ON TWO VARIABLE p-ADIC L-FUNCTIONS

by

Rodney Ian Yager

This thesis was submitted to the

Australian National University

for the degree of

Doctor of Philosophy

July, 1981

STATEMENT

Except where otherwise indicated, the work presented in this thesis is my own.

Rodney Ian Yager

Rodney I. Yager

ACKNOWLEDGEMENTS

The work presented in this thesis was undertaken at the Australian National University and, for a period of eighteen months, at the Université de Paris-Sud. I would like to thank both these institutions for the excellent facilities which they provided for my research, and for the willing assistance which I obtained from each member of staff.

Particular thanks are due to my supervisor, John Coates, who introduced me to the problems considered in this thesis, and whose door was always open to listen to my ideas and answer my many questions. I cannot overstate my indebtedness for his constant encouragement during the last three and a half years, and for his invaluable suggestions and comments on the numerous drafts of this thesis.

I would also like to thank Mrs B.M. Geary, who typed this thesis with her usual skill, care and attention to detail. My wife, Elsie, who helped me proof-read this thesis, and my family also deserve thanks for their constant love and support, without which this work would not have been possible.

Many others have contributed in various ways to the completion of this work, and to all of them I express my sincere thanks, hoping that I may be forgiven for not mentioning them each by name.

Finally, I would like to acknowledge the financial support which I received from the Australian Government, in the form of a Commonwealth Postgraduate Research Award, throughout the period of my research, except for a portion of my stay in France, during which I received a French Government Scholarship. The Australian National University also provided me with a small additional allowance for the entire period of my research, and bore the cost of my travel to and from France.

ABSTRACT

Let E be an elliptic curve defined over an imaginary quadratic field K with complex multiplication by the ring of integers of K. It has long been felt that certain special values of the complex Hecke L-functions attached to powers of the Grossencharacter of the curve E over K are deeply related to the arithmetic of the curve.

Recent results of Katz have shown the existence of two variable p-adic L-functions which interpolate these special values. The purpose of this thesis is to relate these p-adic L-functions to the arithmetic of the curve E. In particular, it will be shown that they are the characteristic power series of certain Iwasawa modules attached to the curve E.

CONTENTS

CHAPTER 1

INTRODUCTION

Let K be an imaginary quadratic field with class number 1 , and $\mathcal{O}$ the ring of integers of K . In this thesis, we shall study the arithmetic of an elliptic curve E defined over K with complex multiplication by $\mathcal{O}$. Let ψ be the Grossencharacter attached to the curve E over K by the theory of complex multiplication, and let $L(\bar{\psi}^k, s)$ be the complex Hecke L-function attached to the powers of ψ $(k = 1, 2, 3, \ldots)$; here we have fixed an embedding of K in $\mathbb{C}$. As Eisenstein seems to have been the first to suggest (see [13]), certain special values of these Hecke L-functions seem to be deeply related to the arithmetic of E . The underlying idea of this thesis is to exhibit some of these connections.

To state our results precisely, we first recall the work of Višik-Manin [12] and Katz [6] on the p-adic interpolation of these special values. Let p be a prime number $\neq 2, 3$, such that E has good reduction above p . In addition, we always assume that p splits in K , say $(p) = \mathfrak{p}\mathfrak{p}^*$ (very little is known about either p-adic interpolation or classical descent theory relative to powers of p when this is not the case). Fix a Weierstrass model for E

$$y^2 = 4x^3 - g_2x - g_3 \tag{1}$$

such that g_2 and g_3 belong to $\mathcal{O}$ and the discriminant of (1) is prime to p . Let L be the period lattice of the Weierstrass $\wp$-function associated with our model, and choose an element $\Omega_\infty \in L$ such that

$L = \Omega_\infty \mathcal{O}$. Then, if $-d_K$ denotes the discriminant of K , Damerell's Theorem shows that the numbers

$$\left(2\pi/\sqrt{d_K}\right)^j \Omega_\infty^{-(k+j)} L\left(\overline{\psi}^{k+j}, k\right)$$

are algebraic, and in fact belong to K for integers k and j satisfying $0 \leq j < k$.

For each pair of integers i_1 and i_2 modulo $(p-1)$, Katz has proved the existence of a power series $G^{(i_1,i_2)}(T_1, T_2)$ with coefficients in the ring of integers $\hat{I}_\infty$ of a certain unramified extension of the completion of K at $\underline{\underline{p}}$ with the following interpolation property. If $0 \leq j < k$, we write

$$L_\infty\left(\overline{\psi}^{k+j}, k\right) = \left(1-\psi(\underline{\underline{p}})^{k+j}/(N\underline{\underline{p}})^{j+1}\right)\left(1-\overline{\psi}(\underline{\underline{p}}^*)^{k+j}/(N\underline{\underline{p}}^*)^k\right) \left(2\pi/\sqrt{d_K}\right)^j \Omega_\infty^{-(k+j)} L\left(\overline{\psi}^{k+j}, k\right) \quad (2)$$

and we fix a topological generator u of $\left(1+p\mathbb{Z}_p\right)^\times$. Then, for each pair of integers k_1 and k_2 satisfying $k_1 > -k_2 \geq 0$ and $\left(k_1, k_2\right) \equiv \left(i_1, i_2\right)$ modulo $(p-1)$,

$$G^{(i_1,i_2)}\left(u^{k_1}-1, u^{k_2}-1\right) = \left(k_1-1\right)!\,\Omega_{\underline{\underline{p}}}^{k_2-k_1} L_\infty\left(\overline{\psi}^{k_1-k_2}, k_1\right)$$

where $\Omega_{\underline{\underline{p}}}$ is a certain unit in $\hat{I}_\infty$ which may be regarded as the $\underline{\underline{p}}$-adic analogue of the period Ω_∞ of E. (For more precise details, see Chapters 5 and 9.) Similar functions also exist if $p = 2$ or 3 .

In the spirit of Iwasawa and of Coates and Wiles, we shall relate these interpolating power series to the structure of a certain Iwasawa module attached to the elliptic curve E. If α is an element of $\mathcal{O}$, we let E_α be the kernel of the endomorphism α of E, and for each $n \geq 0$, we put $K_n = K(E_{\underline{\underline{p}}^{n+1}})$. Let $U_{n,\nu}$ be the local units of the completion of K_n at a prime ν which are congruent to 1 modulo ν, and put $\mathsf{U}_n = \prod_{\nu|\underline{\underline{p}}} U_{n,\nu}$, where the product is taken over all primes of K_n lying above $\underline{\underline{p}}$. Robert's group of elliptic units C_n for the field K_n (see Chapters 4 and 9 for a precise definition) can be embedded in U_n by the diagonal map, and we denote by $\overline{C}_n$ their closure in U_n. Let $\psi(\underline{\underline{p}}) = \pi$ and $\psi(\underline{\underline{p}}^*) = \pi^*$, and denote the canonical characters with values in Z_p giving the action of the Galois group G_0 of K_0 over K on E_π and E_{π^*} by χ_1 and χ_2 respectively. For each pair of integers i_1 and i_2 modulo $(p-1)$, we write $(\mathsf{U}_n/\overline{C}_n)^{(i_1,i_2)}$ for the eigenspace of $\mathsf{U}_n/\overline{C}_n$ on which G_0 acts *via* $\chi_1^{i_1}\chi_2^{i_2}$. Let $K_\infty = \bigcup_{n\geq 0} K_n$, and write Γ for the Galois group of K_∞ over K_0. Then

$$Y_\infty^{(i_1,i_2)} = \varprojlim (\mathsf{U}_n/\overline{C}_n)^{(i_1,i_2)},$$

where the projective limit is taken relative to the norm maps, has a natural structure as a module over the Iwasawa algebra $\mathsf{Z}_p[[\Gamma]]$.

Let $\Lambda = \mathsf{Z}_p[[T_1, T_2]]$ be the ring of formal power series in indeterminates T_1 and T_2 with coefficients in Z_p. The canonical characters κ_1 and κ_2 with values in Z_p giving the action of Γ on $E_{\pi^{n+1}}$ and $E_{\pi^{*n+1}}$ $(n = 0, 1, 2, \ldots)$ respectively, give rise to an isomorphism $(\kappa_1, \kappa_2) : \Gamma \xrightarrow{\sim} (1+p\mathbb{Z}_p)^{\times 2}$. If we let γ_1 and γ_2 denote the unique elements of Γ such that $\kappa_1(\gamma_1) = \kappa_2(\gamma_2) = u$ and $\kappa_1(\gamma_2) = \kappa_2(\gamma_1) = 1$, then γ_1 and γ_2 are topological generators of Γ , and we can make $Y_\infty^{(i_1,i_2)}$ a Λ-module by setting $(1+T_1)y = \gamma_1 y$ and $(1+T_2)y = \gamma_2 y$ for all $y \in Y_\infty^{(i_1,i_2)}$. Our main result is as follows.

THEOREM 1. *The characteristic power series of* $Y_\infty^{(i_1,i_2)}$ *is a power series in* Λ *generating the same ideal in* $\hat{I}_\infty[[T_1, T_2]]$ *as Katz's interpolating power series* $G^{(i_1,i_2)}(T_1, T_2)$ *defined above.*

In fact, we shall prove much more about the structure of $Y_\infty^{(i_1,i_2)}$ (see Theorem 30).

Finally, we mention some of the motivation behind proving Theorem 1. Let $Ш_\infty$ be the Tate-Safarevic group of E over K_∞ (that is those elements of $H^1(G(\overline{K}/K_\infty), E(\overline{K}))$ which are everywhere locally trivial). We define the Selmer group S_∞ to be the inverse image of the $\underline{\underline{p}}$-primary part of $Ш_\infty$ in $H^1(G(\overline{K}/K), E_{p^\infty})$. Then classical descent theory gives us the following exact sequence

$$0 \to E(K_\infty) \otimes_{\mathcal{O}} K_{\underline{\underline{p}}}/\mathcal{O}_{\underline{\underline{p}}} \to S_\infty \to Ш_\infty(\underline{\underline{p}}) \to 0 .$$

Since S_∞ is a discrete Γ-module, the Pontryagin dual of S_∞ , $\hat{S}_\infty = \mathrm{Hom}(S_\infty, \mathbb{Q}_p/\mathbb{Z}_p)$ is a compact $\mathbb{Z}_p[[\Gamma]]$-module and hence can be equipped with a Λ-module structure in the same way as Y_∞ . The fundamental problem in the study of the arithmetic of the curve E over K is to determine the characteristic power series of the eigenspace $\hat{S}_\infty^{(0,0)}$ of $\hat{S}_\infty$ on which G_0 acts trivially.

To relate this to our present work, we need to introduce a certain Galois group. Let M_∞ be the maximal abelian p-extension of K_∞ unramified outside $\underline{\underline{p}}$, and let X_∞ denote the Galois group of M_∞ over K_∞. We equip X_∞ with an action of the Galois group G_∞ of K_∞ over K by inner automorphisms and make X_∞ a Λ-module in the usual way. It is not difficult to show that S_∞ is isomorphic to $\mathrm{Hom}\left(X_\infty, E_{\pi^\infty}\right)$. Hence $\hat{S}_\infty^{(0,0)}$ is isomorphic as a Λ-module to $X_\infty^{(1,0)}(-1)$, where (-1) denotes a twist minus one times by the Tate module E_{π^∞}.

The main conjecture of Iwasawa theory for elliptic curves is that the characteristic power series of $X_\infty^{(1,0)}$ is given by a power series in Λ generating the same ideal in $\hat{I}_\infty[[T_1, T_2]]$ as Katz's interpolating power series $G^{(1,0)}(T_1, T_2)$ defined above. Similar conjectures also exist for the other eigenspaces, except that it is probably necessary to make a minor modification to obtain power series which interpolate special values of *primitive* L-functions.

We write $\mathcal{E}_n$ for the group of global units of K_n which are congruent to 1 modulo each prime of K_n lying above $\underline{\underline{p}}$, and let $\overline{\mathcal{E}}_n$ denote their closure in $\mathcal{U}_n$ under the diagonal embedding. We easily deduce from class field theory the exact sequence

$$0 \to \varprojlim \left(\overline{\mathcal{E}}_n/\overline{C}_n\right) \to \varprojlim \left(\mathcal{U}_n/\overline{C}_n\right) \to X_\infty \to \mathrm{Gal}(H_\infty/K_\infty) \to 0 .$$

where the projective limits are taken relative to the norm maps and H_∞ is the union of the Hilbert class fields H_n of K_n $(n = 0, 1, 2, \ldots)$. By our main theorem, the conjecture as to the characteristic power series of X_∞, and hence of $\hat{S}_\infty$, is equivalent to proving that $\varprojlim (\overline{E}_n/\overline{C}_n)$ and $\mathrm{Gal}(H_\infty/K_\infty)$ have the same characteristic power series. We see no way of resolving this at present, but, as we have mentioned earlier, a solution would have very deep consequences for the study of the arithmetic of the elliptic curve E.

CHAPTER 2

NOTATION

As in the introduction, we let K be an imaginary quadratic field with class number 1 and discriminant $-d_K$ lying inside the complex field $\mathbb{C}$, and denote by $\mathcal{O}$ the ring of integers of K. We let E be an elliptic curve defined over K whose endomorphism ring is isomorphic to $\mathcal{O}$. We shall denote by S the finite set consisting of 2, 3 and the rational primes q such that E has bad reduction at at least one prime of K above q. We fix a Weierstrass model (1) for E such that g_2 and g_3 belong to $\mathcal{O}$ and the discriminant of (1) is divisible only by primes of K lying above primes in S. Let $P(z)$ be the Weierstrass function associated with (1), and L the period lattice of $P(z)$. Put $\xi(z) = (P(z), P'(z))$. As usual, we identify $\mathcal{O}$ with the endomorphism ring of E in such a way that the endomorphism corresponding to α in $\mathcal{O}$ is given by $\xi(z) \mapsto \xi(\alpha z)$.

Let ψ be the Grossencharacter of E over K, and write $\underline{\underline{f}}$ for the conductor of ψ. Choose an element Ω_∞ of the period lattice L such that $L = \Omega_\infty \mathcal{O}$ and a generator f of $\underline{\underline{f}}$.

We fix for the rest of this thesis a prime $\underline{\underline{p}}$ of K lying above a rational prime p such that $p \notin S$ and $\underline{\underline{p}}$ is of degree 1. Hence $(p) = \underline{\underline{p}}\underline{\underline{p}}^*$. Put $\pi = \psi(\underline{\underline{p}})$ and $\pi^* = \psi(\underline{\underline{p}}^*)$, and observe that these are generators of the respective ideals. For each α in $\mathcal{O}$, let E_α be the kernel of the endomorphism α of E, and for each pair of integers $m, n \geq 0$, let F_m denote the field $K(E_{\pi^{*m+1}})$ and $K_{n,m}$ the field

$F_m(E_{\pi^{n+1}})$. It is well known that the extension $K_{n,m}$ over F_m is totally ramified at the primes above $\underline{\underline{p}}$, and that $\underline{\underline{p}}$ is unramified in F_m . In fact, from the definition of the Grossencharacter, we see that the number of primes of F_m lying above $\underline{\underline{p}}$, which we denote by r_m is given by the index of the subgroup generated by π in $(\mathcal{O}/\underline{\underline{p}}^{*m+1})^{\times}$. Hence, there exists an integer M such that $r_m = r_0 p^m$ for $m < M$ and $r_m = r_0 p^M$ for $m \geq M$.

We choose and fix a prime $\underline{\underline{p}}_M$ of F_M lying above $\underline{\underline{p}}$, and let $\underline{\underline{p}}_m$ denote the unique prime of F_m lying above (or below) $\underline{\underline{p}}_M$.

We write $\underline{\underline{p}}_{n,m}$ for the unique prime of $K_{n,m}$ lying above $\underline{\underline{p}}_m$. If ω is any prime of F_m lying above $\underline{\underline{p}}$, we let $\Xi_{n,m,\omega}$ be the completion of $K_{n,m}$ at the unique prime above ω , and we let $\Phi_{m,\omega}$ denote the completion of F_m at ω . We shall write $I_{m,\omega}$ for the ring of integers of $\Phi_{m,\omega}$ and we shall also write ω for the maximal ideal of $I_{m,\omega}$. For simplicity, we shall omit the subscript for the prime when referring to completions at or above $\underline{\underline{p}}_m$. Denote by $K_{\underline{\underline{p}}}$ the completion of K at $\underline{\underline{p}}$, and we shall identify its ring of integers $\mathcal{O}_{\underline{\underline{p}}}$ with $\mathbb{Z}_p$.

Put $K_\infty = \bigcup_{n,m\geq 0} K_{n,m}$, $F_\infty = \bigcup_{m\geq 0} F_m$, and $\Phi_\infty = \bigcup_{m\geq 0} \Phi_m$. Let φ denote the Artin symbol $(\underline{\underline{p}}, F_\infty/K)$ for the extension F_∞ over K and observe that φ induces the Frobenius automorphism for the extension Φ_∞ over $K_{\underline{\underline{p}}}$. Note that we always view our global fields as lying inside the complex numbers, and equipped with embeddings into their completions.

Write G_∞ for the Galois group of K_∞ over K, and let

$E_{\pi^\infty} = \bigcup_{n\geq 0} E_{\pi^{n+1}}$ and $E_{\pi^{*\infty}} = \bigcup_{m\geq 0} E_{\pi^{*m+1}}$. Let $\kappa_1 : G_\infty \to \mathbb{Z}_p^\times$ and

$\kappa_2 : G_\infty \to \mathbb{Z}_p^\times$, respectively, be the characters giving the actions of G_∞ on

E_{π^∞} and $E_{\pi^{*\infty}}$. Observe that if $\sigma \in G_\infty$ and α is an element of $\mathcal{O}$ such

that $u^\sigma = \alpha u$ for all $u \in E_{\pi^{*m+1}}$, then $\kappa_2(\sigma)$ is given modulo p^{m+1} by

a representative lying in $\mathbb{Z}$ of the coset of α modulo $\underline{\underline{p}}^{*m+1}$. These rational integral representatives are precisely the rational integers

belonging to the coset of $\bar{\alpha}$ modulo $\underline{\underline{p}}^{m+1}$, and so, under our identification of $\mathbb{Z}_p$ with $\mathcal{O}_{\underline{\underline{p}}}$, it follows that

$$\kappa_2(\sigma) \equiv \bar{\alpha} \bmod \underline{\underline{p}}^{m+1} . \tag{3}$$

Now it is plain that $G_\infty = \Gamma \times \Delta$, where Γ is the Galois group of K_∞ over $K_{0,0}$, and Δ is the product of two cyclic groups of order $p - 1$

which can be identified with the Galois group of $K_{0,0}$ over K. We

observe that the canonical characters κ_1 and κ_2 provide an isomorphism

$(\kappa_1, \kappa_2) : G_\infty \xrightarrow{\sim} \mathbb{Z}_p^\times \times \mathbb{Z}_p^\times$, and we deduce that $\Gamma \cong \mathbb{Z}_p \times \mathbb{Z}_p$, and that if

χ_1 and χ_2 denote the restriction of κ_1 and κ_2 to Δ respectively,

then together they generate $\mathrm{Hom}\left(\Delta, \mathbb{Z}_p^\times\right)$.

