des matières

INTRODUCTION

Cette thèse consiste en un ensemble de travaux réunis autour de deux thèmes principaux : les fonctions L p-adiques et la construction explicite de certains groupes comme groupes de Galois. Chaque article est précédé par un bref résumé de son contenu.

Article 1. Sur l'invariant-μ des fonctions L p-adiques attachées aux courbes elliptiques à multiplication complexe.

Soit E une courbe elliptique définie sur un corps quadratique imaginaire K, à multiplication complexe par K, et soit p un premier différent de 2 et 3, où E a bonne réduction, qui est décomposé dans K; on écrit $(p) = \mathbf{pp}^*$. Soit F_∞ le corps obtenu en ajoutant à K tous les points de $\mathbf{p}^n$-division de E $(n = 1, 2, \ldots)$, et soit M_∞ la p-extension abélienne maximal de F_∞ non-ramifiée en dehors de p. Soit X_∞ le groupe de Galois de M_∞ sur F_∞. Soit $\Gamma = \mathrm{Gal}(F_\infty/F_0)$, où $F_0 = K(E_p)$. Il est connu que X_∞ est un $\mathbf{Z}_p[[\Gamma]]$-module de torsion de type fini. Nous démontrons ici que son invariant-μ est nul.

La méthode utilisée est de démontrer que l'invariant-μ est nul pour chacune des fonctions L p-adiques $L_{p,i}$, $1 \leq i \leq p-2$, construites par Bernardi-Goldstein-Stephens; il n'est pas difficile à voir que $\mu(X_\infty) = \sum_{i=1}^{p-2} \mu(L_{p,i})$. Pour étudier l'invariant-μ de ces fonctions L, on utilise leur construction en tant que transformée gamma de fractions rationnelles sur la courbe elliptique E, et on donne une formule générale reliant l'invariant-μ d'une telle fraction rationnelle à celui de sa transformée gamma. Explicitement, si R est une fraction rationnelle sur E dont le développement de Laurent est entier, on lui associe une mesure λ sur $\mathbf{Z}_p$, et on définit sa i-ième transformée gamma pour $1 \leq i \leq p-2$ par $\Gamma^i_\lambda(s) = \int_{\mathbf{Z}_p^*} \langle x \rangle^s \omega^i(x)\, d\lambda$, où ω est le caractère de Teichmüller. On a alors:

Théorème: $\mu\Big(\sum_{v \in W} \omega^i(v) \lambda^* \circ (v)\Big) = \mu\big(\Gamma^i_\lambda(s)\big)$, où W est l'ensemble des racines de l'unité dans K, λ^* est la mesure λ restreinte à $\mathbf{Z}_p^*$ et $\lambda \circ (v)$ est la mesure définie par $\lambda \circ (v)(C) = \lambda(vC)$ pour tout ensemble ouvert-compact de $\mathbf{Z}_p$.

Reprinted from JOURNAL OF NUMBER THEORY
All Rights Reserved by Academic Press, New York and London

Vol. 25, No. 1, January 1987
Printed in Belgium

On the μ-Invariant of p-Adic L-Functions Attached to Elliptic Curves with Complex Multiplication

LEILA SCHNEPS

Université de Paris-Sud, Faculté de Mathématiques, Bâtiment 425, 91405 Orsay, France

Communicated by M. Waldschmidt

Received January 5, 1985

The main result of this paper proves that the μ-invariant is zero for the Iwasawa module which arises naturally in the study of p-power descent on an elliptic curve with complex multiplication and good ordinary reduction at the prime p.

0. INTRODUCTION

Let E be an elliptic curve defined over a quadratic imaginary field K, with complex multiplication by K, and let p be a prime different from 2 and 3, where E has good reduction, and which splits in K, say $(p) = \mathfrak{p}\mathfrak{p}^*$. Let F_n be the field obtained by adjoining to K all $\mathfrak{p}^n$-division points on E ($n = 1, 2, \ldots$), and let M_∞ be the maximal abelian p-extension of F_∞ unramified outside p. Write X_∞ for the Galois group of M_∞ over F_∞, endowed with its natural action of the Galois group $\mathrm{Gal}(F_\infty/K)$. Let $\Gamma = \mathrm{Gal}(F_\infty/F_0)$, where $F_0 = K(E_{\mathfrak{p}})$. It is well known that X_∞ is a finitely generated $\mathbb{Z}_p[[\Gamma]]$-trosion $\mathbb{Z}_p[[\Gamma]]$-module. The aim of this paper is to prove that the μ-invariant of X_∞ is zero.

Our methods have been inspired by the recent work of Sinnott [9] in the cyclotomic case. The same result has been obtained independently and simultaneously by Gillard [5]; the key difference between his approach and the one in this paper is in the proof of algebraic independence (Theorem III here, I.2 in [5]). In particular, Gillard studies the schematic closure of a certain subvariety of E^n, whereas here we consider the Zariski closure of a certain subgroup of the formal group of $\tilde{E}^n$, $\tilde{E}$ being the curve reduced mod p, which permits us to establish the theorem by elementary methods. This is the only point in Sinnott's article which does not generalize easily to the elliptic case. It is also noteworthy, however, that in

0022-314X/87 $3.00

applying the results to the p-adic L-functions, Gillard used those constructed by himself in an earlier article [10], whereas here we follow the construction of the p-adic L-functions $L_{p,i}$ for $1 \leqslant i \leqslant p-2$ given in [1].

1. NOTATION

Let K be an imaginary quadratic field of class number 1, with ring of integers $\mathcal{O}$. Let E be an elliptic curve defined over K, with complex multiplication by $\mathcal{O}$, and let ψ be the Grossencharakter of E over K. We fix an algebraic closure $\bar{K}$ of K and an embedding $\bar{K} \subset \mathbb{C}$. Let S be the set containing 2, 3, and rational primes q such that E does not have good reduction for at least one prime lying over q. Let p be a rational prime which is not in S, and such that p splits in K: $(p) = \mathfrak{p}\mathfrak{p}^*$. Let $\pi = \psi(\mathfrak{p})$. Let $K_{\mathfrak{p}}$ be the completion of K at $\mathfrak{p}$ and let $I_{\mathfrak{p}}$ be the ring of integers of the completion of the maximal abelian unramified extension of $K_{\mathfrak{p}}$. We fix a Weierstrass model for E,

$$y^2 = 4x^3 - g_2 x - g_3 \tag{1}$$

such that $g_2, g_3 \in \mathcal{O}$, and $g_2^3 - 27g_3^2$ are minimal at all primes of K not lying above a prime in S. Let L be the period lattice of the Weierstrass $\wp$-function associated with this model. Since K has class number 1, there is an $\Omega \in L$ such that $L = \Omega\mathcal{O}$.

Let $L(\bar{\psi}^k, s)$ be the complex Hecke L-function of $\bar{\psi}^k$. Let $\Omega_{\mathfrak{p}}$ be a p-adic period of E. We follow the notation of [1] in reviewing the construction of the p-adic L-functions $L_{\mathfrak{p},i}(s)$ for $1 \leqslant i \leqslant p-2$, such that for each integer $k \geqslant 1$, $k \equiv i \pmod{p-1}$,

$$\Omega_{\mathfrak{p}}^{-k} L_{\mathfrak{p},i}(k) = (k-1)!\,(1 - (\psi^k(\mathfrak{p})/N_{\mathfrak{p}}))\,\Omega^{-k} L(\bar{\psi}^k, k). \tag{2}$$

Note that the interpolated L-function is the primitive one.

Let $\phi(z, L) = (\wp(z, L), \wp'(z, L))$. Let ω be the Teichmüller character on $\mathbb{Z}_p$, and for each $x \in \mathbb{Z}_p^*$, let $\langle x \rangle = x/\omega(x)$. Let $\hat{E}$ denote the formal group giving the kernel of reduction modulo $\mathfrak{p}$ on E: a local parameter for $\hat{E}$ is given by $t = -2x/y$. If we consider z to be the parameter for the additive formal group $\hat{G}_a$, then $t = -2\wp(z)/\wp'(z)$ gives the exponential map from $\hat{G}_a$ to $\hat{E}$. If we let w be the parameter for the multiplicative formal group $\hat{G}_m$, then since $\hat{E}$ has height 1 (since p is split), there exists a power series $\delta(w) \in wI_{\mathfrak{p}}[[w]]$ which gives an isomorphism of formal groups δ: $\hat{G}_m \to \hat{E}$. The p-adic period is, by definition, the coefficient of w in δ: it is determined up to a unit in $\mathbb{Z}_p^*$.

We now introduce the basic rational functions on E (see [2] for details). Let $\alpha \in \mathcal{O}$, $\alpha \neq 0$ or a unit, and let E_α denote the kernel of α on E. For each

i, $0 \leqslant i \leqslant p-2$, such that $f_i \neq 1$, let Q_i be a primitive f_i-division point on E. Define

$$\xi_\alpha(P) = \prod_{\substack{R \in E_\alpha \\ R \neq 0}} (x(P) - x(R)) \qquad \text{and} \qquad \xi_{\alpha,Q_i}(P) = \prod_{\tau \in G_{f_i}} \xi_\alpha(P + Q_i^\tau), \quad (3)$$

where $G_{f_i} = \mathrm{Gal}(K(E_{f_i})/K)$. We have the following equation [1]. For any ideal $\mathfrak{b}$ of $\mathcal{C}$ prime to α and to f_1,

$$\prod_{S \in E_{\mathfrak{b}}} \xi_{\alpha,Q_i}(P+S) \sim \xi_{\alpha,Q_i,\sigma_{\mathfrak{b}}}(\psi(\mathfrak{b})P), \quad (4)$$

where $\sigma_{\mathfrak{b}}$ is the Artin symbol of $\mathfrak{b}$ relative to $K(E_{f_i})/K$, and the symbol $\sim$ means that the quotient of the two functions is a constant in K^*.

We now consider the development of the rational functions in (3) in the parameter z of the additive formal group, and define

$$R_{\alpha,i}(z, L) = \begin{cases} \xi_\alpha(\phi(z, L)) & \text{if } f_i = 1, \\ \xi_{\alpha,Q_i}(\phi(z, L)) & \text{otherwise.} \end{cases}$$

Let $m_i = \mathrm{card}(\mathrm{Gal}(K(E_{f_i})/K))$ for each i. Consider the set $\mathcal{M}$ of maps μ: $A \to \mathbb{Z}$, where A is the set of elements of $\mathcal{C}$ prime to f_1 and to p, and where

$$\mu(\alpha) = 0 \text{ for almost all } \alpha \in A \qquad \text{and} \qquad \sum_{\alpha \in A} \mu(\alpha)(N\alpha - 1) = 0.$$

For $\mu \in \mathcal{M}$, let $\tilde{R}_{\mu,i}(z, L) = \prod_{\alpha \in A} (\alpha^{2m_i} R_{\alpha,i}(z, L))^{\mu(\alpha)}$. Then $(d/dz) \log \tilde{R}_{\mu,i}(z, L)$ has a Laurent series expansion in t which is an integral power series in $I_p[[t]]$, and for a suitable choice of μ, this is the series underlying the construction of the $L_{p,i}(s)$ (see [1, 3]).

In order to complete the construction, we need to introduce several basic facts about gamma-transforms (for more details see [9]). Let Λ_m be the space of I_p-valued measures on $\mathbb{Z}_p$, and let C denote a compact-open subset of $\mathbb{Z}_p$:

(a) There is an isomorphism $\Lambda_m \to I_p[[w]]$ given by $\lambda \mapsto H_\lambda(w)$, where $H_\lambda(w) = \sum_{n \geqslant 0} (\int_{\mathbb{Z}_p} \binom{x}{n} d\lambda)\, w^n = \int_{\mathbb{Z}_p} (1+w)^x\, d\lambda$.

(b) Let $f(x) = \sum_i a_i \zeta_i^x$ be the characteristic function of C, where ζ_i are p-power roots of unity [9]. We define a measure $\lambda|_C$ by restricting λ to C and extending by zero. Then the power series $H_{\lambda|_C}(w)$ associated to $\lambda|_C$ is given by

$$\sum a_i H_\lambda(\zeta_i(1+w) - 1). \quad (5)$$

In particular, if $C = \mathbb{Z}_p^*$, we write λ^* for $\lambda|_{\mathbb{Z}_p^*}$ and $H_\lambda^*(w)$ for $H_{\lambda^*}(w)$. We then have

$$H_\lambda^*(w) = H_\lambda(w) - \frac{1}{p}\sum_{\zeta^p=1} H_\lambda(\zeta(1+w)-1). \tag{6}$$

(c) We define the measure $\lambda\circ\gamma$ for $\gamma\in\mathbb{Z}_p^*$ by $\lambda\circ\gamma(C) = \lambda(\gamma C)$. Then $H_{\lambda\circ\gamma}(w) = H_\lambda((w+1)^{\gamma^{-1}}-1)$, and we have the formula

$$\lambda\circ\gamma|_C = \lambda|_{\gamma C}\circ\gamma. \tag{7}$$

(d) We now discuss the gamma-transform. Let $J(t)\in I_p[[t]]$, and set $\tilde{J}(w)\in I_p[[w]]$ equal to $J(\delta(w))$ viewed as a power series in w. Let λ be the measure associated to the series $\tilde{J}(w)$. For each i, $0\leqslant i\leqslant p-2$, we define

$$\Gamma_\lambda^{(i)}(s) = \int_{\mathbb{Z}_p^*} \langle x\rangle^s \omega^i(x)\, d\lambda \tag{8}$$

and we may thus speak of the gamma transform of a measure associated with a power series in t. Clearly $\Gamma_\lambda^{(i)}(s)$ is an Iwasawa function, i.e., if u is a topological generator of $1+p\mathbb{Z}_p$, then there exists a power series $G_i(w)\in I_p[[w]]$ such that $G_i(u^s-1) = \Gamma_\lambda^{(i)}(s)$. Let $\phi\colon \mathbb{Z}_p\to U = 1+p\mathbb{Z}_p$ be the isomorphism given by $s\mapsto u^s$. Then as a power series, $G_i(w)$ corresponds to the measure in Λ_m given by

$$\left(\sum_\varepsilon \varepsilon^i\lambda\circ\varepsilon|_U\right)\circ\phi, \tag{9}$$

where the sum is over the $(p-1)$th roots of unity in $\mathbb{Z}_p$ (see [9]). By (c) above, we may write (9) as

$$\left(\sum_\varepsilon \varepsilon^i\lambda|_{\varepsilon U}\circ\varepsilon\right)\circ\phi. \tag{10}$$

We now apply the gamma-transform of (d) to the measure whose associated power series in t is the Laurent expansion of $(d/dz)\log \tilde{R}_{\mu,i}(z, L)$. Up to multiplication by units in the Iwasawa algebra, this gives the functions $L_{p,i}(s)$ for $1\leqslant i\leqslant p-2$ (see [1] for the complete construction). Now, the μ-invariant of $\Gamma_\lambda^{(i)}(s)$ is considered by definition to be the μ-invariant of the associated power series $G_i(w)$, i.e., the infimum of the valuations of its coefficients. Thus it clearly suffices to study the μ-invariant of the gamma-transform to determine the μ-invariant of $L_{p,i}(s)$.

2. μ-Invariants of Certain Gamma-Transforms

Let E be an elliptic curve as in Section 1, and let $R(P)$ be a rational function on E: by a slight abuse of notation we write $R(t)$ for the expansion of R as a Laurent series in t, where $t = -2x/y$ is a local parameter at zero on $\hat{E}$. We suppose that $R(t) \in I_p[[t]]$.

Let δ: $\hat{G}_m \to \hat{E}$ be the isomorphism of formal groups as in Section 1, and consider a measure λ on $\mathbb{Z}_p$ with values in I_p whose associated power series in $I_p[[w]]$ has the form $R(\delta(w))$ for $R(P)$ as above. Let W denote the set of roots of unity in K. The aim of this section is to apply the methods used by Sinnott in the cyclotomic case (see [9]) to prove

THEOREM 1. *For each i, $0 \leqslant i \leqslant p-2$, we have the formula*

$$\mu\left(\sum_{v \in W} \omega^i(v)\, \lambda^*{}_v(v)\right) = \mu(\Gamma_\lambda^{(i)}(s)).$$

Before the proof of Theorem I, we need several preliminary remarks. Let r be the number of roots of unity in K, $m = (p-1)/r$, and $\beta_1, \ldots, \beta_n$ be a basis for the $\mathcal{O}$-module generated by the $(p-1)$th roots of unity in $\mathbb{Z}_p$. For $1 \leqslant j \leqslant m$, let ε_j be representatives of the $(p-1)$th roots of unity modulo W. Then

$$\varepsilon_j = \sum_i a_{ij}\beta_i, \qquad a_{ij} \in \mathcal{O} \tag{11}$$

for $1 \leqslant j \leqslant m$.

Now, since we are considering μ-invariants, we will wish to consider the reduction of our power series $R(\delta(w))$ modulo p. To this end, we denote by $\tilde{\delta}(w)$ the power series $\delta(w)$ modulo p, so $\tilde{\delta}(w)$ has coefficients in $\bar{\mathbb{F}}_p$, the algebraic closure of $\mathbb{F}_p$. Letting $\tilde{E}$ denote the curve reduced mod p, we see that $\tilde{\delta}(w)$ gives a formal group isomorphism from the multiplicative formal group in characteristic p to the formal group of $\tilde{E}$, which we denote by $\hat{\varepsilon}$. But since the points of $\hat{E}$ all reduce to 0 mod p, we let $B = \bar{\mathbb{F}}_p[[T]]$ for an indeterminate T, and we extend the field of definition of $\tilde{E}$ to the quotient field of B. We also consider B to be the underlying set for $\hat{G}_m$ in characteristic p. Then $\tilde{\delta}$ converges to a value on $\hat{\varepsilon}$ whenever w has its value in the maximal ideal of B, which is the ideal generated by T.

We now recall that for each element $\beta \in \mathbb{Z}_p$, there exists a unique power series, usually denoted $[\beta]$ (t), such that $[\beta](t) \equiv \beta t \pmod{\deg 2}$ and $[\beta](t)$ is an endomorphism of $\hat{E}$ (see [8]). We use the notation $q_\beta(t) = [\beta](t)$ and write $\tilde{q}_\beta(t)$ for the reduction of $q_\beta(t)$ mod p.

Now, let E^n be the abelian variety consisting of the product of n copies of E, and let $t_1, \ldots, t_n$ be the copies of t coming from the n coordinate projec-

tions $E^n \to E$. Let $K(E^n)$ denote the field of rational functions on E^n developed out in their Laurent expansions at $t_1, \ldots, t_n$, and let $A = K(E^n) \cap I_p[[t_1, \ldots, t_n]]$. In the same vein, we write $\tilde{A} = K(\tilde{E}^n) \cap B[[t_1, \ldots, t_n]]$ for rational functions on the reduced abelian variety.

We now state two independence results which are fundamental to the proof of Theorem I. For the a_{ij} as in (11), we have

THEOREM II. *For $1 \leqslant j \leqslant m$, let $\Phi_j: \tilde{E}^n \to \tilde{E}$ be the map given by*

$$\Phi_j(P_1, \ldots, P_n) = \sum_i a_{ij} P_i,$$

and suppose $r_1, \ldots, r_m$ *are rational functions on $\tilde{E}$ such that*

$$\sum_{j=1}^{m} r_j(\Phi_j(x)) = 0 \qquad \text{for all} \quad x \in \tilde{E}^n.$$

Then each r_j is a constant function on $\tilde{E}$.

THEOREM III. *Let Θ: $B[[t_1, \ldots, t_n]] \to B[[t]]$ be the map given by $\Theta(t_i) = q_{\beta_i}(t)$. Then the restriction of Θ to $\tilde{A}$ is injective in the sense that if $r \in \tilde{A}$ and $r(\tilde{q}_{\beta_1}(t), \ldots, \tilde{q}_{\beta_n}(t)) = 0$, then $r = 0$ identically.*

Theorems II and III will be proven at the end of this section. We now proceed to the proof of Theorem I. Let λ be a measure on $\mathbb{Z}_p$ as before whose associated power series has the form $R(\delta(w)) \in I_p[[w]]$ for $R \in A$. We have

PROPOSITION. *Let C be a compact-open set in $\mathbb{Z}_p$. Then the power series associated to $\lambda|_C$ has the form $R_C(\delta(w))$, where R_C is also a rational function on E.*

Proof. We may write $\sum_i b_i \zeta_i^x$ for the characteristic function of C, as in Section 1(b). Then the power series associated to $\lambda|_C$ is given by $\sum_i b_i R(\delta(\zeta_i(1+w)-1))$. Now, since δ is an isomorphism of formal groups, and $\zeta_i - 1$ is in the maximal ideal of I_p, we see that $\zeta_i - 1$ corresponds under δ to the t coordinate of a π-power division point V_i on E. Thus,

$$\sum_i b_i R(\delta(\zeta_i(1+w)-1)) = \sum_i b_i R(\delta(\zeta_i - 1) \oplus_E \delta(w))$$

$$= \sum_i b_i R(t(V_i) \oplus_E t),$$

which is the expansion of $\sum_i b_i R(V_i \oplus_E P)$ in t. By definition, this function

is $R_C(P)$. But R_C is a rational function on E since addition on E is rational, and $\lambda|_C$ is associated to $R_C(\delta(w))$, which concludes the proof.

Now, for each i, $0 \leqslant i \leqslant p-2$, define a measure

$$\kappa_i = \sum_{v \in W} \omega^i(v)\, \lambda^{*\circ}(v).$$

We first remark that κ_i is associated with a rational function in $\delta(w)$ on E. For by the preceding proposition, λ^* is associated with a rational function $R^*(\delta(w))$, and then by Section 1(c), $\lambda^{*\circ}(v)$ is associated to $R^*(\delta((1+w)^{v^{-1}}-1)) = R^*([v^{-1}](\delta(w))) = R(v^{-1}P)$ on E. Now, we are considering the μ-invariant of a measure to be the μ-invariant of its associated power series; this is how we investigate the μ-invariants in the statement of Theorem I, which we recall as

$$\mu\left(\sum_{v \in W} \omega^i(v)\, \lambda^{*\circ}(v)\right) = \mu(\Gamma_\lambda^{(i)}(s)). \tag{12}$$

In fact, proving the simpler formula

$$\mu(\kappa_i) = \mu(\Gamma_{\kappa_i}^{(i)}(s)) \tag{13}$$

is equivalent to proving (12), for the left-hand sides are the same by definition, and for the right-hand sides we have

$$\begin{aligned}
\Gamma_{\kappa_i}^{(i)}(s) &= \sum_{v \in W} \omega^i(v) \int_{\mathbb{Z}_p^*} \langle x \rangle^s\, \omega^i(x)\, d\lambda^{*\circ}(v) \\
&= \sum_{v \in W} \omega^i(v) \int_{\mathbb{Z}_p^*} \langle v^{-1}x \rangle^s\, \omega^i(v^{-1}x)\, d\lambda^* \\
&= \sum_{v \in W} \omega^i(v)\, \omega^i(v^{-1}) \int_{\mathbb{Z}_p^*} \langle x \rangle^s\, \omega^i(x)\, d\lambda \\
&= r\Gamma_\lambda^{(i)}(s).
\end{aligned}$$

Thus, since we have stipulated that $p \neq 2$ or 3, and r must always be 2, 4, or 6, we have

$$\mu(\Gamma_\lambda^{(i)}(s)) = \mu(\Gamma_{\kappa_i}^{(i)}(s)).$$

To prove (13), we prove that divisibility by π of κ_i (i.e., of its associated power series) implies that of $\Gamma_{\kappa_i}^{(i)}(s)$ and vice versa, thus, cancelling the factors of π from both sides gives (13). The first implication is evident, since if π divides κ_i then it certainly divides $\sum_\varepsilon \varepsilon^i \kappa_i \circ \varepsilon|_U$ (Eq. (9)), so $\Gamma_{\kappa_i}^{(i)}(s)$, by Section 1(d). The second implication is not trivial. Suppose π divides $\sum_\varepsilon \varepsilon^i \kappa_i \circ \varepsilon|_U$. Then π divides $r\sum_{j=1}^m \varepsilon_j^{-i} \kappa_i|_{(\varepsilon_j^{-1}U)} \circ (\varepsilon_j^{-1})$, reformulating as in (10).

Let $r_j(\delta(w))$ be the power series corresponding to the measure $\varepsilon_j^{-1}\kappa_i|_{(\varepsilon_j^{-1}U)}$. We may then write the assumption that π divides the gamma-transform as

$$\sum_{j=1}^{m} r_j(\delta((1+w)^{\varepsilon_j}-1)) \equiv 0 \pmod{\pi I_p[[w]]}. \tag{14}$$

Considering the rational functions $\tilde{r}_j$ on $\tilde{E}$ and the whole situation in characteristic p, we have

$$\sum_{j=1}^{m} \tilde{r}_j([\tilde{\varepsilon}_j]\,\tilde{\delta}(w)) = 0. \tag{15}$$

Thus using the notation $\tilde{q}_{\varepsilon_j}(t)$ for $[\varepsilon_j](t)$ reduced mod p, we have

$$\sum_{j=1}^{m} \tilde{r}_j(\tilde{q}_{\varepsilon_j}(t)) = 0. \tag{16}$$

Now, in the notation of Theorem II, let $\Phi_j\colon \tilde{E}^n \to \tilde{E}$ be defined by

$$\Phi_j(t_1, \ldots, t_n) = \sum_{i=1}^{n} \tilde{q}_{a_{ji}}(t_i),$$

for the a_{ji} as in (11). Then (16) may be written

$$\sum_{j=1}^{m} \tilde{r}_j(\Phi_j(\tilde{q}_{\beta_1}(t), \ldots, \tilde{q}_{\beta_n}(t))) = 0. \tag{17}$$

Now, by Theorem III, this statement implies that the function $\sum_{j=1}^{m} \tilde{r}_j \circ \Phi_j$ on $\tilde{E}^n$ is identically zero, and by Theorem II, we obtain that each $\tilde{r}_j$ is then a constant function on $\tilde{E}$, so that $\sum_{j=1}^{m} \tilde{r}_j = 0$, or equivalently, $\sum_{j=1}^{m} r_j \equiv 0 \pmod{\pi I_p[[w]]}$.

Finally, recalling that $r_j(P)$ was the rational function on E associated to the measure $\varepsilon_j^{-1}\kappa_i|_{(\varepsilon_j^{-1}U)}$, we obtain

$$\begin{aligned}\kappa_i &= \sum_{j=1}^{m} \sum_{v \in W} \varepsilon_j^{-1}\kappa_i|_{(\varepsilon_j^{-1}U)}(v) \\ &= \sum_{v \in W} \left(\sum_{j=1}^{m} r_j(vP) \right) \equiv 0 \pmod{p},\end{aligned}$$

so κ_i is divisible by π, which concludes the proof.

We note that since the p-adic L-function is constructed by taking the gamma-transform of a measure whose power series is exactly the development in w of a rational function on E, we may apply Theorem I to obtain information on their μ-invariant. This is done in Section 3. We now prove Theorems II and III.

Proof of Theorem II. First, note that since $\varepsilon_j = \sum_{i=1}^{n} a_{ij}\beta_i$ and $\Phi_j(P_1, \ldots, P_n) = \sum_{i=1}^{n} a_{ij}P_i$, we must have the condition

$$a \circ \Phi_i = b \circ \Phi_j \Leftrightarrow a = b = 0$$

for $a, b \in \mathcal{C}$, and $i \neq j$, since this is clearly true of the ε_j. This and algebraicity are the only conditions on the Φ_j which are needed in the proof of Theorem 2. The algebraicity of the Φ_j means that since they are certainly not constant maps, they must be surjective onto E. Now, let $K_j = \operatorname{Ker} \Phi_j$. We will show that whenever $i \neq j$, $\Phi_i \mid_{K_j}$ is still surjective onto E. If it were not, it would be constant, so its image would be e, the identity element of E. Now, obviously, $\Phi_j \mid_{K_j} = e$, so we have induced maps

$$\bar{\Phi}_j \colon \tilde{E}^n / K_j \to \tilde{E} \qquad \text{and} \qquad \bar{\Phi}_i \colon \tilde{E}^n / K_j \to \tilde{E}.$$

Thus, $\bar{\Phi}_i \circ \bar{\Phi}_j^{-1}$ is an endomorphism of E, so some $\gamma \in \mathcal{C}$. But then $1 \circ \Phi_i = \gamma \circ \Phi_j$, which is not possible. So $\Phi_i \mid_{K_j}$ is surjective.

Now, let $P_0 \in \tilde{E}$ be a point at which r_m has a pole. Then $r_m(P_0 \oplus_{\tilde{E}} P)$ has a pole at e. Choose R_0 in $\tilde{E}^n$ such that $\Phi_m(R_0) = P_0$; then we still must have

$$\sum_{j=1}^{m} r_j \circ \Phi_j(R_0 + R) = 0 \qquad \forall R \in \tilde{E}^n,$$

so it suffices to know Theorem II for the functions $r_j(\Phi_j(R_0) \oplus_{\tilde{E}} P)$, i.e., we may suppose that r_m has a pole at e.

Let D_j be the set of poles of r_j; then $\Phi_j^{-1}(D_j) \cap K_m$, for $1 \leqslant j \leqslant m$, must have codimension 1 in K_m, otherwise Φ_j would be constant on K_m, which is not the case. So $\sum_{j=1}^{m-1} \Phi_j^{-1}(D_j) \cap K_m$ has codimension 1 in K_m. Thus, we can choose an R_1 in K_m such that $\Phi_j(R_1) \notin D_j$, $1 \leqslant j \leqslant m-1$. We can now write

$$r_m \circ \Phi_m(R) = r_m \circ \Phi_m(R_1 + R) = -\sum_{j=1}^{m-1} r_j \circ \Phi_j(R_1 + R).$$

But the right-hand side is regular, implying that r_m has no pole at e! Evidently, the procedure works for each of the r_j in the same way, so they are all constant functions on $\tilde{E}$. This concludes the proof of Theorem II.

Proof of Theorem III. We need a long series of lemmas.

LEMMA 1. *Let H be a Zariski-closed subgroup $\subsetneq \tilde{E}^n$. Then there exists a non-trivial homomorphism $\Phi \colon \tilde{E}^n \to \tilde{E}$ such that $H \subset \operatorname{Ker} \Phi$.*

Proof. Let $I_i \colon \tilde{E} \to \tilde{E}^n$ be inclusion of the ith factor for $1 \leqslant i \leqslant n$. Then since H is a proper subgroup, there exists j between 1 and n such that

Im $I_j \not\subseteq H$. Thus the composition τ: $\tilde{E} \to^{I_j} \tilde{E}^n \to \tilde{E}^n/H$ is non-trivial, and since H is closed, $\tilde{E}^n/H$ is an abelian variety. So the dual τ^*: $(\tilde{E}^n/H)^* \to \tilde{E}$ (as abelian varieties) is non-trivial. But $\tilde{E}^n/H$ is isogenous to $(\tilde{E}^n/H)^*$, so choosing an isogeny f: $\tilde{E}^n/H \to (\tilde{E}/H)^*$, we have $\tau^* \circ f$: $\tilde{E}^n/H \to \tilde{E}$ non-trivial. Then Φ: $\tilde{E}^n \to \tilde{E}^n/H \to^{\tau^* \circ f} \tilde{E}$ is non-trivial and $H \subset \operatorname{Ker} \Phi$.

LEMMA 2. *Let Φ: $\tilde{E}^n \to \tilde{E}$ be a homomorphism. Then Φ has the form*

$$\Phi(Q_1, \ldots, Q_n) = \sum_{i=1}^{n} \alpha_i Q_i, \qquad \alpha_i \in \mathcal{O}.$$

Proof. In the notation above, set $\alpha_i = \Phi \circ I_i$: $\tilde{E} \to \tilde{E}$. Then

$$\Phi(Q_1, \ldots, Q_n) = \Phi\left(\sum_{i=1}^{n} I_i(Q_i)\right) = \sum_{i=1}^{n} \alpha_i Q_i.$$

LEMMA 3. *If G is a subgroup of $\tilde{E}^n$, and H is its Zariski closure, then H is also a subgroup.*

Proof. It suffices to show that H is closed under addition and inverses. Let A: $H \times H \to H'$ be addition. For any algebraic map ϕ which is zero on G, we know ϕ must be zero on H. But then $\phi \circ A$ is zero on $H \times H$ since it is zero on $G \times G$ and $H \times H$ is the Zariski closure of $G \times G$. But this means ϕ is zero on H', so $H' \subset H$. The argument for inverses is analogous.

LEMMA 4. *Let $\beta_1, \ldots, \beta_n$ be elements of $\mathbb{Z}_p$ which are linearly independent over $\mathcal{O}$, and write $t = \tilde{\delta}(w)$ as usual. Let F be the algebraic closure of the quotient field of the ring B, R the ring of integers of F, and M the maximal ideal of R. Let*

$$G = \{(\tilde{q}_{\beta_1}(t), \ldots, \tilde{q}_{\beta_n}(t)) \mid t = \tilde{\delta}(w),\ w \in M\}.$$

Then G is Zariski dense in $\tilde{E}^n$ (considered to be defined over F).

Proof. Recall that whenever w is in M, then $\tilde{\delta}(w)$ converges to an actual value on the formal group of $\tilde{E}$. Let H denote the Zariski closure of G. Then by Lemma 3, H is a subgroup of $\tilde{E}^n$. If $H \neq \tilde{E}^n$, then by Lemmas 1 and 2, there exist elements $\alpha_1, \ldots, \alpha_n \in \mathcal{O}$, not all zero, such that

$$\sum_{i=1}^{n} \alpha_i Q_i = 0 \qquad \forall (Q_1, \ldots, Q_n) \in H.$$

But then, we may write this as

$$\sum_{i=1}^{n} \alpha_i \tilde{q}_{\beta_i}(t) = \sum_{i=1}^{n} \alpha_i [\tilde{\beta}_i](t) = \left[\sum_{i=1}^{n} \alpha_i \tilde{\beta}_i\right](t) = 0$$

for all t on the formal group of $\tilde{E}$, so $\sum_{i=1}^{n} \alpha_i \beta_i = 0$. But this is not possible, so we must have $H = \tilde{E}^n$.

We may conclude the proof of Theorem 3. Suppose that for some $r \in \tilde{A}$, we have $\Theta(r) = 0$. This means

$$r(\tilde{q}_{\beta_1}(t), \ldots, \tilde{q}_{\beta_n}(t)) = 0.$$

But r is continuous in the Zariski topology, so it must be zero on all of $\tilde{E}^n$.