If A is any $\mathbb{Z}_p[\Delta]$-module, we define $A^{(i_1,i_2)}$ to be the submodule

of A on which Δ acts *via* $\chi_1^{i_1}\chi_2^{i_2}$. Thus, we have the canonical

decomposition

$$A = \bigoplus_{\substack{i_1, i_2 \\ \bmod (p-1)}} A^{(i_1, i_2)} .$$

Let Λ be the ring of formal power series in the commuting indeterminates T_1 and T_2 with coefficients in $\mathbb{Z}_p$. Choose a topological generator u of $(1+p\mathbb{Z}_p)^\times$ and let γ_1 and γ_2 be the elements of Γ for which $\kappa_1(\gamma_1) = \kappa_2(\gamma_2) = u$ and $\kappa_1(\gamma_2) = \kappa_2(\gamma_1) = 1$. It is clear from our earlier remarks that such a choice is possible and that γ_1 and γ_2 are a set of topological generators for Γ. Any compact $\mathbb{Z}_p$-module B on which Γ acts continuously can be endowed with a unique Λ-module structure such that $\gamma_1 x = (1+T_1)x$ and $\gamma_2 x = (1+T_2)x$ for all x in B.

The rings $\Xi_{n,m} = \prod_{\omega} \Xi_{n,m,\omega}$ and $\Phi_m = \prod_{\omega} \Phi_{m,\omega}$, where the product is taken over the set of primes ω of F_m lying above $\underline{\underline{p}}$, have a natural action of the Galois group G_∞ as follows. Let $\alpha_{k,\omega}$ $(k = 0, 1, 2, \ldots)$ be a Cauchy sequence of elements of $K_{n,m}$ (or F_m) which converge to α_ω in $\Xi_{n,m,\omega}$ (or $\Phi_{m,\omega}$). Then the ω^σ component of $(\alpha_\omega)^\sigma$ is the limit of the Cauchy sequence $\alpha^\sigma_{k,\omega}$ $(k = 0, 1, 2, \ldots)$ in Ξ_{n,m,ω^σ} (or Φ_{m,ω^σ}). We embed $K_{n,m}$ and F_m in these rings *via* the diagonal map, and it is easy to verify that the usual norm and trace maps on $\Xi_{n,m}$, Φ_m, $K_{n,m}$ and F_m, as well as the Galois action, all commute with these embeddings.

Let $\hat{E}$ be the formal group giving the kernel of reduction modulo $\underline{\underline{p}}$ on E. The parameter of $\hat{E}$ is

$$t = -2x/y = -2P(z)/P'(z) = \varepsilon(z) \ . \tag{4}$$

Since $\hat{E}$ is defined over $\mathcal{O}_{\underline{\underline{p}}}$, we have the power series expansions

$$x = t^{-2}a(t) \ , \quad y = -2t^{-3}a(t) \tag{5}$$

where $a(t)$ has coefficients in $\mathcal{O}_{\underline{\underline{p}}}$ and constant term equal to 1. We can view z as being a parameter of the formal additive group G_a, and then $\varepsilon(z)$ is the exponential map of $\hat{E}$. We write $\lambda : \hat{E} \xrightarrow{\sim} G_a$ for the logarithm of $\hat{E}$ which is the inverse of (4). Denote by $\hat{E}_{\pi^{n+1}}$ the kernel of the endomorphism $[\pi^{n+1}]$ on $\hat{E}$, which, of course, we identify with $E_{\pi^{n+1}}$.

Finally, we denote by $U'_{n,m,\omega}$ the units of $\Xi_{n,m,\omega}$ and by $U_{n,m,\omega}$ the subgroup consisting of those units which are congruent to 1 modulo the maximal ideal. Put $\mathrm{U}'_{n,m} = \prod_{\omega} U'_{n,m,\omega}$ and $\mathrm{U}_{n,m} = \prod_{\omega} U_{n,m,\omega}$, where again the product is taken over the primes ω of F_m lying above $\underline{\underline{p}}$, and let U'_{∞} and U_{∞} denote the projective limits of the $\mathrm{U}'_{n,m}$ and $\mathrm{U}_{n,m}$ respectively relative to the norm maps on the $\Xi_{n,m}$. We endow U_{∞} with its natural structure as a $\mathrm{Z}_p[G_{\infty}]$-module. In particular, U_{∞} is a compact Γ-module, and thus also a Λ-module.

CHAPTER 3

COLEMAN POWER SERIES AND LOGARITHMIC DERIVATIVES

Let T_π denote the Tate module $\varprojlim \hat{E}_{\pi^{n+1}}$, where the limit is taken relative to the usual projection maps given by multiplication by powers of π. We fix a basis (u_n) of T_π, and let $\beta = (\beta_{n,m,\omega})$ be an element of U'_∞. Coleman [4] has shown that for each integer $m \geq 0$ and each prime ω of F_m lying above $\underline{\underline{p}}$, there is a unique power series $c_{m,\omega,\beta}(T) \in I_{m,\omega}[[T]]$ such that

$$\beta_{n,m,\omega} = c_{m,\omega,\beta}^{\varphi^{-n}}(u_n) \quad \text{for all } n \geq 0 . \tag{6}$$

(We adopt the convention throughout this thesis that an element of the Galois group written in this position acts only on the coefficients of the power series.)

Moreover, these power series satisfy the functional equation

$$\left(c_{m,\omega,\beta}^{\varphi} \circ [\pi]\right)(T) = \prod_{\eta \in \hat{E}_\pi} c_{m,\omega,\beta}(T * \eta) \tag{7}$$

where $T * \eta$ denotes the sum of T and η under the addition on the formal group $\hat{E}$. It will be convenient to denote by $c_{m,\beta}(T)$ the element $(c_{m,\omega,\beta}(T)) \in \prod_{\omega} I_{m,\omega}[[T]]$, which we shall write as $I_m[[T]]$, with the obvious Galois structure inherited from the structure on Φ_m.

For $m' \geq m$ and ω' a prime of $F_{m'}$ lying above the prime ω of F_m, let $N^n_{\omega',\omega}$ denote the local norm map from $\Xi_{n,m',\omega'}$ to $\Xi_{n,m,\omega}$.

Then it is clear that for each prime ω of F_m lying above $\underline{\underline{p}}$,

$$\prod_{\omega'|\omega} N^n_{\omega',\omega}\left(c^{\varphi^{-n}}_{m',\omega',\beta}(u_n)\right) = \beta_{n,m,\omega} \ ,$$

where the product on the left is taken over all primes ω' of $F_{m'}$ lying above ω . Since $c_{m',\omega',\beta}$ has coefficients in $I_{m',\omega'}$ and u_n belongs to $\Xi_{n,m,\omega}$, it is evident that

$$\prod_{\omega'|\omega}\left[\left(\prod_{\sigma\in\mathrm{Gal}(\Phi_{m',\omega'}/\Phi_{m,\omega})} c^{\sigma}_{m',\omega',\beta}\right)^{\varphi^{-n}}(u_n)\right] = \beta_{n,m,\omega} \ .$$

From the uniqueness of the Coleman power series, it follows that we have the following lemma.

LEMMA 2. *Let $m' \geq m \geq 0$, and let $N_{m',m}$ denote the norm map from $\mathrm{I}_{m'}[[T]]$ to $\mathrm{I}_m[[T]]$. Then, for each $\beta \in \mathrm{U}'_\infty$,*

$$c_{m,\beta}(T) = N_{m',m}\left(c_{m',\beta}(T)\right) \ .$$

The derivative of the logarithm map, $\lambda'(T)$, is a unit of the ring $\mathrm{Z}_p[[T]]$, and hence of $I_{m,\omega}[[T]]$. It is also clear that for each $m \geq 0$ and each prime ω of F_m lying above $\underline{\underline{p}}$, the Coleman power series $c_{m,\omega,\beta}(T)$ attached to an element β of U'_∞ is a unit in $I_{m,\omega}[[T]]$. We denote by $g_{m,\beta}(T)$ the element of $\mathrm{I}_m[[T]]$ whose ω-component $\left(g_{m,\beta}(T)\right)_\omega$ is given by $\lambda'(T)^{-1}\,\frac{d}{dT}\log c_{m,\omega,\beta}(T)$.

We take this opportunity to observe that if $\beta = \left(\beta_{n,m,\omega}\right) \in \mathrm{U}'_\infty$ then $\beta_{n,m,\omega} = \omega_{n,m,\omega}(\beta)\langle\beta_{n,m,\omega}\rangle$, where $\langle\beta_{n,m,\omega}\rangle$ belongs to $U_{n,m,\omega}$ and

$\omega_{n,m,\omega}(\beta)$ is a root of unity in $\Phi_{m,\omega}$. Clearly $\langle\beta_{n,m,\omega}\rangle$ corresponds to an element of U_∞, which we shall denote by $\langle\beta\rangle$, and $(\omega_{n,m,\omega}(\beta))$ is an element of U'_∞ whose Coleman power series for each pair m and ω is $\omega_{0,m,\omega}(\beta) \in I_{m,\omega}[[T]]$.

In particular

$$c_{m,\omega,\beta}(T) = \omega_{0,m,\omega}(\beta)c_{m,\omega,\langle\beta\rangle}(T) , \tag{8}$$

and consequently

$$g_{m,\beta}(T) = g_{m,\langle\beta\rangle}(T) . \tag{9}$$

LEMMA 3. *Let* $m' \geq m \geq 0$ *and let* $\mathrm{Tr}_{m',m}$ *denote the trace map from* $I_{m'}[[T]]$ *to* $I_m[[T]]$. *Then, for each* $\beta \in U'_\infty$,

$$g_{m,\beta}(T) = \mathrm{Tr}_{m',m}g_{m',\beta}(T) ,$$

and $g_{m,\beta}$ *satisfies the functional equation*

$$\pi g^{\varphi}_{m,\beta}([\pi]T) = \sum_{\eta\in\hat{E}_\pi} g_{m,\beta}(T * \eta) . \tag{10}$$

Proof. The first assertion is clear from the previous lemma and the fact that the Galois action commutes with the operator $\lambda'(T)^{-1}\frac{d}{dT}\log$.

Since λ is the logarithm map, it is clear that $\lambda(T * \eta) = \lambda(T)$ for all $\eta \in \hat{E}_\pi$, and hence $\frac{d}{dT}\lambda(T * \eta) = \lambda'(T)$.

Thus

$$\left(g_{m,\beta}(T * \eta)\right)_\omega = \left(\frac{d}{dT}\lambda(T * \eta)\right)^{-1} \cdot \frac{d}{dT}\log c_{m,\omega,\beta}(T * \eta)$$

$$= \lambda'(T)^{-1}\frac{d}{dT}\log c_{m,\omega,\beta}(T * \eta) .$$

The functional equation (7) shows that

$$\sum_{\eta\in\hat{E}_\pi} \left(g_{m,\beta}(T * \eta)\right)_\omega = \lambda'(T)^{-1}\frac{d}{dT}\log\left(c^{\varphi}_{m,\omega,\beta} \circ [\pi]\right)(T) .$$

On the other hand

$$\left(g^{\varphi}_{m,\beta}([\pi]T)\right)_\omega = \left(\frac{d}{dT}\lambda([\pi]T)\right)^{-1} \cdot \frac{d}{dT}\log c^{\varphi}_{m,\omega,\beta}([\pi]T)$$

$$= \pi^{-1}\lambda'(T)^{-1}\frac{d}{dT}\log\left(c^{\varphi}_{m,\omega,\beta} \circ [\pi]\right)(T) ,$$

since $\lambda([\pi]T) = \pi\lambda(T)$. Combining the last two equations, we obtain equation (10).

We denote the subring $\prod_{\omega} I_{m,\omega}$ of Φ_m by I_m , and write $\varprojlim I_m$ for the projective limit of the rings I_m relative to the trace maps. We also put $I_\infty = \bigcup_{m\geq 0} I_m$ and denote the completion of I_∞ by $\hat{I}_\infty$. The following theorem allows us to associate a power series with each element of $\varprojlim I_m$.

THEOREM 4. *Let* $b \in \varprojlim I_m$. *Then there is a unique power series* $h_b(T) \in \hat{I}_\infty[[T]]$ *such that*

$$h_b(T) \equiv \sum_{\sigma\in \mathrm{Gal}(F_m/K)} \left(b^{\sigma}\right)_{m,\underline{\underline{p}}_m} (1+T)^{\kappa_2(\sigma)} \mod\left((1+T)^{p^{m+1}}-1\right)$$

for all $m \geq 0$. *Here* $\left(b^{\sigma}\right)_{m,\underline{\mathfrak{p}}_m}$ *denotes the* $\underline{\mathfrak{p}}_m$*-component of the projection onto* I_m *of the image of* b *under the action of any element of* G_∞ *whose restriction to* F_m *is* σ .

Proof. Observe firstly that if $\theta \in \mathrm{Gal}(K_\infty/K)$ is trivial on F_m , then $\kappa_2(\theta) \equiv 1 \bmod p^{m+1}$, and hence $(1+T)^{\kappa_2(\sigma)}$ is well defined modulo $\left((1+T)^{p^{m+1}}-1\right)$ for all $\sigma \in \mathrm{Gal}\left(F_m/K\right)$. All that we need check is that the appropriate compatibilities are satisfied. Let $m' \geq m$. Then

$$\left(b^{\sigma}\right)_{m,\underline{\mathfrak{p}}_m} = \sum_{\substack{\theta\in\mathrm{Gal}\left(F_{m'}/K\right)\\ \theta|_{F_m}=\sigma}} \left(b^{\theta}\right)_{m',\underline{\mathfrak{p}}_{m'}}$$

as this is precisely the trace compatibility of an element of $\varprojlim \mathrm{I}_m$. Consequently

$$\sum_{\substack{\theta\in\mathrm{Gal}\left(F_{m'}/K\right)\\ \theta|_{F_m}=\sigma}} \left(b^{\theta}\right)_{m',\underline{\mathfrak{p}}_{m'}} (1+T)^{\kappa_2(\theta)} \equiv \left(b^{\sigma}\right)_{m,\underline{\mathfrak{p}}_m} (1+T)^{\kappa_2(\sigma)} \bmod\left((1+T)^{p^{m+1}}-1\right)$$

which is sufficient to prove the theorem.

If $b \in \varprojlim \mathrm{I}_m$, and $j \leq 0$, we define

$$\delta_j(b) = \left((1+T)\frac{d}{dT}\right)^{-j} h_b(T)|_{T=0} \in \hat{\mathrm{I}}_\infty$$

and we note that

$$\delta_j(b) \equiv \sum_{\sigma\in\mathrm{Gal}\left(F_m/K\right)} \kappa_2(\sigma)^{-j}\left(b^{\sigma}\right)_{m,\underline{\mathfrak{p}}_m} \bmod \underline{\underline{\mathfrak{p}}}_\infty^{m+1} , \qquad (11)$$

where $\underline{\underline{p}}_\infty$ is the maximal ideal of $\hat{I}_\infty$.

The following theorem provides the key to the rest of this thesis.

THEOREM 5. *For each* β *in* U'_∞, *there is a unique power series* $g_\beta(T_1, T_2) \in \hat{I}_\infty[[T_1, T_2]]$ *such that*

$$g_\beta(T_1, T_2) \equiv \sum_{\sigma\in\mathrm{Gal}(F_m/K)} \left(g^\sigma_{m,\beta}(T_1)\right)_{\underline{\underline{p}}_m} (1+T_2)^{\kappa_2(\sigma)} \bmod \left((1+T_2)^{p^{m+1}}-1\right)$$

for all $m \geq 0$. *Moreover,* g_β *satisfies the functional equation*

$$\pi g_\beta\left([\pi]T_1, (1+T_2)^{\kappa_2(\varphi)^{-1}}-1\right) = \sum_{\eta\in\hat{E}_\pi} g_\beta(T_1 * \eta, T_2). \tag{12}$$

Proof. The first statement is an obvious corollary of Theorem 4. From the definition of $g_\beta(T_1, T_2)$, it is clear that

$$\pi g_\beta\left([\pi]T_1, (1+T_2)^{\kappa_2(\varphi)^{-1}}-1\right) \equiv \sum_{\sigma\in\mathrm{Gal}(F_m/K)} \pi\left(g^{\sigma\varphi}_{m,\beta}[\pi]T_1\right)_{\underline{\underline{p}}_m} (1+T_2)^{\kappa_2(\sigma)}$$

modulo $\left((1+T_2)^{p^{m+1}}-1\right)$. Now, equation (10) shows that, for all $\sigma \in \mathrm{Gal}(F_m/K)$,

$$\pi\left(g^{\sigma\varphi}_{m,\beta}([\pi]T_1)\right)_{\underline{\underline{p}}_m} = \sum_{\eta\in\hat{E}_\pi} \left(g^\sigma_{m,\beta}(T_1 * \eta)\right)_{\underline{\underline{p}}_m}$$

and so

$$\pi g_\beta\left([\pi]T_1, (1+T_2)^{\kappa_2(\varphi)^{-1}}-1\right) \equiv \sum_{\sigma\in\mathrm{Gal}(F_m/K)} \left[\sum_{\eta\in\hat{E}_\pi} g^\sigma_{m,\beta}(T_1 * \eta)\right]_{\underline{\underline{p}}_m} (1+T_2)^{\kappa_2(\sigma)}$$

modulo $\left((1+T_2)^{p^{m+1}}-1\right)$. Thus, equation (12) is satisfied.

Observe that if $\sigma \in G_\infty$ and $n \geq 0$, then $u_n^\sigma = [\kappa_1(\sigma)](u_n)$. Equation (6) clearly implies that if $\beta \in \mathrm{U}'_\infty$, then the power series

$$c_{m,\beta^\sigma}(T) = c_{m,\beta}^\sigma\left([\kappa_1(\sigma)](T)\right) .$$

Thus

$$g_{m,\beta^\sigma}(T) = \kappa_1(\sigma)g_{m,\beta}^\sigma\left([\kappa_1(\sigma)](T)\right) ,$$

and from this it is easy to see that

$$g_{\beta^\sigma}(T_1, T_2) = \kappa_1(\sigma)g_\beta\left([\kappa_1(\sigma)](T_1), (1+T_2)^{\kappa_2(\sigma)^{-1}}-1\right) . \tag{13}$$

Let $k \geq 1$ and $j \leq 0$. We define, for each $\beta \in \mathrm{U}_\infty$,

$$\delta_{k,j}(\beta) = \left(\lambda'(T_1)^{-1}\frac{\partial}{\partial T_1}\right)^{k-1}\left((1+T_2)\frac{\partial}{\partial T_2}\right)^{-j} g_\beta(T_1, T_2)\big|_{(0,0)} . \tag{14}$$

The following lemma summarises the basic properties of these maps $\delta_{k,j}$.

LEMMA 6. *Let* $k \geq 1$ *and* $j \leq 0$. *Then* $\delta_{k,j}$ *is a homomorphism of* Z_p*-modules from* U_∞ *to* $\hat{\mathrm{I}}_\infty$ *, and for all* $\beta \in \mathrm{U}_\infty$ *and all* $\sigma \in G_\infty$,

$$\delta_{k,j}(\beta^\sigma) = \kappa_1(\sigma)^k\kappa_2(\sigma)^j\delta_{k,j}(\beta) . \tag{15}$$

In particular, if $\beta \in U_\infty^{(i_1,i_2)}$ *, then* $\delta_{k,j}(\beta) = 0$ *unless* $(k, j) \equiv (i_1, i_2) \bmod (p-1)$ *and if* $h(T_1, T_2) \in \Lambda$ *,*

$$\delta_{k,j}\big(h(T_1, T_2)\beta\big) = h\big(u^k-1, u^j-1\big)\delta_{k,j}(\beta) . \tag{16}$$

Proof. It is clear that $\delta_{k,j}$ is a $\mathbb{Z}_p$-homomorphism, and equation (15) is evident from equations (13) and (14). The next assertion follows from the first two if we take $\sigma \in \Delta$, so it remains to prove equation (16). But this is merely a restatement of equation (15) if we take $h(T_1, T_2)$ to be either $1 + T_1$ or $1 + T_2$, and follows in general by linearity and continuity.

Finally, we note that $\left(\lambda'(T)^{-1} \frac{d}{dT}\right)^{k-1} g_{m,\beta}(T)\big|_{T=0} \in I_m$, and, for a fixed β , gives rise to an element $d_k(\beta) \in \varprojlim I_m$. From the definition of $\delta_{k,j}$ and the power series $g_\beta(T_1, T_2)$, it is apparent that $\delta_{k,j}(\beta) = \delta_j\big(d_k(\beta)\big)$.

In particular, we see from equation (11) that

$$\delta_{k,j}(\beta) \equiv \sum_{\sigma\in \mathrm{Gal}(F_m/K)} \kappa_2(\sigma)^{-j}\big(d_k(\beta)^\sigma\big)_{m,\underline{\underline{p}}_m} \bmod \underline{\underline{p}}_\infty^{m+1} . \tag{17}$$

CHAPTER 4

ELLIPTIC UNITS

In this chapter, we shall define and establish a number of basic results about Robert's [10] elliptic units, which will play an important role in the proof of our main theorem.

If L is any lattice in the complex plane, let

$$\sigma(z, L) = z \prod_{\substack{\omega\in L \\ \omega\neq 0}} \left(1-(z/\omega)\right)\exp\left((z/\omega)+\left(\tfrac{1}{2}(z/\omega)^2\right)\right)$$

be the Weierstrass σ-function of L. Let

$$\theta(z, L) = \Delta(L)\exp\left(-6g_2(L)z^2\right).\sigma(z, L)^{12} ,$$

where $\Delta(L)$ is the discriminant function of L and

$$g_2(L) = \lim_{s\to 0^+} \sum_{\substack{\omega\in L \\ \omega\neq 0}} \omega^{-2}|\omega|^{-2s} .$$

Recall that $L = \Omega_\infty \mathcal{O}$ is the period lattice of our model (1) of the curve E. Let $\underline{\underline{a}}$ be an integral ideal of K. We define

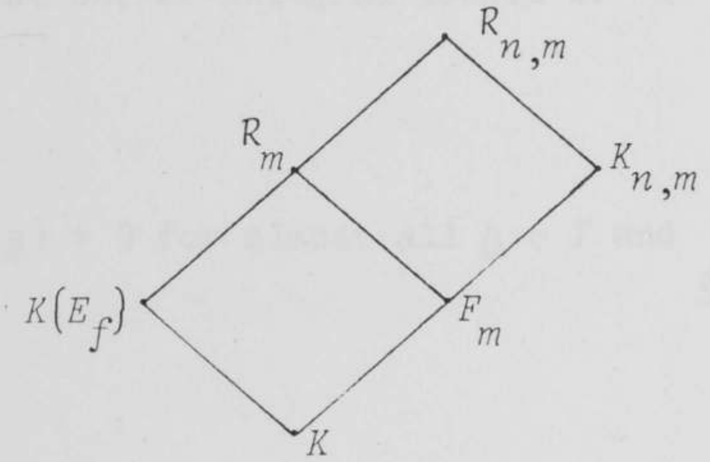
$$\Theta(z, \underline{\underline{a}}) = \theta(z, L)^{N\underline{\underline{a}}}/\theta\left(z, \underline{\underline{a}}^{-1}L\right)$$

where $N\underline{\underline{a}}$ is the absolute norm of $\underline{\underline{a}}$, and $\underline{\underline{a}}^{-1}L$ denotes the lattice $\Omega_\infty\underline{\underline{a}}^{-1}$. In fact, as is shown in [2], $\Theta(z, \underline{\underline{a}})$ is an elliptic function for the lattice L, and an explicit expression for it in terms of $P(z)$ is given by

$$\Theta(z,\ \underline{a}) = \frac{\Delta(L)}{\Delta(\underline{a}^{-1}L)} \prod_{l} \Delta(L)/\bigl(P(z)-P(l)\bigr)^{6} \tag{18}$$

where the product on the right is taken over any set $\{l\}$ of representatives of the non-zero cosets of $\underline{a}^{-1}L$ modulo L.

Let $R_{n,m}$ and R_m denote the ray class fields modulo $\underline{f}\underline{p}^{n+1}\underline{p}^{*m+1}$ and modulo $\underline{f}\underline{p}^{*m+1}$ respectively. It is well known (see, for example [2]) that we have the following diagram of fields.



Put $\rho_m = \Omega_\infty/f\pi^{*m+1}$ and let B_m be a set of integral ideals of K prime to $\underline{f}\underline{p}^*$ such that $\{(\underline{b},\ R_m/K) : \underline{b} \in B_m\}$ is precisely the Galois group of R_m over F_m. If $\underline{a}$ is an integral ideal of K prime to $6p\underline{f}$, set

$$\Lambda_m(z,\ \underline{a}) = \prod_{\underline{b}\in B_m} \Theta\bigl(z+\psi(\underline{b})\rho_m,\ \underline{a}\bigr)\ . \tag{19}$$

LEMMA 7. *The function* $\Lambda_m(z,\ \underline{a})$ *is a rational function of* $P(z)$ *and* $P'(z)$ *with coefficients in* F_m, *and is independent of the choice of the set of ideals* B_m.

Proof. We have already seen that $\Theta(z,\ \underline{a})$ is a rational function of

$P(z)$ with coefficients in K. By the addition theorem $\Theta(z+\rho_m, \underline{\underline{a}})$ is a rational function of $P(z)$ and $P'(z)$ with coefficients in R_m. If $\underline{\underline{b}}$ is any integral ideal prime to $\underline{\underline{fp}}^*$, then $\xi(\rho_m)^{(\underline{\underline{b}}, R_m/K)} = \xi(\psi(\underline{\underline{b}})\rho_m)$, and so we obtain the function $\Theta(z+\psi(\underline{\underline{b}})\rho_m, \underline{\underline{a}})$ on applying $(\underline{\underline{b}}, R_m/K)$ to the coefficients of $\Theta(z+\rho_m, \underline{\underline{a}})$. The lemma is now plain as $\{(\underline{\underline{b}}, R_m/K) : \underline{\underline{b}} \in B_m\}$ is precisely the Galois group of R_m over F_m.

Let I denote the set of integral ideals of K which are prime to $6p\underline{\underline{f}}$, and let

$$S = \left\{\mu : I \to \mathbb{Z} \mid \mu(\underline{\underline{a}}) = 0 \text{ for almost all } \underline{\underline{a}} \in I \text{ and } \sum_{\underline{\underline{a}}\in I} (N\underline{\underline{a}}-1)\mu(\underline{\underline{a}}) = 0\right\}.$$

If $\mu \in S$, we set

$$\Theta(z;\mu) = \prod_{\underline{\underline{a}}\in I} \Theta(z, \underline{\underline{a}})^{\mu(\underline{\underline{a}})} \tag{20}$$

and

$$\Lambda_m(z;\mu) = \prod_{\underline{\underline{a}}\in I} \Lambda_m(z, \underline{\underline{a}})^{\mu(\underline{\underline{a}})}. \tag{21}$$

Choose τ_n (it is unique modulo L) such that $u_n = \varepsilon(\tau_n)$, and choose $\varepsilon_n \in \mathcal{O}$ such that $\varepsilon_n \pi^* \equiv 1 \bmod \underline{\underline{p}}^{n+1}$. Observe that π^* is a unit in $\mathbb{Z}_p$, and that we have $[\pi^{*-(m+1)}]u_n = \varepsilon\left(\varepsilon_n^{m+1}\tau_n\right)$.

Robert has shown that $\Theta\left(\varepsilon_n^{m+1}\tau_n+\rho_m;\mu\right)$ is a unit of $R_{n,m}$ for all $\mu \in S$, and consequently $\Lambda_m\left(\varepsilon_n^{m+1}\tau_n;\mu\right)$ is a unit of $K_{n,m}$. We call the group of such units the elliptic units of $K_{n,m}$ and denote this group by $C'_{n,m}$. It is easy to show that $C'_{n,m}$ is stable under the action of G_∞.

LEMMA 8. *Let* $m' \geq m \geq 0$ *and* $n' \geq n \geq 0$. *Then, for each* $\mu \in S$,

$$N_{R_{n',m'}/R_{n,m}} \Theta\left(\varepsilon_{n'}^{m'+1}\tau_{n'}+\rho_{m'};\ \mu\right) = \Theta^{\left(\underline{\underline{p}}^{n'-n},R_m/K\right)}\left(z+\rho_m;\ \mu\right)\Big|_{z=\varepsilon_n^{m+1}\tau_n} . \tag{22}$$

Proof. Let $\underline{\underline{c}}$ be an integral ideal of K, prime to $6p\underline{\underline{f}}$ whose Artin symbol $\sigma_{\underline{\underline{c}}} = \left(\underline{\underline{c}},\ R_{n',m'}/K\right)$ fixes the subfield $R_{n,m}$. Since, if ρ is any $\underline{\underline{f}}\underline{\underline{p}}^{n+1}\underline{\underline{p}}^{*m+1}$-division point of L, $\xi(\rho)^{\sigma_{\underline{\underline{c}}}} = \xi\left(\psi(\underline{\underline{c}})\rho\right)$, it follows that

$$\psi(\underline{\underline{c}}) \equiv 1 \bmod \underline{\underline{f}}\underline{\underline{p}}^{n+1}\underline{\underline{p}}^{*m+1} . \tag{23}$$

Thus

$$\Theta\left(\varepsilon_{n'}^{m'+1}\tau_{n'}+\rho_{m'};\ \mu\right)^{\sigma_{\underline{\underline{c}}}} = \Theta\left(\psi(\underline{\underline{c}})\varepsilon_{n'}^{m'+1}\tau_{n'}+\psi(\underline{\underline{c}})\rho_{m'};\ \mu\right)$$
$$= \Theta\left(\varepsilon_{n'}^{m'+1}\tau_{n'}+\rho_{m'}+\delta_{\underline{\underline{c}}};\ \mu\right)$$

where $\delta_{\underline{\underline{c}}} = \left(\psi(\underline{\underline{c}})-1\right)\left(\varepsilon_{n'}^{m'+1}\tau_{n'}+\rho_{m'}\right)$.

Since $\left(\varepsilon_{n'}^{m'+1}\tau_{n'}+\rho_{m'}\right)$ is a primitive $\underline{\underline{f}}\underline{\underline{p}}^{n'+1}\underline{\underline{p}}^{*m'+1}$-division point of L, it follows from (23) that $\delta_{\underline{\underline{c}}}$ is a $\underline{\underline{p}}^{n'-n}\underline{\underline{p}}^{*m'-m}$-division point of L. Hence, every conjugate of $\Theta\left(\varepsilon_{n'}^{m'+1}\tau_{n'}+\rho_{m'};\ \mu\right)$ under $\mathrm{Gal}\left(R_{n',m'}/R_{n,m}\right)$ is given by $\Theta\left(\varepsilon_{n'}^{m'+1}\tau_{n'}+\rho_{m'}+\delta;\ \mu\right)$ for some $\underline{\underline{p}}^{n'-n}\underline{\underline{p}}^{*m'-m}$-division point δ of L. There are $p^{n'+m'-(n+m)}$ such division points, which is equal to the number of conjugates, so we must have

$$N_{R_{n',m'}/R_{n,m}}\Theta\left(\varepsilon_{n'}^{m'+1}\tau_{n'}+\rho_{m'};\ \mu\right) = \prod_{\delta}\Theta\left(\varepsilon_{n'}^{m'+1}\tau_{n'}+\rho_{m'}+\delta;\ \mu\right)$$

where the product on the right is taken over any set $\{\delta\}$ of representatives of $\underline{\underline{p}}^{n-n'}\underline{\underline{p}}^{*m-m'}L$ modulo L.

It follows from Lemma 6 of Coates and Wiles [3] and the fact that $\pi^{n'-n}\pi^{*m'-m}$ generates $\underline{\underline{p}}^{n'-n}\underline{\underline{p}}^{*m'-m}$ that

$$N_{R_{n',m'}/R_{n,m}}\Theta\left(\varepsilon_{n'}^{m'+1}\tau_{n'}+\rho_{m'};\ \mu\right) = \Theta\left(\varepsilon_{n}^{m+1}\tau_{n}+\psi(\underline{\underline{p}})^{n'-n}\rho_{m};\ \mu\right).$$

As observed in the proof of the previous lemma,

$$\Theta\left(z+\psi(\underline{\underline{p}})^{n'-n}\rho_{m};\ \mu\right) = \Theta^{\left(\underline{\underline{p}}^{n'-n},R_{m}/K\right)}\left(z+\rho_{m};\ \mu\right)$$

from which we conclude that equation (22) holds.

The importance of this lemma is the following corollary.

COROLLARY 9. *Let* $\mu \in S$ *and put*

$$e_{n,m}(\mu) = \Lambda_{m}^{\varphi^{-n}}(z;\ \mu)\Big|_{z=\varepsilon_{n}^{m+1}\tau_{n}}.$$

Then $\left(e_{n,m}(\mu)\right) \in U'_{\infty}$.

Proof. Observe that, for fixed n and m, $e_{n,m}(\mu)$ is a unit of $K_{n,m}$ and so can be regarded as belonging to $U'_{n,m}$. It remains to check the norm compatibility, which we can do in the global fields.

Now, for the reasons explained in the proof of Lemma 7, and the fact that both $\left(\underline{\underline{p}},\ R_{m'}/K\right)$ and φ induce the same automorphism on $F_{m'}$, Lemma 8 says that

$$N_{K_{n',m'}/K_{n,m}} \Lambda_{m'}^{\varphi^{-n'}}(z;\mu)\Big|_{z=\varepsilon_{n'}^{m'+1}\tau_{n'}} = \Lambda_m^{\varphi^{-n}}(z;\mu)\Big|_{z=\varepsilon_n^{m+1}\tau_n} .$$

Thus, the $e_{n,m}(\mu)$ are compatible with respect to the norm map, and hence $\left(e_{n,m}(\mu)\right) \in U'_\infty$.

We shall denote $\left(e_{n,m}(\mu)\right)$ by $e(\mu)$ in future, and write C'_∞ for the projective limit of the $C'_{n,m}$ with respect to the norm maps. Clearly $e(\mu) \in C'_\infty$ for all $\mu \in S$.

THEOREM 10. *Let* $\mu \in S$. *Then the Coleman power series* $c_{m,e(\mu)}(T) \in I_m[[T]]$ *attached to* $e(\mu)$ *are given by*

$$c_{m,e(\mu)}(T) = \Lambda_m\left(\pi^{*-(m+1)}\lambda(T);\ \mu\right) .$$

Proof. It is necessary, first of all, to explain the notation. Recall that Lemma 7 showed that $\Lambda_m(z;\mu)$ is a rational function of $P(z)$ and $P'(z)$ with coefficients in F_m , and so $\Lambda_m(z;\mu)$ has a power series expansion with coefficients in F_m , and hence in Φ_m . Thus $\Lambda_m\left(\pi^{*-(m+1)}\lambda(T);\ \mu\right)$ can be regarded as an element of $\Phi_m[[T]]$.

Now, observe that since $\left[\pi^{*-(m+1)}\right]u_n = \varepsilon\left(\varepsilon_n^{m+1}\tau_n\right)$, it follows that

$$\Lambda_m^{\varphi^{-n}}\left(\pi^{*-(m+1)}\lambda\left(u_n\right);\ \mu\right) = \Lambda_m^{\varphi^{-n}}(z;\mu)\Big|_{z=\varepsilon_n^{m+1}\tau_n}$$

since λ is the inverse of ε .

Thus, the only thing we need to show is that $\Lambda_m\left(\pi^{*^{-(m+1)}}\lambda(T);\ \mu\right)$ belongs to $I_m[[T]]$. From equation (18), we see that

$$\Theta\left(z+\rho_m,\ \underline{\underline{a}}\right)^{-1} = \frac{\Delta\left(\underline{\underline{a}}^{-1}L\right)}{\Delta(L)^{N\underline{\underline{a}}}} \prod_{l} \left(P\left(z+\rho_m\right)-P(l)\right)^6 \tag{24}$$

where $\{l\}$ runs over a set of representatives of the non-zero cosets of $\underline{\underline{a}}^{-1}L$ modulo L . Let H denote the extension of R_m obtained by adjoining all the $P(l)$, and let $\underline{\underline{P}}$ be any prime of H lying above $\underline{\underline{p}}$.

Consider the expansion of the right hand side of (24) as a power series in $t = \varepsilon(z)$. Since E has good reduction at $\underline{\underline{p}}$, $\Delta(L)$ is a unit at $\underline{\underline{P}}$ and $\Delta\left(\underline{\underline{a}}^{-1}L\right)$ is integral at $\underline{\underline{P}}$. By the addition theorem

$$P\left(z+\rho_m\right) - P(l) = \tfrac{1}{4}\left(\frac{P'(z)-P'\left(\rho_m\right)}{P(z)-P\left(\rho_m\right)}\right)^2 - P(z) - P\left(\rho_m\right) - P(l) . \tag{25}$$

Recall, as was mentioned in Chapter 2, that all the torsion in the kernel of reduction modulo $\underline{\underline{P}}$ of E is contained in E_{π^∞} if $\underline{\underline{P}}|\underline{\underline{p}}$. Thus, since $\xi(l)$ and $\xi\left(\rho_m\right)$ are points of E whose order is prime to π , their co-ordinates must lie in $\mathcal{O}_{\underline{\underline{P}}}$, the ring of integers of the completion of H at $\underline{\underline{P}}$. Thus, substituting the expansions (5) for $P(z)$ and $P'(z)$, we see that $\Theta\left(z+\rho_m,\ \underline{\underline{a}}\right)^{-1}$ has a power series expansion in terms of t with coefficients in $\mathcal{O}_{\underline{\underline{P}}}$. In other words

$$\Theta\left(\lambda(T)+\rho_m,\ \underline{\underline{a}}\right)^{-1} \in \mathcal{O}_{\underline{\underline{P}}}[[T]] .$$

It follows that, for each prime ω of F_m lying above $\underline{\underline{p}}$,

$\Lambda_m\big(\lambda(T);\ \mu\big)^{-1}$ has coefficients which are integral at ω, and so

$$\Lambda_m\big(\pi^{*-m}\lambda(T);\ \mu\big)^{-1} \in \mathrm{I}_m[[T]] \ .$$

In addition

$$\Lambda_m(0;\ \mu)^{-1} = \big(N_{R_m/F_m}\,\Theta(\rho_m;\ \mu)\big)^{-1}$$

and so is a unit of F_m (see [3]).

Thus, it follows that $\Lambda_m\big(\pi^{*-m}\lambda(T);\ \mu\big) \in \mathrm{I}_m[[T]]$.

CHAPTER 5

LOGARITHMIC DERIVATIVES OF ELLIPTIC UNITS

Having defined our group of elliptic units $C'_\infty = \varprojlim C'_{n,m}$, and having determined the Coleman power series associated with an element $e(\mu)$ of this group, we turn now to consider the value of our homomorphisms $\delta_{k,j}$ at $\langle e(\mu)\rangle$. To do this we shall need to introduce some further notation.

Let σ be an element of the Galois group of F_m over K. For each $k \geq 1$, we denote by $\zeta_{F_m}(\sigma, \overline{\psi}^k, s)$ the partial zeta function which is the analytic continuation of the function given by setting

$$\zeta_{F_m}(\sigma, \overline{\psi}^k, s) = \sum_{(\underline{\underline{a}}, F_m/K) = \sigma} \overline{\psi}(\underline{\underline{a}})^k N\underline{\underline{a}}^{-s}, \quad \mathrm{Re}(s) > k/2 + 1, \tag{26}$$

where the sum on the right is taken over all integral ideals $\underline{\underline{a}}$ of K prime to $\underline{\underline{fp}}^*$ whose Artin symbol for the extension F_m over K is σ.