3. The μ-Invariant of the p-Adic L-Function

The aim of this section is to apply the results of Section 2 to the measure associated to the p-adic L-function, as discussed in Section 1. In particular, we prove

THEOREM IV. $\mu(X_\infty) = 0$.

In order to do so, we show that the μ-invariant of each $L_{p,i}(s)$ is zero. Indeed, it is shown in [1] that the μ-invariant of X_∞ is equal to the sum of the μ-invariants of the $L_{p,i}(s)$ for $1 \leqslant i \leqslant p-2$.

Recall from Section 1 that for each i, $1 \leqslant i \leqslant p-2$, and for a suitable choice of μ, the integral power series expansion of the rational function on the curve

$$\frac{d}{dz} \log \tilde{R}_{\mu,i}(z, L) = \frac{d}{dz} \log \prod_{\chi} (\chi^{2m_i} R_{\chi,i}(z, L))^{\mu(\chi)} \tag{18}$$

is exactly the power series which gives the measure associated to $L_{p,i}(s)$ as in Section 1(a).

LEMMA 1. *For each i, $1 \leqslant i \leqslant p-2$, we have $\mu(\lambda_i) = 0$, where the series associated to λ_i is the development in w of $(d/dz) \log \tilde{R}_{\mu,i}(z, L)$.*

Proof. We show that as a rational function on E, $(d/dz) \log \tilde{R}_{\mu,i}(z, L)$ does not reduce to zero mod $\mathfrak{p}$, in fact, we exhibit its poles on $\tilde{E}$. Recall that $r = \# W$.

Let $S = \{\chi \in A \mid \mu(\chi) \neq 0\}$, and $\mathscr{L} = \{R \in E \mid R$ is a point of χ-division for some $\chi \in S\}$. Now, since all $\chi \in S$ are prime to $\mathfrak{p}$ and prime to each other (see [1, Lemma II.7; 3, Lemma 28]), we have that reduction mod $\mathfrak{p}$ is injective on $\mathscr{L}$. We separate the proof into two cases.

Case 1. $f_i = 1$, i.e., r divides i. We explicitly write down the rational function on the curve from (18):

$$\sum_{\chi \in A} \mu(\chi) \frac{d}{dz} \log \prod_{\substack{R \in E_\tau \\ R \neq 0}} (x(P) - x(R))$$

$$= \sum_{\chi \in A} \mu(\chi) \sum_R \frac{-2y(P)}{x(P) - x(R)}, \tag{19}$$

from which it is easy to see that the poles must come from the points 0 and $R \in \mathscr{L}$. Now, in fact, the residue at 0 is exactly $\sum_{\chi \in A} \mu(\chi)(N\chi - 1) = 0$, so there is no pole there. However, the residue at each R is $-2\mu(\chi)$, and since $\mu(\chi) = \pm 1$ (see [1]), this does not reduce to zero mod $\mathfrak{p}$. Moreover, since reduction mod $\mathfrak{p}$ is injective on $\mathscr{L}$, all the points in $\mathscr{L}$ give poles of the reduced function on $\tilde{E}$.

Case 2. $f_i \neq 1$. The only difference with Case 1 is in the explicit expression of the function associated to λ_i:

$$\sum_{\chi} \mu(\chi) \frac{d}{dz} \log \prod_R \prod_\tau (x(P + Q_i^\tau) - x(R))$$

$$= \sum_{\chi} \sum_R \sum_\tau \mu(\chi) \frac{-2y(P + Q_i^\tau)}{x(P + Q_i^\tau) - x(R)}.$$

Here again, the poles come from the points $-Q_i^\tau$ and $R - Q_i^\tau$ for all $\tau \in G_{f_i}$ and $R \in \mathscr{L}$. Now, the residue of each pole at $-Q_i^\tau$ is again $\sum_\chi \mu(\chi)(N\chi - 1) = 0$, so there are actually no poles there. But the poles coming from the $R - Q_i^\tau$ have residue $-2\mu(\chi)$, which as before is prime to $\mathfrak{p}$ for each χ (see [3, Lemma 28]). Moreover, since each $R - Q_i^\tau$ is a primitive χf_i-division point, again reduction mod $\mathfrak{p}$ is injective on this set, so each $R - Q_i^\tau$ gives a pole of the reduced function on $\tilde{E}$. This concludes the proof.

LEMMA 2. *The μ-invariant of λ_i^* is zero.*

Proof. In fact, we show that the μ-invariant of $\lambda_i|_{p\mathbb{Z}_p}$ is not zero, from which the result follows. Note that the characteristic function of $p\mathbb{Z}_p$ is $(1/p)\sum_{\zeta^p=1} \zeta^{-x}$. Now, the power series associated with λ_i is the development in w of $\sum_{\chi \in A} \mu(\chi)(d/dz) \log \xi_{\chi, Q_i}(P)$ when $f_i \neq 1$, so by Section 1(b), the power series associated with $\lambda_i|_{p\mathbb{Z}_p}$ is $\sum_{\chi \in A} \mu(\chi)(d/dz) \log \prod_{S \in E_p} \xi_{\chi, Q_i}(P + S)$, which by the functional equation (4) given in Section 1, can be written

$$\sum_{\chi \in A} \mu(\chi) \frac{1}{p} \left[\frac{d}{dz} \log \xi_{\chi, Q_i, \sigma_p}([\pi]P) \right]. \tag{20}$$

Now, by the chain rule, we can write $\sum_{\alpha \in A} \mu(\alpha)(\pi/p)[(d/dz) \log \xi_{\alpha \cdot Q_i \sigma_\beta}]([\pi]P)$ for (20), which allows us to reduce modulo $\mathfrak{p}$. The poles of this function come from the points $-Q_i^{\tau\sigma_\beta} + S$ and $R - Q_i^{\tau\sigma_\beta} + S$ for all $\tau \in G_{f_i}$, $R \in \mathscr{L}$, and $S \in E_\pi$. But all the S reduce to zero mod $\mathfrak{p}$, so evidently the residue of each pole is a multiple of p, and thus reduces to zero mod $\mathfrak{p}$. Thus the rational function in (20) is divisible by p, which concludes the proof.

LEMMA 3. *The μ-invariant of the measure*

$$\sum_{v \in W} \omega^i(v)\, \lambda_i^* \circ (v)$$

is zero.

Proof. As usual, we divide into two cases.

Case 1. $f_i = 1$, i.e., r divides i. In this case, the measure in the lemma becomes simply $\sum_{v \in W} \lambda_i^* \circ (v)$, since $\omega^i(v) = 1$ for each $v \in W$. But the poles of λ_i^* are given by the points $R \in \mathscr{L}$, and the v are isomorphisms of E, so they only permute the poles. So $\lambda_i^* \circ (v) = \lambda_i^*$ for each v, and the measure can be written $r\lambda_i^*$. Now the result of Lemma 2 concludes the proof.

Case 2. $f_i \neq 1$. Let us consider the set of poles of the form

$$P_R = \{R - Q_i^\tau \mid \tau \in G_{f_i}\}.$$

We attach a P_R to each $R \in \mathscr{L}$. For each P_R, let $v^{-1}P_R$ denote the set $\{v^{-1}(R - Q_i^\tau) \mid \tau \in G_{f_i}\}$. Now, since the orbit of Q_i under the τ lies entirely in one congruence class modulo W, the $v^{-1}P_R$ are completely disjoint sets for R fixed and v varying in W. We show, moreover, that if $v^{-1}P_{R_1} = v^{-1}P_{R_2}$, then $R_1 = R_2$. For first of all, R_1 and R_2 would have to be points of α-division for the same α. But then, letting f_i act on both sides of the equality, we would have $R_1 = R_2$. This shows that for v fixed, the poles of $\lambda_i^* \circ (v)$ are given by the $v^{-1}P_R$ for $R \in \mathscr{L}$, and that all these poles are distinct. It remains to be shown that no pole of $\lambda_i^* \circ (v_1)$ can be a pole of $\lambda_i^* \circ (v_2)$ if $v_1 \neq v_2$. Suppose we had R_1, R_2, τ_1, and τ_2 such that $v_1^{-1}(R_1 - Q_i^{\tau_1}) = v_2^{-1}(R_2 - Q_i^{\tau_2})$. First, we see immediately that R_1 and R_2 must be points of α-division for the same α. But then, letting α act on both sides, we obtain

$$v_1^{-1}(-Q_i^{\tau_1}) = v_2^{-1}(-Q_i^{\tau_2}),$$

which is impossible if $v_1 \neq v_2$ since the two points would be in different congruence classes mod W.

We have now proved that all the poles of $\sum_{v \in W} \omega^i(v)\, \lambda_i^* \circ (v)$ come from

$v^{-1}P_R$ for all $v \in W$ and $R \in \mathscr{L}$. Applying the methods in the proof of Lemma 1 to these points, we easily compute that the residues all have the form $v\mu(\alpha)$ for some $v \in W$, and as before, that this is never congruent to 0 mod p: similarly, we see again that reduction mod p is injective on the entire set of poles. This suffices to prove that the rational function associated with $\sum_{v \in W} \omega^i(v)\, \lambda_i^*(v)$ does not reduce to zero mod p.

Now, for $1 \leqslant i \leqslant p-2$, up to units in the Iwasawa algebra, $L_{p,i}(s)$ is given by the $(i-1)$th gamma-transform of λ_i (see [1] for details), and $L_{p,0}(s)$ is itself given by a unit in the Iwasawa algebra. Thus, applying the result of Theorem I in Section 2 permits us to conclude that the μ-invariants of the $L_{p,i}(s)$ are zero for $0 \leqslant i \leqslant p-2$. This concludes the proof of Theorem IV.

REFERENCES

1. D. BERNARDI, C. GOLDSTEIN, AND N. STEPHENS, Notes p-adiques sur les courbes elliptiques, *J. Reine Angew. Math.* **351** (1984), 129–170.
2. J. COATES AND C. GOLDSTEIN, Some remarks on the main conjecture for elliptic curves with complex multiplication, *Amer. J. Math.* **103** (1983), 411–435.
3. J. COATES AND A. WILES, On the conjecture of Birch and Swinnerton-Dyer, *Invent. Math.* **39** (1977), 223–251.
4. J. COATES AND A. WILES, On p-adic L-functions and elliptic units, *J. Austral. Math. Soc. Ser. A* **26** (1978), 1–25.
5. R. GILLARD, Transformation de Mellin–Leopoldt des fonctions elliptiques, Publication of the University of Geneva, to appear.
6. C. GOLDSTEIN AND N. SCHAPPACHER, Séries d'Eisenstein et fonctions L de courbes elliptiques à multiplication complexe, *J. Reine Angew. Math.* **327** (1981), 184–218.
7. R. GREENBERG, On the structure of certain Galois groups, *Invent. Math.* **47** (1978), 85–99.
8. J. LUBIN, One parameter formal Lie groups over p-adic integer rings, *Ann. of Math.* **80** (1964), 464–484.
9. W. SINNOTT, On the μ-invariant of a rational function, *Invent. Math.* **75** (1984), 273–283.
10. R. GILLARD, Unités elliptiques et fonctions L p-adiques, *Compositio Fascicule* **1** (1980), 57–88.

Printed by the St. Catherine Press Ltd., Tempelhof 41, Bruges, Belgium

Article 2. Interpolation p-adique de valeurs spéciales de fonctions L.

Soit K un corps quadratique imaginaire. Soit $\overline{K}$ sa clôture algébrique et fixons un plongement de $\overline{K}$ dans $\mathbf{C}$ et $\mathbf{C}_p$ pour tout nombre premier p. Soit F une extension de K de degré n. Un caractère de Hecke ψ de K sera appelé K-admissible s'il existe $k(\psi) \in \mathbf{N}$ et $j(\psi) \in \mathbf{N} - \{0\}$ tels que $\psi((\alpha)) = \overline{N_{F/K}(\alpha)}^{k(\psi)} N_{F/K}(\alpha)^{-j(\psi)}$ pour tout $\alpha \in K^*$ congru à 1 modulo le conducteur $\mathbf{m}_\psi$ de ψ. Si ψ est un caractère de Hecke de F qui est K-admissible, on pose $\Lambda(\psi) = \Gamma(j(\psi))^n (2\pi i)^{-nj(\psi)} L(\psi, 0)$, où $L(\psi, s)$ est la fonction L de Hecke attachée à ψ. Une conjecture de Deligne prouvée par Harder prédit la valeur de $\Lambda(\psi)$ à multiplication par un nombre algébrique près. Dans cet article, nous étudions le comportement p-adique de $\Lambda(\psi)$.

Soit $p \neq 2, 3$ un premier qui est décomposé dans K. Soit $\mathbf{p}$ le premier de K induit par le plongement de $\overline{K}$ dans $\mathbf{C}_p$ et $\overline{\mathbf{p}}$ l'autre premier de K sur p. Or il est connu que tout caractère de Hecke ψ de F de type A_0 (et done tout caractère de Hecke de F qui est K-admissible) induit un unique caractère continu $\psi^{(p)}$ de $\mathrm{Gal}(F^{ab}/F)$ à valeurs dans $\mathbf{C}_p^*$. Si $\mathbf{m}$ est un idéal de l'anneau des entiers de F, soit $|\mathbf{m}|$ l'ensemble des places de F qui divisent $\mathbf{m}$, et si S est un ensemble fini de places de F qui ne divisent pas (p), soit $\mathcal{G}_{F,S,p}$ (resp. $\mathcal{G}_{F,S,\mathbf{p}}$) le groupe de Galois group sur F de l'union des extensions abéliennes de niveau $\mathbf{m}$ telles que $|\mathbf{m}| \subset S \cup |(p)|$ (resp. $|\mathbf{m}| \subset S \cup |\mathbf{p}|$). Si ψ est un caractère de Hecke de F qui est K-admissible, de conducteur $\mathbf{m}_\psi$, alors $\psi^{(p)}$ se factorise à travers $\mathcal{G}_{F,S,p}$ pour tout S tel que $|\mathbf{m}_\psi| \subset S \cup |(p)|$ et même à travers $\mathcal{G}_{F,S,\mathbf{p}}$ si $k(\psi) = 0$ et $|\mathbf{m}_\psi| \subset S \cup |\mathbf{p}|$. Finalement, soit $F^\vee$ conjugué complexe de F et si ψ est un caractère de Hecke de F, soit $\psi^\vee$ le caractère de Hecke de $F^\vee$ defini par $\psi^\vee(\mathbf{a}) = N(\mathbf{a})^{-1}\psi^{-1}(\overline{\mathbf{a}})$ pour tout idéal fractionnaire $\mathbf{a}$ de $F^\vee$.

Théorème: (i) Il existe une mesure unique μ_S sur $\mathcal{G}_{F,S,p}$ telle que pour tout caractère de Hecke ψ de F qui est K-admissible et tel que $\psi^{(p)}$ se factorise à travers $\mathcal{G}_{F,S,p}$ (et avec l'hypothèse supplémentaire que $k(\psi) = 0$ ou $j(\psi) = 1$ si $n \geq 3$), on a:

$$\int_{\mathcal{G}_{F,S,p}} \psi^{(p)}\, d\mu_S = E_{|\overline{\mathbf{p}}|}(\psi^\vee) E_{|\overline{\mathbf{p}}|}(\psi) W_{\mathbf{p}}(\psi) E_S(\psi) \Lambda(\psi).$$

(ii) Il existe une unique pseudo-mesure (qui est une mesure si $S \neq \emptyset$) caractère de Hecke K-admissible ψ de F tel que $\psi^{(p)}$ se factorise à travers $\mathcal{G}_{F,S,\mathbf{p}}$, on a:

$$\int_{\mathcal{G}_{F,S,\mathbf{p}}} \psi^{(p)}\, d\lambda_S = E_{|\overline{\mathbf{p}}|}(\psi^\vee) W_{\mathbf{p}}(\psi) E_S(\psi) \Lambda(\psi),$$

où si T est un ensemble fini de places, $E_T(\psi)$ est le facteur d'Euler au-dessus de T (en $s = 0$) de la fonction L attachée à ψ et $W_{\mathbf{p}}(\psi)$ est une racine locale.

P-adic Interpolation of Special Values of Hecke L-functions

Pierre Colmez and Leila Schneps

0. Introduction

Let K be a quadratic imaginary field. Let $\overline{K}$ be its algebraic closure and fix an embedding of $\overline{K}$ into $\mathbf{C}$ and $\mathbf{C}_p$ for all primes p. Let F be an extension of degree n of K. A Hecke character ψ of K will be called K-admissible if there exist $k(\psi) \in \mathbf{N}$ and $j(\psi) \in \mathbf{N} - \{0\}$ such that $\psi\big((\alpha)\big) = \overline{N_{F/K}(\alpha)}^{k(\psi)} N_{F/K}(\alpha)^{-j(\psi)}$ for all $\alpha \in K^*$ congruent to 1 modulo the conductor $\mathbf{m}_\psi$ of ψ. If ψ is a K-admissible Hecke character of F, we set $\Lambda(\psi) = \Gamma\big(j(\psi)\big)^n (2\pi i)^{-nj(\psi)} L(\psi, 0)$, where $L(\psi, s)$ is the Hecke L-function attached to ψ. A conjecture of Deligne [D] proved by Harder [H-S] predicts the value of $\Lambda(\psi)$ up to multiplication by an algebraic number. The aim of this paper is the study of the p-adic behavior of $\Lambda(\psi)$.

Let $p \neq 2, 3$ be a prime splitting in K. Let $\mathbf{p}$ be the prime of K induced by the embedding of $\overline{K}$ into $\mathbf{C}_p$ and $\overline{\mathbf{p}}$ the other prime of K above p. As observed by Weil [W1], any Hecke character ψ of F of type A_0 (thus any K-admissible Hecke character of F) gives rise to a unique continuous character $\psi^{(p)}$ of $\mathrm{Gal}(F^{ab}/F)$ with values in $\mathbf{C}_p^*$. If $\mathbf{m}$ is an ideal of the ring of integers of F, let $|\mathbf{m}|$ be the set of places of F dividing $\mathbf{m}$, and if S is a finite set of places of F not dividing (p), let $\mathcal{G}_{F,S,p}$ (resp. $\mathcal{G}_{F,S,\mathbf{p}}$) be the Galois group over F of the union of all abelian extensions of level $\mathbf{m}$ such that $|\mathbf{m}| \subset S \cup |(p)|$ (resp. $|\mathbf{m}| \subset S \cup |\mathbf{p}|$). If ψ is a K-admissible Hecke character of F of conductor $\mathbf{m}_\psi$, then $\psi^{(p)}$ factors through $\mathcal{G}_{F,S,p}$ for all S such that $|\mathbf{m}_\psi| \subset S \cup |(p)|$ and even through $\mathcal{G}_{F,S,\mathbf{p}}$ if $k(\psi) = 0$ and $|\mathbf{m}_\psi| \subset S \cup |\mathbf{p}|$. Finally, let $F^\vee$ be the complex conjugate of F and if ψ is a Hecke character of F, let $\psi^\vee$ be the Hecke character of $F^\vee$ defined by $\psi^\vee(\mathbf{a}) = N(\mathbf{a})^{-1}\psi^{-1}(\overline{\mathbf{a}})$ for all fractional ideals $\mathbf{a}$ of $F^\vee$.

Our main result can be stated as follows:

Theorem: (i) There exists a unique measure μ_S on $\mathcal{G}_{F,S,p}$ such that for all K-admissible Hecke characters ψ of F such that $\psi^{(p)}$ factors through $\mathcal{G}_{F,S,p}$ (and with the additional assumption that $k(\psi) = 0$ or $j(\psi) = 1$ if $n \geq 3$), we have:

$$\int_{\mathcal{G}_{F,S,p}} \psi^{(p)}\, d\mu_S = E_{|\overline{\mathbf{p}}|}(\psi^\vee) E_{|\overline{\mathbf{p}}|}(\psi) W_{\mathbf{p}}(\psi) E_S(\psi) \Lambda(\psi).$$

(ii) There exists a unique pseudo-measure (which is a measure if $S \neq \emptyset$) such that for all K-admissible Hecke characters ψ of F such that $\psi^{(p)}$ factors through $\mathcal{G}_{F,S,\mathbf{p}}$, we have:

$$\int_{\mathcal{G}_{F,S,\mathbf{p}}} \psi^{(p)}\, d\lambda_S = E_{|\overline{\mathbf{p}}|}(\psi^\vee) W_{\mathbf{p}}(\psi) E_S(\psi) \Lambda(\psi),$$

where if T is a finite set of places, $E_T(\psi)$ is the Euler factor above T (at $s = 0$) of the L-function attached to ψ and $W_{\mathbf{p}}(\psi)$ is a local root number.

Remark: Stated like this the theorem does not really make sense because in each equality, the left hand side belongs to $\mathbf{C}_p$ and the right hand side to $\mathbf{C}$. But as we have fixed embeddings of $\overline{K}$ into $\mathbf{C}$ and $\mathbf{C}_p$, if we choose an elliptic curve E defined over $\overline{K}$ with complex multiplication by K, a generator η of $H^1(X, O_X)$ and a generator γ of the 1-dimensional K-vector space $H_1\big(E(\mathbf{C}), \mathbf{Q}\big)$, we can define a p-adic period $\eta_p = \int_\gamma \eta$ and a complex period $\eta_\infty = \int_\gamma \eta$ (cf. III §2 for details). The fields $\overline{K}(\eta_\infty)$ and $\overline{K}(\eta_p)$ as well as the isomorphism between them sending η_∞ to η_p are independent of the choices of E, η and γ and all equalities take place in $\overline{K}(\eta_\infty) \simeq \overline{K}(\eta_p)$.

Such measures have been previously constructed in the case $n = 1$ by Manin-Vishik [M-V] and Katz [K]. Using ideas of Coates-Wiles [C-W], Yager [Ya1],[Ya2] and Tilouine [T] (see also de Shalit's book [d Sh]) obtained a much more elementary construction of this measure (still in the case $n = 1$).

We obtain our theorem in the following way. Using a method developed in [Co 1], similar to Shintani's method [Sh] in the totally real case, we can define a value $\Lambda^?(\psi)$ explicitly given as a polynomial in Kronecker-Eisenstein series attached to lattices in K and a priori depending on various auxiliary choices (mainly the choice of "Shintani decomposition") which is formally (i.e. without worrying about convergence problems) equal to $\Lambda(\psi)$. To prove that $\Lambda^?(\psi) = \Lambda(\psi)$ in general turned out to be beyond our capacities, but by a suitable modification of the methods of [Co 1], we were able to prove the desired equality whenever $n = 1, 2$ or $n \geq 3$ and $k(\psi) = 0$ or $j(\psi) = 1$. Now, having these explicit formulae allowed us to deduce the general case from the case $n = 1$. A by-product of the existence of this measure is that $\Lambda^?(\psi)$ is independent of all choices.

If χ is a continuous $\mathbf{C}_p^*$-valued character of $\mathcal{G}_{F,S,p}$ (resp. $\mathcal{G}_{F,S,\mathbf{p}}$), we set $L_{p,S}(\chi) = \int_{\mathcal{G}_{F,S,p}} \chi \, d\mu_S$ (resp. $L_{\mathbf{p},S}(\chi) = \int_{\mathcal{G}_{F,S,\mathbf{p}}} \chi \, d\lambda_S$. We can then make the preceding theorem more precise as follows:

Main Theorem: (i) $L_{p,S}(\chi)$ is a holomorphic (and even Iwasawa) function of χ.

(ii) If ψ is an admissible Hecke character of F such that $\psi^{(p)}$ factors through $\mathcal{G}_{F,S,p}$, then

$$L_{p,S}(\psi^{(p)}) = E_{|\overline{\mathbf{p}}|}(\psi)E_{|\overline{\mathbf{p}}|}(\psi^\vee)W_{\mathbf{p}}(\psi)E_S(\psi)\Lambda^?(\psi).$$

(iii) If the conductor of χ is divisible by all the elements of S, then there exists a p-adic unit $W^{(p)}(\chi)$ such that $W^{(p)}(\chi)L_{p,S}(\chi) = L_{p,S}(\chi^\vee)$, where $\chi^\vee$ is the character of $\mathcal{G}_{F^\vee,\overline{S},p}$ obtained from χ in the same way as $\psi^\vee$ was obtained from ψ for ψ a Hecke character of F.

(iv) $L_{\mathbf{p},S}(\chi)$ is a meromorphic function of χ, holomorphic except for a simple pole at $\chi = 1$ if $S = \emptyset$.

(v) If ψ is an admissible Hecke character of F such that $\psi^{(p)}$ factors through $\mathcal{G}_{F,S,\mathbf{p}}$, then $L_{\mathbf{p},S}(\psi^{(p)}) = E_{|\overline{\mathbf{p}}|}(\psi^\vee)W_{\mathbf{p}}(\psi)E_S(\psi)\Lambda(\psi)$.

The paper is organized as follows. After introducing in I the basic notations and recalling some basic facts about Fourier transforms of functions on adèles, we present in II a slight modification of the Shintani-like method developed in [Co 1]. In part III, we prove the existence of p-adic measures attached to n-dimensional generalizations of Eisenstein-Kronecker series attached to lattices in K. As a consequence of the existence of these measures we derive the fact that all choices that we had to make in part II lead to the same result. In part IV we prove a number of functional equations satisfied by $\Lambda(\psi)$ and apply the result of the two preceding parts to compute $\Lambda(\psi)$. Finally, part V is devoted to the construction of μ_S and λ_S using the measures constructed in part III and to the study of the p-adic L-functions $L_{p,S}$ and $L_{\mathbf{p},S}$.

I. Notations and Definitions.

Let K be a quadratic imaginary field. Let $\alpha \to \overline{\alpha}$ denote the non-trivial automorphism of K. Let $F \simeq K[X]/P(X)$, for P an irreducible polynomial of degree n, be an extension of degree n of K. Let $F^\vee = K[X]/\overline{P}(X)$. We still write $\alpha \to \overline{\alpha}$ for the antilinear isomorphism from F to $F^\vee$ sending X to X. We shall use H to denote either F or $F^\vee$ so $H^\vee$ will be $F^\vee$ (resp. F) if $H = F$ (resp. $H = F^\vee$). Let O_H be the ring of integers of H, U_H be the group of units of O_H, $I(H)$ be the group of fractional ideals of H, $I^+(H) \subset I(H)$ be the set of ideals of O_H, $Cl(O_H)$ be the group of ideal classes, $C(H) \subset I^+(H)$ be the set of ideals $\mathbf{a}$ of O_H such that $O_H/\mathbf{a}$ is cyclic, $C^0(H)$ be the set of principal ideals of $C(H)$, $P(H)$ be the set of prime ideals of O_H, $\mathcal{P}(H)$ be the set of finite subsets of $P(H)$, $\mathbf{A}_H$ be the ring of adèles of H, $\mathbf{A}_H^f$ be the ring of finite adèles of H and $\mathbf{d}_H$ be the absolute different of O_H. If V is a subgroup of U_H let $V^\vee = \{\overline{v} \mid v \in V\}$ be the corresponding subgroup of $U_H^\vee$. If $\mathbf{a} \in I(H)$, let $\overline{\mathbf{a}} = \{\overline{\alpha} \mid \alpha \in \mathbf{a}\} \in I(H^\vee)$ and if $S \in \mathcal{P}(H)$, let $\overline{S} = \{\overline{\mathbf{p}} \mid \mathbf{p} \in S\} \in \mathcal{P}(H^\vee)$. If $\mathbf{m} \in I(H)$, let $|\mathbf{m}| = \{\mathbf{q} \in P(H) \mid v_\mathbf{q}(\mathbf{m}) \neq 0\} \in \mathcal{P}(H)$ and if $S \in \mathcal{P}(H)$, let $I_S(H) = \{\mathbf{a} \in I(H) \mid |\mathbf{a}| \cap S = \emptyset\}$. Also let $O_{H,S}$ (resp. $O'_{H,S}$) be the subring of H defined by $x \in O_{H,S}$ (resp. $O'_{H,S}$) if and only if $v_\mathbf{q}(x) \geq 0$ if $\mathbf{q} \in S$ (resp. $\mathbf{q} \notin S$).

Fix an embedding of the algebraic closure $\overline{K}$ of K into $\mathbf{C}$. Let $Y_{H,\infty} = H \otimes_\mathbf{Q} \mathbf{C} \simeq Y_1 \times Y_2$, where $Y_1 = H \otimes_K \mathbf{C}$ and $Y_2 = H^\vee \otimes_K \mathbf{C}$. Let $\tau_1, \ldots, \tau_n$ be the n embeddings of H into $\overline{K}$; we obtain an isomorphism of Y_1 (resp. Y_2) with $\mathbf{C}^n$ sending $\alpha \otimes 1$ to $(\tau_1(\alpha), \ldots, \tau_n(\alpha))$ (resp. to $(\overline{\tau_1(\overline{\alpha})}, \ldots, \overline{\tau_n(\overline{\alpha})})$). With these identifications, H and $H^\vee$ become dense K-vector subspaces of $\mathbf{C}^n$ and $\mathbf{a} \in I(H)$ becomes a lattice in $\mathbf{C}^n$. If $y = (y_1, \ldots, y_n)$ and $z = (z_1, \ldots, z_n)$ belong to $\mathbf{C}^n$, let $Tr(y) = \sum_{i=1}^n y_i$; $N(y) = \prod_{i=1}^n y_i$; $yz = (y_1 z_1, \ldots, y_n z_n)$; $\langle y \mid z \rangle = Tr(y\overline{z} + \overline{y}z)$ and $(y \mid z)_\infty = exp(-2\pi i \langle y \mid z \rangle)$. If B is a basis of H over K, we let $B^\vee$ be the basis of $H^\vee$ over K dual to B with respect to $\langle \mid \rangle$ and if $\mathcal{B}$ is a finite set of bases of H over K, we let $\mathcal{B}^\vee = \{B^\vee \mid B \in \mathcal{B}\}$. If $\mathbf{a} \in I(H)$, let $\mathbf{a}^\vee$ be the dual lattice of $\mathbf{a}$ with respect to $\langle \mid \rangle$. Then, $\mathbf{a}^\vee \in I(H^\vee)$ and we have $\mathbf{a}^\vee = \overline{\mathbf{a}}^{-1} \mathbf{d}_{H^\vee}^{-1} = (\overline{\mathbf{a}\mathbf{d}_H})^{-1}$.

If $\mathbf{q} \in P(H)$, let $H_\mathbf{q}$ be its completion at $\mathbf{q}$ and $O_\mathbf{q}$ be the ring of integers of $H_\mathbf{q}$. If $S \in \mathcal{P}(H)$, let $H_S = \prod_{\mathbf{q} \in S} H_\mathbf{q}$ and $O_S = \prod_{\mathbf{q} \in S} O_\mathbf{q}$. We can describe $\mathbf{A}_H^f$ as the set of $x = (\ldots, x_\mathbf{q}, \ldots)$ such that $x_\mathbf{q} \in H_\mathbf{q}$ for all $\mathbf{q} \in P(H)$ and $x_\mathbf{q} \in O_\mathbf{q}$ for almost all $\mathbf{q} \in P(H)$. We can define a pairing $(\ \mid\ )_H$ on $\mathbf{A}_H^f \times \mathbf{A}_H^f$ with values in the group of roots of unity of $\overline{K}^* \subset \mathbf{C}^*$ in the following way. The above defined pairing $\langle \mid \rangle$ on $\mathbf{C}^n \times \mathbf{C}^n$ induces a pairing on $H \times H^\vee$ with values in $\mathbf{Q}$ which we can extend to a pairing on $\mathbf{A}_H^f \times \mathbf{A}_{H^\vee}^f$ with values in $\mathbf{A}_\mathbf{Q}^f$, and using the canonical isomorphism between $\mathbf{A}_\mathbf{Q}^f / \prod_p \mathbf{Z}_p$ and $\mathbf{Q}/\mathbf{Z}$, we set $(x \mid y)_H = exp(-2\pi i \widetilde{\langle x \mid y \rangle})$ where $\widetilde{\langle x \mid y \rangle}$ is the image of $\langle x \mid y \rangle$ in $\mathbf{Q}/\mathbf{Z}$. This pairing induces local pairings $(\ \mid\ )_S$ on $H_S \times H_S^\vee$ and we have $(x \mid y)_H = \prod_{\mathbf{q} \in P(H)} (x_\mathbf{q} \mid y_{\overline{\mathbf{q}}})_{|\mathbf{q}|}$.

Using these pairings, we can define the (local and global) Fourier transform. Let $\mathcal{S}_{S,H}$ be the space of $\overline{K}$-valued locally constant compactly supported functions on H_S. If $\mathbf{a} \subset \mathbf{b}$ are two fractional ideals of H_S and $\phi \in \mathcal{S}_{S,H}$ is constant modulo $\mathbf{a}$ and zero outside $\mathbf{b}$, we define its Fourier transform $\mathcal{F}_S(\phi) \in \mathcal{S}_{S,H}$ by:

$$\mathcal{F}_S(\phi)(y) = \begin{cases} \sqrt{\frac{N_{\overline{S}}(\mathbf{a}^\vee)}{N_S(\mathbf{a})}} \sum_{x \in \mathbf{b}/\mathbf{a}} \phi(x)(x \mid y)_S & \text{if } x \in \mathbf{a}^\vee \\ 0 & \text{if } x \notin \mathbf{a}^\vee \end{cases},$$

where $\mathbf{a}^\vee$ is the ideal of $H_{\overline{S}}^\vee$ dual to $\mathbf{a}$ with respect to $(\ \mid\ )_S$ and $N_S(\mathbf{a})$ is the norm of $\mathbf{a}$ as a fractional ideal of H_S. It is an exercise to verify that this definition does not depend on the choices of $\mathbf{a}$ and $\mathbf{b}$ and that $\mathcal{F}_{\overline{S}}(\mathcal{F}_S(\phi))(y) = \phi(-y)$.

Let $\mathcal{S}(H)$ be the space of $\overline{K}$-valued locally constant compactly supported functions on $\mathbf{A}_H^f$. The fractional ideals of $\mathbf{A}_H^f$ are in 1-to-1 correspondence with elements of $I(H)$. So if $\mathbf{a} \subset \mathbf{b}$ are elements of $I(H)$ and $\phi \in \mathcal{S}(H)$ is constant modulo $\mathbf{a}$ and zero outside of $\mathbf{b}$, we define its Fourier transform $\mathcal{F}_H(\phi)$ by the same formula as before (with the subscript S replaced by H) and we have $\mathcal{F}_{H^\vee}(\mathcal{F}_H(\phi))(y) = \phi(-y)$.