Let L be a lattice in the complex plane. Then, for each integer $k \geq 1$, the complex valued function

$$H_k(z, s, L) = \sum_{\omega \in L} (\bar{z}+\bar{\omega})^k |z+\omega|^{-2s}, \quad \mathrm{Re}(s) > k/2 + 1,$$

can be analytically continued to the whole complex plane as a function of s. Following Weil [13], we set $E_k^*(z, L) = H_k(z, k, L)$.

It can fairly easily be deduced from Weil [13], that if $\zeta(z, L)$ denotes the Weierstrass zeta function $(d/dz) \log \sigma(z, L)$ and $a(L)$ the area of the fundamental parallelogram of L, we have the following formulae.

LEMMA 11. *(i)* $E_1^*(z, L) = \zeta(z, L) - zg_2(L) - \pi\bar{z}/a(L)$.

(ii) $E_2^*(z, L) = P(z, L) + g_2(L)$.

(iii) $E_k^*(z, L) = \dfrac{(-1)^k}{(k-1)!}\left(\dfrac{d}{dz}\right)^{k-2} P(z, L)\ ,\quad k \geq 3$.

(Here π *denotes the usual real number* 3.141... .*)*

COROLLARY 12. *For all* $k \geq 1$ *, and for all integral ideals* $\underline{\underline{a}}$ *of* K *,*

$$\left(\frac{d}{dz}\right)^k \log \Lambda_m\left(\pi^{*-(m+1)}z, \underline{\underline{a}}\right)\Big|_{z=0}$$

$$= 12(-1)^{k-1}\pi^{*-k(m+1)}(k-1)! \sum_{\underline{\underline{b}}\in B_m} \left\{N\underline{\underline{a}}E_k^*\left(\psi(\underline{\underline{b}})\rho_m, L\right) - E_k^*\left(\psi(\underline{\underline{b}})\rho_m, \underline{\underline{a}}^{-1}L\right)\right\}. \qquad (27)$$

Proof. Using the definitions at the beginning of the previous chapter, one readily sees that

$$\frac{d}{dz}\log\Theta\left(\pi^{*-(m+1)}z+\psi(\underline{\underline{b}})\rho_m, \underline{\underline{a}}\right)$$

$$= 12\pi^{*-(m+1)}\left\{N\underline{\underline{a}}\left(\zeta\left(\pi^{*-(m+1)}z+\psi(\underline{\underline{b}})\rho_m, L\right) - g_2(L)\left(\pi^{*-(m+1)}z+\psi(\underline{\underline{b}})\rho_m\right)\right)\right.$$

$$\left. - \left(\zeta\left(\pi^{*-(m+1)}z+\psi(\underline{\underline{b}})\rho_m, \underline{\underline{a}}^{-1}L\right) - g_2\left(\underline{\underline{a}}^{-1}L\right)\left(\pi^{*-(m+1)}z+\psi(\underline{\underline{b}})\rho_m\right)\right)\right\}.$$

Observing that $a\left(\underline{\underline{a}}^{-1}L\right) = a(L)/N\underline{\underline{a}}$, it follows from Lemma 11 that the right hand side is equal to

$$12\pi^{*-(m+1)}\left\{N\underline{\underline{a}}E_1^*\left(\pi^{*-(m+1)}z+\psi(\underline{\underline{b}})\rho_m, L\right) - E_1^*\left(\pi^{*-(m+1)}z+\psi(\underline{\underline{b}})\rho_m, \underline{\underline{a}}^{-1}L\right)\right\}.$$

The desired formulae can now be obtained by repeated differentiation and applying the definition of $\Lambda_m(z, \underline{\underline{a}})$.

THEOREM 13. *Let* $\underline{\underline{a}} \in I$. *Then we have the following two equalities for all* $k \geq 1$ *and* $m \geq 0$ *;*

$$(i)\quad \left(\frac{d}{dz}\right)^k \log \Lambda_m\left(\pi^{*-(m+1)}z, \underline{\underline{a}}\right)\Big|_{z=0}$$

$$= 12(-1)^{k-1}(k-1)!(\Omega_\infty/f)^{-k}\left(N\underline{\underline{a}}\zeta_{F_m}\left(1, \overline{\psi}^k, k\right) - \psi^k(\underline{\underline{a}})\zeta_{F_m}\left(\sigma_{\underline{\underline{a}}}, \overline{\psi}^k, k\right)\right)$$

where $\sigma_{\underline{\underline{a}}} = \left(\underline{\underline{a}}, F_m/K\right)$ *, and*

$$(ii)\quad \Omega_\infty^{-k}\zeta_{F_m}\left(1, \overline{\psi}^k, k\right) \in F_m \quad \textit{and}$$

$$\left(\Omega_\infty^{-k}\zeta_{F_m}\left(1, \overline{\psi}^k, k\right)\right)^\sigma = \Omega_\infty^{-k}\zeta_{F_m}\left(\sigma, \overline{\psi}^k, k\right)$$

for all $\sigma \in \mathrm{Gal}\left(F_m/K\right)$.

Proof. Observe firstly that the lattice $\underline{\underline{a}}^{-1}L$ is the lattice $\psi(\underline{\underline{a}})^{-1}\rho_m \underline{\underline{f}}\underline{\underline{p}}^{*m+1}$ since $\psi(\underline{\underline{a}})$ is a generator of $\underline{\underline{a}}$. Note also that if $\alpha \in \mathrm{C}^\times$,

$$E_k^*(\alpha z, \alpha L) = \alpha^{-k}E_k^*(z, L) .$$

From this we deduce that

$$E_k^*\left(\psi(\underline{\underline{b}})\rho_m, \underline{\underline{a}}^{-1}L\right) = \psi(\underline{\underline{a}})^k\rho_m^{-k}E_k^*\left(\psi(\underline{\underline{ab}}), \underline{\underline{f}}\underline{\underline{p}}^{*m+1}\right) ,$$

and so to prove the first part of the theorem, it will suffice to show that

$$\sum_{\underline{\underline{b}}\in B_m} E_k^*\left(\psi(\underline{\underline{ab}}),\ \underline{\underline{fp}}^{*m+1}\right) = \zeta_{F_m}\left(\sigma_{\underline{\underline{a}}},\ \overline{\psi}^k,\ k\right) . \tag{28}$$

To see this, first notice that if $\omega \in \underline{\underline{fp}}^{*m+1}$, then $\psi\left(\left(\psi(\underline{\underline{ab}})+\omega\right)\right) = \psi(\underline{\underline{ab}}) + \omega$, since ψ is a Grossencharacter of conductor $\underline{\underline{f}}$. Since K is a field with class number 1 , our very choice of B_m ensures that $\left\{\left(\psi(\underline{\underline{ab}})+\omega\right) : \underline{\underline{b}} \in B_m,\ \omega \in \underline{\underline{fp}}^{*m+1}\right\}$ is precisely the set of ideals of K , prime to $\underline{\underline{fp}}^*$, whose Artin symbol for the extension F_m over K is $\sigma_{\underline{\underline{a}}}$. From this, it follows that

$$\sum_{\underline{\underline{b}}\in B_m} H_k\left(\psi(\underline{\underline{ab}}),\ s,\ \underline{\underline{fp}}^{*m+1}\right) = \zeta_{F_m}\left(\sigma_{\underline{\underline{a}}},\ \overline{\psi}^k,\ s\right) ,\quad \mathrm{Re}(s) > k/2 + 1$$

whence we must have (28).

From Lemma 7, it is clear that $\left(\frac{d}{dz}\right)^k \log \Lambda_m\left(\pi^{*-(m+1)}z,\ \underline{\underline{a}}\right)\big|_{z=0}$ must lie in F_m . By choosing the ideal $\underline{\underline{a}}$ so that $\sigma_{\underline{\underline{a}}} = 1$ but $N\underline{\underline{a}} \neq \psi(\underline{\underline{a}})^k$, it is easy to see that the first assertion of *(ii)* is true.

The final equality can be established by noticing that if $\underline{\underline{c}} \in I$,

$$\Lambda_m^{\left(\underline{\underline{c}},F_m/K\right)}\left(\pi^{*-(m+1)}z,\ \underline{\underline{a}}\right) = \prod_{\underline{\underline{b}}\in B_m} \Theta\left(\pi^{*-(m+1)}z+\psi(\underline{\underline{bc}})\rho_m,\ \underline{\underline{a}}\right) .$$

Hence, for the same reasons as were given in the proof of part *(i)* ,

$$\left(\left(\frac{d}{dz}\right)^k \log \Lambda_m\left(\pi^{*-(m+1)}z,\ \underline{\underline{a}}\right)\big|_{z=0}\right)^{\left(\underline{\underline{c}},F_m/K\right)}$$

$$= 12(-1)^{k-1}(k-1)!(\Omega_\infty/f)^{-k}\left\{N\underline{\underline{a}}\zeta_{F_m}\left(\sigma_{\underline{\underline{c}}},\ \overline{\psi}^k,\ k\right)-\psi(\underline{\underline{a}})^k\zeta_{F_m}\left(\sigma_{\underline{\underline{ac}}},\ \overline{\psi}^k,\ k\right)\right\} .$$

The final equality is now apparent from *(i)*.

For a fixed $k \geq 1$, let $\zeta_m(k) = \Omega_\infty^{-k}\zeta_{F_m}\left(1, \overline{\psi}^k, k\right)$. We have seen that $\zeta_m(k) \in F_m$, and it is clear from Theorem 13 that if $m' \geq m$,

$$\mathrm{Tr}_{F_{m'}/F_m}\zeta_{m'}(k) = \sum_{\sigma\in\mathrm{Gal}\left(F_{m'}/F_m\right)} \Omega_\infty^{-k}\zeta_{F_{m'}}\left(\sigma, \overline{\psi}^k, k\right)$$

$$= \zeta_m(k)\,.$$

Thus $\left(\zeta_m(k)\right) \in \varprojlim \Phi_m$, where the projective limit is taken relative to the trace maps, and we denote it by $\zeta(k)$. Recall that if $b \in \varprojlim I_m$ and $j \leq 0$, $\delta_j(b) = \left[(1+T)\frac{d}{dT}\right]^{-j} h_b(T)|_{T=0} \in \hat{I}_\infty$.

COROLLARY 14. *Let $\mu \in S$, and let $k \geq 1$, $j \leq 0$ be integers. Then*

$$\delta_{k,j}\left(\langle e(\mu)\rangle\right) = \delta_j\left(12(-1)^{k-1}(k-1)!f^k \sum_{\underline{\underline{a}}\in I} \mu(\underline{\underline{a}})\left(N\underline{\underline{a}}\zeta(k)-\psi^k(\underline{\underline{a}})\zeta(k)^{\left(\underline{\underline{a}},F_\infty/K\right)}\right)\right). \tag{29}$$

Proof. Observe that if f is any function,

$$\lambda'(T)^{-1}\frac{d}{dT}f\left(\lambda(T)\right) = \frac{d}{dz}f(z)|_{z=\lambda(T)}\,.$$

In particular, since $\lambda(0) = 0$, we have that

$$\left(\frac{d}{dz}\right)^k \log\Lambda_m\left(\pi^{*-(m+1)}z, \underline{\underline{a}}\right)|_{z=0} = \left(\lambda'(T)^{-1}\frac{d}{dT}\right)^k \log\Lambda_m\left(\pi^{*-(m+1)}\lambda(T), \underline{\underline{a}}\right)|_{T=0}\,.$$

It follows from this, equation (21) and Theorems 10 and 13 that

$$\left\{\lambda'(T)^{-1}\frac{d}{dT}\right\}^{k-1} g_{m,e(\mu)}(T)\Big|_{T=0}$$

$$= 12(-1)^{k-1}(k-1)!f^k \sum_{\underline{\underline{a}}\in I} \mu(\underline{\underline{a}})\left\{N\underline{\underline{a}}\zeta_m(k)-\psi^k(\underline{\underline{a}})\zeta_m(k)^{\sigma_{\underline{\underline{a}}}}\right\} .$$

Equation (29) is now apparent from equation (9) and the remarks at the end of Chapter 3.

Katz [6] allows us to interpret the right hand side of equation (29) in terms of Hecke L-functions. To state this precisely, we need a small amount of extra notation. Tate [11] has shown that to give an isomorphism between two formal groups is equivalent to giving an isomorphism between the corresponding Tate-modules. The Weil pairing shows that $\mathrm{Hom}\left(\varprojlim E_{\pi^{n+1}}, \varprojlim \mu_{p^{n+1}}\right)$ is naturally isomorphic to the Tate-module $\varprojlim E_{\pi^{*n+1}}$, where here all the projective limits are taken relative to the maps given by multiplication by powers of p. Thus, to give an isomorphism between $\hat{E}$ and the formal multiplicative group G_m amounts to choosing a primitive element of $\varprojlim E_{\pi^{*m+1}}$. Recall that we chose $\varepsilon_n \in \mathcal{O}$ such that $\varepsilon_n\pi^* \equiv 1 \bmod \underline{\underline{p}}^{n+1}$. We choose the isomorphism $\eta : \hat{E} \xrightarrow{\sim} G_m$ such that, for all $n \geq 0$,

$$1 + \eta\left(\varepsilon\left(\Omega_\infty/\pi^{n+1}\right)\right) = \left\{\Omega_\infty/\pi^{n+1}, \varepsilon_n^{-n+1}\Omega_\infty/\pi^{*n+1}\right\}_n$$

where $\{\ ,\ \}_n$ denotes the Weil pairing of the p^{n+1}-th division points of L.

It is easy to see that any isomorphism between $\hat{E}$ and G_m must have a power series expansion of the form $\exp\left(\gamma\lambda(T)\right) - 1$, and a careful examination of the proof of the existence of such an isomorphism in [9] shows that γ is a unit in $\hat{I}_\infty$. We conclude then, that our chosen isomorphism $\eta : \hat{E} \xrightarrow{\sim} G_m$ is defined over $\hat{I}_\infty$, and that its power series expansion is given by $\eta(T) = \exp\left(\Omega_{\underline{\underline{p}}}\lambda(T)\right) - 1 = \Omega_{\underline{\underline{p}}}T + \ldots$, where $\Omega_{\underline{\underline{p}}}$ is a unit of $\hat{I}_\infty$. Note that $\Omega_{\underline{\underline{p}}}$ depends on the choice of the embedding of K_∞ in $\mathbf{C}$ and on the embedding of the fields $K_{n,m}$ in $\Xi_{n,m}$. A change in either of these would result in $\Omega_{\underline{\underline{p}}}$ being replaced by a $\mathbb{Z}_p^\times$ multiple.

If, as usual, we let $L\left(\overline{\psi}^k, s\right)$ denote the complex valued function which is the analytic continuation of the function given by setting

$$L\left(\overline{\psi}^k, s\right) = \sum_{(\underline{\underline{a}},\underline{\underline{f}})=1} \overline{\psi}^k(\underline{\underline{a}})N\underline{\underline{a}}^{-s}, \quad \mathrm{Re}(s) > k/2 + 1,$$

then we have the following theorem.

THEOREM 15. *Let $\mu \in S$ and let k and j be integers such that $k \geq 1$ and $j \leq 0$. Then,*

$$\delta_{k,j}\left(\langle e(\mu)\rangle\right) = 12(-1)^{k+1-j}(k-1)!f^k \sum_{\underline{\underline{a}}\in I} \mu(\underline{\underline{a}})\left(N\underline{\underline{a}}-\psi^k(\underline{\underline{a}})\overline{\psi}^j(\underline{\underline{a}})\right)$$

$$\cdot \left(1-\overline{\psi}^{k-j}(\underline{\underline{p}}^*)/N\underline{\underline{p}}^{*k}\right)\left(2\pi/\sqrt{d_K}\right)^{-j}\Omega_{\underline{\underline{p}}}^{j}\Omega_\infty^{j-k}L\left(\overline{\psi}^{k-j}, k\right). \quad (30)$$

Proof. A proof of this theorem, based on the formulae given in [6], is contained in Appendix 1.

CHAPTER 6

SOME BASIC RESULTS ON THE Γ-TRANSFORM

For want of adequate references elsewhere, we shall summarise in this chapter some of the basic properties of the two-variable Γ transform which we shall use later. We recall that the Γ-transform was first introduced by Leopoldt [7]. However, it will be more convenient for us to follow Katz's formulation of this notion in terms of p-adic measures.

Let μ be a measure on $Z_p \times Z_p$ taking values in $\hat{I}_\infty$. Then μ corresponds in a natural way to a power series $f_\mu(T_1, T_2) \in \hat{I}_\infty[[T_1, T_2]]$ where

$$f_\mu(T_1, T_2) = \sum_{n,m \geq 0} \left(\int_{Z_p^2} \binom{x_1}{n} \binom{x_2}{m} d\mu \right) T_1^n T_2^m . \tag{31}$$

Here $\binom{x}{k}$ denotes the binomial coefficient function

$$\binom{x}{k} = \frac{x(x-1)\dots(x-k+1)}{k!}$$

which takes values in Z_p on Z_p.

Conversely, given a power series $f(T_1, T_2) \in \hat{I}_\infty[[T_1, T_2]]$, one can recover the $\hat{I}_\infty$-valued measure μ_f on Z_p^2 to which it corresponds under equation (31) as follows.

Suppose that $n \geq 0$. Then, for k and j modulo p^n, there are uniquely determined elements $b_{k,j} \in \hat{I}_\infty$ such that

$$f(T_1, T_2) \equiv \sum_{k,j \bmod p^n} b_{k,j}(1+T_1)^k(1+T_2)^j \bmod \left[(1+T_1)^{p^n}-1,\ (1+T_2)^{p^n}-1\right] . \qquad (32)$$

Then μ_f is the unique measure for which

$$\int_{\left(k+p^n\mathbb{Z}_p\right)\times\left(j+p^n\mathbb{Z}_p\right)} d\mu_f = b_{k,j} .$$

If x is any unit in $\mathbb{Z}_p$, we write $x = \omega(x)\langle x\rangle$, where $\omega(x)$ is a $(p-1)$th root of unity and $\langle x\rangle \equiv 1 \bmod p$. Then, if i_1 and i_2 are integers $\bmod(p-1)$ and f a power series in $\hat{I}_\infty[[T_1, T_2]]$ corresponding to a measure μ_f, we define a Γ-transform

$$\Gamma_f^{(i_1,i_2)} : \mathbb{Z}_p^2 \to \hat{I}_\infty$$

by

$$\Gamma_f^{(i_1,i_2)}(s_1, s_2) = \int_{\mathbb{Z}_p^\times\times\mathbb{Z}_p^\times} \langle x_1\rangle^{s_1}\langle x_2\rangle^{s_2}\omega^{i_1}(x_1)\omega^{i_2}(x_2)d\mu_f . \qquad (33)$$

Recall that u is a topological generator of $1 + p\mathbb{Z}_p$. Define a homomorphism $l : \mathbb{Z}_p^\times \to \mathbb{Z}_p$ by

$$\langle x\rangle = u^{l(x)} \quad \forall x \in \mathbb{Z}_p^\times . \qquad (34)$$

LEMMA 16. *Let* f *be a power series in* $\hat{I}_\infty[[T_1, T_2]]$ *and let* i_1 *and* i_2 *be integers modulo* $p - 1$ *. Then there is a power series* $f^{(i_1,i_2)} \in \hat{I}_\infty[[T_1, T_2]]$ *such that for all* $s_1, s_2 \in \mathbb{Z}_p$,

$$\Gamma_f^{(i_1,i_2)}(s_1,\, s_2) = f^{(i_1,i_2)}\left(u^{s_1}-1,\, u^{s_2}-1\right) . \tag{35}$$

Proof. Equations (33) and (34) together show that

$$\Gamma_f^{(i_1,i_2)}(s_1,\, s_2) = \int_{\mathbb{Z}_p^\times \times \mathbb{Z}_p^\times} (1+u^{s_1}-1)^{l(x_1)}(1+u^{s_2}-1)^{l(x_2)}\omega^{i_1}(x_1)\omega^{i_2}(x_2)d\mu_f .$$

The binomial theorem shows that the right hand side of this last equation is equal to

$$\sum_{n,m\geq 0} (u^{s_1}-1)^n(u^{s_2}-1)^m \int_{\mathbb{Z}_p^\times \times \mathbb{Z}_p^\times} \binom{l(x_1)}{n}\binom{l(x_2)}{m}\omega^{i_1}(x_1)\omega^{i_2}(x_2)d\mu_f ,$$

and so we may take $f^{(i_1,i_2)}(T_1,\, T_2)$ to be the power series for which the coefficient of $T_1^nT_2^m$ is given by

$$\int_{\mathbb{Z}_p^\times \times \mathbb{Z}_p^\times} \binom{l(x_1)}{n}\binom{l(x_2)}{m}\omega^{i_1}(x_1)\omega^{i_2}(x_2)d\mu_f .$$

LEMMA 17. *Let* D_i *be the operator* $(1+T_i)\frac{\partial}{\partial T_i}$ *on* $\hat{I}_\infty[[T_1,\, T_2]]$ *for* $i = 1,\, 2$ *, and let* μ *be a measure on* $\mathbb{Z}_p^2$ *. Then, for* $n,\, m \geq 0$ *,* $D_1^nD_2^mf_\mu$ *corresponds to the measure* $\mu_{n,m}$ *defined by*

$$\int_{\mathbb{Z}_p^2} \phi d\mu_{n,m} = \int_{\mathbb{Z}_p^2} \phi(x_1,\, x_2)x_1^nx_2^m d\mu$$

for all measurable functions $\phi : \mathbb{Z}_p^2 \to \hat{I}_\infty$ *.*

Proof. It will suffice to show that $D_1 f_\mu$ corresponds to $\mu_{1,0}$.

Now, from equation (31), it is clear that the coefficient of $T_1^k T_2^j$ in

$D_1 f_\mu$ is $\int_{Z_p^2} \left[k\binom{x_1}{k}+(k+1)\binom{x_1}{k+1}\right]\binom{x_2}{j}d\mu$.

It is easy to see that $x_1\binom{x_1}{k} = k\binom{x_1}{k} + (k+1)\binom{x_1}{k+1}$, and so we conclude that this coefficient is equal to $\int_{Z_p^2}\binom{x_1}{k}\binom{x_2}{j}d\mu_{1,0}$.

Thus, equation (31) shows that $D_1 f_\mu$ is indeed the power series corresponding to the measure $\mu_{1,0}$.

We say that a measure μ is supported on a measurable subset A of Z_p^2 if, for all measurable functions $\phi : Z_p^2 \to \hat{I}_\infty$,

$$\int_{Z_p^2} \phi d\mu = \int_A \phi d\mu .$$

LEMMA 18. *Suppose* $f \in \hat{I}_\infty[[T_1, T_2]]$ *is such that the corresponding measure* μ_f *is supported on* $Z_p^\times \times Z_p^\times$. *Let* i_1 *and* i_2 *be integers modulo* $(p-1)$. *Then, for each pair of non-negative integers* k_1, k_2 *such that* $(k_1, k_2) \equiv (i_1, i_2) \bmod (p-1)$,

$$\Gamma_f^{(i_1,i_2)}(k_1, k_2) = \left(D_1^{k_1} D_2^{k_2} f\right)(0, 0) . \tag{36}$$

Proof. From the conditions on k_1 and k_2 it is clear that for all

$(x_1, x_2) \in \mathbb{Z}_p^\times \times \mathbb{Z}_p^\times$, $x_1^{k_1}x_2^{k_2} = \langle x_1\rangle^{k_1}\langle x_2\rangle^{k_2}\omega^{i_1}(x_1)\omega^{i_2}(x_2)$. Since μ_f is supported on $\mathbb{Z}_p^\times \times \mathbb{Z}_p^\times$, it follows from the above and equation (33) that

$$\Gamma_f^{(i_1,i_2)}(k_1, k_2) = \int_{\mathbb{Z}_p^2} x_1^{k_1}x_2^{k_2}d\mu_f .$$

We conclude from the previous lemma and the fact that $\binom{x_1}{0}\binom{x_2}{0}$ is the constant function on $\mathbb{Z}_p^2$ with value 1 , that

$$\Gamma_f^{(i_1,i_2)}(k_1, k_2) = \int_{\mathbb{Z}_p^2} \binom{x_1}{0}\binom{x_2}{0}d\mu_{D_1^{k_1}D_2^{k_2}f} .$$

But, by equation (31), the right hand side of this equation is the constant term of $D_1^{k_1}D_2^{k_2}f$ which is equal to $\left(D_1^{k_1}D_2^{k_2}f\right)(0, 0)$.

Finally, we give a lemma which shows how to construct the power series corresponding to the restriction of a measure to $\mathbb{Z}_p^\times \times \mathbb{Z}_p$.

LEMMA 19. *Let* $f(T_1, T_2) \in \hat{I}_\infty[[T_1, T_2]]$ *and let*

$$\tilde{f}(T_1, T_2) = f(T_1, T_2) - \frac{1}{p}\sum_{\zeta^p=1} f(\zeta(1+T_1)-1, T_2) \tag{37}$$

where the sum on the right is taken over the full group of p*th roots of unity. Then* $\tilde{f}(T_1, T_2) \in \hat{I}_\infty[[T_1, T_2]]$ *and for all measurable functions* $\phi : \mathbb{Z}_p^2 \to \hat{I}'_\infty$,

$$\int_{\mathbb{Z}_p^2} \phi d\mu_{\tilde{f}} = \int_{\mathbb{Z}_p^\times\times\mathbb{Z}_p} \phi d\mu_f .$$

Proof. Observe that equation (32) shows that for $n \geq 0$,

$$f(T_1, T_2) \equiv \sum_{k,j \bmod p^n} \left(\int_{(k+p^n\mathbb{Z}_p)\times(j+p^n\mathbb{Z}_p)} d\mu_f \right) (1+T_1)^k (1+T_2)^j$$

$$\bmod \left((1+T_1)^{p^n} - 1,\ (1+T_2)^{p^n} - 1 \right) .$$

A straightforward calculation shows that

$$\tilde{f}(T_1, T_2) \equiv \sum_{\substack{k,j \bmod p^n \\ k \not\equiv 0 \bmod p}} \left(\int_{(k+p^n\mathbb{Z}_p)\times(j+p^n\mathbb{Z}_p)} d\mu_f \right) (1+T_1)^k (1+T_2)^j$$

$$\bmod \left((1+T_1)^{p^n} - 1,\ (1+T_2)^{p^n} - 1 \right)$$

and so it follows that $\mu_{\tilde{f}}$ is the restriction of μ_f to $\mathbb{Z}_p^\times \times \mathbb{Z}_p$.

CHAPTER 7

p-ADIC INTERPOLATION

In this chapter, we shall use the Γ-transform which we defined in the previous chapter to produce a Λ-homomorphism from U_∞ to the Λ-module $\hat{I}_\infty[[T_1, T_2]]$.

Recall that $\eta(T) = \Omega_{\underline{\underline{p}}} T + \ldots$ is our chosen homomorphism from $\hat{E}$ to G_m defined over $\hat{I}_\infty$. Let $\iota(T) \in \hat{I}_\infty[[T]]$ be the inverse of $\eta(T)$ and recall that $g_\beta(T_1, T_2)$ denotes the two variable power series attached to an element β of U_∞.

LEMMA 20. *Let* $\beta \in U_\infty$ *and put* $h_\beta(T_1, T_2) = g_\beta(\iota(T_1), T_2)$. *Clearly* $h_\beta(T_1, T_2) \in \hat{I}_\infty[[T_1, T_2]]$. *The* $\hat{I}_\infty$*-valued measure on* Z_p^2 *corresponding to* $h_\beta(T_1, T_2)$ *is supported on* $Z_p \times Z_p^\times$.

Proof. From Theorem 5, it is evident that

$$h_\beta(T_1, T_2) \equiv \sum_{\sigma\in \mathrm{Gal}(F_m/K)} \left[g_{m,\beta}^\sigma(\iota(T_1))\right]_{\underline{\underline{p}}_m} (1+T_2)^{\kappa_2(\sigma)} \bmod \left[(1+T_2)^{p^{m+1}} - 1\right].$$

Since κ_2 takes values in $Z_p^\times$, it follows from equation (32) that $h_\beta(T_1, T_2)$ corresponds to a measure supported on $Z_p \times Z_p^\times$.

LEMMA 21. *Let* $k \geq 1$ *and* $j \leq 0$. *For each* $\beta \in U_\infty$, *let* $h_\beta(T_1, T_2) \in \hat{I}_\infty[[T_1, T_2]]$ *be as in Lemma* 20. *Then, if* $\tilde{h}_\beta(T_1, T_2)$ *is the corresponding power series as in equation* (37),

$$D_1^{k-1} D_2^{-j} \tilde{h}_\beta(T_1, T_2)\big|_{(0,0)} = \Omega_{\underline{\underline{p}}}^{1-k}\left(1-\psi(\underline{\underline{p}})^{k-j}/(N\underline{\underline{p}})^{1-j}\right)\delta_{k,j}(\beta) . \tag{38}$$

Proof. Since $\iota \circ \eta(T) = T$, and $\eta(T) = \exp\left(\Omega_{\underline{\underline{p}}}\lambda(T)\right) - 1$, it is easy to see that

$$\left(1+\eta(T)\right)\iota'\left(\eta(T)\right) = \left(\Omega_{\underline{\underline{p}}}\lambda'(T)\right)^{-1} .$$

From this it follows that $\left[\left(\Omega_{\underline{\underline{p}}}\lambda'(T)\right)^{-1} \dfrac{d}{dT} f(T)\right]\Big|_{T=\iota(T_1)} = \left(1+T_1\right) \dfrac{d}{dT_1} f\left(T_1\right)$

and in particular that

$$D_1^{k-1} D_2^{-j} \tilde{h}_\beta(T_1, T_2)\big|_{(0,0)} = \left\{\left(\Omega_{\underline{\underline{p}}}\lambda'(T)\right)^{-1} \frac{\partial}{\partial T}\right\}^{k-1} D_2^{-j}\tilde{h}_\beta\left(\eta(T), T_2\right)\big|_{(0,0)} . \tag{39}$$

Recall that

$$\tilde{h}_\beta\left(\eta(T), T_2\right) = h_\beta\left(\eta(T), T_2\right) - \frac{1}{p} \sum_{\zeta^p=1} h_\beta\left(\zeta\left(1+\eta(T)\right)-1, T_2\right) ,$$

and observe that $h_\beta\left(\eta(T), T_2\right) = g_\beta\left(T, T_2\right)$. Now, if $\zeta^p = 1$, $\zeta - 1$ is a point of order p on G_m, and since ι is an isomorphism, as ζ runs over the solution set of $\zeta^p = 1$, $\iota(\zeta-1)$ runs over the elements of $\hat{E}_\pi$. Moreover, we also have that

$$\eta\left(\iota(\zeta-1) * T\right) = \zeta\left(1+\eta(T)\right) - 1$$

and so

$$h_\beta\left(\zeta\left(1+\eta(T)\right)-1, T_2\right) = g_\beta\left(\iota(\zeta-1) * T, T_2\right) .$$

We conclude that

$$\tilde{h}_\beta(\eta(T),\ T_2) = g_\beta(T,\ T_2) - \frac{1}{p} \sum_{\eta \in \hat{E}_\pi} g_\beta(T * \eta,\ T_2)\ ,$$

and equation (12) shows that the right hand side is equal to

$$g_\beta(T,\ T_2) - \frac{\pi}{p}\, g_\beta\left([\pi]T,\ (1+T_2)^{\kappa_2(\varphi)^{-1}} - 1\right) .$$

Recall that $\varphi = (\underline{\underline{p}},\ F_\infty/K)$ and that it follows from the definition of the Grossencharacter that φ acts on $E_{\pi^{*\infty}}$ *via* $\psi(\underline{\underline{p}})$. We conclude from equation (3) that $\kappa_2(\varphi) = \bar{\pi}$. Notice also that

$$\left(\Omega_{\underline{\underline{p}}}\lambda'(T)\right)^{-1} \frac{d}{dT} f([\pi]T) = \pi\left\{\left(\Omega_{\underline{\underline{p}}}\lambda'(W)\right)^{-1} \frac{d}{dW} f(W)\right\}\Big|_{W=[\pi](T)}$$

and that

$$\left\{(1+T)\ \frac{d}{dT} f\left((1+T)^{\bar{\pi}^{-1}} - 1\right)\right\} = \bar{\pi}^{-1}\left\{(1+W)\ \frac{d}{dW} f(W)\right\}\Big|_{W=(1+T)^{\bar{\pi}^{-1}}-1} .$$

Combining all these facts, we see that equation (39) becomes

$$D_1^{k-1} D_2^{-j} \tilde{h}_\beta(T_1,\ T_2)|_{(0,0)}$$

$$= \Omega_{\underline{\underline{p}}}^{1-k}\left\{\lambda'(T)^{-1}\ \frac{\partial}{\partial T}\right\}^{k-1} D_2^{-j}\left(1 - \pi^{k-j}/p^{1-j}\right) g_\beta(T,\ T_2)|_{(0,0)}\ . \qquad (40)$$

Equation (14) shows that the right hand side of equation (40) is equal to $\Omega_{\underline{\underline{p}}}^{1-k}\left(1 - \psi(\underline{\underline{p}})^{k-j}/(N\underline{\underline{p}})^{1-j}\right)\delta_{k,j}(\beta)$.

The following theorem provides the homomorphism to which we alluded at the beginning of this chapter.

THEOREM 22. *Let* i_1 *and* i_2 *be integers modulo* $(p-1)$ *, and let* $\beta \in U_\infty$. *Then there is a unique power series*

$$G_\beta^{(i_1,i_2)}(T_1, T_2) \in \hat{I}_\infty[[T_1, T_2]]$$

such that for all $k_1 \geq 1$ *and* $k_2 \leq 0$ *satisfying* $(k_1, k_2) \equiv (i_1, i_2) \bmod (p-1)$,

$$G_\beta^{(i_1,i_2)}\left(u^{k_1}-1, u^{k_2}-1\right) = \Omega_{\underline{\underline{p}}}^{1-k_1}\left(1 - \pi^{k_1-k_2}/p^{1-k_2}\right)\delta_{k_1,k_2}(\beta) . \tag{41}$$

Moreover, if $h \in \Lambda$,

$$G_{h\beta}^{(i_1,i_2)}(T_1, T_2) = h(T_1, T_2)G_\beta^{(i_1,i_2)}(T_1, T_2) . \tag{42}$$

Proof. Lemmas 19 and 20 together show that the power series $\tilde{h}_\beta$ of Lemma 21 corresponds to a measure supported on $Z_p^\times \times Z_p^\times$. We deduce from Lemma 18 and equation (38) that for k_1 and k_2 as in the theorem

$$\Gamma_{\tilde{h}_\beta}^{(i_1-1,-i_2)}(k_1-1, -k_2) = \Omega_{\underline{\underline{p}}}^{1-k_1}\left(1 - \pi^{k_1-k_2}/p^{1-k_2}\right)\delta_{k_1,k_2}(\beta) .$$

On the other hand, Lemma 16 shows that there is a power series $\tilde{h}_\beta^{(i_1-1,-i_2)}(T_1, T_2) \in \hat{I}_\infty[[T_1, T_2]]$ such that for all $s_1, s_2 \in Z_p$,

$$\Gamma_{\tilde{h}_\beta}^{(i_1-1,-i_2)}(s_1, s_2) = \tilde{h}_\beta^{(i_1-1, -i_2)}\left(u^{s_1}-1, u^{s_2}-1\right) .$$

Thus, if we set

$$G_\beta^{(i_1,i_2)}(T_1,\ T_2) = \tilde{h}_\beta^{(i_1-1,-i_2)}\left(u^{-1}(1+T_1)-1,\ (1+T_2)^{-1}-1\right) ,$$

it is clear that equation (41) will be satisfied. Such a power series is clearly unique, and so equation (42) follows immediately from equation (16).

CHAPTER 8

THE STRUCTURE OF U_∞

We observe that $\mathrm{Gal}(\Xi_\infty/K_{\underline{\underline{p}}})$ can be decomposed into the product of two groups, the Galois group $\mathrm{Gal}(\Xi_\infty/\Xi_{0,0})$ of Ξ_∞ over $\Xi_{0,0}$, and a group which may be identified with $\mathrm{Gal}(\Xi_{0,0}/K_{\underline{\underline{p}}})$. From our knowledge of the decomposition of $\underline{\underline{p}}$, it is clear that we can identify $\mathrm{Gal}(\Xi_\infty/\Xi_{0,0})$ with $\mathrm{Gal}(K_\infty/K_{0,M}) \subset \Gamma$, and we note that this is the subgroup of Γ which is topologically generated by γ_1 and $\gamma_2^{p^M}$. Thus, any compact $\mathbb{Z}_p$-module B on which $\mathrm{Gal}(\Xi_\infty/\Xi_{0,0})$ acts continuously can be equipped with a structure as a $\mathbb{Z}_p\left[\left[T_1, (1+T_2)^{p^M}-1\right]\right]$-module.

Any $\mathbb{Z}_p[\mathrm{Gal}(\Xi_{0,0}/K_{\underline{\underline{p}}})]$-module A has a canonical decomposition

$$A = \bigoplus_{\substack{i_1 \bmod p-1 \\ i_2 \bmod (p-1)/r_0}} A^{(i_1,i_2)}$$

where $A^{(i_1,i_2)}$ is the submodule of A on which $\mathrm{Gal}(\Xi_{0,0}/K_{\underline{\underline{p}}})$ acts *via* $\chi_1^{i_1}\chi_2^{i_2}$.

If ν is any prime of F_M, we let $U_{\infty,\nu}$ denote the projective limit relative to the local norm maps of the $U_{n,m,\omega}$ for the primes ω lying above (or below) ν. As usual, we omit the subscript for the prime when referring to $\underline{\underline{p}}_M$. Then, both U_∞ and $\varprojlim \mu_{p^{n+1}}$ can be equipped with $\mathbb{Z}_p\left[\left[T_1,\ (1+T_2)^{p^M}-1\right]\right]$-module structures, and possess a natural $\mathrm{Gal}(\Xi_{0,0}/K_{\underline{\underline{p}}})$ action. Moreover, it is well known from the Weil pairing that $(\varprojlim \mu_{p^{n+1}})^{(i_1,i_2)} = 0$ unless $(i_1,\ i_2) \equiv (1,\ 1)\bmod(p-1,\ p-1/r_0)$.

Wintenberger [14] has studied the structure of U_∞ as a $\mathbb{Z}_p\left[\left[T_1,\ (1+T_2)^{p^M}-1\right]\right]$-module and his results may be summarized in the following lemma.