If $S \in \mathcal{P}(H)$, let $\mathcal{S}_S(H)$ be the subspace of $\mathcal{S}(H)$ of functions of the form $\phi_S(x_S) \prod_{\mathbf{q} \notin S} 1_{O_\mathbf{q}}(x_\mathbf{q})$, where $\phi_S \in \mathcal{S}_{S,H}$ and $1_{O_\mathbf{q}}$ is the characteristic funtion of $O_\mathbf{q}$. There is an obvious isomorphism between $\mathcal{S}_{S,H}$ and $\mathcal{S}_S(H)$ and $\mathcal{S}(H) = \bigcup_{S \in \mathcal{P}(H)} \mathcal{S}_S(H)$. If $S \cap S' = \emptyset$ and $\phi = \phi_S(x_S) \prod_{\mathbf{q} \notin S} 1_{O_\mathbf{q}}(x_\mathbf{q}) \in \mathcal{S}_S(H)$ and $\phi' \in \mathcal{S}_{S',H}$, we define $\phi' * \phi \in \mathcal{S}_{S \cup S'}(H)$ by $\phi' * \phi(x) = \phi'(x_{S'}) \phi_S(x_S) \prod_{\mathbf{q} \notin S \cup S'} 1_{O_\mathbf{q}}(x_\mathbf{q})$. Finally, if $\mathbf{b} \in I(H)$, define $\delta_\mathbf{b} \in \mathcal{S}_{|\mathbf{b}|,H}$ by $\delta_\mathbf{b} = 1_{O_{|\mathbf{b}|}} - 1_\mathbf{b}$ where $1_\mathbf{b}$ is the characteristic function of $\mathbf{b}$ considered as an $H_{|\mathbf{b}|}$ fractional ideal, and if $\mathbf{b} \in I(H^\vee)$, let $\delta_\mathbf{b}^\vee \in \mathcal{S}_{|\overline{\mathbf{b}}|,H}$ be defined by $\delta_\mathbf{b}^\vee = 1_{O_{|\overline{\mathbf{b}}|}} - N(\mathbf{b})^{-1} 1_{\overline{\mathbf{b}}^{-1}}$. Let γ be a generator of the fractional ideal of $H_{|\mathbf{b}|}$ generated by $\mathbf{d}_H$. Then we have

$$\mathcal{F}_{|\overline{\mathbf{b}}|}(\delta_{\overline{\mathbf{b}}})(x) = \delta_\mathbf{b}^\vee(\gamma x).$$

II. Shintani's method.

In this section, we shall recall some results obtained in [Co 1] and improve a little bit on them. Let $k \in \mathbf{N}$, $j \in \mathbf{N} - \{0\}$, and let V be a subgroup of finite index in U_H. Let $\mathcal{S}_{k,j,V}(H)$ be the subspace of $\mathcal{S}(H)$ of functions satisfying:

$$\phi(vx)\overline{N_{H/K}(v)}^{k} N_{H/K}(v)^{-j} = \phi(x) \qquad \text{for all} \qquad x \in \mathcal{A}_H^f \quad \text{and} \quad v \in V. \tag{1}$$

If $\phi \in \mathcal{S}_{k,j,V}$, we set

$$\Lambda(k,j,\phi,s) = \frac{1}{[U_H : V]} \frac{\Gamma(j)^n}{(2i\pi)^{nj}} \sum_{\beta \in H^*/V} \phi(\beta) \frac{\overline{\beta_1 \dots \beta_2}^{k}}{(\beta_1 \dots \beta_n)^j} \frac{1}{|\beta_1 \dots \beta_n|^{2s}}. \tag{2}$$

This expression is independent of the choice of V and converges for $Re(s) >> 0$. By a theorem of Hecke, $\Lambda(k,j,\phi,s)$ admits an analytic continuation to the whole complex plane and a functional equation relating it to $\Lambda(j-1, k+1, \mathcal{F}_H(\phi), -s)$. We set

$$\Lambda(k,j,\phi) = \Lambda(k,j,\phi,0), \tag{3}$$

and the functional equation gives

$$\Lambda(k,j,\phi) = (-1)^{n(j-1)} i^n \Lambda\big(j-1, k+1, \mathcal{F}_H(\phi)\big). \tag{4}$$

From now on, V will be a torsion free subgroup of finite index of the subgroup of U_H of elements of norm 1 over K. Let $\mathcal{B}(V)$ be the set of finite sets of bases of H over K satisfying:

$$\frac{1}{z_1 \dots z_n} = \sum_{v \in V} \sum_{B \in \mathcal{B}} f_B(vz), \tag{5}$$

where, if $B = (f_{1,B}, \dots, f_{n,B})$ is a basis of H over K, we set

$$f_B(z) = \det(B) \prod_{i=1}^{n} (Tr(f_{i,B} z)^{-1} \tag{6}$$

for all $z \in (\mathbf{C}^*)^n$ such that the right hand side converges.

Remark: This condition is an "algebraic" version of Shintani's condition [Sh] (in the totally real case), that the union over $B \in \mathcal{B}$ of the cones generated by $f_{1,B}, \dots, f_{n,B}$ is a fundamental domain of $(\mathbf{R}_+^*)^n$ modulo the action of V.

Lemma 1: (i) $\mathcal{B}(V)$ is not empty.

(ii) If $\mathcal{B} \in \mathcal{B}(V)$, then $\mathcal{B}^\vee \in \mathcal{B}(V^\vee)$.

Proof: We shall use theorem 1 of [Co 1] to construct explicit elements of $\mathcal{B}(V)$. By a theorem of Dirichlet, V is of rank $n-1$. Let us choose a basis $\eta_1, \ldots, \eta_{n-1}$ of V, and for each $\sigma \in S_{n-1}$, let $f_{1,\sigma} = 1$ and $f_{i,\sigma} = \prod_{j<i} \eta_{\sigma(j)}$ for $2 \leq i \leq n$. Write $\epsilon(\sigma)$ for the signature of σ and suppose that $(f_{1,\sigma}, \ldots, f_{n,\sigma})$ is a basis of H over K for all $\sigma \in S_{n-1}$ (we can always find $\eta_1, \ldots, \eta_{n-1}$ so that this is true). Then there exists a sign $\epsilon = \epsilon(\eta_1, \ldots, \eta_{n-1})$ such that, if $B_\sigma = (f_{1,\sigma}, \ldots, f_{n,\sigma})$ when $\epsilon\epsilon(\sigma) = 1$ and $B_\sigma = (f_{n,\sigma}, f_{2,\sigma}, \ldots, f_{n-1,\sigma}, f_{1,\sigma})$ when $\epsilon\epsilon(\sigma) = -1$, then $\mathcal{B} = \{B_\sigma \mid \sigma \in S_{n-1}\} \in \mathcal{B}(V)$. Part (ii) of the lemma follows by taking the Fourier transform of both sides of (5) and using the fact that the Fourier transform of $F_B(z)$ with respect to $(\ |\ )_\infty$ is $i^n F_{B^\vee}(z)$.

Let $z_i = (z_{i,1}, \ldots, z_{i,n})$ for $i = 1, 2$ be variables in $Y_i \simeq \mathbf{C}^n$. Let $\nabla_i = \prod_{j=1}^n (-\frac{\partial}{\partial z_{i,j}})$. We deduce from (5) and the fact that $\nabla_1 \circ v = \nabla_1$ if $v \in V$, that whenever the right hand side converges and $\mathcal{B} \in \mathcal{B}(V)$, we have

$$\frac{\Gamma(j)^n}{(2i\pi)^{(n-j)}} \frac{\overline{\beta_1 \cdots \beta_n}^k}{(\beta_1 \cdots \beta_n)^j} = \frac{1}{(2i\pi)^{n(k+j)}} \nabla_1^{j-1} \nabla_2^k \Big(\sum_{v \in V} \sum_{B \in \mathcal{B}} (v\beta + z_1 | z_2)_\infty f_B(v\beta + z_1) \Big)_{z_1 = z_2 = 0}. \tag{7}$$

If $\mathcal{B}$ is a finite set of bases of H over K and $\phi \in \mathcal{S}(H)$, we set

$$K(z_1, z_2, \phi, \mathcal{B}) = \sum_{\beta \in H} \sum_{B \in \mathcal{B}} \phi(\beta) f_B(\beta + z_1)(\omega + z_1 | z_2)_\infty. \tag{8}$$

This series is not absolutely convergent but makes sense as a distribution, and the resulting distribution can be expressed in terms of elliptic functions attached to lattices in K (cf. [Co 1] and III §3 of this paper).

If $o \in \mathcal{S}_{k,j,V}$ and $\mathcal{B} \in \mathcal{B}(V)$, we set

$$F(z_1, z_2, \phi, \mathcal{B}) = \frac{1}{[U_H : V]} \frac{1}{(2\pi i)^n} K\Big(\frac{z_1}{2\pi i}, \frac{z_2}{2i\pi}, \phi, \mathcal{B}\Big). \tag{9}$$

Now, plugging (7) into (2) with $s = 0$ yields the following **formal** identity:

$$\Lambda(k, j, \phi) = \nabla_1^{j-1} \nabla_2^k \big(F(z_1, z_2, \phi, \mathcal{B}) \big)_{z_1 = z_2 = 0}. \tag{10}$$

The main problem with (10) is that $F(z_1, z_2, \phi, \mathcal{B})$ is in general not regular at $z_1 = z_2 = 0$. In fact, we have the following lemma:

Lemma 2: The singularities of $K(z_1, z_2, \phi, \mathcal{B})$ are simple poles situated on the hyperplanes $Tr\big(f_{i,B}(\beta + z)\big) = 0$ (resp. $Tr\big(f_{i,B^\vee}(\beta + z)\big) = 0$) where β runs through elements of H

(resp. $H^\vee$) such that $\phi(\beta) \neq 0$ (resp. $\mathcal{F}_H(\phi)(\beta) \neq 0$), B runs through elements of $\mathcal{B}$ and $1 \leq i \leq n$.

Proof: The proof results from the expression of $K(z_1, z_2, \phi, \mathcal{B})$ in terms of elliptic functions.

Remark: The poles on the hyperplanes of equation $Tr\big(f_{i,B}(\beta + z)\big)$ are already apparent in formula (8); the others appear if we use the following functional equation which is a direct consequence of the Poisson summation formula:

$$K(z_1, z_2, \phi, \mathcal{B}) = i^n (z_1 \mid z_2)_\infty K(z_2, -z_1, \mathcal{F}_H(\phi), \mathcal{B}^\vee). \tag{11}$$

We shall say that $(\phi, \mathcal{B})$ satisfies the condition (*) if $K(z_1, z_2, \phi, \mathcal{B})$ has no singularity at $z_1 = z_2 = 0$. This is equivalent to

1) $\phi(x) \neq 0 \Rightarrow Tr(f_{i,B}x) \neq 0$ for all $x \in H$, $B \in \mathcal{B}$ and $1 \leq i \leq n$.

2) $\mathcal{F}_H(\phi)(x) \neq 0 \Rightarrow Tr(f_{i,B^\vee}x) \neq 0$ for all $x \in H^\vee$, $B \in \mathcal{B}$ and $1 \leq i \leq n$.

We shall say that $(\phi, \mathcal{B})$ satisfies (**) if it satisfies (*) and if we have moreover

3) $\phi(x) \neq 0 \Rightarrow Tr(fx) \neq 0$ for all $x \in H$ and $f \in \mathcal{E}(\mathcal{B})$

4) $\mathcal{F}_H(x) \neq 0 \Rightarrow Tr(fx) \neq 0$ for all $x \in H^\vee$ and $f \in \mathcal{E}(\mathcal{B}^\vee)$,

where $\mathcal{E}(\mathcal{B})$ (resp. $\mathcal{E}(\mathcal{B}^\vee)$) is a finite subset of H (resp. $H^\vee$) which will appear in the proof of Theorem 3.

If $(\phi, \mathcal{B}) \in \mathcal{S}_{k,j,V}(H) \times \mathcal{B}(V)$ satisfies condition (*), we set

$$\Lambda_{\mathcal{B}}(k, j, \phi) = \nabla_1^{j-1} \nabla_2^k \big(F(z_1, z_2, \phi, \mathcal{B})\big)_{z_1 = z_2 = 0} \tag{12}$$

and

$$F_j(z_2, \phi, \mathcal{B}) = \nabla_1^{j-1} \big(F(z_1, z_2, \phi, \mathcal{B})\big)_{z_1 = 0}. \tag{13}$$

Let g be a C^∞ compactly supported function on $\mathbf{C}$ equal to 1 in a neighborhood of 0. Let $\epsilon > 0$ and $\mu_k(s) = i^k \frac{\Gamma(k+1-s)}{\pi^{k+1-s}} \frac{\pi^s}{\Gamma(s)}$, and set

$$\Lambda_{\mathcal{B},\epsilon}(k, j, \phi, s) = \int_{\mathbf{C}^n} F_j(z_1, \phi, \mathcal{B}) \prod_{i=1}^n \Big(g(\epsilon z_{2,i}) \mu_k(s) \frac{\overline{z_{2,i}}^k}{|z_{2,i}|^{2(k+1-s)}} \Big). \tag{14}$$

Theorem 3: (i) $\Lambda_{\mathcal{B},\epsilon}(k, j, \phi, s)$ is a meromorphic function of $s \in \mathbf{C}$ and the locus of its poles is independent of ϵ.

(ii) When ϵ goes to 0, $\Lambda_{\mathcal{B},\epsilon}(k, j, \phi, s)$ converges uniformly (outside the poles) to $\Lambda(k, j, \phi, s)$ on each compact subset of $Re(s) > \frac{k}{2} + 1$.

(iii) For all $\epsilon > 0$, we have $\Lambda_{\mathcal{B},\epsilon}(k,j,\phi,0) = \Lambda_{\mathcal{B}}(k,j,\phi)$.

(iv) If $(\phi,\mathcal{B})$ satisfies condition (**), then $\Lambda_{\mathcal{B},\epsilon}(k,j,\phi,s)$ converges uniformly (outside the poles) on each compact subset of $Re(s) > \frac{k}{2} - \frac{1}{4n-10}$ (resp. **C**), if $n \geq 3$ (resp. $n = 1,2$).

(v) $\Lambda_{\mathcal{B}}(k,j,\phi) = (-1)^{n(j-1)} i^n \Lambda_{\mathcal{B}^\vee}\big(j-1, k+1, \mathcal{F}_H(\phi)\big)$.

Corollary: If $(\phi,\mathcal{B})$ satisfies condition (**), we have $\Lambda_{\mathcal{B}}(k,j,\phi) = \Lambda(k,j,\phi)$ if $n = 1,2$ or if $n \geq 3$ and $k = 0$ or $j = 1$.

Proof of theorem 3: (v) is an immediate consequence of formula (11). Using the same method as in [Co 1, p. 198], we see that $\Lambda(k,j,\phi,s)$ is a finite combination of the functions studied in [Co 1, II]. Granting this, (i) follows from [Co 1, II Lemma 8], (ii) from [Co 1, II Lemma 9] and (iii) from [Co 1, II, §6]. The only thing which is new is (iv), which will allow us to remove from [Co 1, Th. 5 and 6] the meaningless condition about embeddings of F into $\overline{K}$. This improvement is made possible by replacing Lemma 1 of [Co 1, III] by the following stronger theorem of Schmidt:

Lemma 4: (Schmidt's subspace theorem) Let $\delta > 0$ and $\{(L_{j,1},\ldots,L_{j,n}) \mid j \in J\}$ be a finite set of families of n linearly independent linear forms with algebraic coefficients. Then there exists a finite set $\mathcal{E}$ of elements of $H^\vee$ such that for all $\phi \in \mathcal{S}(H^\vee)$, the set of elements of $H^\vee$ satisfying

(i) $\phi(x) \neq 0$

(ii) there exists $j \in J$ such that $\prod_{i=1}^n |L_{j,i}(x)| \leq \| x \|^{-\delta}$

is contained in the union of the hyperplanes of equation $Tr(fx) = 0$ for $f \in \mathcal{E}$ up to a finite set.

For the proof of this statement see [Sch, Th. 7A]. Let us go back to the proof of (iv). Let $\delta > 0$. A slight modification of the proof of [Co 1, II, Lemme 10] shows that there exists a finite set $\mathcal{L}(\mathcal{B}^\vee) = \{(L_{j,1},\ldots,L_{j,n}) \mid j \in J\}$ of families of n linearly independent linear forms with algebraic coefficients (they are the $N_{I,j}$ of [Co 1, Th. 2]) such that if, for all $j \in J$, the set of $x \in H^\vee$ such that $\mathcal{F}_H(\phi)(x) \neq 0$ and $\prod_{i=1}^n |L_{j,i}(x)| \leq \| x \|^{-\delta}$ is finite, then $\Lambda_{\mathcal{B},\epsilon}(k,j,\varphi,s)$ converges uniformly (outside the poles) on each compact subset of $Re(s) > \frac{k}{2} - \frac{1-2(n-1)\delta}{2(n-2)-4(n-1)\delta}$ (resp. **C**) if $n \geq 3$ (resp. $n = 1,2$). To finish with the proof, we just have to take $\mathcal{E}(\mathcal{B})$ (resp. $\mathcal{E}(\mathcal{B}^\vee)$) of condition (**) to be the set $\mathcal{E}$ associated to $\mathcal{L}(\mathcal{B}^\vee)$ (resp. $\mathcal{L}(\mathcal{B})$) and $\delta = \big(4(n-1)\big)^{-1}$ by Lemma 4.

When $(\phi,\mathcal{B})$ does not satisfy condition (*), we cannot define $\Lambda_{\mathcal{B}}(k,j,\phi)$ by formula (12). As the singularities of $F(z_1,z_2,\phi,\mathcal{B})$ are simple enough, we could give a meaning to (12) by taking a suitable finite part as in [Co 1, II, §6], but here we shall use the

standard technique of replacing ϕ by a suitable linear combination to eliminate the pole. If $S \in \mathcal{P}(H)$, let $S_K = \{\mathbf{q} \cap O_K \mid \mathbf{q} \in S\} \in \mathcal{P}(K)$ and if $S \in \mathcal{P}(K)$, let $S^H = \{\mathbf{q} \in \mathcal{P}(H) \mid \exists \mathbf{p} \in S$ such that $\mathbf{q}|\mathbf{p}\} \in \mathcal{P}(H)$.

Lemma 5: Let $\mathcal{E}$ be a finite subset of H^*; then there exist $S(\mathcal{E}) \in \mathcal{P}(H)$ such that for all $S \in \mathcal{P}(H)$, all $\mathbf{b} \in C(H)$ satisfying $|\mathbf{b}| \cap \left(S(\mathcal{E}) \cup (S_K)^H\right) = \emptyset$ and all $f \in \mathcal{E}$, we have: if $x \in \mathbf{b}^{-1}O'_{H,S} - O'_{H,S}$, then $Tr(fx) \notin O'_{K,(S_K)^H}$ and in particular $Tr(fx)$ is non-zero.

Proof: Let $S' = |\mathbf{d}_H| \cup_{f \in \mathcal{E}} |(f)|$ and $S(\mathcal{E}) = (S'_K)^H$. Let $\mathbf{b} \in C(H)$ be such that $|\mathbf{b}| \cap \left(S(\mathcal{E}) \cup (S_K)^H\right) = \emptyset$ and $x \in \mathbf{b}^{-1}O'_{H,S} - O'_{H,S}$. There exists $\mathbf{q} \in |\mathbf{b}|$ such that $v_{\mathbf{q}}(x) < 0$. As $O_H/\mathbf{b}$ is cyclic, $\mathbf{q}$ is of degree 1 and if $\mathbf{p} = \mathbf{q} \cap O_K$ and $\mathbf{q}' \in |\mathbf{p}| - \{\mathbf{q}\}$, then $\mathbf{q}' \notin |\mathbf{b}|$, hence $v_{\mathbf{q}'}(x) \geq 0$; and this implies, as $\mathbf{q} \notin S'$, that $v_{\mathbf{p}}(Tr(fx)) = v_{\mathbf{q}}(x)$ which implies $Tr(fx) \notin O'_{K,(S_K)^H}$.

If $S \in \mathcal{P}(H)$ and $S' \in \mathcal{P}(H^\vee)$, let $C(S,S') = \{(\mathbf{b}_1, \mathbf{b}_2) \in C(H) \times C(H^\vee) \mid |\mathbf{b}_1| \cap (S_K)^H = \emptyset, |\mathbf{b}_2| \cap (S'_K)^{H^\vee} = \emptyset$ and $|\mathbf{b}_1|_K \cap |\overline{\mathbf{b}}_2|_K = \emptyset\}$, and if $T \in \mathcal{P}(H)$, let $C_T(S,S') = C(S \cup T, S' \cup T)$. Also let $C^0(S,S')$ (resp. $C^0_T(S,S')$) be the intersection of $C(S,S')$ (resp. $C_T(S,S')$) with $C^0(H) \times C^0(H^\vee)$. If $\phi \in \mathcal{S}(H)$, and $\mathbf{b}_1 \in I(H), \mathbf{b}_2 \in I(H^\vee)$, set $\phi_{\mathbf{b}_1,\mathbf{b}_2} = \delta_{\mathbf{b}_1^{-1}} * \delta^\vee_{\mathbf{b}_2^{-1}} * \phi$, whenever this is defined.

Lemma 6: Let $\mathcal{B}$ be a finite set of bases of H over K. Then there exist $S = S_1(\mathcal{B}) \in \mathcal{P}(H)$ and $S' = S'_1(\mathcal{B}) \in \mathcal{P}(H^\vee)$ such that, for all $T \in \mathcal{P}(H)$, all $\phi \in \mathcal{S}_T(H)$ and all $(\mathbf{b}_1, \mathbf{b}_2) \in C_T(S,S')$, the conditions (*) and (**) are satisfied by $(\phi_{\mathbf{b}_1,\mathbf{b}_2}, \mathcal{B})$.

Proof: $\phi_{\mathbf{b}_1,\mathbf{b}_2}(x) \neq 0$ implies $x \in \mathbf{b}_1^{-1}O'_{H,T} - O'_{H,T}$ and $\mathcal{F}_H(\phi_{\mathbf{b}_1,\mathbf{b}_2})(x) \neq 0$ implies $x \in \mathbf{b}_2^{-1}O'_{H^\vee,\overline{T}} - O'_{H^\vee,\overline{T}}$. Hence, the result is an immediate consequence of Lemma 5.

Let O^*_T act on $\mathcal{S}_{H,T}$ by $\phi \to \phi \circ \gamma$ where $\phi \circ \gamma(x) = \phi(\gamma x)$. Any $\phi \in \mathcal{S}_{H,T}$ has a unique decomposition $\phi = \sum_\chi \phi_\chi$ where $\phi_\chi = 0$ for almost all χ, χ running through the locally constant characters of O^*_T, and $\phi_\chi \circ \gamma = \chi(\gamma)\phi_\chi$ for all $\gamma \in O^*_S$. Now, using the identification between $\mathcal{S}_{H,T}$ and $\mathcal{S}_T(H)$, we can decompose any $\phi \in \mathcal{S}_T(H)$ as $\sum_\chi \phi_\chi$ and if ϕ belongs to $\mathcal{S}_{k,j,V}(H)$ then so does ϕ_χ. Let $(\mathbf{b}_1, \mathbf{b}_2) \in C^0_T(S_1(\mathcal{B}), S'_1(\mathcal{B}))$ and $\beta_1 \in H$ be a generator of $\mathbf{b}_1$ and $\beta_2 \in H^\vee$ be a generator of $\mathbf{b}_2$. If $\gamma \in H^*$ and $\phi \in \mathcal{S}(H)$, let $\phi \circ \gamma \in \mathcal{S}(H)$ be defined by $(\phi \circ \gamma)(x) = \phi(\gamma x)$. Then we have

$$(\phi_\chi)_{\mathbf{b}_1,\mathbf{b}_2} = \phi_\chi - \chi(\beta_1)^{-1}\phi_\chi \circ \beta_1 - N(\mathbf{b}_2)\chi(\overline{\beta}_2)\phi_\chi \circ \overline{\beta}_2^{-1} + N(\mathbf{b}_2)\chi(\overline{\beta}_2\beta_1^{-1})\phi_\chi \circ (\beta_1\overline{\beta}_2^{-1}), \quad (15)$$

but as

$$\Lambda(k,j,\phi \circ \gamma) = \frac{N_{H/K}(\gamma)^j}{\overline{N_{H/K}(\gamma)}^k}\Lambda(k,j,\phi), \quad (16)$$

we obtain

$$\Lambda(k,j,\phi) = \sum_{\chi} \nu_{\beta_1,\beta_2}(k,j,\chi)\Lambda(k,j,(\phi_\chi)_{\mathbf{b}_1,\mathbf{b}_2}), \tag{17}$$

where

$$\nu_{\beta_1,\beta_2}(k,j,\chi) = \Big(1 - \frac{\chi(\beta_1)^{-1}N_{H/K}(\beta_1)^j}{\overline{N_{H/K}(\beta_1)}^k}\Big)^{-1}\Big(1 - \frac{\chi(\overline{\beta}_2)N_{H^\vee/K}(\beta_2)^{k+1}}{\overline{N_{H^\vee/K}(\beta_2)}^{j-1}}\Big)^{-1}. \tag{18}$$

To be coherent with formula (17), we set, if $\phi \in \mathcal{S}_T(H) \cap \mathcal{S}_{k,j,V}(H)$, $\mathcal{B} \in \mathcal{B}(V)$ and $(\mathbf{b}_1,\mathbf{b}_2) = \big((\beta_1),(\beta_2)\big) \in C_T\big(S_1(\mathcal{B}),S_1'(\mathcal{B})\big)$,

$$\Lambda_{\mathcal{B},\beta_1,\beta_2}(k,j,\phi) = \sum_{\chi} \nu_{\beta_1,\beta_2}(k,j,\chi)\Lambda_{\mathcal{B}}\big(k,j,(\phi_\chi)_{\mathbf{b}_1,\mathbf{b}_2}\big), \tag{19}$$

and the right hand side is well-defined by Lemma 6.

Remark: We expect that $\Lambda_{\mathcal{B},\beta_1,\beta_2}(k,j,\phi) = \Lambda(k,j,\phi)$ and by the corollary to theorem 3, this equality is true if $n = 1,2$ or if $n \geq 3$ and $k = 0$ or $j = 1$. Moreover, we shall prove using p-adic methods (cf. III §4 of this paper) that, to a large extent, $\Lambda_{\mathcal{B},\beta_1,\beta_2}(k,j,\phi)$ does not depend on the auxiliary choices of $\mathcal{B}$, β_1 and β_2.

III. Construction of the basic measure

§1. P-adic measures

Let $p \neq 2,3$ be a prime which splits in K. Fix an embedding of $\overline{K}$ into $\mathbf{C}_p$ (and keep the previous embedding of $\overline{K}$ into $\mathbf{C}$). Let $\mathbf{p}$ be the prime ideal of O_K determined by this embedding, $O_{\mathbf{p}}$ be the completion of O_K at $\mathbf{p}$ and $\overline{\mathbf{p}}$ the other prime ideal of O_K above p. Let $Y_{H,\mathbf{p}} = O_H \otimes_{O_K} O_{\mathbf{p}} \simeq O_{H^\vee} \otimes_{O_K} O_{\overline{\mathbf{p}}}$ and $Y_{H,p} = O_H \otimes \mathbf{Z}_p = Y_1 \times Y_2$ where $Y_1 = Y_{H,\mathbf{p}}$ and $Y_2 = Y_{H^\vee,\mathbf{p}}$. We can also describe Y_1 (resp. Y_2) as the topological closure of O_H (resp. $O_{H^\vee}$) into $\mathbf{C}_p^n$ via the map $\alpha \to (\tau_1(\alpha),\dots,\tau_n(\alpha))$(resp. $(\overline{\tau_1(\overline{\alpha})},\dots,\overline{\tau_n(\overline{\alpha})})$). With this description, we can write $y_i \in Y_i$ as $(y_{i,1},\dots,y_{i,n})$. If $z \in \mathbf{C}_p^n$, we set $Tr(z) = \sum_{i=1}^n z_i$ and $N(z) = \prod_{i=1}^n z_i$. If ℓ is a prime ideal of O_K, let $\mathbf{d}_{H,\ell}$ be the part of $\mathbf{d}_H$ above ℓ. Fix a basis $B = (f_1,\dots,f_n)$ of $\mathbf{d}_{H,\overline{\mathbf{p}}}^{-1} O_{H,p}$ over $O_{K,p}$. Let $B^* = (g_1,\dots,g_n)$ be the basis of H over K dual to B with respect to the bilinear form $Tr_{H/K}(xy)$ and $B^\vee = ({f_1}^\vee,\dots,{f_n}^\vee)$ and $(B^*)^\vee = ({g_1}^\vee,\dots,{g_n}^\vee)$ be the bases of $H^\vee$ over K dual to B and B^* with respect to $\langle\ |\ \rangle$. Then B^* is a basis of $\mathbf{d}_{H,\mathbf{p}}^{-1} O_{H,p}$ over $O_{K,p}$, $B^\vee$ is a basis of $\mathbf{d}_{H^\vee,\overline{\mathbf{p}}}^{-1} O_{H^\vee,p}$ over $O_{K,p}$ and $(B^*)^\vee$ is a basis of $\mathbf{d}_{H^\vee,\mathbf{p}}^{-1} O_{H^\vee,p}$ over $O_{K,p}$.

If $y_i \in Y_i$, we set $x_i = (x_{i,1},\dots,x_{i,n})$, where $x_{1,j} = Tr(g_j y_1)$ and $x_{2,j} = Tr({g_j}^\vee y_2)$. The map $y_i \to x_i$ induces an isomorphism of $O_{\mathbf{p}}$-modules between Y_i and $O_{\mathbf{p}}^n \simeq \mathbf{Z}_p^n$. If $z_i = (z_{i,1},\dots,z_{i,n})$ for i=1,2 is sufficiently close to zero in $\mathbf{C}_p^n$, we set $w_i = (w_{i,1},\dots,w_{i,n})$, where $w_{1,j} = exp\big(-Tr(f_j z_1)\big) - 1$ and $w_{2,j} = exp\big(-Tr({f_j}^\vee z_2)\big) - 1$.

Let Λ be a closed subring of $\hat{O}$ the ring of integers of $\mathbf{C}_p$. A Λ-valued measure on a compact and totally disconnected topological space X is a continuous (for the supremum norm) linear map on the space of continuous functions on X with values in $\mathbf{C}_p$ whose values on characteristic functions of compact open subsets of X are in Λ. If μ is a Λ-valued measure on $Y_{H,p}$, we define its Fourier-Laplace transform by

$$F_\mu(z_1,z_2) = \int_{Y_{H,p}} exp\big(-Tr(y_1 z_1 + y_2 z_2)\big) d\mu = \int_{\mathbf{Z}_p^{2n}} \prod_{i=1}^{2} \prod_{j=1}^{n} (1 + w_{i,j})^{x_{i,j}}\, d\lambda_B,$$

where λ_B is the measure on $\mathbf{Z}_p^{2n}$ deduced from μ via the map $(y_1,y_2) \to (x_1,x_2)$.

Lemma 7: If μ is a Λ-valued measure on $Y_{H,p}$, then $F_\mu(z_1,z_2)$ is given by a power series in a neighborhood of zero, and reciprocally, if $F(z_1,z_2)$ is a power series, then for $F(z_1,z_2)$ to be the Fourier-Laplace transform of a Λ-valued measure, it is necessary and sufficient that $F(z_1,z_2)$ expressed in w_1,w_2 is a power series with coefficients in Λ.

Proof: The general case reduces easily to the case n=1 which is well-known.

We shall write $W_{B,\mu}(w_1, w_2)$ for the Fourier-Laplace transform of μ expressed in w_1, w_2. If $\gamma \in H/\mathbf{d}_{H,\mathbf{p}}^{-1} O_{H,\mathbf{p}}$, we define a locally constant character χ_γ of Y_1 identified with $O_{H^\vee} \otimes_{O_K} O_{\overline{\mathbf{p}}}$ by the formula $\chi_\gamma(y_1) = (\gamma \mid y_1)_{|\mathbf{p}|}$ (cf. I), and if $\gamma \in H^\vee/\mathbf{d}_{H^\vee,\mathbf{p}}^{-1} O_{H^\vee,\mathbf{p}}$, we define a locally constant character χ_γ of $Y_2 \simeq O_H \otimes_{O_K} O_{\overline{\mathbf{p}}}$ by the formula $\chi_\gamma(y_2) = (y_2 \mid \gamma)_{|\overline{\mathbf{p}}|}$. The map $\gamma \to \chi_\gamma$ induces an isomorphism from $H/\mathbf{d}_{H,\mathbf{p}}^{-1} O_{H,\mathbf{p}}$ (resp. $H^\vee/\mathbf{d}_{H^\vee,\mathbf{p}}^{-1} O_{H^\vee,\mathbf{p}}$) to the group of locally constant characters on Y_1 (resp. Y_2).

Lemma 8: Let $j, k \in \mathbf{N}$ and $\gamma_1 \in H/\mathbf{d}_{H,\mathbf{p}}^{-1} O_{H,\mathbf{p}}$ and $\gamma_2 \in H^\vee/\mathbf{d}_{H^\vee,\mathbf{p}}^{-1} O_{H^\vee,\mathbf{p}}$. Then

(i) $\int_{Y_{H,p}} \chi_{\gamma_1}(y_1)\chi_{\gamma_2}(y_2) N(y_1)^j N(y_2)^k \, d\mu = \nabla_1^j \nabla_2^k \left(F_{\chi_{\gamma_1}\chi_{\gamma_2}\mu}(z_1, z_2)\right)_{z_1=z_2=0}$,

where, if ϕ is a continuous function on $Y_{H,p}$ then $\phi\mu$ is the measure defined by $\int_{Y_{H,p}} \psi \, d(\phi\mu) = \int_{Y_{H,p}} \phi\psi \, d\mu$, and

(ii) $F_{\chi_{\gamma_1}\chi_{\gamma_2}\mu}(z_1, z_2) = W_{B,\mu}(\ldots, \epsilon_{i,j}(1 + w_{i,j}) - 1, \ldots)$,

where the $\epsilon_{i,j}$ are p^∞-th roots of unity defined by $\epsilon_{1,j} = \chi_{\gamma_1}(\overline{f}_j)$ and $\epsilon_{2,j} = \chi_{\gamma_2}(f_j{}^\vee)$.