LEMMA 23. *Let* i_1 *and* i_2 *be integers. Then we have the following exact sequence of* $\mathbb{Z}_p\left[\left[T_1,\ (1+T_2)^{p^M}-1\right]\right]$ *modules*

$$0 \to U_\infty^{(i_1,i_2)} \xrightarrow{w^{(i_1,i_2)}} \mathbb{Z}_p\left[\left[T_1,\ (1+T_2)^{p^M}-1\right]\right] \to (\varprojlim \mu_{p^{n+1}})^{(i_1,i_2)} \to 0 .$$

There is an obvious isomorphism between U_∞ and $\prod_\nu U_{\infty,\nu}$, where the product is taken over the primes ν of F_M lying above $\underline{\underline{p}}$, whose inverse may be constructed as follows. Let $(\beta_\nu) \in \prod_\nu U_{\infty,\nu}$. Then (β_ν) is mapped onto the element of U_∞ whose projection onto $U_{n,m}$ has its ω-component given by the product over the primes ν of F_M lying above (or below) ω of the projection of $\beta_\nu \in U_{\infty,\nu}$ onto $U_{n,m,\omega}$. From this, it is easy to see that $U_\infty^{(i_1,i_2)} \cong \prod_{\nu|\underline{\underline{p}}_0} U_{\infty,\nu}^{(i_1,i_2)}$, where the product is now taken over primes ν of F_M lying above $\underline{\underline{p}}_0$. This is because all the components of an element $(\beta_\nu) \in \left(\prod_\nu U_{\infty,\nu}\right)^{(i_1,i_2)}$ are uniquely determined by those associated to primes lying above $\underline{\underline{p}}_0$.

LEMMA 24. *Let i_1 and i_2 be integers. Then there is an injection $W^{(i_1,i_2)} : \mathrm{U}_\infty^{(i_1,i_2)} \to \Lambda$ which is a homomorphism of Λ-modules. Moreover, if $(i_1, i_2) \not\equiv (1, 1) \bmod (p-1, (p-1)/r_0)$, $W^{(i_1,i_2)}$ is an isomorphism; and if $(i_1, i_2) \equiv (1, 1) \bmod (p-1, (p-1)/r_0)$, the image of $W^{(i_1,i_2)}$ is the ideal of Λ generated by $1 + T_1 - u$ and $(1+T_2)^{p^M} - u^{p^M}$.*

Proof. If $\beta \in \mathrm{U}_\infty^{(i_1,i_2)}$, let $(\beta)_{\underline{\underline{p}}_M}$ denote the $\underline{\underline{p}}_M$-component of β viewed as an element of $\prod_\nu U_{\infty,\nu}$. Since $\underline{\underline{p}}_M^{\gamma_2^j}$ $(j = 0, \ldots, p^M-1)$ is the complete set of primes of F_M lying above $\underline{\underline{p}}_0$, it follows from the remarks above that β is completely determined by the set

$$\left\{\left(\beta^{\gamma_2^j}\right)_{\underline{\underline{p}}_M} : j = 0, \ldots, p^M-1\right\}.$$

Let $W^{(i_1,i_2)}(\beta) = \sum_{j=0}^{p^M-1} (1+T_2)^{-j} w^{(i_1,i_2)} \left(\beta^{\gamma_2^j}\right)_{\underline{\underline{p}}_M}$. It is easy to see that $W^{(i_1,i_2)}$ is a Λ-homomorphism. Furthermore, since the $(1+T_2)^{-j}$ $(j = 0, \ldots, p^M-1)$ provide a complete set of representatives for the additive group $\Lambda/\mathbb{Z}_p\left[\left[T_1, (1+T_2)^{p^M}-1\right]\right]$, we conclude from Lemma 23 that

$W^{(i_1,i_2)}$ is injective, and an isomorphism unless $(i_1, i_2) \equiv (1, 1) \bmod (p-1, (p-1)/r_0)$.

Since $\mathrm{Gal}(\Xi_\infty/K_{\underline{\underline{p}}})$ acts on $(\varprojlim \mu_{p^{n+1}})$ *via* $\kappa_1\kappa_2$ (this is clear from the Weil-pairing), the image of $w^{(i_1,i_2)}$ is the ideal of $\mathbb{Z}_p\left[\left[T_1, (1+T_2)^{p^M}-1\right]\right]$ generated by (T_1+1-u) and $(1+T_2)^{p^M} - u^{p^M}$ if $(i_1, i_2) \equiv (1, 1) \bmod (p-1, (p-1)/r_0)$, and hence the image of $W^{(i_1,i_2)}$ is as described in the lemma.

In future, we shall denote the image of $W^{(i_1,i_2)}$ by $H^{(i_1,i_2)}$.

We now seek to establish a connection between the two Λ-homomorphisms $G^{(i_1,i_2)}$ and $W^{(i_1,i_2)}$. In order to do this, we need to first establish the existence of certain elements of U_∞.

LEMMA 25. *Let* $(\beta_{n,m,\omega}) \in \mathrm{U}_{n,m}$. *Then there exists* $\beta \in \mathrm{U}_\infty$ *whose projection onto* $\mathrm{U}_{n,m}$ *is* $(\beta_{n,m,\omega})$ *if and only if, for all primes* ω *of* F_m *lying above* $\underline{\underline{p}}$, *the local norm from* $\Xi_{n,m,\omega}$ *to* $K_{\underline{\underline{p}}}$ *of* $\beta_{n,m,\omega}$ *is* 1.

Proof. Thanks to our isomorphism between U_∞ and $\prod_\nu U_{\infty,\nu}$, it will suffice to show that if $\beta_{n,m} \in U_{n,m}$, then there exists $\beta \in U_\infty$ whose projection onto $U_{n,m}$ is $\beta_{n,m}$ if and only if the norm from $\Xi_{n,m}$ to $K_{\underline{\underline{p}}}$ of $\beta_{n,m}$ is 1.

Now the extension $\Xi_{n,m}$ over $K_{\underline{\underline{p}}}$ decomposes into an unramified extension and a totally ramified extension of degree $(p-1)p^n$, and so the image of $U_{n,m}$ under the norm map from $\Xi_{n,m}$ to $K_{\underline{\underline{p}}}$ is precisely $1 + \underline{\underline{p}}^{p^n}$. From local class field theory, we know that if $H \subset J \subset L$ are local fields, then $\alpha \in N_{L/J}L^\times$ if and only if $N_{J/H}\alpha \in N_{L/H}L^\times$, and so $\beta_{n,m}$ can be lifted to an element of U_∞ if and only if its norm to $K_{\underline{\underline{p}}}$ is 1.

LEMMA 26. *Let* i_1 *and* i_2 *be integers modulo* $(p-1)$, *and let* k_1 *and* k_2 *be integers such that* $1 \le k_1 < p$, $k_2 \le 0$ *and* $(k_1, k_2) \equiv (i_1, i_2) \bmod p-1$. *Then there is an element* $\alpha \in \mathrm{U}_\infty$ *such that* $\delta_{k_1,k_2}(\alpha)$ *is a unit in* $\hat{\mathrm{I}}_\infty$.

Proof. We denote by $\mathrm{I}_0^{(j)}$ the subspace of I_0 on which $\mathrm{Gal}(F_0/K)$ acts *via* χ_2^j. It is easily seen that $\mathrm{I}_0^{(j)}$ is a free Z_p-module of rank 1, and that each component of any basis of $\mathrm{I}_0^{(j)}$ is a unit of the appropriate component ring.

Let $\nu(T)$ be an isomorphism of formal groups over Z_p; $\nu : \hat{E} \xrightarrow{\sim} \hat{\mathrm{E}}$, where $\hat{\mathrm{E}}$ is the Lubin-Tate formal group on which the endomorphism π is given by $[\pi]T = \pi T + T^p$. We remark that we only introduce this special formal group in order to simplify the construction, which could be made appealing only to the properties of $\hat{E}$. We shall treat the construction of the element α in two cases.

Firstly, suppose $k_1 < p-1$. Let a be a Z_p-basis of $\mathrm{I}_0^{(i_2)}$ and put

$\alpha'_{0,0} = 1 + a(\nu(u_0))^{k_1} \in \mathsf{U}_{0,0}$. Since $\nu(u_0)$ belongs to the maximal ideal of each component of $\Xi_{0,0}$, the norm to $K_{\underline{\underline{p}}}$ of each component of $\alpha'_{0,0}$ is clearly congruent to $1 \bmod \underline{\underline{p}}$. It follows that we can choose an element $x \in \mathsf{U}_{0,0}$ in such a way that each component of x belongs to $1 + \underline{\underline{p}}\mathcal{O}_{\underline{\underline{p}}}$ and has the same norm to $K_{\underline{\underline{p}}}$ as the corresponding component of $\alpha'_{0,0}$. We set $\alpha_{0,0} = x^{-1}\alpha'_{0,0}$, and it is clear that $\alpha_{0,0}$ can be lifted to an element $\alpha \in \mathsf{U}_\infty$ and that $\alpha_{0,0} \equiv 1 + a(\nu(u_0))^{k_1} \bmod \underline{\underline{p}}_{0,0}^{p-1}$. (This is a slight abuse of notation to denote in each component a congruence modulo the $(p-1)$th power of the maximal ideal of the local field.) It follows that for such an α ,

$$c_{0,\omega,\alpha}(T) \equiv 1 + (a)_\omega(\nu(T))^{k_1} \bmod (\omega, T^{p-1}) .$$

On the other hand, if $k_1 = p - 1$, we proceed as follows. Again we choose a $\mathbb{Z}_p$-basis a for $\mathrm{I}_0^{(i_2)}$ and we set

$$\alpha'_{1,0} = (1+\pi a^{\varphi^{-1}}) + a^{\varphi^{-1}}(\nu(u_1))^{p-1} \in \mathsf{U}_{1,0} .$$

Observe that, by the definition of ν , $\nu(u_1)^p + \pi\nu(u_1) = \nu(u_0)$, and so

$$\alpha'_{1,0} = 1 + a^{\varphi^{-1}}\nu(u_0)/\nu(u_1) .$$

The minimal equation satisfied by $1/\nu(u_1)$ over $\Xi_{0,0}$ is $X^p - \frac{\pi}{\nu(u_0)}X^{p-1} - \frac{1}{\nu(u_0)}$, and so, since p is odd and $\nu(u_0)^{p-1} = -\pi$, it follows that the norm to $\Xi_{0,0}$ of $\alpha'_{1,0}$ is equal to $1+\pi\left(a^{\varphi^{-1}}-\left(a^{\varphi^{-1}}\right)^p\right)$.

If ω is any prime of F_0 lying above $\underline{\underline{p}}$, $\left(a^{\varphi^{-1}}\right)^p_\omega \equiv (a)_\omega \bmod \omega$, and we deduce from this that the norm to $K_{\underline{\underline{p}}}$ of each component of $\alpha'_{1,0}$ is congruent to 1 modulo $\underline{\underline{p}}^2$. We can choose $x \in U_{1,0}$ in such a way that each component of x belongs to $1+\underline{\underline{p}}\mathcal{O}_{\underline{\underline{p}}}$ and has the same norm to $K_{\underline{\underline{p}}}$ as the corresponding component of $\alpha'_{1,0}$. We set $\alpha_{1,0}=x^{-1}\alpha'_{1,0}$, and it is clear that $\alpha_{1,0}$ can be lifted to an element α of U_∞ and that $\alpha_{1,0} \equiv 1+a^{\varphi^{-1}}\left(\nu(u_1)\right)^{p-1} \bmod \underline{\underline{p}}_{1,0}^{p(p-1)}$. It follows that, for such an α, $c_{0,\omega,\alpha}(T) \equiv 1+(a)_\omega\left(\nu(T)\right)^{p-1} \bmod \left(\omega, T^{p(p-1)}\right)$.

Thus, in both cases, we have an element $\alpha \in U_\infty$ such that the corresponding Coleman power series satisfy

$$c_{0,\omega,\alpha}(T) \equiv 1+(a)_\omega\left(\nu(T)\right)^{k_1} \bmod \left(\omega, T^{k_1+1}\right),$$

where a is a $\mathbb{Z}_p$-basis for $I_0^{(i_2)}$.

The logarithm map $\lambda_{\hat{E}}$ of $\hat{E}$ satisfies $\lambda'_{\hat{E}}(T) \equiv 1 \bmod \left(\underline{\underline{p}}, T^{p-1}\right)$ (see, for example [2]). Since $\lambda(T)=\lambda_{\hat{E}}\left(\nu(T)\right)$ by the uniqueness of the logarithm map, it follows that $\lambda'(T)^{-1}\frac{d}{dT}f\left(\nu(T)\right)=\lambda'_{\hat{E}}\left(\nu(T)\right)^{-1}f'\left(\nu(T)\right)$, and so we see that

$$\left(g_{0,\alpha}(T)\right)_\omega \equiv k_1(a)_\omega\left(\nu(T)\right)^{k_1-1} \bmod \left(\omega, T^{k_1}\right).$$

It is evident that

$$\left[\left(\lambda'(T)^{-1}\frac{d}{dT}\right)^{k_1-1} g_{0,\alpha}(T)\right]_\omega \equiv k_1!(a)_\omega \operatorname{mod}(\omega, T) ,$$

and so

$$\delta_{k_1,k_2}(\alpha) \equiv \sum_{\sigma\in\mathrm{Gal}(F_0/K)} \kappa_2(\sigma)^{-k_2} k_1!\left(a^\sigma\right)_{\underline{\underline{p}}_0} \bmod \underline{\underline{p}}_\infty$$

$$\equiv k_1! \sum_{\sigma\in\mathrm{Gal}(F_0/K)} \chi_2^{-i_2}(\sigma)\left(a^\sigma\right)_{\underline{\underline{p}}_0} \bmod \underline{\underline{p}}_\infty .$$

But σ acts on a *via* $\chi_2^{i_2}(\sigma)$, and so

$$\delta_{k_1,k_2}(\alpha) \equiv (p-1)k_1!(a)_{\underline{\underline{p}}_0} \bmod \underline{\underline{p}}_\infty ,$$

and is therefore a unit of $\hat{I}_\infty$.

THEOREM 27. *Let* i_1 *and* i_2 *be integers modulo* $p - 1$. *Then there is a power series* $\phi^{(i_1,i_2)}(T_1, T_2) \in \hat{I}_\infty[[T_1, T_2]]$ *such that, for all* $\beta \in U_\infty^{(i_1,i_2)}$,

$$G_\beta^{(i_1,i_2)}(T_1, T_2) = \phi^{(i_1,i_2)}(T_1, T_2)W^{(i_1,i_2)}(\beta) . \tag{43}$$

Furthermore, $\phi^{(i_1,i_2)}(T_1, T_2)$ *is a unit.*

Proof. Suppose for the moment that $(i_1, i_2) \not\equiv (1, 1)\operatorname{mod}(p-1, (p-1)/r_0)$. If we let $\alpha^{(i_1,i_2)}$ be the element of $U_\infty^{(i_1,i_2)}$ such that $W^{(i_1,i_2)}\left(\alpha^{(i_1,i_2)}\right) = 1$, then it is clear that $\phi^{(i_1,i_2)}(T_1, T_2) = G_{\alpha^{(i_1,i_2)}}^{(i_1,i_2)}(T_1, T_2)$ satisfies equation (43).

Let k_1 and k_2 be as in Lemma 26, and choose $\alpha \in U_\infty^{(i_1,i_2)}$ such that $\delta_{k_1,k_2}(\alpha)$ is a unit in $\hat{I}_\infty$. (This is possible since Lemma 6 shows that $\delta_{k_1,k_2}(\beta)$ depends only on the $\chi_1^{i_1}\chi_2^{i_2}$ part of β.) Equations (41) and (43) together show that

$$\phi^{(i_1,i_2)}(T_1, T_2)W^{(i_1,i_2)}(\alpha)\Big|_{\left(u^{k_1}-1,u^{k_2}-1\right)} \underset{\underline{\underline{p}}}{=} \Omega^{1-k_1}\left(1-p^{k_1-1}/\bar{\pi}^{k_1-k_2}\right)\delta_{k_1,k_2}(\alpha) .$$

Since $(k_1, k_2) \not\equiv (1, 1)\operatorname{mod}\left(p-1, (p-1)/r_0\right)$, $\left(1-p^{k_1-1}/\bar{\pi}^{k_1-k_2}\right)$ is a unit of Z_p, and so the right-hand side is a unit.

Hence $\phi^{(i_1,i_2)}\left(u^{k_1}-1, u^{k_2}-1\right)$ is a unit of $\hat{I}_\infty$, and so $\phi^{(i_1,i_2)}(T_1, T_2)$ is a unit of $\hat{I}_\infty[[T_1, T_2]]$.

Suppose now that $(i_1, i_2) \equiv (1, 1)\operatorname{mod}\left(p-1, (p-1)/r_0\right)$. Let α_1 and α_2 be the elements of $U_\infty^{(i_1,i_2)}$ such that $W^{(i_1,i_2)}(\alpha_1) = T_1 + 1 - u$ and $W^{(i_1,i_2)}(\alpha_2) = (1+T_2)^{p^M} - u^{p^M}$. It clearly follows from equation (42) that

$$\left((1+T_2)^{p^M}-u^{p^M}\right)G_{\alpha_1}^{(i_1,i_2)}(T_1, T_2) = (T_1+1-u)G_{\alpha_2}^{(i_1,i_2)}(T_1, T_2) .$$

From the Weierstrass preparation theorem, we conclude that there is a power series $\phi^{(i_1,i_2)}(T_1, T_2) \in \hat{I}_\infty[[T_1, T_2]]$ such that

$$G_{\alpha_1}^{(i_1,i_2)}(T_1, T_2) = \phi^{(i_1,i_2)}(T_1, T_2)(T_1+1-u) .$$

Hence we also have that

$$G_{\alpha_2}^{(i_1,i_2)}(T_1, T_2) = \phi^{(i_1,i_2)}(T_1, T_2)\left\{(1+T_2)^{p^M}-u^{p^M}\right\}$$

and, since α_1 and α_2 generate $U_\infty^{(i_1,i_2)}$ as a Λ-module by Lemma 24, it follows from Theorem 22 that equation (43) holds for all $\beta \in U_\infty^{(i_1,i_2)}$.

Let $k_2 \le 0$ be chosen so that $k_2 \equiv i_2 \bmod (p-1)$ and $1 - k_2$ is prime to p . Then, by Lemma 26, we can choose an $\alpha \in U_\infty^{(1,i_2)}$ such that $\delta_{1,k_2}(\alpha)$ is a unit in $\hat{I}_\infty$. Once again, we see that

$$\left\{\phi^{(1,i_2)}(T_1, T_2)W^{(1,i_2)}(\alpha)\right\}\Big|_{(u-1,u^{k_2}-1)} = \left(1-\left(1/\bar{\pi}^{1-k_2}\right)\right)\delta_{1,k_2}(\alpha) .$$

Since $\bar{\pi}$ generates a subgroup of index r_0p^M in $(\mathcal{O}/\underline{\underline{p}}^{M+2})^\times$, and this is a cyclic group of order $(p-1)p^{M+1}$, $\bar{\pi}^{1-k_2} \not\equiv 1 \bmod \underline{\underline{p}}^{M+2}$.

Now $W^{(1,i_2)}(\alpha) \in (1+T_1-u)\Lambda + \left\{(1+T_2)^{p^M}-u^{p^M}\right\}\Lambda$, and so $W^{(1,i_2)}(\alpha)\Big|_{(u-1,u^{k_2}-1)} \in \underline{\underline{p}}^{M+1}$. It follows that $\phi^{(1,i_2)}(u-1, u^{k_2}-1)$ is a unit in $\hat{I}_\infty$, and hence $\phi^{(1,i_2)}(T_1, T_2)$ is a unit of $\hat{I}_\infty[[T_1, T_2]]$.

CHAPTER 9

p-ADIC INTERPOLATION OF SPECIAL VALUES OF L-FUNCTIONS

Recall that for $k > j \geq 0$, we defined $L_\infty(\overline{\psi}^{k+j}, k)$ to be the element of K given by equation (2). In fact, it follows from Theorem 15 that, if we define $L_\infty(\overline{\psi}^{k+j}, k)$ to be the algebraic number given by equation (2) for all $k \geq 1$ and $j \geq 0$, then $L_\infty(\overline{\psi}^{k+j}, k)$ belongs to $K_{\underline{\underline{p}}}$ when viewed in the manner described in the appendix. In this chapter we shall produce power series giving p-adic interpolations of the numbers $L_\infty(\overline{\psi}^{k}, j)$, and in the process we shall determine the image under $W^{(i_1,i_2)}$ of the Λ-submodule D of U_∞ generated by $\{\langle e(\mu)\rangle : \mu \in S\}$.

Before doing that, we shall make one remark about the relationship between this submodule D and the group of elliptic units. Recall that $C'_{n,m}$ is the group of elliptic units of $K_{n,m}$. We denote by $C_{n,m}$ the subgroup of $C'_{n,m}$ consisting of those elements which are congruent to 1 modulo each prime of $K_{n,m}$ lying above $\underline{\underline{p}}$ (that is, $C_{n,m} = C'_{n,m} \cap \mathrm{U}_{n,m}$), and we let $\overline{C}_{n,m}$ denote the closure of $C_{n,m}$ in $\mathrm{U}_{n,m}$ (which is the Λ-module generated by $C_{n,m}$). Then, if we let $\overline{C}_\infty$ denote the projective limit of the $\overline{C}_{n,m}$ relative to the norm maps, it is clear that $\overline{C}_\infty$ is a Λ-submodule of U_∞ containing D . Moreover, the image of D under the projection map from U_∞ to $\mathrm{U}_{n,m}$ is precisely $\overline{C}_{n,m}$.

If $\mu \in S$ and i_1 and i_2 are integers modulo $p - 1$, we define

$$h_\mu^{(i_1,i_2)}(T_1,\,T_2)$$

$$= \sum_{\underline{\underline{a}}\in I} \mu(\underline{\underline{a}})\left(N\underline{\underline{a}}-\omega^{i_1}(\psi(\underline{\underline{a}}))\omega^{i_2}(\overline{\psi}(\underline{\underline{a}}))(1+T_1)^{l(\psi(\underline{\underline{a}}))}(1+T_2)^{l(\overline{\psi}(\underline{\underline{a}}))}\right), \quad (44)$$

and observe that for all $(k_1,\,k_2) \equiv (i_1,\,i_2)\bmod(p-1)$,

$$h_\mu^{(i_1,i_2)}(u^{k_1}-1,\,u^{k_2}-1) = \sum_{\underline{\underline{a}}\in I} \mu(\underline{\underline{a}})(N\underline{\underline{a}}-\psi^{k_1}(\underline{\underline{a}})\overline{\psi}^{k_2}(\underline{\underline{a}})) . \quad (45)$$

LEMMA 28. *Let* $H^{(i_1,i_2)}$ *be the* Λ*-module generated by* $\left\{h_\mu^{(i_1,i_2)}(T_1,\,T_2) : \mu\in S\right\}$. *Then* $H^{(i_1,i_2)} = \Lambda$ *unless* $(i_1,\,i_2) \equiv (0,\,0)$ *or* $(1,\,1)\bmod(p-1)$; $H^{(0,0)}$ *is the* Λ*-module generated by* T_1 *and* T_2 *and* $H^{(1,1)}$ *is the module generated by* T_1+1-u *and* T_2+1-u .

Proof. Observe firstly that, for all $\mu\in S$,

$$h_\mu^{(0,0)}(0,\,0) = \sum_{\underline{\underline{a}}\in I} \mu(\underline{\underline{a}})(N\underline{\underline{a}}-1) = 0$$

and

$$h_\mu^{(1,1)}(u-1,\,u-1) = \sum_{\underline{\underline{a}}\in I} \mu(\underline{\underline{a}})(N\underline{\underline{a}}-\psi(\underline{\underline{a}})\overline{\psi}(\underline{\underline{a}})) = 0 ,$$

and so it follows that the $H^{(i_1,i_2)}$ are all contained in the Λ-module to which the lemma asserts they are equal. Since Λ is Noetherian, it will suffice to show that the $H^{(i_1,i_2)}$ contain elements which are congruent modulo $(p,\,T_1,\,T_2)^m$ to generators of the appropriate Λ-modules for each integer $m\geq 0$.

To do this, let ζ be a primitive $(p-1)$th root of unity in $Z_p^\times$, and let a, b, c and d be integers which we shall fix later according to the case under consideration. Choose elements α_1 and α_2 in O which are prime to each element of S such that $\alpha_1 \equiv 1 \bmod \underline{\underline{\mathrm{fp}}}^{*m}$, $\alpha_1 \equiv \zeta^a u^b \bmod \underline{\underline{\mathrm{p}}}^m$, $\alpha_2 \equiv 1 \bmod \underline{\underline{\mathrm{fp}}}^m$ and $\bar{\alpha}_2 \equiv \zeta^c u^d \bmod \underline{\underline{\mathrm{p}}}^m$. Clearly the ideals $\underline{\underline{\mathrm{a}}}_1 = (\alpha_1)$ and $\underline{\underline{\mathrm{a}}}_2 = (\alpha_2)$ both belong to I, and we consider the function $\mu \in S$ defined by $\mu(\underline{\underline{\mathrm{a}}}_1) = N\underline{\underline{\mathrm{a}}}_2 - 1$, $\mu(\underline{\underline{\mathrm{a}}}_2) = 1 - N\underline{\underline{\mathrm{a}}}_1$ and $\mu(\underline{\underline{\mathrm{a}}}) = 0$ otherwise. A simple calculation shows that

$$h_\mu^{(i_1,i_2)}(T_1, T_2) \equiv (\zeta^c u^d - \zeta^a u^b) + \zeta^{i_1 a}(1-\zeta^c u^d)(1+T_1)^b$$
$$+ \zeta^{i_2 c}(\zeta^a u^b - 1)(1+T_2)^d \bmod (p, T_1, T_2)^m .$$

Now, if $a = c = 1$ and $b = d = 0$, we see that

$$h_\mu^{(i_1,i_2)}(T_1, T_2) \equiv (\zeta^{i_1} - \zeta^{i_2})(1-\zeta) \bmod (p, T_1, T_2)^m ,$$

and $(\zeta^{i_1} - \zeta^{i_2})(1-\zeta)$ is a generator of Λ unless $i_1 \equiv i_2 \bmod p-1$. On the other hand, if $a = 1$, $c = \frac{p-1}{2}$ and $b = d = 0$, then

$$h_\mu^{(i_1,i_1)}(T_1, T_2) \equiv 2(\zeta^{i_1} - 1) + (1-(-1)^{i_1})(1-\zeta) \bmod (p, T_1, T_2)^m ,$$

and so we conclude that $H^{(i_1,i_2)} = \Lambda$ unless $i_1 \equiv i_2 \equiv 0$ or $1 \bmod p-1$.

These last two cases can be dealt with as follows. Observe that when $a = d = 0$ and $b = c = 1$,

$$h_\mu^{(0,0)}(T_1, T_2) \equiv (1-\zeta)T_1 \bmod (p, T_1, T_2)^m$$

and

$$h_\mu^{(1,1)}(T_1, T_2) \equiv (1-\zeta)(T_1+1-u) \bmod (p, T_1, T_2)^m .$$

Moreover, when $a = d = 1$ and $b = c = 0$,

$$h_\mu^{(0,0)}(T_1, T_2) \equiv (\zeta-1)T_2 \bmod (p, T_1, T_2)^m$$

and

$$h_\mu^{(1,1)}(T_1, T_2) \equiv (\zeta-1)(T_2+1-u) \bmod (p, T_1, T_2)^m .$$

It follows that $H^{(0,0)}$ is the module generated by T_1 and T_2 and that $H^{(1,1)}$ is the module generated by $T_1 + 1 - u$ and $T_2 + 1 - u$ as claimed.

THEOREM 29. *Let i_1 and i_2 be integers modulo $p - 1$. Then there is a power series $G^{(i_1,i_2)}(T_1, T_2) \in \hat{I}_\infty[[T_1, T_2]]$ such that, for all integers $k_1 \geq 1$ and $k_2 \leq 0$ satisfying $(k_1, k_2) \equiv (i_1, i_2) \bmod (p-1)$,*

$$G^{(i_1,i_2)}\left(u^{k_1}-1, u^{k_2}-1\right) = (k_1-1)!\,\underline{\underline{\Omega}}_p^{k_2-k_1} L_\infty\left(\overline{\psi}^{k_1-k_2}, k_1\right) . \qquad (46)$$

Moreover

$$W^{(i_1,i_2)}\left(D^{(i_1,i_2)}\right) = \Omega_{\underline{\underline{p}}}\, \phi^{(i_1,i_2)}(T_1, T_2)^{-1} G^{(i_1,i_2)}(T_1, T_2) H^{(i_1,i_2)} .$$

Proof. Equations (2), (30), (41) and (45) together show that if k_1 and k_2 are as in the theorem and $\mu \in S$, then the value of

$G^{(i_1,i_2)}_{\langle e(\mu)\rangle}(T_1, T_2)$ at $(u^{k_1}-1, u^{k_2}-1)$ is

$$12(-1)^{1+k_1-k_2}f^{k_1}h_\mu^{(i_1,i_2)}(u^{k_1}-1, u^{k_2}-1)(k_1-1)!\Omega_{\underline{\underline{p}}}^{1+k_2-k_1}L_\infty\left(\overline{\psi}^{k_1-k_2}, k_1\right) .$$

Observe that $12(-1)^{1+i_1-i_2}\omega^{i_1}(f)(1+T_1)^{l(f)}$ is a unit power series in Λ whose value at $(u^{k_1}-1, u^{k_2}-1)$ is $12(-1)^{1+k_1-k_2}f^{k_1}$ whenever $(k_1, k_2) \equiv (i_1, i_2)\mathrm{mod}(p-1)$. It follows by the linearity in Theorem 22 that for each element $h \in H^{(i_1,i_2)}$ there is a corresponding element e_h of D such that for k_1 and k_2 as in the theorem

$$G^{(i_1,i_2)}_{e_h}(u^{k_1}-1, u^{k_2}-1)$$

$$= h(u^{k_1}-1, u^{k_2}-1)(k_1-1)!\Omega_{\underline{\underline{p}}}^{1+k_2-k_1}L_\infty\left(\overline{\psi}^{k_1-k_2}, k_1\right) . \quad (47)$$

(And conversely, for each e in D , there is an $h \in H^{(i_1,i_2)}$ such that equation (47) holds.)

The theorem is now clear from the previous lemma and Theorem 27 unless $(i_1, i_2) \equiv (0, 0)$ or $(1, 1)\mathrm{mod}(p-1)$, in which case it still remains to be shown that there is a power series satisfying equation (46).

Suppose $(i_1, i_2) \equiv (0, 0)\mathrm{mod}(p-1)$, and let e_0 be the element of D corresponding to the power series T_2 in $H^{(0,0)}$ as in equation (47). Observe that $G^{(0,0)}_{e_0}(u^{k_1}-1, 0) = 0$ for all $k_1 \geq 1$ such that

$k_1 \equiv 0 \bmod p\text{-}1$, and so $G_{e_0}^{(0,0)}(T_1, T_2) = \Omega_{\underline{\underline{p}}} T_2 G^{(0,0)}(T_1, T_2)$ for some power series $G^{(0,0)}(T_1, T_2) \in \hat{I}_\infty[[T_1, T_2]]$. It is clear from equation (47) that $G^{(0,0)}(T_1, T_2)$ has the desired properties.

This leaves the case where $(i_1, i_2) \equiv (1, 1)\bmod(p\text{-}1)$. Consider the element e_1 of D corresponding to the power series $T_1 + 1 - u$, and observe that $G_{e_1}^{(1,1)}(u\text{-}1, u^{k_2}\text{-}1) = 0$ for all $k_2 \leq 0$ such that $k_2 \equiv 1 \bmod (p\text{-}1)$. It follows that there is a power series $G^{(1,1)}(T_1, T_2) \in \hat{I}_\infty[[T_1, T_2]]$ such that

$$G_{e_1}^{(1,1)}(T_1, T_2) = \Omega_{\underline{\underline{p}}}(T_1 + 1 - u) G^{(1,1)}(T_1, T_2)$$

and it is clear that it has the properties required by the theorem.

CHAPTER 10

THE STRUCTURE OF $Y_\infty^{(i_1,i_2)}$

As in the introduction, we define Y_∞ to be $\varprojlim \mathrm{U}_{n,m}/\bar{C}_{n,m}$, where the projective limit is taken relative to the norm maps.

THEOREM 30. *Let* i_1 *and* i_2 *be integers modulo* $p - 1$. *Let* $G^{(i_1,i_2)}(T_1, T_2)$ *be an element of* Λ *which generates the same ideal in* $\hat{I}_\infty[[T_1, T_2]]$ *as* $G^{(i_1,i_2)}(T_1, T_2)$. *Then* $Y_\infty^{(i_1,i_2)}$ *is isomorphic to* $H^{(i_1,i_2)}/G^{(i_1,i_2)}(T_1, T_2)H^{(i_1,i_2)}$.

Proof. We recall that in Chapter 8 we defined $H^{(i_1,i_2)}$ to be the image of $W^{(i_1,i_2)}$ and that this is Λ unless $(i_1, i_2) \equiv (1, 1) \bmod (p-1, (p-1)/r_0)$, in which case $H^{(i_1,i_2)}$ is generated by $T_1 + 1 - u$ and $(T_2+1)^{p^M} - u^{p^M}$.

The projection map $p_{n,m} : \mathrm{U}_\infty^{(i_1,i_2)} \to \mathrm{U}_{n,m}^{(i_1,i_2)}$ has as its image those elements of $\mathrm{U}_{n,m}^{(i_1,i_2)}$ for which the local norm to $K_{\underline{p}}$ of each component is 1. It is clear that $\bigcap_{n,m\geq 0} \ker p_{n,m} = \{1\}$. As we have already observed

$$p_{n,m}\left(D^{(i_1,i_2)}\right) = \bar{C}_{n,m}^{(i_1,i_2)} . \tag{48}$$

Let $j_{n,m}$ be the composition of $p_{n,m}$ with the canonical surjection of $\mathcal{U}_{n,m}^{(i_1,i_2)}$ onto $\mathcal{U}_{n,m}^{(i_1,i_2)}/\overline{C}_{n,m}^{(i_1,i_2)}$. The image of $j_{n,m}$ is precisely the image of $Y_\infty^{(i_1,i_2)}$ under the projection onto $\mathcal{U}_{n,m}^{(i_1,i_2)}/\overline{C}_{n,m}^{(i_1,i_2)}$. In view of equation (47), it is plain that the kernel of $j_{n,m}$ is $D^{(i_1,i_2)}$ ker $p_{n,m}$, and that $j_{n,m}$ is a Λ-homomorphism.

Thus $Y_\infty^{(i_1,i_2)} \cong \varprojlim \mathcal{U}_\infty^{(i_1,i_2)}/D^{(i_1,i_2)}$ ker $p_{n,m}$. But $\bigcap_{n,m\geq 0}$ ker $p_{n,m} = \{1\}$ and so it follows that $Y_\infty^{(i_1,i_2)} \cong \mathcal{U}_\infty^{(i_1,i_2)}/D^{(i_1,i_2)}$.
The theorem is now clear from Theorems 27 and 29.

We see from the above theorem that we have the following exact sequence of Λ-modules:

$$0 \to A \to \frac{H^{(i_1,i_2)}}{G^{(i_1,i_2)}(T_1,T_2)H^{(i_1,i_2)}}$$

$$\to \frac{\Lambda}{G^{(i_1,i_2)}(T_1,T_2)} \to \frac{\Lambda}{H^{(i_1,i_2)}+G^{(i_1,i_2)}(T_1,T_2)\Lambda} \to 0\ , \qquad (49)$$

where

$$A = \frac{H^{(i_1,i_2)} \cap G^{(i_1,i_2)}(T_1,T_2)\Lambda}{G^{(i_1,i_2)}(T_1,T_2)H^{(i_1,i_2)}} .$$

Clearly A injects into $\dfrac{\Lambda}{H^{(i_1,i_2)}}$, and $H^{(i_1,i_2)}$ and

$H^{(i_1,i_2)} + G^{(i_1,i_2)}(T_1, T_2)\Lambda$ are clearly contained in no proper principal ideal of Λ , and so $Y_\infty^{(i_1,i_2)}$ is pseudo-isomorphic to $\Lambda/G^{(i_1,i_2)}(T_1, T_2)\Lambda$. This proves Theorem 1.

APPENDIX 1

CONSTRUCTION OF MEASURES ON Z_p^2

In this appendix, we shall indicate how one may deduce the existence of measures on Z_p^2 with certain properties from the results in Katz [6]. In particular, we shall construct a measure which will enable us to prove the congruence in Theorem 15.

Let N be any positive rational integer which is prime to p, and denote by μ_N the group of Nth roots of unity. Observe that $\underline{\underline{p}}_\infty$ is unramified in the extension $F_\infty(\mu_N)$ over F_∞, and fix a prime $\underline{\underline{P}}_\infty$ of $F_\infty(\mu_N)$ lying above $\underline{\underline{p}}_\infty$. We denote by $\sigma_{\underline{\underline{p}}}$ the Artin symbol $(\underline{\underline{p}}, F_\infty(\mu_N)/K)$, and by W the ring of integers of the completion of $F_\infty(\mu_N)$ at $\underline{\underline{P}}_\infty$. As usual, we regard $F_\infty(\mu_N)$ as lying in the complex field $\mathbf{C}$, and we equip it with an embedding into its completion at $\underline{\underline{P}}_\infty$.

In §6 of his paper, Katz produces measures which, when evaluated at a suitable test object, give rise to W-valued measures on Z_p^2. Moreover, as we shall see, Katz has shown how certain integrals over these measures may be evaluated and related to transcendental expressions for numbers which lie in $F_\infty(\mu_N)$. We shall borrow much of our notation from Katz [6], and the references in all that follows refer to the numbered equations and paragraphs in that paper.