Proof: (i) follows by developing $exp\big(-Tr(y_1 z_1 + y_2 z_2)\big)$ as a power series and (ii) is evident if we remark that $\chi_{\gamma_i}(y_i) = \prod_{j=1}^n \epsilon_{i,j}^{x_{i,j}}$, which gives

$$F_{\chi_{\gamma_1}\chi_{\gamma_2}\mu}(z_1, z_2) = \int_{Y_{H,p}} \prod_{i=1}^{2} \prod_{j=1}^{n} \big(\epsilon_{i,j}(1 + w_{i,j})\big)^{x_{i,j}} \, d\lambda_B.$$

Our aim in the rest of this section will be to prove that under suitable conditions, the holomorphic part of $K(z_1, z_2, \phi, \mathcal{B})$ is the Fourier-Laplace transform of a measure on $Y_{H,p}$. We shall first consider the case $H = K$, and this will involve the study of the p-adic behavior of Eisenstein-Kronecker series. This is the aim of the next paragraph, and in the paragraph after that we shall reduce the general case to the case $H = K$.

§2. P-adic properties of Eisenstein-Kronecker series.

Let us begin by recalling the definitions and some basic facts about Eisenstein-Kronecker series. We refer to [W2] for the proofs. Let L be a lattice in $\mathbf{C}$ and $A(L) = \pi^{-1}Vol(L)$. If $u, z \in \mathbf{C}$, we set

$$\langle z, u\rangle_L = exp\big(A(L)^{-1}(z\overline{u} - u\overline{z})\big). \tag{20}$$

If $k \geq 1$ is an integer, we define for $\mathrm{Re}(s) >> 1$ the function $H_k(s, z, u, L)$ by the formula

$$H_k(s, z, u, L) = \Gamma(s)A(L)^{s-k}\sum_{\omega\in L}{}'\langle\omega, u\rangle_L\frac{(\overline{z}+\overline{\omega})^k}{|z+\omega|^{2s}}. \tag{21}$$

This function has an analytic continuation to the whole complex plane and satisfies the functional equations

$$H_k(s, z, u, L) = \langle u, z\rangle_L H_k(k+1-s, u, z, L), \tag{22}$$

$$H_k(s, z, u, L') = [L' : L]^{k-s}\sum_{\gamma\in L'/L}\langle\gamma, u\rangle_{L'}H_k(s, z+\gamma, [L' : L]u, L) \tag{23}$$

if L is a sublattice of L', and

$$H_k(s, \lambda z, \lambda u, \lambda L) = \lambda^{-k}H_k(s, z, u, L) \quad \text{for} \quad \lambda \in \mathbf{C}. \tag{24}$$

From (4) and (5) one deduces that if $u \in \mathbf{Q}L$ and $b \in \mathbf{C}$ is an endomorphism of L such that $\overline{b}u \in L$,

$$H_k(s, z, u, L) = \frac{\overline{b}^k}{|b|^{2s}}\sum_{\gamma\in b^{-1}L/L}\langle\gamma, \overline{b}u\rangle_L H_k(s, \gamma + b^{-1}z, 0, L). \tag{25}$$

If j is an integer such that $1 \leq j \leq k$, we define

$$E_{k,j}(z, L) = H_{k+j}(j, z, 0, L) \quad \text{and} \quad E_j(z, L) = E_{0,j}(z, L), \tag{26}$$

$$a_j(L) = E_j(0, L) = E_{1,j-1}(0, L), \tag{27}$$

and

$$\wp(z, L) = E_2(z, L) - a_2(L) \quad \big(\text{so } \wp'(z, L) = -E_3(z, L)\big). \tag{28}$$

$E_1(z,L)$ has the following Laurent expansion in a neighborhood of 0:

$$E_1(z,L) = -\frac{\overline{z}}{A(L)} + z^{-1} + \sum_{n=1}^{\infty} a_{n+1}(L)\frac{(-z)^n}{n!}, \tag{29}$$

and $E_{k,j}(z,L) - \left(\frac{\overline{z}}{A(L)}\right)^k \frac{\Gamma(j)}{z^j}$ is real analytic in a neighborhood of 0.

Proposition 9: There exists a (non-unique) polynomial $P_{k,j}$ with rational coefficients in the variables $E(z,L) = \{E_1(z,L),\ldots,E_j(z,L),\ldots\}$ and $a(L) = \{a_1(L),\ldots,a_j(L),\ldots\}$ such that $P_{k,j}\big(E(z,L),a(L)\big) = E_{k,j}(z,L)$ for $z \notin L$.

Proof: The proof is by induction. The statement is trivial for $k = 0$ and $j \geq 1$. Moreover, as $\frac{d}{dz}E_{k,j}(z,L) = -E_{k,j+1}(z,L)$, if the statement is true for (k,j) it is true for $(k,j+1)$. Thus the problem is to show the existence of $P_{n+1,1}$ assuming the existence of $P_{k,j}$ for $k \leq n$ and $j \geq 1$. If we write down a Laurent expansion for $E_{n+1,1}(z,L) + \frac{1}{n+2}E_1(z,L)^{n+2}$ in a neighborhood of 0, we obtain

$$E_{n+1,1}(z,L) + \frac{1}{n+2}E_1(z,L)^{n+2} = \sum_{k=0}^{n}\sum_{j=1}^{n+2-k} Q_{n,k,j}\big(a(L)\big)\left(\frac{\overline{z}}{A(L)}\right)^k \frac{\Gamma(j)}{z^j} + R_n(z),$$

where the $Q_{n,k,j}$ are polynomials with rational coefficients and $R_n(z)$ is real analytic in a neighborhood of 0. From this we deduce that

$$E_{n+1,1}(z,L) + \left(\frac{1}{n+2}E_1(z,L)^{n+2} - \sum_{k=0}^{n}\sum_{j=1}^{n+2-k} P_{k,j}\big(E(z,L),a(L)\big)Q_{n,k,j}\big(a(L)\big)\right)$$

is a doubly periodic real analytic function annihilated by a power of $\left(\frac{\partial}{\partial\overline{z}}\right)$ and hence a constant. Using the fact that $E_{n+1,1}(0,L) = a_{n+2}(L)$ we find that this constant can be expressed as a polynomial in the $a_j(L)$ with rational coefficients, which concludes the proof.

Let E be an elliptic curve with Weierstrass model $y^2 = x^3 - g_2x - g_3$, defined over $O_{\overline{K}}$ with complex multiplication by O_K and with good ordinary reduction at p. Let L be the period lattice of $\omega = dx/y$. Choose a basis (γ_1,γ_2) of $H_1(E(\mathbf{C}),\mathbf{Z})$: then $\int_{\gamma_2}\omega = \tau\int_{\gamma_1}\omega$ for some $\tau \in K$, and $\mathbf{a} = \mathbf{Z} + \mathbf{Z}\tau$ is a fractional ideal of K. We assume that we have chosen our basis (γ_1,γ_2) in such a way that $v_{\mathfrak{p}}(\mathbf{a}) = v_{\overline{\mathfrak{p}}}(\mathbf{a}) = 0$. Let $\eta = \big(x + a_2(L)\big)\omega$. Then (ω,η) is a basis of $H^1_{DR}(E)$ and if $\alpha \in O_K$, then $\alpha^*\omega = \alpha\omega$ and $\alpha^*\eta = \overline{\alpha}\eta$ in $H^1_{DR}(E)$. Set $\omega_\infty = \int_{\gamma_1}\omega$ and $\eta_\infty = \int_{\gamma_1}\eta$. Using Legendre's relation, we obtain $A(L) = -\overline{\omega}_\infty/\eta_\infty$. If $\alpha \in K$, we let $\tilde{\alpha} = \alpha\omega_\infty \in \mathbf{Q}L$, and if P is a torsion point on E, we let $z(P) \in K$ be any element such that $\tilde{z}(P) = \omega_\infty z(P)$ corresponds to P via the isomorphism $\mathbf{C}/L \simeq E(\mathbf{C})$. Of course, $z(P)$ is only determined up to an element in $\mathbf{a}$.

Let $t = -2x/y = -2\wp(z)/\wp'(z) = (z + \cdots)$ be the parameter of the formal group $\hat{E}$ which is the kernel of reduction mod p, $\lambda(t)$ be the power series giving z in terms of t (it is the logarithm of $\hat{E}$ and we have $d\lambda(t) = \omega(t)$), and $\oplus$ denote the formal group law on $\hat{E}$. Let $I_p \subset \hat{O}$ be the ring of integers of the completion of the maximal unramified extension of $\mathbf{Q}_p$ and $M = \mathbf{Q}_p(g_2, g_3)$. The formal groups $\hat{E}$ and $\mathbf{G}_m$ are then isomorphic over $I_{p,E} \stackrel{\text{def}}{=} I_p(g_2, g_3)$. We shall fix an isomorphism ι from $\hat{E}$ to $\mathbf{G}_m$ by requiring that the following condition holds. Let Q be a point of $\mathbf{p}^\infty$-division on E. Then we want $1 + \iota\big(t(Q)\big) = \langle \tilde{z}(Q), \tilde{1} \rangle_L$ where the left hand side is a p^∞-th root of unity in $\mathbf{C}_p$ and the right hand side is a p^∞-th root of unity in $\mathbf{C}$. We will write $\epsilon(Q)$ for this $p/infty$-th root of unity. For reasons to become obvious later, we write $-\eta_p$ for the coefficient of t in $\iota \in I_{p,E}[[t]]$ (ι has no constant term), and extend the isomorphism from $\overline{K} \subset \mathbf{C}$ to $\overline{K} \subset \mathbf{C}_p$ to an isomorphism from $\overline{K}(\eta_\infty)$ to $\overline{K}(\eta_p)$ sending η_∞ to η_p. Note that this is possible because η_∞ is transcendent due to a theorem of Čudnovskiĭ (cf. [Wa]) and η_p also in a more trivial way.

Suppose $G(z_1, \ldots, z_n)$ is locally real analytic around 0. We define the holomorphic part of G to be $\mathcal{H}\big(G(z_1, \ldots, z_n)\big)$, the power series in $z_1, \ldots, z_n$ obtained by equating $\overline{z}_1, \ldots, \overline{z}_n$ to 0 in the formal Taylor series expansion of G in $z_1, \ldots, z_n, \overline{z}_1, \ldots, \overline{z}_n$. If $H(z_1, \ldots, z_n)$ is locally of the form $F(z_1, \ldots, z_n)/G(z_1, \ldots, z_n)$, where F is real analytic around 0 and G holomorphic, we define the holomorphic part of H, $\mathcal{H}\big(H(z_1, \ldots, z_n)\big) \in \mathbf{C}\big((z_1, \ldots, z_n)\big)$, by $\mathcal{H}(H) = \mathcal{H}(F)/G$. If moreover $\mathcal{H}(F)$ and G have coefficients in $\overline{K}(\eta_\infty)$, we shall also view $\mathcal{H}(H)$ as an element of $\mathbf{C}_p\big((z_1, \ldots, z_n)\big)$.

Proposition 10: Let $\alpha \in (K - \mathbf{p}^{-\infty}\mathbf{a}) \cup \mathbf{a}$, which means that the division point $P(\alpha)$ corresponding to α is either 0 or does not belong to $\hat{E}$. Then if $1_{\mathbf{a}}$ is the characteristic function of $\mathbf{a}$, we have:

(i) $\mathcal{H}\big(E_1(\alpha + \lambda(t), L)\big) = 1_{\mathbf{a}}(\alpha)t^{-1} + E_1(\tilde{\alpha}, L) + \sum_{n=1}^{\infty} b_n(\alpha)t \stackrel{\text{def}}{=} G_1(\alpha, t)$, where $b_n(P)$ is in the ring of integers of $M\big(P(\alpha)\big)$.

(ii) $E_1((\tilde{\alpha}, L) \equiv \overline{\alpha}\eta_p \pmod{\hat{O}}$.

(iii) If Q is a $\mathbf{p}^\infty$-division point, then $G_1\big(\alpha, t(Q)\big)$ (which converges by (i)) is equal to $E_1\big(\tilde{\alpha} + \tilde{z}(Q), L\big)$.

Proof: Let $\phi(z, u) = E_1(z + u, L) - E_1(z, L) - E_1(u, L)$. Then ϕ is a meromorphic function in u and z and hence an algebraic function on $E \times E$. Moreover, it is easily seen to belong to $M(E \times E)$ and to have a well-defined reduction mod p. Now, if $\alpha \in K - \mathbf{p}^{-\infty}\mathbf{a}$, then $\mathcal{H}\big(E_1(\lambda(t) + \tilde{\alpha}, L) - E_1(\lambda(t), L) - E_1(\tilde{\alpha}, L)\big) + t^{-1}$ is an algebraic function on E without singularities on $\hat{E}$ and whose reduction mod p is defined, and so is given on $\hat{E}$ by a power series in t with coefficients in the ring of integers of $M\big(P(\alpha)\big)$. Hence, to prove (i) and (iii) for any α, it suffices to prove them for $\alpha = 0$.

Let $\beta \in O_K$ such that β is prime to p. By the same arguments as before, one sees that $\mathcal{H}\big(E_1(\beta\lambda(t), L) - \overline{\beta}E_1(\lambda(t), L)\big) - \beta^{-1}\big(N(\beta) - 1\big)t^{-1}$ is an algebraic function on E with no singularities on $\hat{E}$, and so is given on $\hat{E}$ by a power series $G_\beta(t)$ with coefficients in the ring of integers of M. Now take $\beta_n \in O_K$ satisfying $\beta_n \equiv 1 \pmod{\mathbf{p}^n}$ and $\beta_n \equiv 1 \pmod{\overline{\mathbf{p}}^n}$. Let n tend to $+\infty$. Then $G_{\beta_n}(t)$ obviously tends to $\big(E_1(\lambda(t))\big) - t^{-1}$ which concludes the proof of (i). To prove (iii), suppose Q is a $\mathbf{p}^m$-torsion point. Then if $n \geq m$, we have $\beta_n Q = Q$ and so $G_{\beta_n}\big(t(Q)\big) = (1 - \overline{\beta}_n)E_1(\tilde{z}(Q), L) - \beta_n^{-1}\big(N(\beta_n) - 1\big)t(Q)^{-1}$ (as G_{β_n} is an algebraic function, one can evaluate it at a point defined over $\overline{K}$ using complex arguments). But when n tends to $+\infty$, $G_{\beta_n}\big(t(Q)\big)$ tends to $G_1\big(0, t(Q)\big) - t(Q)^{-1}$ and the right hand side tends to $E_1(\tilde{z}(Q), L) - t(Q)^{-1}$ which concludes the proof of (iii).

It remains to prove (ii). First note that if $\alpha \in \mathbf{a}$, there is nothing to prove as $E_1(\tilde{\alpha}, L) = 0$. So suppose $\alpha \notin \mathbf{a}$ and write $\alpha = \alpha_0 + \alpha_1$ where $\alpha_1 \in \mathbf{p}^{-\infty}\mathbf{a}$ and $v_{\mathbf{p}}(\alpha_0) \geq 0$. Then, using (i) and (iii) with $\alpha = \alpha_0$ and Q corresponding to $\tilde{\alpha}_1$, we deduce that if (ii) is true for α_0 then it is true for α and we are reduced to the case when $\alpha \notin \mathbf{a}$ and $v_{\mathbf{p}}(\alpha) \geq 0$. Now, if $\beta \in O_K$, then $F_\beta(z) = E_1(\beta z, L) - \overline{\beta}E_1(z, L)$ is an algebraic function on E whose reduction mod p is defined, so if z corresponds to a point defined over $\overline{K}$ which does not reduce to a β-division point mod p, then $F_\beta(z) \in \hat{O}$. One deduces from this that if (ii) is true for α it is true for $\beta\alpha$, and if β is prime to p and (ii) is true for α then it is true for $\beta^{-1}\alpha$. Now let h be the class number of K and let π be a generator of $\mathbf{p}^h$. By the previous reductions, it suffices to verify (ii) for $\alpha = \overline{\pi}^{-n}$ and $n \geq 1$. Let $k \in \mathbf{Z}$ and $\alpha_n = \overline{\pi}^{-n}$. Then

$$E_1(k\tilde{\alpha}_n, L) = H_1(1, k\tilde{\alpha}_n, 0, L) = H_1(1, 0, k\tilde{\alpha}_n, L) = \frac{1}{\pi^n} \sum_{\substack{\gamma \in \pi^{-n}L/L \\ \gamma \neq 0}} \langle \gamma, \tilde{k} \rangle_L E_1(\gamma, L).$$

Let $\epsilon = \langle \gamma, \tilde{1} \rangle_L$. Then using the isomorphism ι, we see that

$$E_1(k\tilde{\alpha}_n, L) = \frac{1}{\pi^n} \sum_{\substack{\epsilon^{p^{nh}} = 1 \\ \epsilon \neq 1}} \epsilon^k G_1\big(0, \iota^{-1}(\epsilon - 1)\big).$$

So

$$E_1(\tilde{\alpha}_n, L) = E_1(\tilde{\alpha}_n, L) - E_1(0, L) = \frac{1}{\pi^n} \sum_{\substack{\epsilon^{p^{nh}} = 1 \\ \epsilon \neq 1}} (\epsilon - 1) G_1\big(0, \iota^{-1}(\epsilon - 1)\big).$$

But as $tG_1\big(0, \iota^{-1}(t)\big) \in -\eta_p + tI_{p,E}[[t]]$, we obtain the desired result by applying the following obvious identities:

$$\sum_{\substack{\epsilon^{p^{nh}} = 1 \\ \epsilon \neq 1}} (\epsilon - 1)^i \equiv \begin{cases} -1 \pmod{\pi^n} & \text{if } i = 0 \\ 0 \pmod{\pi^n} & \text{if } i \geq 1 \end{cases}.$$

Corollary: $\eta_p = \lim_{n\to\infty} p^n E_1(p^{-n}\omega_\infty, L)$.

Thus η_p appears as the p-adic period of the differential form $\eta = (x + a_2(L))(dx/y)$ integrated along the cycle γ_1 viewed in $T_p(E)$ in the obvious way (cf. [P-R], [de S]). Using this remark, it is easy to show that the isomorphism between $\overline{K}(\eta_\infty)$ and $\overline{K}(\eta)$ does not depend on the choice of E or γ_1; it depends only on the embeddings of $\overline{K}$ into $\mathbf{C}$ and $\mathbf{C}_p$.

Proposition 11: Let $\alpha \in (K - \mathbf{p}^{-\infty}\mathbf{a})$ and let $G_{k,j}(\alpha, t) = \mathcal{H}\big(E_{k,j}(\tilde{\alpha} + \lambda(t), L)\big)$. Then

(i) $G_{k,j}(\alpha, t) \in \hat{O}[[t]] \otimes \mathbf{Q}_p$.

(ii) If Q is a $\mathbf{p}^\infty$-division point, then $G_k\big(\alpha, t(Q)\big) = E_{k,j}(\tilde{\alpha} + \tilde{z}(Q), L)$.

Proof: If $k = 0$, then (i) follows from Proposition 10 and the fact that $E_{0,j} = -\frac{d}{dz}E_{0,j-1}$ and $\frac{d}{dz} = \frac{dt}{dz}\frac{d}{dt}$ where $\frac{dt}{dz} \in 1 + t\hat{O}[[t]]$, and (ii) follows from the fact that $E_{0,j}$ is a rational function on E. The general case follows then from the existence of $P_{k,j}$ (Proposition 9).

Proposition 12: Let $\alpha \in K$, $v_{\mathbf{p}}(\alpha) \geq 0$. Let $\Delta_\alpha(z) = \langle z, \tilde{\alpha}\rangle_L$. Then

(i) $\mathcal{H}\Big(\Delta_\alpha\big(\lambda(t)\big)\Big) \in \hat{O}[[t]]$.

(ii) If Q is a $\mathbf{p}^\infty$-division point, then $\mathcal{H}\Big(\Delta_\alpha\big(\lambda(t)\big)\Big)$ evaluated at $t = t(Q)$ is equal to $\Delta_\alpha\big(\tilde{z}(Q)\big)$ where $z(Q)$ has to be chosen so that $\overline{\alpha}z(Q) \in \mathbf{p}^{-\infty}\mathbf{a}$ (this restriction being due to the fact that $\Delta_\alpha(z)$ is not periodic of period L in z).

Proof: Everything is obvious once we have proved that $\mathcal{H}\Big(\Delta_\alpha\big(\lambda(t)\big)\Big) = \big(1 + \iota(t)\big)^{\overline{\alpha}}$. But we have $\Delta_\alpha(z) = exp\big(A(L)^{-1}(z\overline{\alpha\omega}_\infty - \alpha\omega_\infty\overline{z})\big)$. So using the identity $A(L) = -\overline{\omega}_\infty\eta_\infty^{-1}$ we obtain: $\mathcal{H}\big(\Delta_\alpha(z)\big) = exp(-\eta_\infty\overline{\alpha}z)$, and p-adically, $\mathcal{H}\Big(\Delta_\alpha\big(\lambda(t)\big)\Big) = exp(-\eta_p\overline{\alpha}\lambda(t))$. As λ is an isomorphism from $\hat{E}$ to $\mathbf{G}_a$, we find that $\iota(t) = exp\big(u\lambda(t)\big) - 1$ for some $u \in \mathbf{C}_p$. Equating terms of degree 1 in t gives $u = -\eta_p$ which allows us to conclude.

Proposition 13: Let $\alpha \in K - \mathbf{p}^{-\infty}\mathbf{a}$ and $\beta \in K$ such that $v_{\mathbf{p}}(\beta) \geq 0$. Then for $1 \leq j \leq k$ we have:

(i) $\mathcal{H}\Big(H_k\big(j, \tilde{\alpha} + \lambda(t), \tilde{\beta}, L\big)\Big) \in \hat{O}[[t]] \otimes \mathbf{Q}_p$.

(ii) If Q is a $\mathbf{p}^\infty$-division point then the previous series evaluated at $t = t(Q)$ is equal to $H_k\big(j, \tilde{\alpha} + \tilde{z}(Q), \tilde{\beta}, L\big)$, where $z(Q)$ has to be chosen in such a way that $\overline{\beta}z(Q) \in \mathbf{p}^{-\infty}\mathbf{a}$.

Proof: Choose $b \in O_K$ satisfying $(b, \mathbf{p}) = 1$ and $\overline{b}\beta \in \mathbf{a}$. Then formula (25) gives:

$$H_k\big(j, \tilde{\alpha} + \lambda(t), \tilde{\beta}, L\big) = \frac{\overline{b}^{k-j}}{b^j} \sum_{\gamma \in b^{-1}L/L} \langle \gamma, \overline{b}\tilde{\beta}\rangle_L E_{k-j,j}\Big(\gamma + \frac{\tilde{\alpha}}{b} + \frac{\lambda(t)}{b}, L\Big).$$

Since b is prime to $\mathbf{p}$, b^{-1} is an endomorphism of $\hat{E}$ and $b^{-1}\lambda(t) = \lambda([b^{-1}]t)$. Then (i) follows directly from Proposition 11 (i).

Now let Q be a $\mathbf{p}^n$-division point and let $b^* \in O_K$ be such that $b^*b \equiv 1 \pmod{\mathbf{p}^n}$. Then $[b^{-1}]t(Q) = t(b^*Q)$ and so by Proposition 11 (ii), we obtain that $\mathcal{H}\Big(H_k\big(j, \tilde{\alpha} + \lambda(t), \tilde{\beta}, L\big)\Big)$ evaluated at $t = t(Q)$ is equal to

$$\frac{\overline{b}^{k-j}}{b^j} \sum_{\gamma \in b^{-1}L/L} \langle \gamma, \overline{b}\tilde{\beta} \rangle_L E_{k-j,j}\big(\gamma + \tilde{\alpha}b^{-1} + b^*\tilde{z}(Q), L\big) = H_k\big(j, \tilde{\alpha} + bb^*\tilde{z}(Q), \tilde{\beta}, L\big),$$

which allows us to conclude.

Proposition 14: Let $\alpha \in K$ be such that $v_{\overline{\mathbf{p}}}(\alpha) \geq 0$ and $\beta \in K - \mathbf{p}^{-\infty}\mathbf{a}$. Then for $1 \leq j \leq k$

(i) $\mathcal{H}\Big(H_k\big(j, \tilde{\alpha}, \tilde{\beta} + \lambda(t), L\big)\Big) \in \hat{O}[[t]] \otimes \mathbf{Q}_p$.

(ii) If Q is a $\mathbf{p}^\infty$-division point, then the previous series evaluated at $t = t(Q)$ is equal to $H_k\big(j, \tilde{\alpha}, \tilde{\beta} + \tilde{z}(Q), L\big)$,

Proof: Everything follows easily from the previous proposition and the functional equation for $H_k(j, u, z, L)$ which says that

$$\mathcal{H}\Big(H_k\big(j, \tilde{\alpha}, \tilde{\beta} + \lambda(t), L\big)\Big) = \big(1 + \iota(t)\big)^{\overline{\alpha}} \mathcal{H}\Big(H_k\big(k + 1 - j, \tilde{\beta} + \lambda(t), \tilde{\alpha}, L\big)\Big).$$

Note however that Proposition 5 (ii) would give some restrictions as to the possible value of $z(Q)$ which makes (ii) work, but since $H_k(j, u, z, L)$ is periodic of period L in z this restriction is unnecessary.

Proposition 15: Let $\alpha, \beta \in K - \mathbf{a}$. Let $k, l \in \mathbf{N}$ and $G_{k,l,\alpha,\beta}(t_1, t_2)$ be the power series defined by

$$G_{k,l,\alpha,\beta}(t_1, t_2) = \mathcal{H}\Big(H_{k+l}\big(l, \tilde{\alpha} + \lambda(t_1), \tilde{\beta} + \lambda(t_2), L\big)\Big).$$

If $\alpha, \beta \in O_{K,p}$, then

(i) $G_{k,l,\alpha,\beta}(t_1, t_2) \in I_{p,E}[[t_1, t_2]]$.

(ii) If Q_1, Q_2 are $\mathbf{p}^\infty$-division points, then

$$G_{k,l,\alpha,\beta}\big(t(Q_1), t(Q_2)\big) = H_{k+l}\big(l, \tilde{\alpha} + \tilde{z}(Q_1), \tilde{\beta} + \tilde{z}(Q_2), L\big),$$

where $z(Q_1)$ has been chosen so that $z(Q_1)\big(\overline{\beta + z(Q_2)}\big) \in \mathbf{p}^{-\infty}\mathbf{a}$.

The proof of this proposition will need several lemmas (as well as the preceding propositions). First, call a power series $H(t_1, t_2) = \sum_{i,j} a_{i,j} t_1^i t_2^j$ "almost bounded" if, when i

is fixed, $a_{i,j}$ is bounded as j varies and if Q is a $\mathbf{p}^\infty$-division point, then $H\big(t_1, t(Q)\big)$, which converges because of what precedes, is a bounded power series in t_1. If H is almost bounded, then if Q_1 and Q_2 are $\mathbf{p}^\infty$-division points we can define $H\big(t(Q_1), t(Q_2)\big)$ as the value of $H\big(t_1, t(Q_2)\big)$ at $t_1 = t(Q_1)$.

Lemma 16: If H is an almost bounded power series satisfying $H\big(t(Q_1), t(Q_2)\big) = 0$ whenever Q_1 and Q_2 are $\mathbf{p}^\infty$-division points, then H is identically equal to 0.

Proof: If you fix Q_2, then the series $H\big(t_1, t(Q_2)\big)$ is bounded and is equal to 0 if $t_1 = t(Q)$ where Q is a $\mathbf{p}^\infty$-division point. This implies that $H\big(t_1, t(Q_2)\big)$ is equal to 0 as a power series in t_1, hence for all $i \geq 0$, $\sum_{j=0}^{\infty} a_{i,j}\big(t(Q_2)\big)^j = 0$. But this is true for all $\mathbf{p}^\infty$-division points Q_2, so $a_{i,j} = 0$ for all i and j.

Lemma 17: $G_{k,l,\alpha,\beta}$ is almost bounded.

Proof: We have

$$G_{k,l,\alpha,\beta}(t_1, t_2) = \sum_{i=0}^{\infty} \frac{\big(-\lambda(t_1)\big)^i}{i!} \mathcal{H}\Big(H_{k+l+i}\big(l+i, \tilde{\alpha}, \tilde{\beta} + \lambda(t_2), L\big)\Big) = \sum_{i,j} a_{i,j} t_1^i t_2^j.$$

By Proposition 14 (i) and the fact that $\lambda(t)$ has no constant term, we obtain that when i is fixed, $a_{i,j}$ is bounded as j varies. Moreover, by Proposition 14 (ii), if Q_2 is a $\mathbf{p}^\infty$-division point then:

$$\begin{aligned} G_{k,l,\alpha,\beta}\big(t_1, t(Q_2)\big) &= \sum_{i=0}^{\infty} \frac{\big(-\lambda(t_1)\big)^i}{i!} H_{k+l+i}\big(l+i, \tilde{\alpha}, \tilde{\beta} + \tilde{z}(Q_2), L\big) \\ &= \mathcal{H}\Big(H_{k+l}\big(l, \tilde{\alpha} + \lambda(t_1), \tilde{\beta} + \tilde{z}(Q_2), L\big)\Big). \end{aligned}$$

Then Proposition 13 (i) allows us to conclude. But in addition, Proposition 13 (ii) gives (ii) of Proposition 15.

Lemma 18: Let $\delta \in O_{K,p}$, $d \in O_K$ satisfy $\bar{d}\delta \in \mathbf{a}$ and $(d, p) = 1$. Let π be a generator of $\mathbf{p}^h$ and $\delta_0 \in \mathbf{a}$ satisfy $\delta_0 \equiv \delta \pmod{\bar{\pi}^n}$. Then

$$S = \sum_{\gamma \in d\pi^{-n} L/dL} \langle \tilde{\delta}, \gamma \rangle_L H_1(1, z, u + \gamma, L) = \pi^n \langle u, \tilde{\delta}_0 \rangle_L H_1\Big(1, \frac{z - \tilde{\delta}_0}{\bar{\pi}^n}, \pi^n u, L\Big).$$

Proof: We have

$$S = \sum_{\gamma \in d\pi^{-n} L/dL} \sum_{\omega \in L} \frac{\langle \tilde{\delta} + \omega, \gamma \rangle_L}{\omega + z} \langle \omega, u \rangle_L.$$

But

$$\sum_{\gamma\in d\pi^{-n}L/dL}\langle\tilde{\delta}+\omega,\gamma\rangle_L=\begin{cases}p^{nh} & \text{if } \tilde{\delta}_0+\omega\in\overline{\pi}^nL\\ 0 & \text{otherwise}\end{cases}.$$

The result follows easily using formula (24).

Lemma 19: Let $a.b\in\mathbf{Z}$, and set $G_{\alpha,\beta}=G_{0,1,\alpha,\beta}$. Then we have:

$$\Sigma_{a,b,n,m}\overset{\text{def}}{=}\frac{1}{p^{h(n+m)}}\sum_{Q_1\in E_{\pi^m}}\sum_{Q_2\in E_{\pi^n}}\epsilon(Q_1)^{-a}\epsilon(Q_2)^{-b}G_{\alpha,\beta}\big(t(Q_1),t(Q_2)\big)$$
$$=\langle\tilde{\alpha},\tilde{\beta}\rangle_L\overline{\pi}^{-(n+m)}H_1\big(1,(\pi^m/\overline{\pi}^n)(\tilde{\alpha}+\tilde{a}),(\pi^n/\overline{\pi}^m)(\tilde{\beta}-\tilde{\beta}_0+\tilde{b}),L\big),$$

where $\beta_0\in\mathbf{a}$ and $\beta_0\equiv\beta\pmod{\overline{\pi}^m}$.

Proof: Using Lemma 18 and the value of $G_{\alpha,\beta}\big(t(Q_1),t(Q_2)\big)$, we obtain

$$\frac{1}{p^{hn}}\sum_{Q_2\in E_{p^n}}\epsilon(Q_2)^{-b}G_{\alpha,\beta}\big(t(Q_1),t(Q_2)\big)$$
$$=\langle\tilde{a},\tilde{\beta}\rangle_L\overline{\pi}^{-n}H_1\big(1,(\tilde{\alpha}+\tilde{z}(Q_1)-\tilde{a})/\overline{\pi}^n,\pi^n\tilde{\beta},L\big)$$
$$=\overline{\pi}^{-n}\langle\tilde{\beta},\tilde{\alpha}+\tilde{z}(Q_1)\rangle_LH_1\big(1,\pi^n\tilde{\beta},(\tilde{\alpha}+\tilde{z}(Q_1)-\tilde{a})/\overline{\pi}^n,L\big).$$

Now using Lemma 18 again and writing $\langle\tilde{\beta},\tilde{z}(Q_1)\rangle_L=\langle\pi^n\tilde{\beta},\overline{\pi}^{-n}\tilde{z}(Q_1)\rangle_L$ and not forgetting that $z(Q_1)\in(\overline{\pi}^n/\pi^m)\mathbf{a}$, we find that $\Sigma_{a,b,n,m}$ is equal to

$$\overline{\pi}^{-(n+m)}\langle\tilde{\beta},\tilde{\alpha}\rangle_L\langle\tilde{\alpha}+\tilde{a},\tilde{\beta}_0-\tilde{b}\rangle_LH_1\big(1,(\pi^n/\overline{\pi}^m)(\tilde{\beta}-\tilde{\beta}_0+\tilde{b}),(\pi^m/\overline{\pi}^n)(\tilde{\alpha}+\tilde{a}),L\big).$$

The result follows from the functional equation of H_1.

Lemma 20: Let $\gamma.\delta\in K-\mathbf{a}$ verify $v_{\mathbf{p}}(\gamma)\geq 0$, $v_{\mathbf{p}}(\delta)\geq 0$, $v_{\mathbf{p}}(\gamma)+v_{\overline{\mathbf{p}}}(\delta)\geq 0$. Then $H_1(1,\gamma,\delta,L)\in I_{p.E}$.

Proof: Choose $d\in O_K$ such that $v_{\mathbf{p}}(d)=sup\big(0,-v_{\overline{\mathbf{p}}}(\delta)\big)$, $v_{\overline{\mathbf{p}}}(d)=0$ and $\overline{d}\delta\in\mathbf{a}$. By formula (25), $H_1(1,\gamma,\delta,L)=(1/d)\sum_{y\in d^{-1}L/L}\langle y,\overline{d}\tilde{\delta}\rangle_LE_1\big((\tilde{\gamma}/d)+y,L\big)$. Writing $(d)=\mathbf{p}^k\mathbf{d}$ where $\mathbf{d}$ is prime to p, we can write $y\in d^{-1}L/L$ in a unique way as $\tilde{z}_0+\tilde{z}_1$ where $z_0\in\mathbf{d}^{-1}\mathbf{a}/\mathbf{a}$ and $z_1\in\mathbf{p}^{-k}\mathbf{a}/\mathbf{a}$. Set $\delta'=\overline{d}\delta$ and $\gamma'=d^{-1}\gamma$. We obtain

$$H_1(1,\gamma,\delta.L)=d^{-1}\sum_{z_0\in\mathbf{d}^{-1}\mathbf{a}/\mathbf{a}}\langle\tilde{z}_0,\tilde{\delta}'\rangle_L\sum_{z_1\in\mathbf{p}^{-k}\mathbf{a}/\mathbf{a}}\langle\tilde{z}_1,\tilde{\delta}'\rangle_LE_1(\tilde{\gamma}'+\tilde{z}_0+\tilde{z}_1,L).$$

By Proposition 10, we can write

$$d^{-1}\sum_{z_1\in p^{-k}\mathbf{a}/\mathbf{a}}\langle\tilde{z}_1,\tilde{\delta}'\rangle_LE_1(\tilde{\gamma}'+\tilde{z}_0+\tilde{z}_1,L)=d^{-1}\sum_{\epsilon^{p^k}=1}\epsilon^{\overline{\delta}'}G_1\big(\gamma'+z_0,\iota^{-1}(\epsilon-1)\big).$$

But $G_1(\gamma'+z_0,t) \in M\big(P(\gamma'+z_0)\big)$ and with the exception of the constant term has integral coefficients. As $\gamma'+z_0 \in O_{K,p}$, $P(\gamma'+z_0)$ is defined over the maximal unramified extension of M which implies that $G_1\big(\gamma'+z_0,\iota^{-1}(w)\big) \in E_1(\tilde{\gamma}'+\tilde{z}_0,L)+wI_{p,E}[[w]]$. But we also have $E_1(\tilde{\gamma}'+\tilde{z}_0,L) \equiv \eta_p(\overline{\gamma}'+\overline{z}_0) \equiv \eta_p\overline{\gamma}' \pmod{I_{p,E}}$, so we see that $G_1\big(\gamma'+z_0,\iota^{-1}(w)\big)-\eta_p\overline{\gamma}' \in I_{p,E}[[w]]$. As $\sum_{\epsilon^{p^k}=1}(\epsilon-1)^i\epsilon^{\overline{\delta}'} \in \mathbf{Z}$ and is congruent to 0 (mod p^k), we finally obtain

$$H_1(1,\gamma,\delta,L)-\eta_p\overline{\gamma}' \sum_{y\in d^{-1}L/L} \langle y,\tilde{\delta}'\rangle_L \;\in\; (p^k/d)I_{p,E},$$

which gives the result, since $(p^k/d) \in I_{p,E}$ and $\sum_{y\in d^{-1}L/L}\langle y,\delta'\rangle_L = 0$ when $\delta \notin \mathbf{a}$.

Corollary: $\Sigma_{a,b,n,m} \in I_{p,E}$.

Define a measure $\mu_{\alpha,\beta}$ on $Y_{K,p} = O_{\mathbf{p}} \times O_{\overline{\mathbf{p}}}$ by

$$\mu_{\alpha,\beta}\big((a+\mathbf{p}^{mh}) \times (b+\overline{\mathbf{p}}^{nh})\big) = \Sigma_{a,b,n,m}.$$

This is an $I_{p,E}$-valued measure. Let

$$H(t_1,t_2) = \int_{Y_{K,p}} \big(1+\iota(t_1)\big)^x\big(1+\iota(t_2)\big)^y \, d\mu_{\alpha,\beta}(x,y);$$

then $H(t_1,t_2) \in I_{p,E}[[t_1,t_2]]$ and if Q_1, Q_2 are p^∞-division points, then by construction of $\mu_{\alpha,\beta}$, $H\big(t(Q_1),t(Q_2)\big) = G_{\alpha,\beta}\big(t(Q_1),t(Q_2)\big)$ and so $H = G_{\alpha,\beta}$ by virtue of Lemma 16. This concludes the proof of Proposition 15 for $k=0$ and $l=1$. The general case follows from the following identity:

$$H_{k+j}(j,\tilde{\alpha}+z,\tilde{\beta}+u,L) = \langle u,\tilde{\alpha}+z\rangle_L\Big(-\frac{\partial}{\partial u}\Big)^k\Big[\langle\tilde{\alpha}+z,u\rangle_L\Big(-\frac{\partial}{\partial z}\Big)^{j-1}H_1(1,\tilde{\alpha}+z,\tilde{\beta}+u,L)\Big],$$

which yields

$$G_{k,j,\alpha,\beta}(t_1,t_2) = \big(1+\iota(t_2)\big)^{\overline{\alpha}}\Big(-\frac{\partial}{\partial\lambda(t_2)}\Big)^k\Big[\big(1+\iota(t_2)\big)^{-\overline{\alpha}}\Big(-\frac{\partial}{\partial\lambda(t_1)}\Big)^{j-1}G_{\alpha,\beta}(t_1,t_2)\Big]. \quad (30)$$

Proposition 21: If Q_1 and Q_2 are $\mathbf{p}^\infty$-division points, then

$$G_{\alpha,\beta}\big(t_1 \oplus t(Q_1), t_2 \oplus t(Q_2)\big) = \big(1+\iota(t_2)\big)^{-\overline{z(Q_1)}}G_{\alpha+z(Q_1),\beta+z(Q_2)}(t_1,t_2).$$

where $z(Q_1)$ has to be chosen so that $z(Q_1)\big(\overline{\beta+z(Q_2)}\big) \in \mathbf{p}^{-\infty}\mathbf{a}$.

Proof: Set $G'_{k,j,\alpha,\beta}(t_1,t_2) = (1+\iota(t_2))^{-\overline{\alpha}} G_{k,j,\alpha,\beta}(t_1,t_2)$. Then formula (20) becomes:

$$\Big(-\frac{\partial}{\partial\lambda(t_1)}\Big)^{j-1}\Big(-\frac{\partial}{\partial\lambda(t_2)}\Big)^{k} G'_{\alpha,\beta}(t_1,t_2) = G'_{k,j,\alpha,\beta}(t_1,t_2),$$

so that, as power series, we get

$$G'_{\alpha,\beta}(t_1\oplus w_1, t_2\oplus w_2) = \sum_{j,k}\frac{\big(-\lambda(t_1)\big)^j}{j!}\frac{\big(-\lambda(t_2)\big)^k}{k!} G'_{k,j+1,\alpha,\beta}(w_1,w_2).$$

Now, let $w_1 = t(Q_1)$ and $w_2 = t(Q_2)$. Using Proposition 15 (ii) and Proposition 12, we obtain:

$$G_{\alpha,\beta}(t_1\oplus t(Q_1), t_2\oplus t(Q_2)) =$$
$$(1+\iota(t_2))^{\overline{\alpha}}\sum_{j,k}\frac{\big(-\lambda(t_1)\big)^j}{j!}\frac{\big(-\lambda(t_2)\big)^k}{k!} H_{k+j+1}\big(j+1,\tilde{\alpha}+\tilde{z}(Q_1),\tilde{\beta}+\tilde{z}(Q_2),L\big).$$

But using (30) applied to $t_1 = t_2 = 0$ and $\alpha = \alpha + z(Q_1)$, $\beta = \beta + z(Q_2)$, we find that:

$$\sum_{j,k}\frac{\big(-\lambda(t_1)^j\big)}{j!}\frac{\big(-\lambda(t_2)^k\big)}{k!} H_{k+j+1}\big(j+1,\tilde{\alpha}+\tilde{z}(Q_1),\tilde{\beta}+\tilde{z}(Q_2),L\big)$$

is the Taylor expansion in $-\lambda(t_1), -\lambda(t_2)$ of $(1+\iota(t_2))^{-\overline{\alpha}-\overline{z}(Q_1)} G_{\tilde{\alpha}+\tilde{z}(Q_1),\tilde{\beta}+\tilde{z}(Q_2)}(t_1,t_2)$, which concludes the proof.

If $\mathbf{a}$ is a fractional ideal of K, let $K(z_1,z_2,\mathbf{a}) = \sum_{\omega\in\mathbf{a}}\frac{1}{\omega+z_1}(\omega+z_1 \mid z_2)_\infty$. If $1_{\mathbf{a}}$ is the characteristic function of $\mathbf{a}$, then we have $K(z_1,z_2,\mathbf{a}) = K\big(z_1,z_2,1_{\mathbf{a}},(1)\big)$ in the notations of part II. Set $w_i = exp(-z_i) - 1$ for $i = 1,2$.

Proposition 22: Let $\delta\in K$, $\beta_1\in K-\delta O_K$ and $\beta_2\in K-(\delta O_K)^\vee$. Then

(i) $\mathcal{H}\big(\frac{1}{2\pi i}K(\beta_1+\frac{z_1}{2\pi i},\beta_2+\frac{z_2}{2\pi i},\delta O_K)\big)\in\overline{K}(\eta_\infty)[[z_1,z_2]]$.

(ii) If moreover δ is a unit in $O_{K,p}$, β_1 and β_2 belong to $O_{K,p}$ and $W_{\delta,\beta_1,\beta_2}(w_1,w_2)\in \mathbf{C}_p[[w_1,w_2]]$ is equal to $\mathcal{H}\big(\frac{1}{2\pi i}K(\beta_1+\frac{z_1}{2\pi i},\beta_2+\frac{z_2}{2\pi i},\delta O_K)\big)$ expressed in w_1,w_2, then $W_{\delta,\beta_1,\beta_2}\in I_p[[w_1,w_2]]$.

(iii) If $\gamma_1,\gamma_2\in K/\mathbf{p}^{-\infty}O_{K,p}$ and $\epsilon_i = \chi_{\gamma_i}(1)$, then

$$W_{\delta,\beta_1,\beta_2}\big((1+w_1)\epsilon_1-1,(1+w_2)\epsilon_2-1\big) =$$
$$\mathcal{H}\Big(\frac{1}{2\pi i}K(\beta_1+\hat{\gamma}_1+\frac{z_1}{2\pi i},\beta_2+\hat{\gamma}_2+\frac{z_2}{2\pi i},\delta O_K)(-\beta_2\mid\frac{z_1}{2\pi i})_\infty\Big),$$

where $\hat{\gamma}_1$ is a representative of γ_1 in $\mathbf{p}^{-\infty}\delta O_K$ and $\hat{\gamma}_2$ a representative of γ_2 in $\mathbf{p}^{-\infty}\big(\delta O_K + (\beta_1) + (\gamma_1)\big)^{\vee}$.

(iv) If $\beta \in K$, then $\mathcal{H}\big((\beta \mid \frac{z_1}{2\pi i})_\infty\big) = (1+w_1)^{\overline{\beta}}$.

Proof: Part (iv) is obvious. To prove (i), (ii) and (iii), let us introduce an elliptic curve E with Weierstrass model defined over the ring of integers of the Hilbert class field of K with good reduction at all places above p and j-invariant equal to $j(O_K)$. This implies that the period lattice of E has the form $\omega_\infty(E)O_K$ for some $\omega_\infty(E) \in \mathbf{C}^*$. If $O_K = \mathbf{Z} + \mathbf{Z}\tau$, then $\eta_\infty(E) = \frac{2\pi i}{\omega_\infty(E)}\frac{1}{\overline{\tau}-\tau}$ and $\eta_p(E) \in I_{\mathbf{p}}^*$. Now, straightforward computation yields

$$\begin{aligned}
\frac{1}{2\pi i}K(\frac{z_1}{2\pi i},\frac{z_2}{2\pi i},\delta O_K) &= \frac{1}{2\pi i}H_1\big(1,(\tau-\overline{\tau})|\delta|^2\frac{z_2}{2\pi i},\frac{z_1}{2\pi i},\delta O_K\big)\\
&= \frac{\omega_\infty}{2\pi i\delta}H_1\big(1,\frac{(\tau-\overline{\tau})\omega_\infty}{2\pi i}\overline{\delta}z_2,\frac{z_1}{\delta}\frac{\omega_\infty}{2\pi i},\omega_\infty O_K\big)\\
&= \frac{1}{\delta(\overline{\tau}-\tau)\eta_\infty}H_1\big(1,\overline{\delta}\frac{z_2}{\eta_\infty},\frac{z_1}{\eta_\infty}\frac{1}{\delta(\overline{\tau}-\tau)},\omega_\infty O_K\big).
\end{aligned}$$

Hence,

$$W_{\delta,\beta_1,\beta_2}(w_1,w_2) = \frac{1}{\delta(\overline{\tau}-\tau)\eta_{\mathbf{p}}}G_{\alpha_1,\alpha_2}\big([\overline{\delta}]\cdot\iota^{-1}(w_2),[\delta(\tau-\overline{\tau})]^{-1}\cdot\iota^{-1}(w_2)\big),$$

where ι is the isomorphism between $\hat{E}$ and $\mathbf{G}_m$ and $[\beta]$ is the endomorphism of $\hat{E}$ associated to β, $\alpha_1 = \overline{\delta}\beta_2$ and $\alpha_2 = \frac{1}{\delta(\overline{\tau}-\tau)}\beta_1$. Now (i), (ii) and (iii) are just reinterpretations of Propositions 15 and 21.

§3. Construction of p-adic measures attached to generalized Eisenstein-Kronecker series.

If $\phi \in \mathcal{S}_T(H)$ where $T \cap |(p)| = \emptyset$, set $\tilde{\phi} = \phi_{\mathbf{p}} * \phi$ where $\phi_{\mathbf{p}} = N(\mathbf{d}_{H,\mathbf{p}})^{-\frac{1}{2}} 1_{\mathbf{d}_H^{-1}} \in \mathcal{S}_{|\mathbf{p}|,H}$ is the Fourier transform of the characteristic function of $O_{|\overline{\mathbf{p}}|}$ considered as an element of $\mathcal{S}_{|\overline{\mathbf{p}}|,H^\vee}$. Let $I_{p,H}$ be the ring of integers of the completion of the maximal unramified extension of the field generated over $\mathbf{Q}_p$ by all conjugates of H and $sqrtN(\mathbf{d}_{H,\mathbf{p}})$. The aim of this paragraph is to prove the following theorem:

Theorem 23: Let $\mathcal{B}$ be a finite set of bases of H over K. Then there exists $S = S_2(\mathcal{B}) \in \mathcal{P}(H)$ and $S' = S_2'(\mathcal{B}) \in \mathcal{P}(H^\vee)$ such that for all $T \in \mathcal{P}(H)$ satisfying $T \cap |(p)| = \emptyset$, all $\phi \in \mathcal{S}_T(H)$, all $(\mathbf{b}_1, \mathbf{b}_2) \in C_{T \cup |(p)|}(S, S')$, we have:

(i) $\mathcal{H}((2\pi i)^{-n} K(\frac{z_1}{2\pi i}, \frac{z_2}{2\pi i}, \tilde{\phi}_{\mathbf{b}_1,\mathbf{b}_2}, \mathcal{B})) \in \overline{K}(\eta_\infty)[[z_1, z_2]]$ and is the Fourier Laplace transform of an $I_{p,H}$-valued measure $\mu_{\mathbf{b}_1,\mathbf{b}_2,\phi,\mathcal{B}}$ on $Y_{H,p}$.

(ii) Let o_1 be a locally constant function on Y_1 which can also be considered as an element of $\mathcal{S}_{|\overline{\mathbf{p}}|,H^\vee}$, and o_2 a locally constant function on Y_2 also considered as an element of $\mathcal{S}_{|\overline{\mathbf{p}}|,H}$. Then the Fourier-Laplace transform of $\phi_1 \phi_2 \mu_{\mathbf{b}_1,\mathbf{b}_2,\phi,\mathcal{B}}$ is

$$\mathcal{H}\Big((2\pi i)^{-n} K\big(\frac{z_1}{2\pi i}, \frac{z_2}{2\pi i}, \mathcal{F}_{|\overline{\mathbf{p}}|}(\phi_1) * \phi_2 * \phi_{\mathbf{b}_1,\mathbf{b}_2}, \mathcal{B}\big)\Big).$$

Lemma 24: Let A be a principal ideal domain having only a finite number of prime ideals and let K be its field of fractions. Let $v_1, \ldots, v_n \in A^n$ be a basis of K^n over K but not of A^n over A; then there exists $w \in A^n$ such that for all $1 \leq i \leq n$, $\det(v_1, \ldots, v_{i-1}, w, v_{i+1}, \ldots, v_n)$ is either 0 or a strict divisor of $\det(v_1, \ldots, v_n)$.

Proof: Choose $w_1 = \sum_{i=1}^n a_i v_i$ with $a_i \in K$, belonging to A^n but not to the submodule of A^n spanned by the v_i's. By the Chinese remainder theorem, we can find $b_i \in A$ such that $a_i - b_i = 0$ if $a_i \in A$ and $a_i - b_i = c_i/d_i$ where c_i is a unit in A and d_i is not invertible in A if $a_i \notin A$. Then $w = \sum_{i=1}^n (a_i - b_i) v_i$ obviously answers the question.

If $M \in M_n(K)$, we set $M \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix} = \begin{pmatrix} M_1(z) \\ \vdots \\ M_n(z) \end{pmatrix}$ and $F_M(z) = \det(M) \prod_{i=1}^n M_i(z)^{-1}$.

Lemma 25: Let A be as in Lemma 24 and $M \in GL_n(K)$. We can find a finite family $\mathcal{N}$ of elements of $GL_n(A)$ such that

$$F_M(z) = \sum_{N \in \mathcal{N}} F_N(z).$$

Proof: First note that $F_M(z)$ does not change if M is multiplied by a scalar; so we may suppose that $M \in M_n(A)$. Let $v_1, \ldots, v_n$ be the rows of this matrix. Then either $v_1, \ldots, v_n$ generate A^n in which case $M \in GL_n(A)$ and there is nothing to prove, or we can find w as in the preceding lemma. Let $v_{i,j}$ (resp. w_j) for $1 \leq j \leq n$ be the coordinates of v_i (resp. of w) and $M_{n+1}(z) = \sum_{i=1}^{n} w_j z_j$. Let N_i be the matrix whose j-th row is equal to v_j if $j \neq i$ and w if $j = i$. We obtain:

$$0 = \det \begin{pmatrix} v_{1,1} & \ldots & v_{1,n} & M_1(z) \\ \vdots & \ldots & \vdots & \vdots \\ v_{n,1} & \ldots & v_{n,n} & M_n(z) \\ w_1 & \ldots & w_n & M_{n+1}(z) \end{pmatrix} = \left(F_M(z) - \sum_{i=1}^{n} F_{N_i}(z)\right) \prod_{j=1}^{n+1} M_j(z),$$

where the first equality is obtained remarking that the last column is a linear combination of the others, and the second is obtained by developing the determinant with respect to the last column. Now, removing from the N_i those with determinant 0, we obtain $F_M(z) = \sum_N F_N(z)$, where the $\det(N)$ are strict divisors of $\det(M)$. We just go on with this process until we reach the desired result.

Corollary: Let B be a basis of H over K. We can find a finite family $\mathcal{C}(B)$ of bases of $\mathbf{d}_{H,\mathfrak{P}}^{-1} O_{H,p}$ over $O_{K,p}$ such that, for all $\phi \in \mathcal{S}(H)$, we have

$$K(z_1, z_2, \phi, B) = \sum_{C \in \mathcal{C}(B)} K(z_1, z_2, \phi, C).$$

Proof: Choose a basis C_o of $\mathbf{d}_{H,\mathfrak{P}}^{-1} O_{H,p}$ over $O_{K,p}$; then there exists $M \in GL_n(K)$ such that $B = MC_o$. We just apply Lemma 25 to this M and $A = O_{K,p}$ (which has only two prime ideals) to conclude.

Remark: Replacing $\mathcal{B}$ in theorem 23 by $\bigcup_{B \in \mathcal{B}} \mathcal{C}(B)$, we see that we can suppose that all elements of $\mathcal{B}$ are bases of $\mathbf{d}_{H,\mathfrak{P}}^{-1} O_{H,p}$ over $O_{K,p}$. On the other hand if $\mathcal{B}_1$ and $\mathcal{B}_2$ are finite sets of bases of H over K satisfying theorem 23, then setting $S_2(\mathcal{B}_1 \cup \mathcal{B}_2) = S_2(\mathcal{B}_1) \cup S_2(\mathcal{B}_2)$ and $S_2'(\mathcal{B}_1 \cup \mathcal{B}_2) = S_2'(\mathcal{B}_1) \cup S_2'(\mathcal{B}_2)$, we see that $\mathcal{B}_1 \cup \mathcal{B}_2$ also satisfies theorem 23. Hence, it is enough to treat the case where $\mathcal{B} = B$ and $B = (f_1, \ldots, f_n)$ is a basis of $\mathbf{d}_{H,\mathfrak{P}}^{-1} O_{H,p}$ over $O_{K,p}$ which we can take to be the B used in III, §1.

If $\mathbf{a} \in I(H)$, set $\tilde{\mathbf{a}} = \mathbf{d}_{H,\mathfrak{P}}^{-1} \mathbf{a}$. If ϕ belongs to $\mathcal{S}_T(H)$ with $T \cap |(p)| = \emptyset$, then $\tilde{\phi}$ is constant modulo $\tilde{\mathbf{a}}$ for some $\mathbf{a} \in I(H)$ satisfying $|\mathbf{a}| \subset T$; so by linearity, we are reduced to the case where $\tilde{\phi}$ is the characteristic function of $\alpha + \tilde{\mathbf{a}}$, where $|\mathbf{a}| \subset T$ and $\alpha \in \mathbf{d}_{H,\mathfrak{P}}^{-1} O'_{H,T}$. Let

$g_B: \mathbf{C}^n \to \mathbf{C}^n$ be defined by $g_B(z) = \big(Tr(f_1 z), \ldots, Tr(f_n z)\big)$. As B is a basis of $\mathbf{d}_{H,\mathbf{p}}^{-1} O_{H,p}$ over $O_{K,p}$, the image of $\mathbf{d}_{H,p}^{-1}$ by g_B is a lattice L contained in $(O_{K,p})^n$ such that $O_{K,p}L = (O_{K,p})^n$ and so contains $(\delta_B O_K)^n$ for some $\delta_B \in O_K$ relatively prime to p. There exists $\delta_{\mathbf{a}} \in K^*$ with $|(\delta_{\mathbf{a}})| \subset T_K$ such that $\mathbf{a}$ contains $\delta_{\mathbf{a}} O_H$. Hence, if we set $\delta_{\mathbf{a},B} = \delta_{\mathbf{a}}\delta_B$, we have $|(\delta_{\mathbf{a},B})| \subset T_K \cup |(\delta_B)|$ and $g_B(\tilde{\mathbf{a}})$ contains $(\delta_{\mathbf{a},B} O_K)^n$. Let Y be a set of representatives of $g_B(\tilde{\mathbf{a}})$ modulo $(\delta_{\mathbf{a},B} O_K)^n$. Using the identity $(z_1 \mid z_2)_\infty = \prod_{i=1}^n (Tr\, f_i z_1 \mid Tr\, f_i^\vee z_2)_\infty$, we obtain

$$K(z_1, z_2, \tilde{\phi}, B) = \frac{\det B}{\sqrt{N(\mathbf{d}_{H,\mathbf{p}})}} \sum_{\substack{y \in Y \\ y=(y_1,\ldots,y_n)}} \prod_{j=1}^n K\big(y_j + Tr(f_j(z_1+\alpha)), Tr(f_j^\vee z_2), \delta_{\mathbf{a},B} O_K\big). \tag{31}$$

On the other hand, a straightforward computation yields

$$K(z_1, z_2, \tilde{\phi}_{\mathbf{b}_1,\mathbf{b}_2}, B) = \sum_{\substack{\beta_1 \in \mathbf{b}_1^{-1}\tilde{\mathbf{a}}/\tilde{\mathbf{a}} \\ \beta_1 \notin \tilde{\mathbf{a}}}} \sum_{\substack{\beta_2 \in \mathbf{b}_2^{-1}\bar{\mathbf{b}}_1\tilde{\mathbf{a}}^\vee/\bar{\mathbf{b}}_1\tilde{a}^\vee \\ \beta_2 \notin \bar{\mathbf{b}}_1\tilde{\mathbf{a}}^\vee}} (-\beta_2 \mid \alpha + z_1)_\infty K(z_1+\beta_1, z_2+\beta_2, \tilde{\phi}, B). \tag{32}$$

Now, by Lemma 5, we can find $S(B) \in \mathcal{P}(H)$ and $S'(B) \in \mathcal{P}(H^\vee)$ such that if $(\mathbf{b}_1, \mathbf{b}_2) \in C_{T\cup|(p)|}(S(B), S'(B))$, then for all $\mathbf{a} \in I(H)$ with $|\mathbf{a}| \subset T$, all α in $\mathbf{d}_{H,\mathbf{p}}^{-1} O'_{H,T}$, all β_1, β_2 as above, we have $Tr(f_i(\alpha+\beta_1)) \notin \delta_{\mathbf{a},B} O_K$ and $Tr(f_i^\vee \beta_2) \notin (\delta_{\mathbf{a},B} O_K)^\vee$. On the other hand $Tr(f_i(\alpha+\beta_1))$ and $Tr f_i^\vee \beta_2$ belong to $O_{K,p}$, so putting together formulae (31) and (32) we see that $K(z_1, z_2, \tilde{\phi}_{\mathbf{b}_1,\mathbf{b}_2}, B)$ can be expressed in terms of the functions studied in Proposition 22. Thus part (i) of theorem 23 is a direct consequence of (i) and (ii) of this proposition. To prove (ii), we can restrict ourselves to the case $\phi_1 = \chi_{\gamma_1}$ and $\phi_2 = \chi_{\gamma_2}$, since the χ_γ form a basis of the space of locally constant functions. Now, using Proposition 22 (iii) along with formulae (31) and (32), we obtain that the Fourier-Laplace transform of $\chi_{\gamma_1}\chi_{\gamma_2}\mu_{\mathbf{b}_1,\mathbf{b}_2,\phi,B}$ is:

$$\mathcal{H}\Big(\frac{1}{(2\pi i)^n}(-\hat{\gamma}_2 \mid \frac{z_1}{2\pi i})_\infty K(\hat{\gamma}_1 + \frac{z_1}{2\pi i}, \hat{\gamma}_2 + \frac{z_2}{2\pi i}, \tilde{\phi}_{\mathbf{b}_1,\mathbf{b}_2}, B)\Big), \tag{33}$$

where $\hat{\gamma}_1$ is a representative of γ_1 in $\mathbf{p}^{-\infty}\mathbf{a}\bar{\mathbf{b}}_2$ and $\hat{\gamma}_2$ is a representative of γ_2 in $\mathbf{p}^{-\infty}\bar{\mathbf{b}}_1(\mathbf{a} + (\alpha) + (\gamma_1) + d_{H,\bar{\mathbf{p}}}^{-1})^\vee$, from which we can deduce the result after a straightforward computation (the main ingredient being the fact that if $\omega \in \hat{\gamma}_1 + \alpha + \mathbf{b}_1^{-1}\tilde{\mathbf{a}}$, then $\chi_{\gamma_2}(\omega) = (\hat{\gamma}_2 \mid \omega)_\infty$).

§4. Complements to Shintani's method.

In this paragraph, we shall use the results of the preceding paragraph to prove that $\Lambda_{\mathcal{B},\beta_1,\beta_2}(k,j,\phi)$ does not really depend on the choice of $\mathcal{B}$, β_1 or β_2.

Theorem 26: Let $\phi \in \mathcal{S}_{k,j,V}(H)$. We can define a number $\Lambda^?(k,j,\phi)$ such that

(i) For all $\mathcal{B} \in \mathcal{B}(V)$, there exist $S(\mathcal{B}) \in \mathcal{P}(H)$ and $S'(\mathcal{B}) \in \mathcal{P}(H^\vee)$ such that $\Lambda_{\mathcal{B},\beta_1,\beta_2}(k,j,\phi) = \Lambda^?(k,j,\phi)$ for all $\phi \in \mathcal{S}_T(H)$ and all $\big((\beta_1),(\beta_2)\big) \in C_T^0\big(S(\mathcal{B}),S'(\mathcal{B})\big)$,

(ii) $\Lambda^?(k,j,\phi) = \Lambda(k,j,\phi)$ if either $n = 1,2$ or $n \geq 3$ and $k = 0$ or $j = 1$,

(iii) $\Lambda^?(k,j,\phi \circ \gamma) = N_{H/K}(\gamma)^j \overline{N_{H/K}(\gamma)}^{-k} \Lambda^?(k,j,\phi)$,

(iv) $\Lambda^?(k,j,\phi) = (-1)^{n(j-1)} i^n \Lambda^?\big(j-1,k+1,\mathcal{F}_H(\phi)\big)$.

Remark: Of course, we expect that $\Lambda^?(k,j,\phi)$ is always equal to $\Lambda(k,j,\phi)$. In this direction, (iii) and (iv) are functional equations also satisfied by $\Lambda(k,j,\phi)$ (formulae (4) and (16)).

Proof: Suppose $\phi \in \mathcal{S}_T(H)$. By linearity, we can restrict ourselves to the case $\phi = \phi_\chi$ for some locally constant character χ of O_T^*. Choose a prime p splitting in K such that $T \cap |(p)| = \emptyset$ and $|\mathfrak{d}_H| \cap |(p)| = \emptyset$. Let $\mathcal{B} \in \mathcal{B}(V)$ and let $S(\mathcal{B}) = S_1(\mathcal{B}) \cup S_2(\mathcal{B}) \cup |(p)|$ and $S'(\mathcal{B}) = S_1'(\mathcal{B}) \cup S_2'(\mathcal{B}) \cup |(p)|$, where $S_1(\mathcal{B})$ and $S_1'(\mathcal{B})$ are defined in lemma 6 and $S_2(\mathcal{B})$ and $S_2'(\mathcal{B})$ are defined in theorem 23.

If μ is a measure on $Y_{H,p}$ and $\gamma \in O_{H,p}^*$, we define a measure $\mu \circ \gamma$ on $Y_{H,p}$ and a measure $\pi(\mu)$ on $Y_{K,p} = O_{\mathfrak{p}} \times O_{\overline{\mathfrak{p}}}$ by the following formulae:

$$\int_{Y_{H,p}} f(y_1,y_2)\, d(\mu \circ \gamma) = \int_{Y_{H,p}} f(\gamma y_1, \gamma^{-1} y_2)\, d\mu, \tag{34}$$

$$\int_{Y_{K,p}} f(x_1,x_2)\, d\,\pi(\mu) = \int_{Y_{K,p}} f\big(N(y_1),N(y_2)\big)\, d\mu. \tag{35}$$

Lemma 27: If $(\mathbf{b}_1,\mathbf{b}_2) \in C_T^0\big(S(\mathcal{B}),S'(\mathcal{B})\big)$ and $\gamma \in O_{H,p}^+$ satisfies $|(\gamma)|_K \cap (|\mathbf{b}_1| \cup |\overline{\mathbf{b}_2}|) = \emptyset$, then

$$\pi(\mu_{\mathbf{b}_1,\mathbf{b}_2,\phi\circ\gamma,\mathcal{B}}) = N_{H/K}(\gamma)\big(\pi(\mu_{\mathbf{b}_1,\mathbf{b}_2,\phi,\mathcal{B}} \circ \gamma)\big).$$

Proof: To prove that two measures μ_1 and μ_2 on $Y_{K,p}$ are equal, it is sufficient to verify that $\int_{Y_{K,p}} x_1^i \psi(x_2)\, d\mu_1 = \int_{Y_{K,p}} x_1^i \psi(x_2)\, d\mu_2$ for all $i \in \mathbf{N}$ and all locally constant functions ψ on $O_{\overline{\mathfrak{p}}}$. But we have

$$\int_{Y_{K,p}} x_1^i \psi(x_2)\, d\,\pi(\mu_{\mathbf{b}_1,\mathbf{b}_2,\phi\circ\gamma,\mathcal{B}}) = \int_{Y_{K,p}} N(y_1)^i \psi \circ N(y_2)\, d\mu_{\mathbf{b}_1,\mathbf{b}_2,\phi\circ\gamma,\mathcal{B}}, \tag{36}$$

and by Lemma 8, this is equal to ∇_1^i applied to the Fourier-Laplace transform of $\psi \circ N(y_2)\ d\mu_{\mathbf{b}_1,\mathbf{b}_2,\phi\circ\gamma,\mathcal{B}}$ and evaluated at $z_1 = z_2 = 0$. Now, as $\psi \circ N$ is locally constant, we can use theorem 23 (ii) to obtain (cf. formula (12))

$$\int_{Y_{K,p}} x_1^i \psi(x)\ d\,\pi(\mu_{\mathbf{b}_1,\mathbf{b}_2,\phi\circ\gamma,\mathcal{B}}) = \Lambda_{\mathcal{B}}(0, i+1, \psi \circ N * (\phi \circ \gamma)_{\mathbf{b}_1,\mathbf{b}_2}). \tag{37}$$

The same computation gives

$$N_{H/K}(\gamma) \int_{Y_{K,p}} x_1^i \psi(x)\ d\big(\pi(\mu_{\mathbf{b}_1,\mathbf{b}_2,\phi,\mathcal{B}} \circ \gamma)\big)$$

$$= N_{H/K}(\gamma)^{i+1} \int_{Y_{K,p}} N(y_1)^i \psi\big(N(\gamma^{-1}y_2)\big)\ d\mu_{\mathbf{b}_1,\mathbf{b}_2,\phi,\mathcal{B}}$$

$$= N_{H/K}(\gamma)^{i+1} \Lambda_{\mathcal{B}}(0, i+1, (\psi' * \phi)_{\mathbf{b}_1,\mathbf{b}_2}), \tag{38}$$

where $\psi'(y_2) = \psi\big(N(\gamma^{-1}y_2)\big)$.

Let $\phi' = (\psi' * \phi)_{\mathbf{b}_1,\mathbf{b}_2}$. Then $\psi \circ N * (\phi \circ \gamma)_{\mathbf{b}_1,\mathbf{b}_2}$ is neither more nor less than $\phi' \circ \gamma$. Now, using the corollary to theorem 3, we obtain $\Lambda_{\mathcal{B}}(0, i+1, \phi') = \Lambda(0, i+1, \phi')$ and $\Lambda_{\mathcal{B}}(0, i+1, \phi' \circ \gamma) = \Lambda(0, i+1, \phi \circ \gamma)$, and the desired equality follows from formula (16).

Corollary 1: Under the same hypothesis as in Lemma 27, we have

$$\Lambda_{\mathcal{B},\beta_1,\beta_2}(k, j, \phi \circ \gamma) = N_{H/K}(\gamma)^j \overline{N_{H/K}(\gamma)}^{-k} \Lambda_{\mathcal{B},\beta_1,\beta_2}(k, j, \phi).$$

Proof: By the very definition of $\Lambda_{\mathcal{B},\beta_1,\beta_2}(k, j, \phi)$ (cf. (19)) and of $\mu_{\mathbf{b}_1,\mathbf{b}_2,\phi,\mathcal{B}}$, we obtain, using lemma 8,

$$\Lambda_{\mathcal{B},\beta_1,\beta_2}(k, j, \phi) = \nu_{\beta_1,\beta_2}(k, j, \chi) \int_{Y_{K,p}} x_1^{j-1} x_2^k\ d\,\pi(\mu_{(\beta_1),(\beta_2),\phi,\mathcal{B}}), \tag{39}$$

and the result is an immediate consequence of lemma 27.

Corollary 2: Let $((\beta_1),(\beta_2))$ and $((\beta_1'),(\beta_2'))$ belong to $C_T^0\big(S(\mathcal{B}), S'(\mathcal{B})\big)$. Then

$$\Lambda_{\mathcal{B},\beta_1,\beta_2}(k, j, \phi) = \Lambda_{\mathcal{B},\beta_1',\beta_2'}(k, j, \phi).$$

Proof: Up to introducing an auxiliary $((\beta_1''),(\beta_2'')) \in C_T^0\big(S(\mathcal{B}), S'(\mathcal{B})\big)$, we may suppose $\big(|(\beta_1)|_K \cup |(\overline{\beta}_2)|_K\big) \cap \big(|(\beta_1')|_K \cup |(\overline{\beta}_2')|_K\big) = \emptyset$. As $(\phi_{(\beta_1),(\beta_2)})_{(\beta_1'),(\beta_2')} = (\phi_{(\beta_1'),(\beta_2')})_{(\beta_1),(\beta_2)}$, we have

$$\mu_{(\beta_1),(\beta_2),\phi_{(\beta_1'),(\beta_2')},\mathcal{B}} = \mu_{(\beta_1'),(\beta_2'),\phi_{(\beta_1),(\beta_2)},\mathcal{B}},$$

hence by formula (39) we have

$$\nu_{\beta_1,\beta_2}(k,j,\chi)^{-1}\Lambda_{\mathcal{B},\beta_1,\beta_2}(k,j,\phi_{(\beta_1'),(\beta_2')}) = \nu_{\beta_1',\beta_2'}(k,j,\chi)^{-1}\Lambda_{\mathcal{B},\beta_1',\beta_2'}(k,j,\phi_{(\beta_1),(\beta_2)}).$$

We obtain the result using formula (15) and the previous Corollary.

Corollary 3: $\Lambda^?(k,j,\phi)$ does not depend on the choice of $\big((\beta_1),(\beta_2)\big) \in C_T^0\big(S(\mathcal{B}),S'(\mathcal{B})\big)$.

It remains to check that $\Lambda^?(k,j,\phi)$ is independent of the choice of $\mathcal{B}$ and this follows from the following Lemma whose proof is identical to that of Lemma 27.

Lemma 28: Let $\mathcal{B}_1,\mathcal{B}_2 \in \mathcal{B}(V)$ and $S = S(\mathcal{B}_1)\cup S(\mathcal{B}_2)$, $S' = S'(\mathcal{B}_1)\cup S'(\mathcal{B}_2)$. If $\phi \in \mathcal{S}_T(H)$ and $\big((\beta_1),(\beta_2)\big) \in C_T^0(S,S')$ then $\pi(\mu_{(\beta_1),(\beta_2),\phi,\mathcal{B}_1}) = \pi(\mu_{(\beta_1),(\beta_2),\phi,\mathcal{B}_2})$.

This concludes the proof of (i). Now (ii) is a consequence of the corollary of theorem 3, while (iii) follows from corollary 1 of lemma 27 and (iv) from theorem 3 (v).

IV. Special values of Hecke L-functions.

Let ψ be a Hecke character of H (i.e. a continuous $\mathbf{C}^*$-valued character of $\mathbf{A}_H^*/H^*$). Let $\mathbf{m}_\psi$ be the conductor of ψ. We can associate to ψ a character of $I_{\mathbf{m}_\psi}(H)$, still denoted by ψ, by the formula: if $\mathbf{q} \in P(H) - |\mathbf{m}_\psi|$, then $\psi(\mathbf{q}) = \psi\big((1,\dots,1,w_\mathbf{q}^{-1},1,\dots,1)\big)$, where $w_\mathbf{q}$ is a uniformizing parameter of $O_\mathbf{q}$. If ψ is a Hecke character of H, let $\psi^\vee$ be the Hecke character of $H^\vee$ defined by $\psi^\vee(\mathbf{a}) = N(\mathbf{a})^{-1}\psi(\bar{\mathbf{a}}^{-1})$ if $\mathbf{a} \in I_{\overline{\mathbf{m}}_\psi}(H^\vee)$.

A Hecke character of H will be called admissible if there exists $k(\psi) \in \mathbf{N}$ and $j(\psi) \in \mathbf{N} - \{0\}$ such that for all $\alpha \equiv 1 \pmod{\mathbf{m}_\psi}$,

$$\psi((\alpha)) = \overline{N_{H/K}(\alpha)}^{k(\psi)} N_{H/K}(\alpha)^{-j(\psi)},$$

In particular, an admissible Hecke character is of type A_0 and critical in the sense of Deligne (cf. [D]). If ψ is admissible, so is $\psi^\vee$ and we have $k(\psi^\vee) = j(\psi) - 1$ and $j(\psi^\vee) = k(\psi) + 1$.

If ψ is a Hecke character of H and $S \in \mathcal{P}(H)$ contains $|\mathbf{m}_\psi|$, we set

$$L_S(\psi, s) = \sum_{\mathbf{b} \in I_S^+(H)} \frac{\psi(\mathbf{b})}{N(\mathbf{b})^s}, \tag{40}$$

and if $\dot{\mathbf{a}} \in Cl(O_H)$, we set

$$L_S(\psi, \dot{\mathbf{a}}, s) = \sum_{\mathbf{b} \in I_S^+(H) \cap \dot{\mathbf{a}}} \frac{\psi(\mathbf{b})}{N(\mathbf{b})^s}. \tag{41}$$

These two series converge for $Re(s) >> 0$ and define functions of s possessing meromorphic continuations to the whole s-plane, holomorphic except for a simple pole at $s = t + 1$ if $\psi(\mathbf{b}) = N(\mathbf{b})^t$. If ψ is an admissible Hecke character, we set

$$\Lambda_S(\psi) = \frac{\Gamma(j(\psi))^n}{(2\pi i)^{nj(\psi)}} L_S(\psi, 0) \quad \text{and} \quad \Lambda_S(\psi, \dot{\mathbf{a}}) = \frac{\Gamma(j(\psi))^n}{(2\pi i)^{nj(\psi)}} L_S(\psi, \dot{\mathbf{a}}. 0), \tag{42}$$

and if $S = |\mathbf{m}_\psi|$, we drop it from the notations.

If $\mathbf{q} \in P(H)$, let $\psi_\mathbf{q} \in \mathcal{S}_{|\mathbf{q}|,H}$ be defined by

$$\psi_\mathbf{q}(x_\mathbf{q}) = \begin{cases} \psi\big((1,\dots,1,x_\mathbf{q},1,\dots,1)\big) & \text{if } x_\mathbf{q} \in O_\mathbf{q}^* \\ 0 & \text{if } x_\mathbf{q} \notin O_\mathbf{q}^* \end{cases}. \tag{43}$$

Hence, if $\mathbf{q} \notin |\mathbf{m}_\psi|$, we have $\psi_\mathbf{q} = \delta_\mathbf{q}$. If $S \in \mathcal{P}(H)$ contains $|\mathbf{m}_\psi|$ and $\mathbf{a} \in I_S(H)$, let $\psi_{S,\mathbf{a}} \in \mathcal{S}(H)$ be defined by

$$\psi_{S,\mathbf{a}}(x) = \prod_{\mathbf{q} \in S} \psi_\mathbf{q}(x_\mathbf{q}) \prod_{\mathbf{q} \notin S} 1_{\mathbf{a}_\mathbf{q}^{-1}}(x), \tag{44}$$

where $1_{\mathfrak{a}_{\mathbf{q}}^{-1}}$ is the characteristic function of the fractional ideal of $H_{\mathbf{q}}$ generated by $\mathbf{a}^{-1}$. If $\mathbf{a} \in I_S(H)$ is in the ideal class $\dot{\mathbf{a}}$, writing $\mathbf{b} \in I_S^+(H) \cap \dot{\mathbf{a}}$ in the form $\mathbf{b} = (\beta)\mathbf{a}$, where $\beta \in \mathbf{a}^{-1}$ is uniquely determined modulo U_H, we see that $\Lambda_S(\psi, \mathbf{a})$ is neither more nor less than $\psi(\mathbf{a})\Lambda\big(k(\psi), j(\psi), \psi_{S,\mathbf{a}}\big)$.

Whenever it is defined, we have

$$\delta_{\mathbf{b}} * \psi_{S,\mathbf{a}} = \psi_{S,\mathbf{a}} - \psi_{S,\mathbf{ab}^{-1}} \quad \text{and} \quad \delta_{\mathbf{c}}^{\vee} * \psi_{S,\mathbf{a}} = \psi_{S,\mathbf{a}} - N(\mathbf{c})^{-1}\psi_{S,\mathbf{a}\bar{\mathbf{c}}}, \tag{45}$$

from which we deduce, using the fact that multiplication by an ideal induces a bijection on $Cl(O_H)$, that if A is a set of representatives of $Cl(O_H)$, we have

$$\sum_{\mathbf{a}\in A} \psi(\mathbf{a})\Lambda\big(k(\psi),j(\psi), \overset{k}{\underset{i=1}{*}} \delta_{\mathbf{b}_i} \overset{l}{\underset{j=1}{*}} \delta_{\mathbf{c}_j}^{\vee} * \psi_{S,\mathbf{a}}\big) =$$

$$\prod_{i=1}^{k}(1 - \psi(\mathbf{b}_i)) \prod_{j=1}^{l}(1 - \psi^{\vee}(\mathbf{c}_j))\Lambda_S(\psi), \tag{46}$$

whenever everything is defined. As an application, since $\psi_{S,\mathbf{a}} = \overset{*}{\underset{\mathbf{q}\in S-|\mathbf{m}_\psi|}} \delta_{\mathbf{q}} * \psi_{\mathbf{m}_\psi,\mathbf{a}}$, we obtain

$$\Lambda_S(\psi) = \sum_{\mathbf{a}\in A} \psi(\mathbf{a})\Lambda\big(k(\psi), j(\psi), \psi_{S,\mathbf{a}}\big) = E_S(\psi)\Lambda(\psi), \tag{47}$$

where, by definition, $E_S(\psi) = \prod_{\mathbf{q}\in S-|\mathbf{m}_\psi|}(1 - \psi(\mathbf{q}))$ is the Euler factor of ψ above S.

We can attach local and global root numbers to ψ in the following way. For each $\mathbf{q} \in |\mathbf{m}_\psi \mathbf{d}_H|$, choose $\gamma_{\mathbf{q}} \in H^*$ such that $v_{\mathbf{q}}(\gamma_{\mathbf{q}}) = 1$ and $v_{\mathbf{q}'}(\gamma_{\mathbf{q}}) = 0$ if $\mathbf{q}' \in |\mathbf{m}_\psi \mathbf{d}_H| - \{\mathbf{q}\}$. Let $a_{\mathbf{q}} = v_{\mathbf{q}}(\mathbf{m}_\psi \mathbf{d}_H)$.

Lemma 29: (i) There exists a constant $W_{\mathbf{q},\gamma_{\mathbf{q}}}(\psi)$ such that

$$\mathcal{F}_{\bar{\mathbf{q}}}(\psi_{\bar{\mathbf{q}}}{}^{\vee})(x) = W_{\mathbf{q},\gamma_{\mathbf{q}}}(x)\psi_{\mathbf{q}}(\gamma_{\mathbf{q}}^{\mathbf{a}_{\mathbf{q}}} x).$$

(ii) Set

$$W_{\mathbf{q}}(\psi) = W_{\mathbf{q},\gamma_{\mathbf{q}}}\left[\psi(\mathbf{q}^{-1}(\gamma_{\mathbf{q}}))\frac{N_{H/K}(\gamma_{\mathbf{q}})^{j(\psi)}}{\overline{N_{H/K}(\gamma_{\mathbf{q}})}^{k(\psi)}} \prod_{\mathbf{q}'\in|\mathbf{m}_\psi|-\{\mathbf{q}\}} \psi_{\mathbf{q}'}(\gamma_{\mathbf{q}}^{-1})\right]^{\mathbf{a}_{\mathbf{q}}}.$$

Then $W_{\mathbf{q}}(\psi)$ is independent of the choice of $\gamma_{\mathbf{q}}$ and is by definition the local root number of ψ at $\mathbf{q}$.

(iii) $W_{\mathbf{q}}(\psi)W_{\bar{\mathbf{q}}}(\psi^{\vee}) = \psi_{\mathbf{q}}(-1)$.

Proof: Everything follows from standard computations (cf. [L]).

The global root number $W(\psi)$ is defined by $W(\psi) = (-1)^{nk(\psi)} \prod_{\mathbf{q}\in|\mathbf{m}_\psi \mathbf{d}_H|} W_{\mathbf{q}}(\psi)$. If $S \in \mathcal{P}(H)$, let $W_S(\psi) = \prod_{\mathbf{q}\in S\cap|\mathbf{m}_\psi \mathbf{d}_H|} W_{\mathbf{q}}(\psi)$. Let $S_o \subset S$, and define $\psi_{S,S_o,\mathbf{a}} \in \mathcal{S}(H)$ by

$$\psi_{S,S_o,\mathbf{a}}(x) = \prod_{\mathbf{q}\in S-S_o} \psi_{\mathbf{q}}(x_{\mathbf{q}}) \prod_{\mathbf{q}\in S_o} \mathcal{F}_{\overline{\mathbf{q}}}(\psi_{\overline{\mathbf{q}}}^{\vee})(x_{\mathbf{q}}) \prod_{\mathbf{q}\notin S} 1_{\mathbf{a}_{\mathbf{q}}^{-1}}(x_{\mathbf{q}}). \tag{48}$$

Lemma 30: If $A \subset I_S(H)$ is a set of representatives of $Cl(O_H)$, then

$$\sum_{\mathbf{a}\in A} \psi(\mathbf{a})\Lambda\big(k(\psi), j(\psi), \psi_{S,S_o,\mathbf{a}}\big) = \big(W_{S_o}(\psi)\big) E_{\overline{S}_o}(\psi^{\vee}) E_{S-S_o}(\psi)\Lambda(\psi).$$

Proof: Let $\gamma = \prod_{\mathbf{q}\in S_o} \gamma_{\mathbf{q}}^{\mathbf{a}_{\mathbf{q}}}$. Using Lemma 29 (i) and the fact that the Fourier transform of $\delta_{\mathbf{q}}$ is $\delta_{\overline{\mathbf{q}}}^{\vee}(\gamma x)$ if $\mathbf{q} \in S \to |\mathbf{m}_\psi|$, we obtain

$$\psi_{S,S_o,\mathbf{a}}(x) = W\phi_{\mathbf{a}}(\gamma x), \tag{49}$$

where

$$W = \prod_{\mathbf{q}\in S-S_o} \psi_{\mathbf{q}}(\gamma^{-1}) \prod_{\mathbf{q}\in S_o\cap|\mathbf{m}_\psi \mathbf{d}_H|} \big(\psi_{\mathbf{q}}(\gamma_{\mathbf{q}}^{\mathbf{a}_{\mathbf{q}}}\gamma^{-1}) W_{\mathbf{q},\gamma_{\mathbf{q}}}(\psi)\big), \tag{50}$$

$$\phi_a = \underset{\mathbf{q}\in S-(S_0\cup|\mathbf{m}_\psi|)}{*} \delta_{\mathbf{q}} \underset{\mathbf{q}\in S_0-|\mathbf{m}_\psi|}{*} \delta_{\overline{\mathbf{q}}}^{\vee} * \psi_{\mathbf{m}_\psi,\mathbf{a}'}, \tag{51}$$

and

$$\mathbf{a}' = \mathbf{a}(\gamma^{-1}) \prod_{\mathbf{q}\in S_o} \mathbf{q}^{\mathbf{a}_{\mathbf{q}}}. \tag{52}$$

Now, using formula (16) we obtain

$$\psi(\mathbf{a})\Lambda\big(k(\psi), j(\psi), \psi_{S,S_o,\mathbf{a}}\big) = \psi(\mathbf{a}) W \frac{N_{H/K}(\gamma)^{j(\psi)}}{N_{H/K}(\gamma)^{k(\psi)}} \Lambda\big(k(\psi), j(\psi), \phi_{\mathbf{a}}\big). \tag{53}$$

Writing $\psi(\mathbf{a}) = \psi(\mathbf{a}') \prod_{\mathbf{q}\in S_o} \psi(\gamma_{\mathbf{q}}\mathbf{q}^{-1})^{\mathbf{a}_{\mathbf{q}}}$ and using the fact that $\mathbf{a} \to \mathbf{a}'$ induces a bijection on $Cl(O_H)$ and formula (46), we obtain

$$\sum_{\mathbf{a}\in A} \psi(\mathbf{a})\Lambda\big(k(\psi), j(\psi), \psi_{S,S_o,\mathbf{a}}\big) =$$

$$W \frac{N_{H/K}(\gamma)^{j(\psi)}}{N_{H/K}(\gamma)^{k(\psi)}} \Big(\prod_{\mathbf{q}\in S_o} \psi(\gamma_{\mathbf{q}}\mathbf{q}^{-1})^{\mathbf{a}_{\mathbf{q}}} \Big) E_{S_o}(\psi^{\vee}) E_{S-S_o}(\psi)\Lambda(\psi), \tag{54}$$

and the result follows, using Lemma 29 (ii).

Lemma 31: (Hecke's functional equation) $W(\psi)\Lambda(\psi) = i^{-n}\Lambda(\psi^\vee)$.

Proof: Let $\mathbf{a} \in I_{|\mathbf{m}_\psi \mathbf{d}_H|}(H)$ and let $\gamma = \prod_{\mathbf{q}\in|\mathbf{m}_\psi \mathbf{d}_H|} \gamma_{\mathbf{q}}^{\mathbf{a}_\mathbf{q}}$. Using Lemma 29 (i), we obtain

$$\mathcal{F}_{H^\vee}(\psi^\vee_{\overline{m}_\psi,\overline{\mathbf{a}}})(x) = N(\mathbf{a})\, W\, \psi_{\mathbf{m}_\psi,\mathbf{a}'}(\gamma x), \tag{55}$$

where $\mathbf{a}' = (\gamma^{-1})\mathbf{m}_\psi \mathbf{d}_H \mathbf{a}^{-1}$ and

$$W = \Big(\prod_{\mathbf{q}\in|\mathbf{m}_\psi \mathbf{d}_H|} W_{\mathbf{q},\gamma_\mathbf{q}}(\psi)\Big) \prod_{\substack{\mathbf{q}\neq\mathbf{q}' \\ \mathbf{q},\mathbf{q}'\in|\mathbf{m}_\psi \mathbf{d}_H|}} \psi_{\mathbf{q}'}(\gamma_\mathbf{q}^{-\mathbf{a}_\mathbf{q}}). \tag{56}$$

So we get

$$\psi^\vee(\overline{\mathbf{a}})\Lambda\big(k(\psi), j(\psi), \mathcal{F}_{H^\vee}(\psi^\vee_{\overline{m}_\psi,\overline{\mathbf{a}}})\big) = N(\mathbf{a})\psi^\vee(\overline{\mathbf{a}})\, W\, \frac{N_{H/K}(\gamma)^{j(\psi)}}{\overline{N_{H/K}(\gamma)}^{k(\psi)}} \Lambda\big(k(\psi), j(\psi), \mathbf{a}'\big). \tag{57}$$

Now, we have

$$N(\mathbf{a})\psi^\vee(\overline{\mathbf{a}}) = \psi(\mathbf{a}^{-1}) = \psi(\mathbf{a}')\psi(\gamma \mathbf{m}_\psi^{-1}\mathbf{d}_H^{-1}), \tag{58}$$

and

$$W\, \frac{N_{H/K}(\gamma)^{j(\psi)}}{\overline{N_{H/K}(\gamma)}^{k(\psi)}} \psi(\gamma \mathbf{m}_\psi^{-1}\mathbf{d}_H^{-1}) = \prod_{\mathbf{q}\in|\mathbf{m}_\psi \mathbf{d}_H|} W_\mathbf{q}(\psi), \tag{59}$$

and by formula (4),

$$\Lambda\big(k(\psi), j(\psi), \mathcal{F}_{H^\vee}(\psi^\vee_{\overline{\mathbf{m}}_\psi,\overline{\mathbf{a}}})\big) = (-1)^{nk(\psi)} i^{-n} \Lambda\big(k(\psi^\vee), j(\psi^\vee), \psi^\vee_{\overline{\mathbf{m}}_\psi,\overline{\mathbf{a}}}\big). \tag{60}$$

We obtain the result by summing up (57) over a set of representatives of $Cl(O_H)$.

Set $\Lambda_S^?(\psi, \mathbf{a}) = \psi(\mathbf{a})\Lambda^?(k(\psi), j(\psi), \psi_{S,\mathbf{a}})$. An immediate consequence of theorem 26 is that the above computations are valid with $\Lambda_S(\psi, \mathbf{a})$ replaced by $\Lambda_S^?(\psi, \mathbf{a})$. More precisely, if A is a set of representatives of $Cl(O_H)$, set $\Lambda_S^?(\psi) = \sum_{\mathbf{a}\in A} \Lambda_S^?(\psi, \mathbf{a})$. Then we have:

Proposition 32: (i) $\Lambda_S^?(\psi, \mathbf{a})$ depends only on the image of $\mathbf{a}$ in $Cl(O_H)$.

(ii) $\Lambda_S^?(\psi) = E_S\Lambda^?(\psi)$.

(iii) $\sum_{\mathbf{a}\in A} \psi(a)\Lambda^?(k(\psi), j(\psi), \psi_{S,S_o,\mathbf{a}}) = \big(\prod_{\mathbf{q}\in S_o} W_\mathbf{q}(\psi)\big) E_{\bar{S}_o}(\psi^\vee) E_{S-S_o}(\psi)\Lambda^?(\psi)$.

(iv) $W(\psi)\Lambda^?(\psi) = i^{-n}\Lambda^?(\psi^\vee)$.

(v) $\Lambda^?(\psi) = \Lambda(\psi)$ if $n = 1, 2$ or $n \geq 3$ and $k(\psi) = 0$ or $j(\psi) = 1$.

V. P-adic measures on Galois groups and P-adic L-functions.

§1. Preliminary constructions.

Let ψ be a Hecke character of H of type A_0 and conductor $\mathbf{m}_\psi$. We can associate to ψ a unique continuous character $\psi^{(p)}$ with values in $\mathbf{C}_p^*$ satisfying $\psi^{(p)}(\mathbf{a}) = \psi(\mathbf{a})$ for any $\mathbf{a} \in I_{\mathbf{m}_\psi(p)}(H)$ (cf. [W1]). But, as $\psi^{(p)}$ is trivial on the connected component of 1 of $\mathbf{A}_H^*/H^*$, it can be interpreted as a character of $\mathrm{Gal}(H^{ab}/H)$. In fact $\psi^{(p)}$ factors through $\mathcal{G}_{H,\mathbf{m},p} = \mathrm{Gal}(H_{\mathbf{m}(p)^\infty}/H)$, where $\mathbf{m}$ is the prime-to-p part of $\mathbf{m}_\psi$ and $H_{\mathbf{m}(p)^\infty}$ is the union of all abelian extensions of H of level $\mathbf{m}(p)^k$ for $k \geq 0$. We shall say that ψ is p-admissible if it is admissible and $\psi^{(p)}$ factors through $\mathcal{G}_{H,\mathbf{m},\mathbf{p}} = \mathrm{Gal}(H_{\mathbf{m}\mathbf{p}^\infty}/H)$ (note that this is equivalent to $k(\psi) = 0$ and $\psi_{\overline{\mathbf{p}}} = 1$ on $O_{|\overline{\mathbf{p}}|}^*$). Let us choose a set $A \subset I_{|\mathbf{m}(p)|}(H)$ of representatives of $Cl(O_H)$. We have the following isomorphisms of topological spaces:

$$\mathcal{G}_{H,\mathbf{m},p} \simeq A \times ((O_H/\mathbf{m})^* \times Y_{H,p}^*)/\overline{U_H} \quad \text{and} \quad \mathcal{G}_{H,\mathbf{m},\mathbf{p}} \simeq A \times (O_H^*/\mathbf{m} \times Y_{H,\mathbf{p}}^*)/\overline{U_H},$$

where $\overline{U_H}$ denotes the topological closure of U_H in the space considered. If f is a function on $\mathcal{G}_{H,\mathbf{m},p}$ (resp. on $\mathcal{G}_{H,\mathbf{m},\mathbf{p}}$), let $\tilde{f}$ be the function on $A \times (O_H/\mathbf{m})^* \times Y_{H,p}^*$ (resp. $A \times (O_H/\mathbf{m})^* \times Y_{H,\mathbf{p}}^*$) obtained by composing with the projection modulo $\overline{U_H}$.

Choose a torsion free subgroup V of finite index of the subgroup of U_H of elements of norm 1 over K and $\mathcal{B} \in \mathcal{B}(V)$. Let $T \in \mathcal{P}(H)$ contain $|\mathbf{m}|$, $|(p)|$ and $|\mathbf{a}|$ for all $\mathbf{a} \in A$. If $\alpha \in (O_{H,|\mathbf{m}|})^*$ and $\mathbf{a} \in A$, let $\phi_{\alpha,\mathbf{a}} \in \mathcal{S}_T(H)$ be the function defined by

$$\phi_{\alpha,\mathbf{a}}(x) = \phi_{\alpha,|\mathbf{m}|}(x_{|\mathbf{m}|}) \cdot \phi_{\mathbf{p}}(x_{\mathbf{p}}) \prod_{\mathbf{q} \notin |\mathbf{m}\mathbf{p}|} 1_{\mathbf{a}^{-1}}(x_{\mathbf{q}}), \tag{61}$$

where $\phi_{\alpha,|\mathbf{m}|}(x_{|\mathbf{m}|}) = 1$ if $x_{|\mathbf{m}|} \in \alpha + \mathbf{m}O_{|\mathbf{m}|}$ and 0 otherwise, and $\phi_{\mathbf{p}}$ is the function defined in III §3.

For all $(\mathbf{b}_1, \mathbf{b}_2) \in C_T(S(\mathcal{B}), S'(\mathcal{B}))$, where $S(\mathcal{B})$ and $S'(\mathcal{B})$ are as defined in theorem 26 we define a measure $\lambda_{\mathbf{b}_1,\mathbf{b}_2,\mathbf{m}}$ on $\mathcal{G}_{H,\mathbf{m},\mathbf{p}}$ and a measure $\mu_{\mathbf{b}_1,\mathbf{b}_2,\mathbf{m}}$ on $\mathcal{G}_{H,\mathbf{m},p}$ by the formulae:

$$\int_{\mathcal{G}_{H,\mathbf{m},\mathbf{p}}} f \, d\lambda_{\mathbf{b}_1,\mathbf{b}_2,\mathbf{m}} = \frac{1}{[U_H : V]} \sum_{\mathbf{a} \in A} \sum_{\alpha \in (O_H/\mathbf{m})^*} \int_{Y_1^* \times Y_2} \tilde{f}(\mathbf{a}, \alpha, y_1) \, d\tilde{\mu}_{\mathbf{b}_1,\mathbf{b}_2,\phi_{\alpha,\mathbf{a}},\mathcal{B}}, \tag{62}$$

$$\int_{\mathcal{G}_{H,\mathbf{m},p}} f \, d\mu_{\mathbf{b}_1,\mathbf{b}_2,\mathbf{m}} = \frac{1}{[U_H : V]} \sum_{\mathbf{a} \in A} \sum_{\alpha \in (O_H/\mathbf{m})^*} \int_{Y_1^* \times Y_2^*} \tilde{f}(\mathbf{a}, \alpha, y_1, y_2) \, d\tilde{\mu}_{\mathbf{b}_1,\mathbf{b}_2,\phi_{\alpha,\mathbf{a}},\mathcal{B}}, \tag{63}$$

where $\mu_{\mathbf{b}_1,\mathbf{b}_2,\phi,\mathcal{B}}$ is the measure constructed in theorem 23, and if μ is a measure on $Y_1^* \times Y_2$, then $\tilde{\mu}$ is the measure defined by

$$\int_{Y_1^* \times Y_2} f(y_1, y_2)\, d\tilde{\mu} = \int_{Y_1^* \times Y_2} N(y_1)^{-1} f(y_1^{-1}, y_2)\, d\mu. \tag{64}$$

Let $\nu_{\mathbf{b}_1,\mathbf{b}_2}(\psi) = \big(1 - \psi(\mathbf{b}_1^{-1})\big)\big(1 - \psi^{\vee}(\mathbf{b}_2^{-1})\big)$.

Proposition 33: (i) $\lambda_{\mathbf{b}_1,\mathbf{b}_2,\mathbf{m}}$ is the unique measure on $\mathcal{G}_{H,\mathbf{m},\mathbf{p}}$ such that

$$\int_{\mathcal{G}_{H,\mathbf{m},\mathbf{p}}} \psi^{(p)}\, d\lambda_{\mathbf{b}_1,\mathbf{b}_2,\mathbf{m}} = \nu_{\mathbf{b}_1,\mathbf{b}_2}(\psi) E_{|\overline{\mathbf{p}}|}(\psi^{\vee}) W_{|\mathbf{p}|}(\psi) E_{|\mathbf{m}|}(\psi) \Lambda(\psi) \tag{65}$$

for all $\mathbf{p}$-admissible Hecke characters of H of conductor dividing $\mathbf{m}\mathbf{p}^{\infty}$.

(ii) $\mu_{\mathbf{b}_1,\mathbf{b}_2,\mathbf{m}}$ is the unique measure on $\mathcal{G}_{H,\mathbf{m},p}$ such that

$$\int_{\mathcal{G}_{H,\mathbf{m},p}} \psi^{(p)}\, d\mu_{\mathbf{b}_1,\mathbf{b}_2,\mathbf{m}} = \nu_{\mathbf{b}_1,\mathbf{b}_2}(\psi) E_{|\overline{\mathbf{p}}|}(\psi^{\vee}) W_{|\mathbf{p}|}(\psi) E_{|\mathbf{m}\overline{\mathbf{p}}|}(\psi) \Lambda(\psi) \tag{66}$$

for all admissible Hecke characters of H of conductor dividing $\mathbf{m}(p)^{\infty}$ satisfying $k(\psi) = 0$ or $j(\psi) = 1$.

(iii) Moreover, if we do not assume $k(\psi) = 0$ or $j(\psi) = 1$, then

$$\int_{\mathcal{G}_{H,\mathbf{m},p}} \psi^{(p)}\, d\mu_{\mathbf{b}_1,\mathbf{b}_2,\mathbf{m}} = \nu_{\mathbf{b}_1,\mathbf{b}_2}(\psi) E_{|\overline{\mathbf{p}}|}(\psi^{\vee}) W_{|\mathbf{p}|}(\psi) E_{|\mathbf{m}\overline{\mathbf{p}}|}(\psi) \Lambda^{?}(\psi). \tag{67}$$

Corollary: If one can prove by any other method (for example using refinements of Harder's proof) that there exists a measure satisfying (ii) for all admissible ψ, then $\Lambda(\psi) = \Lambda^{?}(\psi)$ in all cases.

Proof: Let ψ be an admissible Hecke character. By definition of $\mu_{\mathbf{b}_1,\mathbf{b}_2,\mathbf{m}}$, we have

$$\int_{\mathcal{G}_{H,\mathbf{m},p}} \psi^{(p)}\, d\mu_{\mathbf{b}_1,\mathbf{b}_2,\mathbf{m}} = \frac{1}{[U_H : V]} \sum_{\mathbf{a} \in A} \psi(\mathbf{a}) \sum_{\alpha \in (O_H/m)^*} G(\alpha) \tag{68}$$

where

$$G(\alpha) = \psi_{|\mathbf{m}|}(\alpha) \int_{Y_{H,p}} \psi_{\overline{\mathbf{p}}}^{\vee}(y_1) \psi_{\overline{\mathbf{p}}}(y_2) N(y_1)^{j(\psi)-1} N(y_2)^{k(\psi)}\, d\mu_{\mathbf{b}_1,\mathbf{b}_2,\phi_{\alpha,\mathbf{a}},\mathcal{B}}. \tag{69}$$

Now, using theorem 23 (ii) and formula (48), we obtain that the Fourier-Laplace transform of

$$\frac{1}{[U_H : V]} \sum_{\alpha \in (O_H/\mathbf{m})^*} \psi_{|\mathbf{m}|}(\alpha) \psi_{\overline{\mathbf{p}}}^{\vee}(y_1) \psi_{\overline{\mathbf{p}}}(y_2)\, d\mu_{\mathbf{b}_1,\mathbf{b}_2,\phi_{\alpha,\mathbf{a}},\mathcal{B}}$$

is

$$\frac{1}{[U_H:V]}\mathcal{H}\Big(\frac{1}{2\pi i}K\big(\frac{z_1}{2\pi i},\frac{z_2}{2\pi i},(\psi_{|\mathbf{m}(p)|,|\mathbf{p}|,\mathbf{a}})_{\mathbf{b}_1,\mathbf{b}_2},\mathcal{B}\big)\Big), \tag{70}$$

and we can deduce (iii) from Lemma 8 and Proposition 32 (ii). Then (ii) follows from the fact that $\Lambda^?(\psi) = \Lambda(\psi)$ if $k(\psi) = 0$ or $j(\psi) = 1$ and (i) is obtained in exactly the same way as (iii). The unicity of $\lambda_{\mathbf{b}_1,\mathbf{b}_2,\mathbf{m}}$ and $\mu_{\mathbf{b}_1,\mathbf{b}_2,\mathbf{m}}$ is due to the fact that the subspace of the space of continuous functions on $\mathcal{G}_{H,\mathbf{m},p}$ (resp. $\mathcal{G}_{H,\mathbf{m},\mathbf{p}}$) generated by the $\psi^{(p)}$ with $k(\psi) = 0$ and $j(\psi) = 1$ is dense (we are allowed to multiply by any locally constant character).

§2. Measures and pseudo-measures on profinite abelian groups.

In order to put the results of the preceding paragraph in a more satisfactory form, we shall shift to the language of pseudo-measures. In this paragraph, we shall collect from [Se] the definitions and some basic facts about pseudo-measures.

Let G be a profinite abelian group and Λ be a closed subring of $\hat{O}$. We define the Iwasawa algebra $\Lambda[[G]]$ of G as $\varprojlim \Lambda[G/H]$ where H runs through the open subgroups of G. Then $\Lambda[G]$ is a dense subalgebra of $\Lambda[[G]]$ and we have a canonical isomorphism between $\Lambda[[G]]$ and the algebra of Λ-valued measures on G, the multiplication in $\Lambda[[G]]$ corresponding to convolution of measures. This will enable us to view a Λ-valued measure on G as an element of $\Lambda[[G]]$. For example, the measure associated to $g \in G$ is the Dirac measure at g.

Let $X(G)$ be the group of continuous $\mathbf{C}_p^*$-valued homomorphisms of G endowed with the topology of uniform convergence. If $\chi \in X(G)$ and $\mu \in \Lambda[[G]]$, we write $\langle \chi, \mu \rangle$ instead of $\int_G \chi \, d\mu$ and let $\chi\mu \in \Lambda[[G]]$ be defined by $\langle \psi, \chi\mu \rangle = \langle \psi\chi, \mu \rangle$. Then we have $\langle \chi, \mu\lambda \rangle = \langle \chi, \mu \rangle \langle \chi, \lambda \rangle$ and $\chi(\mu\lambda) = (\chi\mu)(\chi\lambda)$.

Suppose from now on that G has a quotient isomorphic to $\mathbf{Z}_p$ and let $\Gamma \subset G$ be a lifting of $\mathbf{Z}_p$. Let $\Lambda'[[G]]$ be the total fraction ring of $\Lambda[[G]]$ (i.e. the ring of $\alpha^{-1}\beta$ where α, β are elements of $\Lambda[[G]]$ and α is not a zero divisor). If $\lambda = \alpha^{-1}\beta \in \Lambda'[[G]]$ and $\chi \in X(G)$ satisfies $\langle \chi, \alpha \rangle \neq 0$, we set $\langle \chi, \lambda \rangle = \langle \chi, \alpha \rangle^{-1} \langle \chi, \beta \rangle$ and this depends only on λ, not on the particular decomposition of λ in the form $\alpha^{-1}\beta$. The map $\chi \to \langle \chi, \lambda \rangle$ is defined on a dense open subset of $X(G)$. If $\lambda \in \Lambda'[[G]]$ and $\chi \in X(G)$ we can still define $\chi\lambda \in \Lambda'[[G]]$ and we still have $\chi(\lambda\mu) = (\chi\lambda)(\chi\mu)$. An element $\lambda \in \Lambda'[[G]]$ will be called a "pseudo-measure" if $(1-g)\lambda \in \Lambda[[G]]$ for all $g \in G$. We shall write $\tilde{\Lambda}[[G]]$ for the space of pseudo-measures.

Let $\pi: G' \to G$ be a surjective morphism of profinite abelian groups. Then π induces a surjective morphism from $\Lambda[[G']]$ to $\Lambda[[G]]$ which can be prolonged in a unique way to a morphism from $\tilde{\Lambda}[[G']]$ to $\tilde{\Lambda}[[G]]$ in the following way. If $g \in G$, then $g-1$ is a zero divisor if and only if the topological closure of the subgroup generated by g in G has a finite p-Sylow subgroup; in particular if the image of g in $\mathbf{Z}_p$ is non-zero, then $g-1$ is not a zero divisor and the set of $g \in G$ such that $g-1$ is a zero divisor is contained in a closed subset with empty interior. So take $\lambda \in \tilde{\Lambda}[[G']]$ and $g \in G'$ such that $\pi(g)-1$ is not a zero divisor and set $\pi(\lambda) = \big(\pi(g)-1\big)^{-1}\pi\big((g-1)\lambda\big)$. This clearly does not depend on the choice of g and defines a pseudo-measure on G.

Lemma 34: (i) If the p-Sylow subgroup of G/Γ is infinite, then $\tilde{\Lambda}[[G]] = \Lambda[[G]]$, or otherwise stated, all pseudo-measures are measures.

(ii) If $\pi: G' \to G$ is a surjective morphism of profinite abelian groups and λ is a pseudo-measure on G' such that $\pi(\lambda)$ is a measure, then λ itself is a measure.

Proof: This follows easily from the structure of $\tilde{\Lambda}[[G]]$ given in Th. 1.15 of [Se].

Corollary: Suppose G has a quotient isomorphic to $\mathbf{Z}_p^2$. Let $\chi_1, \ldots, \chi_n \in X(G)$ and $\lambda \in \Lambda'[[G]]$ such that $\forall (g_1, \ldots, g_n) \in G^n$, $\lambda \prod_{i=1}^n (1 - \chi_i(g_i)g_i) \in \Lambda[[G]]$, then λ is a measure.

Proof: An immediate induction reduces the study to the case $n = 1$. So let $\chi \in X(G)$ and $\lambda \in \Lambda'[[G]]$ be such that $(1 - \chi(g)g)\lambda \in \Lambda[[G]]$ for all $g \in G$. We then find that $\chi^{-1}\big((1 - \chi(g)g)\lambda\big) = (1 - g)(\chi^{-1}\lambda)$ is a measure for all $g \in G$. As G has a quotient isomorphic to $\mathbf{Z}_p^2$ this implies by a) that $\chi^{-1}\lambda$ is a measure, hence λ also.

§3. P-adic L-functions

If $S \in \mathcal{P}(H)$ satisfies $S \cap |(p)| = \emptyset$, let $\mathcal{G}_{H,S,p}$ (resp. $\mathcal{G}_{H,S,\mathbf{p}}$) be the Galois group over H of the union of all abelian extensions of H of level $\mathbf{m}$ with $|\mathbf{m}| \subset S \cup |(p)|$ (resp. $|\mathbf{m}| \subset S \cup |\mathbf{p}|$). If ρ denotes the complex conjugation on $\overline{K}$ induced by the embedding of $\overline{K}$ into $\mathbf{C}$, the map $\sigma \to \overline{\sigma}$ defined by $\overline{\sigma}(x) = \rho\big(\sigma(\rho(x))\big)$ induces a (canonical) isomorphism between $\mathcal{G}_{H,S,p}$ and $\mathcal{G}_{H^\vee,\overline{S},p}$. If $x \in A_H^*/H^*$, let $\sigma_x \in \mathrm{Gal}(H^{ab}/H)$ be its Artin symbol. If $\mathbf{b} \in I_{S\cup|(p)|}(H)$, let $\sigma_{\mathbf{b}} \in \mathcal{G}_{H,S,p}$ (resp. $\mathcal{G}_{H,S,\mathbf{p}}$) be the Artin symbol of the idèle $(\ldots, x_{\mathbf{q}}, \ldots)$, where $v_{\mathbf{q}}(x_{\mathbf{q}}) = -v_{\mathbf{q}}(\mathbf{b})$ and $\sigma_{-1} \in \mathcal{G}_{H,S,p}$ be the Artin symbol of $(\ldots, x_{\mathbf{q}}, \ldots)$ where $x_{\mathbf{q}} = -1$ if $\mathbf{q} \in |\overline{\mathbf{p}}|$ and $x_{\mathbf{q}} = 1$ otherwise. If $\mathbf{b} \in I_{S\cup|(p)|}(H)$, we have $\sigma_{\overline{\mathbf{b}}} = \overline{\sigma_{\mathbf{b}}}$ in

$\mathcal{G}_{H^\vee,\overline{S},p}$. Let N be the cyclotomic character of $\mathcal{G}_{H,S,p}$ defined by $N(\sigma_{\mathbf{b}}) = N(\mathbf{b})$ and if χ is a $\mathbf{C}_p^*$-valued continuous character of $\mathcal{G}_{H,S,p}$, let $\chi^\vee$ be the character of $\mathcal{G}_{H^\vee,\overline{S},p}$ defined by $\chi^\vee(\sigma) = N(\sigma)^{-1}\chi(\overline{\sigma}^{-1})$.

If $(\mathbf{b}_1, \mathbf{b}_2) \in C_T\big(S(\mathcal{B}), S'(\mathcal{B})\big)$, we let $\mu_{\mathbf{b}_1,\mathbf{b}_2,S} \in I_{p,H}[[\mathcal{G}_{H,S,p}]]$ and $\lambda_{\mathbf{b}_1,\mathbf{b}_2,S} \in I_{p,H}[[\mathcal{G}_{H,S,\mathbf{p}}]]$ be the respective projective limits of the $\mu_{\mathbf{b}_1,\mathbf{b}_2,\mathbf{m}}$ and $\lambda_{\mathbf{b}_1,\mathbf{b}_2,\mathbf{m}}$ defined in Proposition 33. If χ is a continuous $\mathbf{C}_p^*$-valued character of $\mathcal{G}_{H,S,\mathbf{p}}$ (resp. $\mathcal{G}_{H,S,p}$), we set

$$L_{\mathbf{p},S}(\chi) = \Big[\big(1-\chi(\sigma_{\mathbf{b}_1})^{-1}\big)\big(1-N(\mathbf{b}_2)\chi(\sigma_{\overline{\mathbf{b}}_2})\big)\Big]^{-1}\int_{\mathcal{G}_{H,S,\mathbf{p}}} \chi\, d\lambda_{\mathbf{b}_1,\mathbf{b}_2,S},$$

and

$$L_{p,S}(\chi) = \Big[\big(1-\chi(\sigma_{\mathbf{b}_1})^{-1}\big)\big(1-\chi^\vee(\sigma_{\mathbf{b}_2})\big)^{-1}\Big]^{-1}\int_{\mathcal{G}_{H,S,p}} \chi\, d\mu_{\mathbf{b}_1,\mathbf{b}_2,S}.$$

$L_{\mathbf{p},S}$ and $L_{p,S}$ are independent of the choice of $(\mathbf{b}_1, \mathbf{b}_2)$ as can easily be deduced from Proposition 33. We can now state our main result:

Theorem 35: (i) $L_{p,S}(\chi)$ is an Iwasawa function of χ, i.e. there exists a (unique) measure μ_S on $\mathcal{G}_{H,S,p}$ such that $L_{p,S}(\chi) = \int_{\mathcal{G}_{H,S,p}} \chi\, d\mu_S$.

(ii) If ψ is an admissible Hecke character of conductor $\mathbf{m}_\psi$ satisfying $|\mathbf{m}_\psi| \subset S \cup |(p)|$, then $L_{p,S}(\psi^{(p)}) = E_{|\overline{\mathbf{p}}|}(\psi^\vee)E_{S\cup|\overline{\mathbf{p}}|}(\psi)W_{|\mathbf{p}|}(\psi)\Lambda^?(\psi)$.

(iii) If the conductor of χ is divisible by all elements of S, then there exists a p-adic unit $W^{(p)}(\chi)$ such that

$$W^{(p)}(\chi)L_{p,S}(\chi) = \chi(\sigma_{-1})L_{p,\overline{S}}(\chi^\vee).$$

Moreover, if ψ is an admissible Hecke character, then

$$W^{(p)}(\psi^{(p)}) = i^n \prod_{\mathbf{q}\in S\cup|\mathbf{d}_H|-|(p)|} W_{\mathbf{q}}(\psi).$$

(iv) There exists a (unique) pseudo-measure λ_S on $\mathcal{G}_{H,S,\mathbf{p}}$ such that

$$L_{\mathbf{p},S}(\chi) = \int_{\mathcal{G}_{H,S,\mathbf{p}}} \chi\, d\lambda_S,$$

and λ_S is a measure if $S \neq \emptyset$ or if the p-adic regulator $R_{\mathbf{p}}$ of U_H is equal to 0.

(v) If ψ is a p-admissible Hecke character of H of conductor $\mathbf{m}_\psi$ satisfying $|\mathbf{m}_\psi| \subset S \cup |\mathbf{p}|$, then $L_{\mathbf{p},S}(\psi^{(p)}) = E_{|\overline{\mathbf{p}}|}(\psi^\vee)W_{|\mathbf{p}|}(\psi)E_S(\psi)\Lambda(\psi)$.

Proof: (i) First note that $\mathcal{G}_{H,S,p}$ has a quotient isomorphic to $\mathbf{Z}_p^2$, namely $\mathrm{Gal}(HK_\infty/H)$, where K_∞ is the union of all $\mathbf{Z}_p$-extensions of K, and that the image of $C_T\big(S(\mathcal{B}), S'(\mathcal{B})\big)$

by the Artin map is dense in $\mathcal{G}_{H,S,p} \times \mathcal{G}_{H^\vee,\overline{S},p}$ by Tchebotarev's density theorem. Hence, there exists a subset C of $C_T\big(S(\mathcal{B}), S'(\mathcal{B})\big)$ dense in $\mathcal{G}_{H,S,p} \times \mathcal{G}_{H^\vee,\overline{S},p}$ such that the quotient of $\mu_{\mathbf{b}_1,\mathbf{b}_2,S}$ by $(1-\sigma_{\mathbf{b}_1}^{-1})\big(1-N(\mathbf{b}_2)\overline{\sigma_{\mathbf{b}_2}}\big)$ is well-defined. An immediate consequence of proposition 33 is that this quotient is independent of the choice of $(\mathbf{b}_1,\mathbf{b}_2) \in C$. We shall denote it by μ_S. We see that $(1-\sigma_{\mathbf{b}_1}^{-1})\big(1-N(\mathbf{b}_2)\overline{\sigma_{\mathbf{b}_2}}\big)\mu_S$ is a measure on $\mathcal{G}_{H,S,p}$ for all $(\mathbf{b}_1,\mathbf{b}_2) \in C$. As C is dense in $\mathcal{G}_{H,S,p} \times \mathcal{G}_{H^\vee,\overline{S},p}$, this implies that $(1-\sigma_1)\big(1-N(\sigma_2)\sigma_2\big)\mu_S$ is a measure for all $\sigma_1, \sigma_2 \in \mathcal{G}_{H,S,p}$; hence, μ_S is a measure by virtue of the corollary of Lemma 34.

(ii) and (v) These are immediate consequences of Proposition 33.

(iii) Let ψ be an admissible Hecke character of conductor $\mathbf{m}_\psi$ satisfying $S \supset |\mathbf{m}_\psi| \supset S \cup |(p)|$. We have:

$$L_{p,S}(\psi^{(p)}) = E_{|\overline{\mathbf{p}}|}(\psi^\vee)E_{|\overline{\mathbf{p}}|}(\psi^\vee)W_{|\mathbf{p}|}(\psi)\Lambda^?(\psi),$$

$$L_{p,S}\big((\psi^\vee)^{(p)}\big) = E_{|\overline{\mathbf{p}}|}(\psi^\vee)E_{|\overline{\mathbf{p}}|}(\psi)W_{|\mathbf{p}|}(\psi^\vee)\Lambda^?(\psi^\vee),$$

$$W(\psi)\Lambda^?(\psi) = i^{-n}\Lambda^?(\psi^\vee),$$

$$W_{|\mathbf{p}|}(\psi^\vee)W_{|\overline{\mathbf{p}}|}(\psi) = \psi_{|\overline{\mathbf{p}}|}(-1),$$

$$W(\psi) = (-1)^{nk}W_{|\mathbf{p}|}(\psi)W_{|\overline{\mathbf{p}}|}(\psi) \prod_{\mathbf{q}\in|\mathbf{m}_\psi \mathbf{d}_H|-|(p)|} W_{\mathbf{q}}(\psi),$$

$$\psi^{(p)}(\sigma_{-1}) = (-1)^{nk}\psi_{|\overline{\mathbf{p}}|}(-1),$$

from which the formula for $W^{(p)}(\psi^{(p)})$ follows immediately. The fact that $W^{(p)}(\psi^{(p)})$ is a p-adic unit is a consequence of the fact that $W_{\mathbf{q}}(\psi)$ is a unit at all places prime to $N(\mathbf{q})$. The general case can be deduced from this case as in [d Sh, II, §6].

(iv) The definition of λ_S is about the same as that of μ_S. The quotient of $\lambda_{\mathbf{b}_1,\mathbf{b}_2,S}$ by $(1-\sigma_{\mathbf{b}_1}^{-1})(1-N(\mathbf{b}_2)\sigma_{\overline{\mathbf{b}_2}})$ does not depend on the choice of $(\mathbf{b}_1,\mathbf{b}_2) \in C_T\big(S(\mathcal{B}), S'(\mathcal{B})\big)$ and will be denoted by λ_S. The difference with a) is that now, $N(\mathbf{b}_2)$ is not a continuous function of $\sigma_{\overline{\mathbf{b}_2}}$ and the image of $C_T\big(S(\mathcal{B}), S'(\mathcal{B})\big)$ in $(\mathcal{G}_{H,S,\mathbf{p}})^2 \times O_{\mathbf{p}}^*$ by the map $(\mathbf{b}_1,\mathbf{b}_2) \to (\sigma_{\mathbf{b}_1^{-1}}, \sigma_{\overline{\mathbf{b}_2}}, N(\mathbf{b}_2))$ is dense. This implies that $(1-\sigma_1)(1-\alpha\sigma_2)\lambda_S$ is a measure for all $\sigma_1, \sigma_2 \in \mathcal{G}_{H,S,p}$ and $\alpha \in O_{\mathbf{p}}^*$. Hence $(1-\sigma_1)(1-p\sigma_2)\lambda_S = 2(1-\sigma_1)(1-\frac{1+p}{2}\sigma_2)\lambda_S - (1-\sigma_1)(1-\sigma_2)\lambda_S$ is a measure. But $(1-p\sigma_2)^{-1} = \sum_{k=0}^{\infty} p^k\sigma_2^k$ is a measure and so $(1-\sigma_1)\lambda_S$ is a measure for all $\sigma_1 \in \mathcal{G}_{H,S,\mathbf{p}}$, which means that λ_S is a pseudo-measure.

Now, if $S \neq \emptyset$, take $\mathbf{q} \in S$ and let $S' = S - \mathbf{q}$. Let π be the projection from $\mathcal{G}_{H,S,\mathbf{p}}$ to $\mathcal{G}_{H,S',\mathbf{p}}$. Then we have $\pi(\lambda_S) = (1-\sigma_{\mathbf{q}})\lambda_{S'}$ and thus $\pi(\lambda_S)$ is a measure which implies by Lemma 34 (b) that λ_S is a measure is $S \neq \emptyset$. The fact that $\lambda_\emptyset$ is a measure if $R_{\mathbf{p}} = 0$ can be obtained by the same method as in [Se], which concludes the proof.

References

[C-W] Coates, J., Wiles, A. On p-adic L-functions and elliptic units. J. Austral. Math. Soc. (series A) 26 (1978), 1-25.

[Co 1] Colmez, P. Algébricité de valeurs spéciales de fonctions L. Inv. Math. 95, 161-205 (1989).

[Co 2] Colmez, P. Résidu en $s = 1$ des fonctions zêta p-adiques. Inv. Math. 91, 371-389 (1988).

[D] Deligne, P. Valeurs de fonctions L et périodes d'intégrales. Proc. Symp. Pure Math. **33**, 313-346 (1979).

[d Sh] de Shalit, E. Iwasawa Theory of Elliptic Curves with Complex Multiplication. Perspectives in Mathematics, Vol. **3**, Academic Press, 1987.

[H-S] Harder, G., Schappacher, N., Special values of Hecke L-functions and Abelian Integrals. (Lecture Notes in Math., Vol. 1111, pp. 17-49). Berlin-Heidelberg-New York: Springer 1985.

[K] Katz, N., p-adic Interpolation of real analytic Eisenstein series. Ann. Math. 104 (1976), 459-571.

[L] Lang, S. Algebraic Number Theory. Addison-Wesley (1970).

[M-V] Manin, J., Višik, M. p-adic Hecke series of imaginary quadratic fields. Math. Sbornik (N.S.) 95 (1974), 357-383. English trans.: Math. USSR-Sb. 24 (1974), 345-371.

[P-R] Perrin-Riou, B. Périodes p-adiques. C.R.Acad. Sci. tôme 300, série 1 (1985), p. 455-457.

[Sch] Schmidt, W. Diophantine Approximation. Lecture Notes in Math. **785**, Berlin, Heidelberg, New York: Springer (1980). [Se] Serre, J.-P. Sur le résidu de la fonction zêta p-adique d'un corps de nombres. C. R. Acad. Sci. Paris **287**, 83-126 (1978), série A.

[Sh] Shintani, T. An evaluation of zeta-functions of totally real algebraic fields at non positive integers. J. Fac. Sci., Univ. Tokyo, Sect. IA, **23**, 393-417 (1976).

[T] Tilouine, J. Fonctions L p-adiques à deux variables et $\mathbf{Z}_p^2$-extensions. Bull. Soc. Math. France, 114 (1986), 3-66.

[Wa] Waldschmidt, M. Les travaux de C. V. Čudnovskiĭsur les Nombres Transcendents. Sém. Bourbaki 488 (1975/76), Lecture Notes in Math. **567**, Berlin, Heidelberg, New York: Springer (1977).

[W1] Weil, A. On a certain type of characters of the idèle class group of an algebraic number field. In: Proc. Int. Symp. on Alg. Number Theory Tokyo (1955), p. 1-7.

[W2] Weil, A. Elliptic functions according to Eisenstein and Kronecker. Springer-Verlag (1976).

[Y1] Yager, R. On two variable p-adic L functions. Ann. Math. 115 (1982), 411-449.

[Y2] Yager, R. p-adic measures on Galois groups. Inv. Math. 76 (1984), 331-343.

Article 3. Sous-groupes de $GL_2(\mathbf{F}_3)$ comme groupes de Galois.

Soit H un groupe fini et G une extension centrale non scindée de H par $\mathbf{Z}/2\mathbf{Z}$. Soit F un corps de caractéristique différent de 2 et K une extension galoisienne de F de groupe de Galois isomorphe à H. Soit $E(H, G, F, K)$ l'ensemble des corps L, quadratiques sur K et galoisiens sur F, tels que le diagramme suivant commute:

$$\begin{array}{ccc} \mathrm{Gal}(L/F) & \to & \mathrm{Gal}(K/F) \\ \downarrow & & \downarrow \\ H & \to & G. \end{array}$$

Quand F est un corps de nombres, Witt a calculé explicitement l'ensemble $E(\mathbf{Z}/2\mathbf{Z}, H_8, F, K)$. Dans cet article nous généralisons sa méthode pour calculer les ensembles $E(D_4, \tilde{D}_4, F, K)$, $E(A_4, SL_2(\mathbf{F}_3), F, K)$ et $E(S_4, GL_2(\mathbf{F}_3), F, K)$.

Explicit realisations of subgroups of $GL_2(\mathbb{F}_3)$ as Galois groups

Leila Schneps

Let F be a number field and K an extension of F with Galois group D_4 (resp. A_4 or S_4). In this article we explicitly construct all of the quadratic extensions L of K having Galois group $\tilde{D}_4$ (the 2-Sylow subgroup of $GL_2(\mathbb{F}_3)$) (resp. $SL_2(\mathbb{F}_3)$ or $GL_2(\mathbb{F}_3)$) over F, whenever such extensions exist.

We wish to thank the Max-Planck Institut für Mathematik for its hospitality and financial support during the preparation of this paper.

§1. Introduction

Let G be a finite group, and H an extension of G by $\{\pm 1\}$, i.e.

$$1 \to \{\pm 1\} \to H \to G \to 1.$$

Let $\{v_\sigma \in H \mid \sigma \in G\}$ be a set of representatives of $H/\{\pm 1\}$ such that $v_\sigma \to \sigma$ under reduction mod ± 1. Let F be a number field, and K a Galois extension of F having Galois group G. The following result is well-known:

Lemma 1: Let $A = \sum_\sigma Kv_\sigma = (K/F, \zeta_{\sigma,\tau})$ be the crossed-product algebra whose multiplicative law is given by

$$\alpha v_\sigma = v_\sigma \sigma(\alpha) \text{ for } \alpha \in K \quad \text{and} \quad v_\sigma v_\tau = \zeta_{\sigma,\tau} v_{\sigma\tau} \quad (\zeta_{\sigma,\tau} = \pm 1),$$

where the $\zeta_{\sigma,\tau}$ are given by multiplication in H. Let $E(K,F,G,H)$ be the set of quadratic extensions L of K, Galois over F of Galois group H and

such that the diagram $\begin{array}{ccc} \mathrm{Gal}(L/F) & \to & \mathrm{Gal}(K/F) \\ \downarrow & & \downarrow \\ G & \to & H \end{array}$ commutes. Then

$E(K,F,G,H)$ is non-empty if and only if the class of A in the Brauer group $Br(F)$ is equal to the identity class. Moreover if $\gamma \in K$ is such that $K(\sqrt{\gamma}) \in E(K,F,G,H)$, then $E = \{ K(\sqrt{r\gamma}) \mid r \in F \}$.

Proof: Suppose there exists $\gamma \in K$ such that $L = K(\sqrt{\gamma})$ is Galois over F of Galois group H. Let $\omega = \sqrt{\gamma}$: for each $\sigma \in \mathrm{Gal}(K/F)$, set $c_\sigma = v_\sigma(\omega)/\omega$. Then $c_\sigma \sigma(c_\tau) c_{\sigma\tau}^{-1} \zeta_{\sigma,\tau} = 1$, so the cocycle defining A is equivalent to the trivial cocycle and A splits. In the other direction, suppose such c_σ exist in K. Then $c_\sigma^2 \sigma(c_\tau)^2 = c_{\sigma\tau}^2$, so by Hilbert's Theorem 90, there exists $\gamma \in K$ such that $c_\sigma^2 = \sigma(\gamma)/\gamma$. But then $K(\omega)$ is Galois over F with Galois group H.

It is easy to see moreover that if $K(\sqrt{\gamma}) \in E(K,F,G,H)$ then so are the $K(\sqrt{r\gamma})$ for $r \in F$: if $K(\sqrt{\gamma})$ and $K(\sqrt{\lambda})$ are both in E one deduces the existence of $r \in F$ such that $\lambda = r\gamma$ from Hilbert's Theorem 90.

Let $\tilde{S}_4$ denote the central extension of S_4 by $\{\pm 1\}$ described in terms of generators and relations by :

$$t_i^2 = 1,\ w^2 = 1,\ wt_i = t_i w,\ (t_i t_{i+1})^3 = 1,\ t_1 t_3 = w t_3 t_1$$

for generators w, t_1, t_2, t_3 (see [2]). For the rest of this article we only consider $G \subset S_4$ and $H = \tilde{G}$, the lifting of G in $\tilde{S}_4$.

§2. The quaternion group H_3

Let G be the Vierergruppe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, which we identify with the subgroup $\{1, (12)(34), (13)(24), (14)(23)\} \subset S_4$. $\tilde{G}$ is the quaternion group H_3 of order 8. Let K/F be a biquadratic extension, the v_σ an the algebra A as in §1. Witt [4] constructs L explicitly whenever

A splits. We briefly recall his method here.

Let 1, σ_1, σ_2 and σ_3 be the elements of G, and let $\{ \xi_\sigma \mid \sigma \in G\}$ be a basis of K/F such that $\xi_1 = 1$, $\xi_\sigma^2 = a_\sigma \in F$, $\prod_{\sigma \in G} \xi_\sigma = 1$ and $\sigma(\xi_\tau) = \xi_{\sigma\tau}$. The v_σ generate a quaternion algebra $(-1,-1)$ over F and the $\xi_\tau v_\tau$ generate $(-a_{\sigma_1}, -a_{\sigma_2})$: since the v_σ commute with the $\xi_\tau v_\tau$, we have $A = (-1,-1) \otimes_F (-a_{\sigma_1}, -a_{\sigma_2})$.

The fact that A splits implies that $(-1,-1) \simeq (-a_{\sigma_1}, -a_{\sigma_2})$ and therefore there exist elements $p_{ij} \in F$ such that setting $w_{\sigma_i} = \sum_{j=1}^{3} p_{ij} v_{\sigma_j}$, we have $\sum_{i=1}^{3} w_{\sigma_i} = -1$ and $w_{\sigma_i}^2 = -1/a_{\sigma_i}$ for i=1,2,3. Let $w_1 = 1$. Witt now extends the scalars of $(-1,-1)$ to K (so K is now the center of this algebra), and sets $j_\sigma = \xi_\sigma w_\sigma$: he then constructs the element $C = \sum_{\sigma \in G} v_\sigma^{-1} j_\sigma$. This element is non-zero and verifies the identity $C j_\sigma C^{-1} = v_\sigma$ for each $\sigma \in G$. Replacing C by $v_\sigma C^\sigma$ in this equation also works. Now set $\mu_\sigma = v_\sigma C^\sigma C^{-1}$. Then since $\mu_\sigma v_\sigma \mu_\sigma^{-1} = (\mu_\sigma C) j_\sigma (\mu_\sigma C)^{-1} = v_\sigma$, we find that $\mu_\sigma \in K$. Let $\gamma = NC$ (the quaternion norm). Then $\gamma \in K$ and $\gamma^\sigma \gamma^{-1} = \mu_\sigma^2$ for all $\sigma \in G$, so $L = K(\sqrt{\gamma})$ is Galois over F. Moreover, the μ_σ satisfy the cocycle relation $\mu_\sigma \mu_\tau^\sigma / \mu_{\sigma\tau} = \zeta_{\sigma,\tau}$, and $(\zeta_{\sigma,\tau})$ is exactly the factor system describing H_8, so $Gal(K/F) = H_8$. Direct calculation shows that $\gamma = 1 + p_{11}\sigma_1 + p_{22}\sigma_2 + p_{33}\sigma_3$, so we have proved the following

Lemma 2: (Witt) Let K be an extension of F of Galois group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Then $E(K,F,H_8,\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) = \{ K(\sqrt{r\gamma}) \mid r \in F \}$, for γ defined as above.

§3. The generalized dihedral group $\tilde{D}_4$

We now let F be a number field and K a Galois extension of F such that $\mathrm{Gal}(K/F) = D_4$, the dihedral group of order 8. Such a field always occurs as the splitting field of a polynomial of the form

$$P(X) = X^4 + bX^2 + d, \quad b,d \in F,$$

where d, b^2-4d and $d(b^2-4d)$ are not squares in F. K contains three quadratic subfields, $F(\sqrt{b^2-4d})$, $F(\sqrt{D}) = F(\sqrt{d})$ (where $D = 16(b^2-4d)^2 d$ is the discriminant of the polynomial P(X)) and $F(\sqrt{d(b^2-4d)})$.

In Theorem 4 we explicitly give the set of Galois extensions of F containing K and having Galois group $\tilde{D}_4$ (this group is also known as the generalized dihedral group and is generated by elements a and b such that $a^4 = (ab)^2 = -1$ and $b^2 = 1$.)

Let α_1, α_2, α_3 and α_4 be the roots of P(X), numbered in such a way that $\alpha_1 + \alpha_3 = 0$. We have:

$$\alpha_1^2 = \alpha_3^2 = \frac{-b}{2} - \frac{\sqrt{b^2-4d}}{2} \quad \text{and} \quad \alpha_2^2 = \alpha_4^2 = \frac{-b}{2} + \frac{\sqrt{b^2-4d}}{2}.$$

$\mathrm{Gal}(K/F)$ is then the subgroup $\langle (1), (12)(34), (13)(24), (14)(23), (13), (24), (1234), (1432)\rangle \subset S_4$. $F(\alpha_1)$ is fixed by $\rho = (24)$.

Let $\xi_1 = \alpha_1 + \alpha_2$, $\xi_2 = 1/(\alpha_1+\alpha_2)(\alpha_1+\alpha_4) = -1/\sqrt{b^2-4d}$ and $\xi_3 = \alpha_1 + \alpha_4$ (we write ξ_i for ξ_{σ_i} in the preceding notation). Then $1, \xi_1, \xi_2$ and ξ_3 form a basis of $K/F(\sqrt{d})$. Moreover if for $1 \leq i \leq 3$ we define $a_i = \xi_i^2$, the a_i are in $F(\sqrt{d})$ and $\mathrm{Gal}(K/F(\sqrt{d})) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (identified with the subgroup

{1, (12)(34), (13)(24), (14)(23)} of D_4), so over $F(\sqrt{d})$ we are in the quaternion case of Witt. We form Witt's algebra

$(-1,-1) \otimes_{F(\sqrt{d})} (-a_1,-a_2)$.

Lemma 3: Let $(a,b)^\rho$ denote the part of the quaternion algebra (a,b) fixed by the action of ρ, this action being conjugation by v_ρ. Let A be the algebra associated to $\tilde{D}_4$ and D_4 as in Lemma 1. Then

$$[A] = [(-1,-1)^\rho \otimes_F (-a_1,-a_2)^\rho],$$

where $[A]$ denotes the class of A in the Brauer group $Br(F)$.

Proof: In fact, $A = (-1,-1)^\rho \otimes_F (-a_1,-a_2)^\rho \otimes_F (1,d)$ where $(1,d)$ is generated by v_ρ ($v_\rho^2 = 1$) and d. But $[(1,d)]$ is trivial in $Br(F)$.

The part of (a,b) fixed by ρ consists of the elements $x + v_\rho x v_\rho$ for all $x \in (a,b)$. $(-1,-1)$ is generated over $F(\sqrt{d})$ by v_1, v_2 and $v_3 = -1/v_1v_2$, so since $v_\rho v_1 v_\rho = -v_3$ and $v_\rho\, dv_2 v_\rho = dv_2$, $(-1,-1)^\rho$ is generated by $s_1 = v_1 - v_3$ and $s_2 = dv_2$. This gives the quaternion algebra $(-2,-d)$ over F. Similarly, setting $u_1 = \xi_1 v_1$, $u_2 = \xi_2 v_2$ and $u_3 = -\xi_3 v_3 = -1/u_1u_2$, the u_i generate $(-a_1,-a_2)$ over $F(\sqrt{d})$ and $t_1 = u_1 - u_3$, $t_2 = \sqrt{d}(b^2-4d)u_2$ generate $(-a_1,-a_2)^\rho = (2b,-d(b^2-4d))$ over F. Thus,

$$[A] = [(-2,-d) \otimes_F (2b,-d(b^2-4d))]$$

in the Brauer group $Br(F)$. We note that this algebra is equal to $(-2b,-d) \otimes_F (2b,b^2-4d) \otimes_F (2,d) = (\text{Witt invariant of } Tr(x^2)) \otimes_F (2,d)$, so the splitting of A is identical to the condition for the existence of L given in Serre's theorem [3].

If A splits then there exists an isomorphism of algebras

$\pi: (-2,-d) \to (2b,-d(b^2-4d))$, and elements $q_{ij} \in F$ such that $t_i = \sum_{j=1}^{3} q_{ij}\pi(s_j)$. By extension of scalars, the isomorphism f gives rise to a unique isomorphism $\pi: (-1,-1) \to (-a_1,-a_2)$ and an associated matrix $R = (r_{ij})$ such that:

$$u_i = \sum_{j=1}^{3} r_{ij}\pi(v_j), \quad i=1,2,3.$$

Let $P = (p_{ij}) = {}^tR^{-1}$. Then R is a "Witt's matrix", i.e. setting $\gamma = 1 + r_{11}\xi_1 + r_{22}\xi_2 + r_{33}\xi_3$, the field $L = K(\sqrt{\gamma})$ is Galois over $F(\sqrt{d})$ with Galois group H_8.

Theorem 4: Let K and γ be as above. Then $E(K,F,\tilde{D}_4,D_4) = \{K(\sqrt{r\gamma}) \mid r \in F\}$.

Proof: We first show that $\gamma^{\rho}\gamma^{-1}$ is a square in F. Define $w_i = \sum_{j=1}^{3} p_{ji}v_j$ for p_{ij} as above. Then $w_i^2 = -1/a_i$. Let $j_\sigma = \xi_\sigma w_\sigma$, and let C be the element $\sum_{\sigma\in G} v_\sigma^{-1} j_\sigma$ constructed by Witt in the algebra $(-1,-1)$ over K (with scalars extended to K). For any quaternion $q = a + bv_1 + cv_2 + dv_3$, $v_\rho q v_\rho = \rho(a) - \rho(b)v_3 - \rho(c)v_2 - \rho(d)v_2$, so $N(v_\rho q v_\rho) = \rho(Nq)$. Now, we saw before that the matrix $R = (r_{ij})$ corresponds to an isomorphism $\pi: (-1,-1) \to (-a_1,-a_2)$ satisfying $u_i = \sum_{j=1} r_{ij}\pi(v_j)$: this gives $w_i = \sum_{j=1} p_{ij}\pi(v_j)$!

If $q \in (-1,-1)$, $q = \sum_i a_i \times x_i$ for $a_i \in (-2,-d)$ and $x_i \in F(\sqrt{d})$, then $v_\rho q v_\rho = \sum_i a_i \otimes \rho(x_i)$ since ρ acts trivially on $(-2,-d)$. Thus, the isomorphism π commutes with conjugation by v_ρ on $(-1,-1)$. This allows us to calculate the $v_\rho w_i v_\rho$:

$v_\rho w_i v_\rho = v_\rho \pi(v_i) v_\rho = \pi(v_\rho v_i v_\rho) = -w_{4-i}$. Now we calculate

$$v_\rho C v_\rho = 1 + v_\rho(v_1^{-1}j_1)v_\rho + v_\rho(v_2^{-1}j_2)v_\rho + v_\rho(v_3^{-1}j_3)v_\rho$$

$$= 1 + v_\rho(v_1^{-1}\xi_1 w_1)v_\rho + v_\rho(v_2^{-1}\xi_2 w_2)v_\rho + v_\rho(v_3^{-1}\xi_3 w_3)v_\rho$$

$$= 1 + (-v_3^{-1})\rho(\xi_1)(-v_3) + (-v_2^{-1})\rho(\xi_2)(-v_2) + (v_1^{-1})\rho(\xi_3)(-v_1) = C$$

since $\rho(\xi_i) = \xi_{4-i}$. Thus, $\gamma^\rho = (\mathrm{NC})^\rho = \mathrm{N}(v_\rho C v_\rho) = \mathrm{NC} = \gamma$! One can further verify that if $\mu_\sigma = v_\sigma C^\sigma C^{-1}$ for $\sigma \in \{1, (12)(34), (13)(24), (14)(23)\}$ and $\mu_{\rho\sigma} = \mu_\sigma^\rho \zeta_{\rho,\sigma}$, the μ_σ verify the cocycle relation $\mu_\sigma \mu_\tau^\sigma / \mu_{\sigma\tau} = \zeta_{\sigma,\tau}$ for $\sigma, \tau \in D_4$ and therefore $\mathrm{Gal}(K(\sqrt{\gamma})/F) = \tilde{D}_4$ and $K(\sqrt{\gamma}) \in E(K, F, \tilde{D}_4, D_4)$. Lemma 1 suffices to conclude.

We remark in particular that the γ constructed in this way is in fact an element of $F(\alpha_1)$.

Example: Let $P(X) = X^4 - X^2 + d$, d, $1-4d$ and $d(1-4d)$ not squares in F. In this case, $(2b, -d(b^2-4d)) = (-2, -d(1-4d))$, so the condition for the existence of L becomes $(-2, -d(1-4d)) = (-2, -d)$, or $(-2, 1-4d) = 1$ in the Brauer group $\mathrm{Br}(F)$. This is equivalent to the condition

there exist $u, v \in F$ such that $-2u^2 + (1-4d)v^2 = 1$.

Suppose this condition is satisfied. Then a matrix Q as above is given by $Q^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{v(1-4d)} & \frac{2du}{v} \\ 0 & \frac{-u}{dv(1-4d)} & \frac{1}{v} \end{pmatrix}$, and this gives

$$t_P = \begin{pmatrix} \frac{1}{2va_1} + \frac{1}{2} & \frac{-u}{v} & \frac{1}{2va_3} - \frac{1}{2} \\ \frac{u}{va_1} & \frac{1}{v} & \frac{u}{va_3} \\ \frac{1}{2va_1} - \frac{1}{2} & \frac{-u}{v} & \frac{1}{2va_3} + \frac{1}{2} \end{pmatrix}.$$

Thus we can take $\gamma = 1 + (\frac{1}{2} + \frac{1}{2va_1})\xi_1 + (\frac{1}{v})\xi_2 + (\frac{1}{2} + \frac{1}{2va_3})\xi_3 =$

$$1 + \alpha_1 - \frac{1}{v\sqrt{1-4d}} - \frac{\alpha_1}{v\sqrt{1-4d}} \quad .$$

If $Q(X)$ is the minimal polynomial of this element, then $Q(X^2)$ is a polynomial having Galois group $\tilde{D}_4$.

§4. The group $\tilde{A}_4 \simeq SL_2(\mathbb{F}_3)$

Let $P(X)$ be a polynomial over F having splitting field K such that $Gal(K/F) = A_4$. Let $\Gamma = \{1, (12)(34), (13)(24), (14)(23)\} \subset A_4$, and let $R \subset K$ be the fixed field of Γ. Then $[R:F] = 3$ and $Gal(K/R) = \Gamma$, so over R we are in the quaternion case of Witt. Let $\tau = (234) \in A_4$, so τ fixes $F(\alpha_1)$.

Theorem 5: Suppose there exists an element $\gamma \in K$ such that $K(\sqrt{\gamma})$ is Galois over R with Galois group H_8. Set $\beta = \gamma\,\gamma^{\tau}\,\gamma^{\tau^2}$. Then $E(K, F, \tilde{A}_4, A_4) = \{ K(\sqrt{r\beta}) \mid r \in F \}$.

Proof: In order to show that $Gal(K(\sqrt{\beta})/F) = \tilde{A}_4$, we must show that $\beta\beta^{\sigma}$ is a square for all $\sigma \in A_4$. Now, $A_4 = \Gamma \times \langle 1, \tau, \tau^2 \rangle$, so we can write $\sigma = \delta\omega$, with $\delta \in \Gamma$ and $\omega \in \langle 1, \tau, \tau^2 \rangle$. Then $\beta\beta^{\sigma} = (\gamma\gamma^{\tau}\gamma^{\tau^2})(\gamma^{\delta\omega}\gamma^{\delta\omega\tau}\gamma^{\delta\omega\tau^2})$ $= (\gamma\gamma^{\tau}\gamma^{\tau^2})(\gamma^{\delta}\gamma^{\delta\tau}\gamma^{\delta\tau^2})$ since ω permutes 1, τ and τ^2. But $\Gamma = Gal(K/R)$, so $\gamma\gamma^{\delta}$ is a square in K for each $\delta \in \Gamma$. Moreover, writing $\delta\tau = \tau\delta_1$ and $\delta\tau^2 = \tau^2\delta_2$, we find that δ_1 and δ_2 are in Γ, so

$$\beta\beta^{\sigma} = (\gamma\gamma^{\delta})(\gamma^{\tau}\gamma^{\delta\tau})(\gamma^{\tau^2}\gamma^{\tau^2\delta}) = (\gamma\gamma^{\delta})(\gamma^{\tau}\gamma^{\tau\delta_1})(\gamma^{\tau^2}\gamma^{\tau^2\delta_2})$$

$$= (\gamma\gamma^{\delta})(\gamma\gamma^{\delta_1})^{\tau}(\gamma\gamma^{\delta_2})^{\tau^2} \quad \text{is a square.}$$

The usual remark on the cocycle relation satisfied by the μ_σ shows that $Gal(K(\sqrt{\beta})/F)$ is really $\tilde{A}_4$ and Lemma 1 suffices to conclude.

We remark that the β obtained in this way is an element of $F(\alpha_1)$.

Example: Let $P(X) = X^4 - 12X^2 - 8X + 9$. Then the discriminant of P is 1008^2 and it is easy to check that the Galois group of P over $\mathbb{Q}$ is A_4. Let α_1, α_2, α_3, α_4 be the roots of P(X). Let $\xi_1 = \alpha_1 + \alpha_3$, $\xi_2 = \alpha_1 + \alpha_4$, and $\xi_3 = -(\alpha_1 + \alpha_2)/8$. Then $\xi_1\xi_2\xi_3 = 1$ and together with 1, these elements form Witt's basis over the field $R = \mathbb{Q}((\alpha_1+\alpha_3)^2)$. Let K be the splitting field of P(X). For $1 \leq i \leq 3$, let $a_i = \xi_i^2$. Witt's methods give the following expression for an element γ such that $K(\sqrt{\gamma})$ is Galois over R of Galois group H_8:

$$\gamma = 672+(-8-192a_2a_3+4a_1)\xi_1+(-192+320a_1a_3+12a_2)\xi_2+(1472-8a_1a_2-4096a_3)\xi_3.$$

Let τ be the permutation of the roots given by the 3-cycle (234), and let $\beta = (\gamma\ \gamma^\tau\ \gamma^{\tau^2})/(2^{11}\cdot 7^2)$. Then if Q(X) is the minimal polynomial of β, $Q(X^2)$ has Galois group $\tilde{A}_4$ over $\mathbb{Q}$: we have

$$Q(X^2) = X^8 - 12884X^6 + 41492682X^4 - 7985480580X^2 - 5051798406522$$

$$= X^8 - 2^2\cdot 3221X^6 + 2\cdot 3^3\cdot 7\cdot 11\cdot 17\cdot 587X^4 - 2^2\cdot 3^7\cdot 5\cdot 7\cdot 11\cdot 2371X^2$$
$$- 2\cdot 3^6\cdot 7\cdot 494983187.$$

§5. The group $\tilde{S}_4 \simeq GL_2(\mathbb{F}_3)$

The argument is analogous to that for A_4, using D_4 instead of Γ. Let $Gal(K/F) = S_4$, and let $D_4 \subset S_4$ be given by $\{1, (12)(34), (13)(24), (14)(23), (13), (24), (1234), (1432)\} \subset S_4$. Let R be the fixed field of D_4. Then $[R:F] = 3$, but R is not Galois over F. Let $\tau = (234) \in S_4$. Then $\tau^{-1}D_4\tau = Gal(K/R^{\tau})$ and $\tau D_4 \tau^{-1} = Gal(K/R^{\tau^2})$.

Theorem 6: Suppose there exists γ in K such that $K(\gamma)$ is Galois over R with Galois group D_4. Let $\beta = \gamma\gamma^{\tau}\gamma^{\tau^2}$. Then $K(\sqrt{\beta})$ is Galois over F with Galois group $\tilde{S}_4$, and therefore $E(K, F, \tilde{S}_4, S_4) = \{ K(\sqrt{r\beta}) \mid r \in F \}$.

Proof: As before, we must show that $\beta\beta^{\sigma}$ is a square in K for all $\sigma \in K$. We first suppose that $\sigma \in S_3 = \{1, (234), (243), (23), 24), 34)\}$, i.e. the set of elements of S_4 fixing $F(\alpha_1)$. Now, by the argument for D_4, we know that $\gamma \in R(\alpha_1)$ and therefore $\beta \in F(\alpha_1)$, so $\beta\beta^{\sigma} = \beta^2$ in K. Next we let $\sigma \in \Gamma = \{1, (12)(34), (13)(24), (14)(23)\}$. This subgroup is normal in S_4 and therefore $\beta\beta^{\sigma}$ is a square in K by the same argument as in the case of A_4. Now, $S_4 = \Gamma \times S_3$, so any $\sigma \in S_4$ can be written $\sigma = \delta\omega$, $\delta \in \Gamma$, $\omega \in S_3$. Then $\beta\beta^{\sigma} = \beta\beta^{\delta\omega} = \beta\beta^{\delta}\beta^{\delta}\beta^{\delta\omega}(\beta^{\delta})^{-2} = (\beta\beta^{\delta})(\beta\beta^{\omega})^{\delta}(\beta^{\delta})^{-2}$ which is a square in K.

We note that we may use these methods to derive Serre's theorem directly for n=4 (see [3]).

Lemma 7: Let P(X) be a polynomial over F with splitting field K, and Galois group S_4: we assume P has the form $X^4 + bX^2 + cX + d$. Let $W_2(P)$ be the Witt invariant of the quadratic form $Tr_{K/F}(x^2)$. Then there exists a quadratic extension L of K such that L is Galois over F with

Galois group $\tilde{S}_4$ if and only if the algebra $B = W_2(P) \otimes_F (2,D)$ splits in $Br(F)$, where D is the discriminant of P.

Proof: Let α_1, α_2, α_3 and α_4 be the roots of $P(X)$, and let $Y = (\alpha_1+\alpha_3)^2$. Let R be the field $F(Y)$. Then $[R:F] = 3$, and a polynomial over R having K as splitting field and D_4 as Galois group is :

$$X^4 + (2Y-4b)X^2 + (16d-4bY-3Y^2),$$

obtained by taking $Q(X^2)$, where $Q(X)$ is the minimal polynomial of $(\alpha_1-\alpha_3)^2$ over R. Let $W_2(Q)$ be the Witt invariant of $Tr_{K/R}(x^2)$. By Lemma 5, in order to show existence of L, it suffices to prove existence of L' containing K such that $Gal(L'/R) = \tilde{D}_4$. In §3, we saw that L' exists if and only if $A = W_2(Q) \otimes_R (2,D_Q)$ splits in $Br(R)$ where D_Q is the discriminant of $Q(X^2)$. But $W_2(Q) = W_2(P) \otimes_F R$ and $(2,D_Q) = (2,D) \otimes_F R$, so $A = B \otimes_F R$. But if A splits, either B splits or R is a neutralising field for this B. Since $[R:F] = 3$, R cannot be isomorphic to a maximal commutative subfield of B, so B must split over F.

Corollary: Suppose $P(X)$ has the form $X^4 + cX + d$. Let D be the discriminant of P. Then the condition for L to exist is $(-2,-D)$ splits, i.e. there exist $u,v \in F$ such that $-D = 2u^2 + v^2$.

Proof: In this case the polynomial over R whose splitting field is K is given by

$$X^4 + 2(\alpha_1+\alpha_3)^2X^2 + (16d-3(\alpha_1+\alpha_3)^4).$$

It is easy to see that up to squares in R, if we let $Y = (\alpha_1+\alpha_3)^2$, then $Y = Y^2-4d$ and $D = 16d-3Y^2$. An extension L of K with $Gal(L/R) = \tilde{D}_4$

exists if and only if $(-2,-D)(Y,-DY)$ splits: but in this case $(Y,-DY) = (Y,D) = (Y^2-4d, 16d-3Y^2)$ splits because $4(Y^2-4d) + (16d-3Y^2) = Y^2$ which is a square in R. So $(-2,-D)$ must split for L to exist.

References

[1] I. Reiner, Maximal Orders. Academic Press, London, New York, San Francisco, 1975.

[2] I. Schur, Über die Darstellung der symmetrischen und der alternierenden Gruppe durch gebrochene lineare Substitutionen, J. Reine Angew. Math. 139 (1911), 155-250.

[3] J-P. Serre, L'invariant de Witt de la forme $Tr(x^2)$, Comment. Math. Helvetici 59 (1984), 651-676.

[4] E. Witt, Konstruktion von galoisschen Körper der Charakteristik p zu vorgegebener Gruppe der Ordnung p^r. J. Reine Angew. Math. 174 (1936), 237-245.

Leila Schneps
Max-Planck Institut für Mathematik
Gottfried-Clarenstraße 26
5300 Bonn 3

Article 4. $\tilde{D}_4$ et $\hat{D}_4$ comme groupes de Galois.

Soit $E(H, G, F, K)$ comme dans l'article précédent. Nous calculons explicitement $E(D_4, \tilde{D}_4, F, K)$ pour tout corps F de caractéristique différent de 2 et $E(D_4, \hat{D}_4, F, K)$ pour tout corps global F. Cette méthode nous permet de donner des exemples explicites d'extensions régulières de $\mathbf{Q}(t)$ de groupe de Galois $\tilde{D}_4$ et $\hat{D}_4$.

C. R. Acad. Sci. Paris, t. 308, Série I, p. 33-36, 1989

Algèbre/*Algebra*

$\tilde{D}_4$ et $\hat{D}_4$ comme groupes de Galois

Leila SCHNEPS

Résumé — On construit explicitement des corps ayant $\tilde{D}_4$ ou $\hat{D}_4$ comme groupe de Galois.

$\tilde{D}_4$ and $\hat{D}_4$ as Galois groups

Abstract — *Explicit fields having $\tilde{D}_4$ or $\hat{D}_4$ as Galois groups are constructed.*

Soit H un groupe fini, et soit G une extension centrale non scindée de H par C_2, le groupe multiplicatif $\{1, \omega\}$ d'ordre 2. Le groupe G satisfait $1 \to C_2 \to G \to H \to 1$. Soit F un corps de caractéristique différente de 2, et soit K une extension galoisienne de F telle que $\mathrm{Gal}(K/F) \cong H$. Soit $E(H, G, F, K)$ l'ensemble des corps L quadratiques sur K et galoisiens sur F tels que $\mathrm{Gal}(L/F) \cong G$ et que le diagramme $\begin{array}{ccc} \mathrm{Gal}(L/F) & \to & \mathrm{Gal}(K/F) \\ \downarrow & & \downarrow \\ G & \to & H \end{array}$ commute. Dans ce qui suit, nous prenons $H = D_4$, le groupe diédral d'ordre 8 dont on fixe un plongement dans S_4, et G l'un des deux groupes $\tilde{D}_4$ et $\hat{D}_4$ qui apparaissent comme 2-sous-groupes de Sylow des groupes $\tilde{S}_4$ et $\hat{S}_4$ [1]. Nous donnons une description explicite de $E(D_4, \tilde{D}_4, F, K)$ et une description de $E(D_4, \hat{D}_4, F, K)$ dans le cas où F est un corps vérifiant certaines conditions, par exemple quand F est un corps global. Nous utilisons des méthodes basées sur des idées de Witt [2], que nous illustrons par des exemples d'extensions régulières de $\mathbf{Q}(t)$ de groupe de Galois $\tilde{D}_4$ et $\hat{D}_4$.

Nous tenons à remercier le Max-Planck Institut für Mathematik pour son hospitalité et son soutien financier pendant la préparation de cette Note.

1. LE THÉORÈME DE WITT POUR LE GROUPE DES QUATERNIONS H_8. — Soit $\Gamma = \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ et soit K une extension d'un corps R de caractéristique différente de 2, telle que $\mathrm{Gal}(K/R) \cong \Gamma$. Écrivons $\Gamma = \{1, \sigma_1, \sigma_2, \sigma_3\}$. Soit $\{\xi_\sigma \mid \sigma \in \Gamma\}$ une base de K sur R satisfaisant $\xi_1 = 1$, $\prod_\sigma \xi_\sigma = 1$, $\sigma(\xi_\sigma) = \xi_\sigma$ et $\xi_\sigma^2 \in R$. Posons $a_\sigma = \xi_\sigma^2$.

Witt s'intéresse au groupe des quaternions H_8, qui est une extension de Γ par C_2. Soit $\{h_\sigma \mid \sigma \in \Gamma\}$ un système de représentants de H_8/C_2. Pour $\sigma, \tau \in \Gamma$ on définit $\zeta_{\sigma,\tau} = h_\sigma h_\tau h_{\sigma\tau}^{-1}$, où $\zeta_{\sigma,\tau}$ est un élément de $C_2 = \{1, \omega\}$ que l'on identifie avec $\{1, -1\}$. Soit T le produit croisé $(K/R, \zeta_{\sigma,\tau})$. Rappelons que T est une algèbre centrale simple de dimension 16, contenant K. Soit $\{v_\sigma \mid \sigma \in \Gamma\}$ une base de T telle que $T = \sum_{\sigma \in \Gamma} K v_\sigma$ avec $v_\sigma v_\tau = \zeta_{\sigma,\tau} v_{\sigma\tau}$ et $v_\sigma \alpha = \sigma(\alpha) v_\sigma$ si $\alpha \in K$. Soit A la sous-algèbre de T engendrée par les v_σ pour $\sigma \in \Gamma$ et B celle engendrée par les $\xi_\sigma v_\sigma$ pour $\sigma \in \Gamma$. Les algèbres A et B sont isomorphes respectivement aux algèbres de quaternions $(-1, -1)$ et $(-a_{\sigma_1}, -a_{\sigma_2})$. On voit facilement que $T = A \otimes_R B$. Il est connu que $E(\Gamma, H_8, R, K)$ est non vide si et seulement si T est décomposée.

THÉORÈME 1 (Witt [2]). — *Supposons que* T *soit décomposée, donc qu'il existe un isomorphisme d'algèbres* $g : A \xrightarrow{\sim} B$. *Pour un tel g, soit* $c_g \in A \otimes_R K$ *le quaternion* $c_g = \sum_{\tau \in \Gamma} v_\tau^{-1} \xi_\tau^{-1} g^{-1}(\xi_\tau v_\tau)$. *Soit* $\gamma = N_A c_g$ *la norme de* c_g. *Alors les éléments de* $E(\Gamma, H_8, R, K)$ *sont les* $L_r = K(\sqrt{r\gamma})$, *où r parcourt* R^*.

Note présentée par Jean-Pierre SERRE.

0249-6291/89/03080033 $ 2.00

De plus, en posant $\delta_\sigma = v_\sigma c_g^\sigma c_g^{-1}$ pour $\sigma \in \Gamma$ et $\delta_{\rho\sigma} = \delta_\sigma^\rho \zeta_{\rho,\sigma}$, on constate que $\delta_\sigma \delta_\tau \delta_{\sigma\tau}^{-1} = \zeta_{\sigma,\tau}$ pour tout σ, $\tau \in D_4$ et donc que $\mathrm{Gal}(L/F)$ est bien $\tilde{D}_4$. On a donc montré que L est dans $E(D_4, \tilde{D}_4, F, K)$. Les autres éléments sont donnés par $K(\sqrt{r\gamma})$, $r \in F^*$.

Cas 2. — $G = \hat{D}_4$ et F est un corps global. Le fait que T est décomposée signifie que les algèbres $A_1 = A^\rho \otimes_F (-1, d)$ et $B_1 = B^\rho \otimes_F (1, d)$ sont isomorphes. L'algèbre A_1 est engendrée par A et un élément α tel que $\alpha^2 = -1$ et $\alpha^{-1} x \alpha = x^\rho$ pour tout $x \in A$. De même B_1 est engendrée par B et un élément β tel que $\beta^2 = 1$ et $\beta y \beta = y^\rho$ pour tout $y \in B$.

On a $A = A^\rho \otimes_F R$ et $B^\rho \otimes_F R$; comme $(-1, d)$ et $(1, d)$ sont décomposées sur R, l'hypothèse $A_1 \cong B_1$ entraîne $A \cong B$. D'après le théorème de Skolem-Noether, il existe un isomorphisme $h : A_1 \xrightarrow{\sim} B_1$ qui applique A sur B et est R-linéaire. A un tel h on associe un élément $\lambda(h)$ de B tel que $h(\sqrt{d}.\alpha) = \lambda(h)\beta$ (notons que, puisque $h(\sqrt{d}.\alpha)$ anticommute avec $\sqrt{d}$, il se trouve forcément dans $B\beta$). L'élément $\lambda(h)$ a les deux propriétés suivantes :

(i) $\lambda(h)\beta\lambda(h)\beta = \lambda(h)\lambda(h)^\rho = d$.

(ii) Pour $x \in A$, on a $(\lambda(h)\beta)^{-1} h(x)(\lambda(h)\beta) = h(x)$, autrement dit

$$\beta h(x) \beta = h(x)^\rho = \lambda(h)^{-1} h(x) \lambda(h).$$

LEMME. — *On peut choisir h de telle sorte que* $N_B \lambda(h) = d$.

Démonstration. — Choisissons un isomorphisme $h_0 : A_1 \xrightarrow{\sim} B_1$ comme ci-dessus. Pour tout $q \in B^*$, $q^{-1} h_0 q$ est aussi un tel isomorphisme. Nous allons construire un $q \in B^*$ tel que $N_B(\lambda(q^{-1} h_0 q)) = d$. On commence par remarquer que

$$\lambda(q^{-1} h_0 q)\beta = q^{-1} h_0(\sqrt{d}.\alpha) q = q^{-1} \lambda(h_0) \beta q = q^{-1} \lambda(h_0) q^\rho \beta.$$

Donc $N_B \lambda(q^{-1} h_0 q) = (N_B \lambda(h_0))(N_B q)^\rho (N_B q)^{-1}$. Soit $z = N_B(\lambda(h_0))/d \in F(\sqrt{d})$. On a alors $zz^\rho = 1$ et donc par le théorème 90 de Hilbert, il existe $y \in F(\sqrt{d})$ tel que $z = y/y^\rho$. Donc $(N_B(\lambda(h_0)) y^\rho / y = d$. On remarque qu'à chaque place réelle de $F(\sqrt{d})$ où $N_B x$ est définie positive, z est positif et donc y et y^ρ ont même signe : on peut donc rendre y positif à chacune de ces places en le multipliant par un élément convenable de F. Or, la norme d'un quaternion est une forme quadratique à 4 variables, donc par le théorème de Hasse-Minkowski, l'équation $N_B q = y$ a une solution dans B. On pose $h(x) = q^{-1} h_0(x) q$, ce qui permet de conclure.

Choisissons h comme dans le lemme, et soit g sa restriction à A, qui est un isomorphisme de A sur B. L'application $x \mapsto f_g(x) = \alpha^{-1} g^{-1}(\beta g(x) \beta)\alpha$ est un automorphisme de A. Il existe donc un élément $u \in A^*$ tel que $u^{-1} x u = \alpha^{-1} g^{-1}(\beta g(x)\beta)\alpha$ pour tout $x \in A$. Pour tout $x \in A$,

$$u^{-1} x u = \alpha^{-1} g^{-1}(\beta g(x)\beta)\alpha$$
$$= \alpha^{-1} g^{-1}(\lambda(h)^{-1} g(x) \lambda(h))\alpha = \alpha^{-1} g^{-1}(\lambda(h)^{-1})\alpha x \alpha^{-1} g^{-1}(\lambda(h))\alpha,$$

donc $u = \alpha^{-1} g^{-1}(\lambda(h))\alpha$. Ceci donne $N_A u = N_A(g^{-1}(\lambda(h))^\rho = N_A(\lambda(h))^\rho = d$ par le lemme.

Soit $\gamma = N_A c_g$ la norme du quaternion $c_g \in A \otimes_R K$ associé à g. Comme dans le cas $G = \tilde{D}_4$, pour montrer que L est galoisien sur F il suffit de montrer que $\gamma^\rho \gamma^{-1}$ est un carré dans K. Tout d'abord, on a

$$c_g = \sum_{\tau \in \Gamma} (-v_{\rho\tau\rho})^{-1} (v_\rho^{-1} \xi_\tau^{-1} g^{-1}(\xi_\tau v_\tau) v_\rho)$$
$$= \sum_{\tau \in \Gamma} (-v_{\rho\tau\rho})^{-1} \rho(\xi_\tau)^{-1} \alpha^{-1} g^{-1}(\xi_\tau v_\tau)\alpha$$
$$= \sum_{\tau \in \Gamma} (-v_{\rho\tau\rho})^{-1} \xi_{\rho\tau\rho}^{-1} u^{-1} g^{-1}(\beta \xi_\tau v_\tau \beta) u$$
$$= \sum_{\tau \in \Gamma} -v_{\rho\tau\rho}^{-1} \xi_{\rho\tau\rho}^{-1} u^{-1} g^{-1}(-\xi_{\rho\tau\rho} v_{\rho\tau\rho}) u = \sum_{\tau \in \Gamma} v_\tau^{-1} \xi_\tau^{-1} u^{-1} g^{-1}(\xi_\tau v_\tau) u.$$

On emploie alors l'identité suivante, facile à vérifier :

$$v_\tau^{-1} = c_g(\xi_\tau^{-1} g^{-1}(\xi_\tau v_\tau))\, c_g^{-1} = c_g^\rho (u^{-1}\xi_\tau^{-1} g^{-1}(\xi_\tau v_\tau) u)\,(c_g^\rho)^{-1}.$$

On en tire : $c_g^{-1} c_g^\rho u^{-1}(\xi_\tau^{-1} g^{-1}(\xi_\tau v_\tau)) = (\xi_\tau^{-1} g^{-1}(\xi_\tau v_\tau))\, c_g^{-1} c_g^\rho u^{-1}$, d'où le fait que $c_g^{-1} c_g^\rho u^{-1}$ est dans le centre de $A \otimes_R K$, donc dans K. Donc $N_A c_g = N_A c_g . N_A u$ modulo $(K^*)^2$. Mais par construction $N_A u = d$, qui est un carré dans K. On voit donc que $L = K(\sqrt{\gamma})$ est galoisien sur F. Pour vérifier que Gal(L/F) est bien $\hat{D}_4$, on remarque qu'en posant $\delta_\sigma = v_\sigma c_g^\sigma c_g^{-1}$ pour $\sigma \in \Gamma$ et $\delta_\rho = \sqrt{d}.c_g^{-1} c_g^\rho u^{-1}$ on a $\delta_\sigma \delta_\tau \delta_{\sigma\tau}^{-1} = \zeta_{\sigma,\tau}$ pour tout $\sigma, \tau \in D_4$. Donc $K(\sqrt{\gamma}) \in E(D_4, \hat{D}_4, F, K)$ et les autres éléments sont les $K(\sqrt{r\gamma})$ où r parcourt F^*.

Exemples. — Soit $P(X) = X^4 - X^2 + d$, où d, $1-4d$ et $d(1-4d)$ ne sont pas des carrés dans F, et soient α_1, α_2, α_3 et α_4 les racines de P(X) comme ci-dessus.

Cas 1. — $G = \tilde{D}_4$. On a $A^\rho = (-2, -d)$ et $B^\rho = (-2, -d(1-4d))$, donc si $A^\rho = B^\rho$ il existe u et $v \in F$ tels que $-2u^2 + (1-4d)v^2 = 1$. La méthode décrite ci-dessus donne

$$\gamma = 1 + \alpha_1 - \frac{1}{v\sqrt{1-4d}} - \frac{1}{v\sqrt{1-4d}}\alpha_1, \qquad \text{où} \qquad \sqrt{1-4d} = \frac{1}{2} - \alpha_1^2.$$

Soit Q(X) le polynôme minimal de γ. Alors le groupe de Galois de $Q(X^2)$ est $\tilde{D}_4$ et

$$Q(X^2) = X^8 - 4X^6 + \left(\frac{2v + 10u^2 v - 2 - 4u^2}{v(1+2u^2)}\right)X^4 - \left(\frac{4u^2(v-1)}{v(1+2u^2)}\right)X^2 + \left(\frac{4u^4 d}{(1+2u^2)^2}\right).$$

En prenant $v = 2$, par exemple, et $u = t$, ce polynôme donne une extension régulière de $\mathbf{Q}(t)$ de groupe de Galois $\tilde{D}_4$.

Cas 2. — $G = \hat{D}_4$. On considère le cas où l'algèbre $(-1, d)$ est décomposée : dans ce cas on n'a pas besoin de supposer que F est un corps global. Si $(-1, d)$ est décomposée, il existe x et $y \in F$ tels que $-x^2 + dy^2 = 1$. On envoie A^ρ sur B^ρ comme dans le cas 1 et $\alpha \mapsto x\beta + y\beta\sqrt{d}$. Posons $\lambda = -yd + x\sqrt{d} \in F(\sqrt{d})$. Alors la méthode décrite ci-dessus permet de calculer

$$\gamma = (2yd\lambda)\left[1 + \alpha_1 - \frac{1}{v\sqrt{1-4d}} - \frac{1}{v\sqrt{1-4d}}\alpha_1\right].$$

On en déduit des extensions régulières de $\mathbf{Q}(t)$ à groupe de Galois le groupe quaternionien d'ordre 16.

Note remise le 21 novembre 1988, acceptée le 23 novembre 1988.

RÉFÉRENCES BIBLIOGRAPHIQUES

[1] I. SCHUR, Über die Darstellung der symmetrischen und der alternierenden Gruppe durch gebrochene lineare Substitutionen, *J. reine angew. Math.*, 139, 1911, p. 155-250 (*Ges. Abh.*, I, p. 346-441).

[2] E. WITT, Konstruktion von galoisschen Körpern der Charakteristik p zu vorgegebener Gruppe der Ordnung p^f, *J. reine angew. Math.*, 174, 1935, p. 237-245.

Max-Planck Institut für Mathematik,
Gottfried-Clarenstrasse 26, 5300 *Bonn* 3, *R.F.A.*