Consider the test object $(\mathcal{O}, \phi, \alpha)$ where ϕ is an isomorphism of

Z_p-modules $\mathfrak{X} : Q_p/Z_p \xrightarrow{\sim} \bigcup_{m\geq 0} \underline{\underline{p}}^{*-(m+1)}/\mathcal{O}$ and α is any level N-structure $\alpha : (Z/NZ)^2 \xrightarrow{\sim} \mathcal{O}/N\mathcal{O}$. If we identify Q_p/Z_p with $K_{\underline{\underline{p}}}/\mathcal{O}_{\underline{\underline{p}}}$ in the usual way, we may associate with $\mathfrak{X}$ a unique element $\rho \in \mathrm{Gal}(F_\infty/K)$ such that

$$\mathfrak{X}\left(\bar{\pi}^{*-(m+1)} \bmod \mathcal{O}_{\underline{\underline{p}}}\right) = \kappa_2(\rho)\pi^{*-(m+1)} \bmod \mathcal{O} \quad \text{for all} \quad m \geq 0 \, .$$

The isomorphism $\varphi : \bigcup_{m\geq 0} \underline{\underline{p}}^{-(m+1)}/\mathcal{O} \xrightarrow{\sim} \mu_{p^\infty}$ which Katz associates with $\mathfrak{X}$ in 8.3.15 is given by

$$\varphi\left(\pi^{-(m+1)}\right) = \left(\Omega_\infty/\pi^{m+1}, \mathfrak{X}\left(p^{-(m+1)}\right)\Omega_\infty\right)_m$$

where $(\ ,\ )_m$ denotes the Weil-pairing of the $\left(p^{m+1}\right)$th division points of L . The corresponding isomorphism of formal groups in 8.3.17, which we shall denote for the moment by $\eta_\rho : \hat{E} \xrightarrow{\sim} G_m$, is the unique isomorphism defined over $\hat{I}_\infty$ satisfying

$$\eta_\rho\left(\varepsilon\left(\Omega_\infty/\pi^{m+1}\right)\right) = \varphi\left(\pi^{-(m+1)}\right) - 1 \, .$$

It will be useful to relate η_ρ to our standard isomorphism η chosen in Chapter 5. Recall that we chose $\varepsilon_n \in \mathcal{O}$ such that $\varepsilon_n\pi^* \equiv 1 \bmod \underline{\underline{p}}^{n+1}$, and observe that $\mathfrak{X}\left(p^{-(m+1)}\right) = \mathfrak{X}\left(\varepsilon_m^{m+1}\bar{\pi}^{*-(m+1)}\right)$. It follows from the definitions of η_ρ and of η that $\eta_\rho\left(\varepsilon\left(\Omega_\infty/\pi^{m+1}\right)\right) = \eta\left(\varepsilon\left(\Omega_\infty/\pi^{m+1}\right)\right)^{\kappa_2(\rho)}$. On the other hand, $\mathrm{Gal}(K_\infty/K)$ acts on μ_{p^∞} *via* $\kappa_1\kappa_2$, and so we easily deduce that $\eta_\rho(T) = \eta^\rho(T)$. Moreover, the power series expansion of

$\eta_\rho(T)$ is clearly $\exp\{\kappa_2(\rho)\Omega_{\underline{\underline{p}}}\lambda(T)\} - 1$, and so we conclude that

$\Omega^\rho_{\underline{\underline{p}}} = \kappa_2(\rho)\Omega_{\underline{\underline{p}}}$.

Observe that $\eta^*_\rho(dT/1+T) = \Omega^\rho_{\underline{\underline{p}}}\lambda'(T)dT$, and that, since $\lambda'(T)dT$ is defined over K and is equal to $\varepsilon^*(dz)$, where dz is the standard differential on $\mathbb{C}/L$, we may take $\left(\Omega^\rho_{\underline{\underline{p}}}\right)^{-1}$ as the unit c in 8.3.16 and Ω_∞ as the period Ω in 8.3.17.

Let g be any function $g : \mathcal{O}/N\mathcal{O} \to \mathcal{O}$ and let ε be any locally constant function $\varepsilon : \mathbb{Z}_p^2 \to \mathcal{O}$. We write f for the function $f : (\mathbb{Z}/N\mathbb{Z})^2 \to W$, depending on both g and α , given by

$$f(u, v) = \sum_{w \bmod N} g\{\alpha(w, v)\}(\det\alpha)^{uw}$$

where $\det\alpha$ is the Nth root of unity associated with α in 2.0. If ε is constant on cosets modulo p^r , we write $(\varepsilon f)_r$ for the function $(\varepsilon f)_r : \{\mathbb{Z}/p^rN\mathbb{Z}\}^2 \to W$ defined by

$$(\varepsilon f)_r\{u \bmod p^rN,\ v \bmod p^rN\} = \varepsilon(u, v)\{f(u \bmod N,\ v \bmod N)\}^{\sigma^{-r}_{\underline{\underline{p}}}} .$$

Consider the p-adic modular form $2\Phi_{k,j,(\varepsilon f)_r} \in V\{W,\ \Gamma(p^rN)^{\text{arith}}\}$ defined in 5.11.2. It is clear from Lemma 8.3.25 that $2\Phi_{k,j,(\varepsilon f)_r}(\mathcal{O}, \phi, \alpha)$ belongs to W . In fact, as we see in 8.6.5-8.6.7,

$$2\Phi_{k,j,(\varepsilon f)_r}(O,\, \mathfrak{F},\, \alpha) = \left(\Omega_{\underline{\underline{p}}}^{\rho}\right)^{-(k+j+1)} 2G_{k+j+1,-j,(\varepsilon f)_r}\left(E_O,\, \Omega_\infty dz,\, \beta_{\mathfrak{F}} \times \beta_\alpha\right) \tag{50}$$

where $2G_{k+j+1,-j,(\varepsilon f)_r}\left(E_O,\, \Omega_\infty dz,\, \beta_{\mathfrak{F}} \times \beta_\alpha\right)$ belongs to $F_\infty(\mu_N)$. The function on O/p^rNO which occurs in the transcendental expression given in 8.6.8 for this element of $F_\infty(\mu_N)$ is easily seen from the diagram 8.8.2 and equation 3.6.1 to be given explicitly by

$$\alpha \longmapsto g(\alpha)\, \frac{1}{p^r} \sum_{t=1}^{p^r} \varepsilon\left(Nt,\, \kappa_2^{-1}(\rho)\bar{\alpha}\right)\varphi\left(-\frac{t\alpha}{p^r}\right). \tag{51}$$

Before applying this to the construction of W-valued measures with certain properties on Z_p^2, we need one more result about p-adic modular forms which will enable us to perform Katz's "changing level trick". Suppose $F \in V\left(W,\, \Gamma(p^rN)^{\text{arith}}\right)$ and let $F^{(r)} \in V\left(W,\, \Gamma(N)^{\text{arith}}\right)$ be the image of F under the "exotic" isomorphism 5.6.4. Then we see from Lemmas 8.3.25 and 8.6.2 that both F and $F^{(r)}$ take values in W and are related by the formula

$$F^{(r)\sigma_{\underline{\underline{p}}}^{r}}(O,\, \mathfrak{F},\, \alpha) = \left(F(O,\, \mathfrak{F},\, \alpha)\right)^{\sigma_{\underline{\underline{p}}}^{r}}. \tag{52}$$

Choose an element $a \in Z_p^\times$ and consider the W-valued measures $\mu_g^{\rho(a)}$ and μ_g^{ρ} on Z_p^2 defined by

$$\int \phi(x,\, y)d\mu_g^{\rho(a)} = \int \phi(x,\, y)f(u,\, v)d\mu_N^{(a,1)}(O,\, \mathfrak{F},\, \alpha)$$

and

$$\int \phi(x, y)d\mu_g^\rho = \int \phi(x, y)f(u, v)d\mu_N(\mathcal{O}, \mathfrak{F}, \alpha)$$

where $\mu_N^{(a,1)}$ and μ_N are the measures constructed in Theorems 6.1.1 and 6.4.7 respectively. Of course, μ_g^ρ is supported on $Z_p^{\times 2}$. It follows from 8.5.0 and equation (52) that, if b is any integer chosen so that $b \equiv 1 \bmod N$ and $b \equiv a \bmod p^r$,

$$\int x^k y^j \varepsilon(x, y)d\mu_g^{\rho(a)} = \left(\left[2\Phi_{k,j,(\varepsilon f)_r} - 2a^{k+j+1}\Phi_{k,j,[b](\varepsilon f)_r}\right](\mathcal{O}, \mathfrak{F}, \alpha)\right)^{\sigma_{\underline{\underline{p}}}^r}$$

and

$$\int x^k y^j \varepsilon(x, y)d\mu_g^\rho = \left(2\Phi^*_{k,j,(\varepsilon f)_r}(\mathcal{O}, \mathfrak{F}, \alpha)\right)^{\sigma_{\underline{\underline{p}}}^r}.$$

Here $[b](\varepsilon f)_r$ denotes the function on $(Z/p^r NZ)^2$ which we obtain if we replace ε by the function $(u, v) \longmapsto \varepsilon(bu, bv)$. Moreover, $\Phi^*_{k,j,(\varepsilon f)_r}$ depends only on the restriction of ε to $Z_p^{\times 2}$, and we see from the proof of Corollary 8.5.4 that if ε is supported on $Z_p^{\times 2}$, $\Phi^*_{k,j,(\varepsilon f)_r} = \Phi_{k,j,(\varepsilon f)_r}$. Thus, we can calculate these integrals explicitly using equations (50) and (51) together with 8.6.8.

We shall now specialize to a particular choice of the function g. Let N be a positive rational integer belonging to $\underline{\underline{f}}$ which is prime to p, and consider the function $g : (\mathcal{O}/N\mathcal{O}) \to \mathcal{O}$ defined by

$$g(\alpha) = \begin{cases} 1 & \text{if } \psi\big((\alpha)\big) = \alpha\ , \\ 0 & \text{otherwise.} \end{cases}$$

We see immediately that

$$2\Phi_{k,j,f}(0, \mathfrak{F}, \alpha) = \left(-\Omega_{\underline{\underline{p}}}^{\rho}\right)^{-(k+j+1)} k!N^{k+1}\left(2\pi/\sqrt{d_K}\right)^{j}\Omega_{\infty}^{-(k+j+1)}L\left(\overline{\psi}^{k+j+1},\ k+1\right)\ . \quad (53)$$

Now, as mentioned in the introduction, if $k \geq j \geq 0$, $\left(2\pi/\sqrt{d_K}\right)^{j}\Omega_{\infty}^{-(k+j+1)}L\left(\overline{\psi}^{k+j+1},\ k+1\right) \in K$, and so it follows that, for such k and j , $\int x^k y^j d\mu_g^{\rho(a)}$ lies in $\hat{I}_{\infty}$. Because of the p-adic continuity of $\mu_g^{\rho(a)}$, this is sufficient to prove that $\mu_g^{\rho(a)}$, and hence μ_g^{ρ} , is an $\hat{I}_{\infty}$-valued measure. The obvious consequence of this is that the numbers $\left(2\pi/\sqrt{d_K}\right)^{j}\Omega_{\infty}^{-(k+j+1)}L\left(\overline{\psi}^{k+j+1},\ k+1\right)$, which lie in $K\left(\mu_N\right)$ for $k,\ j \geq 0$, when viewed as elements of the completion of $F_{\infty}\left(\mu_N\right)$ at $\underline{\underline{P}}_{\infty}$, actually lie in $K_{\underline{\underline{p}}}$.

Let $\mu^{\rho(a)}$ and μ^{ρ} denote the $\hat{I}_{\infty}$-valued measures defined by

$$\int \phi(x,\ y)d\mu^{\rho(a)} = -\frac{1}{N}\int \phi\left(-\frac{x}{N},\ -y\right)d\mu_g^{\rho(a)}$$

and

$$\int \phi(x,\ y)d\mu^{\rho} = -\frac{1}{N}\int \phi\left(-\frac{x}{N},\ -y\right)d\mu_g^{\rho}\ .$$

It is evident from equation (53) that these measures are independent of the choice of N , and that if we omit the superscript ρ when $\mathfrak{F}$ is the isomorphism corresponding to the identity in $\mathrm{Gal}(F_{\infty}/K)$,

$$\int \phi(x,\ y)d\mu^{\rho(a)} = \left(\int \phi(x,\ y)d\mu^{(a)}\right)^{\rho}$$

and

$$\int \phi(x, y)d\mu^{\rho} = \left(\int \phi(x, y)d\mu\right)^{\rho} .$$

THEOREM 31 (Katz). *Let* $\mu^{(a)}$ *and* μ *be the* $\hat{I}_{\infty}$*-valued measures defined above, and let* $h : \mathbb{Z}_p^{\times} \to \mathbb{Z}_p$ *be any function which is constant on cosets modulo* p^r. *Extend* h *to the whole of* $\mathbb{Z}_p$ *by zero. Then, for* $k \geq 1$ *and* $j \geq 0$, *we have the following formulae:*

$$\int x^{k-1}y^j d\mu^{(a)} = \left(1-a^{k+j}\right)\left(\Omega_{\underline{\underline{p}}}\Omega_{\infty}\right)^{-(k+j)}\left(2\pi/\sqrt{d_K}\right)^j(k-1)!L\left(\overline{\psi}^{k+j}, k\right) , \tag{54}$$

$$\int x^{k-1}y^j d\mu = \left(\Omega_{\underline{\underline{p}}}\Omega_{\infty}\right)^{-(k+j)}\left(2\pi/\sqrt{d_K}\right)^j(k-1)!$$
$$\cdot \left(1-\psi^{k+j}(\underline{\underline{p}})/N\underline{\underline{p}}^{j+1}\right)\left(1-\overline{\psi}^{k+j}(\underline{\underline{p}}^*)/N\underline{\underline{p}}^{*k}\right)L\left(\overline{\psi}^{k+j}, k\right) , \tag{55}$$

$$\int x^{k-1}y^j h(-y)d\mu^{(a)} = \left(\Omega_{\underline{\underline{p}}}\Omega_{\infty}\right)^{-(k+j)}\left(2\pi/\sqrt{d_K}\right)^j(k-1)!$$
$$\cdot \sum_{\sigma\in\mathrm{Gal}\left(F_r/K\right)} \left\{h\left(\kappa_2(\sigma)\right)-a^{k+j}h\left(a\kappa_2(\sigma)\right)\right\}\zeta_{F_r}\left(\sigma, \overline{\psi}^{k+j}, k\right) \tag{56}$$

and

$$\int x^{k-1}y^j h(-y)d\mu = \left(\Omega_{\underline{\underline{p}}}\Omega_{\infty}\right)^{-(k+j)}\left(2\pi/\sqrt{d_K}\right)^j(k-1)!$$
$$\cdot \sum_{\sigma\in\mathrm{Gal}\left(F_r/K\right)} \left\{h\left(\kappa_2(\sigma)\right) - \frac{\psi^{k+j}(\underline{\underline{p}})}{N\underline{\underline{p}}^{j+1}} h\left(\kappa_2\left(\sigma\sigma_{\underline{\underline{p}}}^{-1}\right)\right)\right\}\zeta_{F_r}\left(\sigma, \overline{\psi}^{k+j}, k\right) . \tag{57}$$

Proof. The first integral follows from the definition of $\mu^{(a)}$ and equation (53). The remaining integrals can be determined in the same way by calculating the value of $2\Phi_{k-1,j,(\varepsilon f)_r}(0, \phi, \alpha)$ for the appropriate choice of ε.

We remark here that equation (55) plainly shows the existence of the power series $G^{(i_1, i_2)}(T_1, T_2)$. However, from our knowledge of the action of $\mathrm{Gal}(F_\infty/K)$ on $\Omega_{\underline{\underline{p}}}$, it is clear that the generator λ of $\underline{\underline{p}}$ chosen in 8.7.3 is $\psi(\underline{\underline{p}})$, and so, with an appropriate choice of function g, it is clear that the existence of the power series $G^{(i_1, i_2)}(T_1, T_2)$ is already implied by equation 8.7.6.

Finally, we turn to the proof of Theorem 15. Let $k \geq 1$ and $j \leq 0$ and let $\mu \in S$. Choose a unit $a \in \mathbb{Z}_p^\times$ such that $a^{k-j} \neq 1$. To prove Theorem 15, it will clearly suffice to show that

$$\left(1-a^{k-j}\right) \sum_{\underline{\underline{a}} \in I} \mu(\underline{\underline{a}})\left(N\underline{\underline{a}}-\psi^k(\underline{\underline{a}})\overline{\psi}^j(\underline{\underline{a}})\right)\left(\Omega_{\underline{\underline{p}}}\Omega_\infty\right)^{j-k}\left(2\pi/\sqrt{d_K}\right)^j$$

$$\cdot\ (k-1)!\left(1-\overline{\psi}^{k-j}(\underline{\underline{p}}^*)/N\underline{\underline{p}}^{*k}\right)L\left(\overline{\psi}^{k-j}, k\right)$$

$$= \left(1-a^{k-j}\right)(-1)^j\Omega_{\underline{\underline{p}}}^{-k}\delta_j\left[(k-1)! \sum_{\underline{\underline{a}} \in I} \mu(\underline{\underline{a}})\left(N\underline{\underline{a}}\zeta(k)-\psi^k(\underline{\underline{a}})\zeta(k)^{(\underline{\underline{a}}, F_\infty/K)}\right)\right]. \quad (58)$$

Let $h_j : \mathbb{Z}_p^\times \to \mathbb{Z}_p$ be a function which is constant on cosets modulo p^m and which satisfies

$$h_j(-y) \equiv y^j \bmod p^m \quad \text{for all} \quad y \in \mathbb{Z}_p^\times .$$

Now, we see from Theorem 31 that the left hand side of equation (58) is equal to

$$\int_{\mathbb{Z}_p \times \mathbb{Z}_p^\times} \sum_{\underline{\underline{a}} \in I} \mu(\underline{\underline{a}})\left(N\underline{\underline{a}}-\psi^k(\underline{\underline{a}})\overline{\psi}^j(\underline{\underline{a}})\right)x^{k-1}y^j d\mu^{(a)} .$$

On the other hand, this is clearly congruent to

$$\int_{Z_p \times Z_p^\times} x^{k-1} \sum_{\underline{\underline{a}} \in I} \mu(\underline{\underline{a}}) \left\{ N\underline{\underline{a}} h_j(-y) - \psi^k(\underline{\underline{a}}) h_j\left(-\bar{\psi}^{-1}(\underline{\underline{a}})y\right) \right\} d\mu^{(a)} \bmod \underline{\underline{p}}_\infty^m ,$$

and Theorem 31 shows that this integral is equal to

$$\Omega_{\underline{\underline{p}}}^{-k}(k-1)! \sum_{\sigma \in \mathrm{Gal}(F_m/K)} \left\{ h_j\left(\kappa_2(\sigma)\right) - a^k h_j\left(a\kappa_2(\sigma)\right) \right\}$$

$$\cdot \left\{ \sum_{\underline{\underline{a}} \in I} \mu(\underline{\underline{a}}) \left\{ N\underline{\underline{a}} \zeta_m(k) - \psi^k(\underline{\underline{a}}) \zeta_m(k)^{(\underline{\underline{a}}, F_\infty/K)} \right\}^\sigma \right\} .$$

But, $(k-1)! \sum_{\underline{\underline{a}} \in I} \mu(\underline{\underline{a}}) \left\{ N\underline{\underline{a}} \zeta_m(k) - \psi^k(\underline{\underline{a}}) \zeta_m(k)^{(\underline{\underline{a}}, F_\infty/K)} \right\}$ belongs to I_m , as was shown in Corollary 14, and

$$h_j\left(\kappa_2(\sigma)\right) - a^k h_j\left(a\kappa_2(\sigma)\right) \equiv (-1)^j \left(1 - a^{k-j}\right) \kappa_2(\sigma)^j \bmod p^m .$$

It follows that the last mentioned integral is congruent to the right hand side of equation (58) modulo $\underline{\underline{p}}_\infty^m$. Thus equation (58) holds modulo $\underline{\underline{p}}_\infty^m$ for an arbitrary choice of m , and so we must have equality. This establishes the assertion of Theorem 15.

APPENDIX 2

A KUMMER CRITERION

As an application of the ideas developed in this thesis, we shall relate the following simple arithmetic property of the curve E to $\mathfrak{p}$-adic properties of special values of primitive Hecke L-functions.

Let F be any Galois extension of K contained in $K_{0,0}$. We say that $\mathfrak{p}$ is irregular for F if there is a cyclic extension of F of degree p which is unramified outside the primes of F lying above $\mathfrak{p}$, and which is distinct from the composition of F and the first layer of the unique $\mathbb{Z}_p$-extension K of K unramified outside $\mathfrak{p}$.

The best result in this direction is due to Coates and Wiles [1] who give a criterion for determining whether $\mathfrak{p}$ is irregular for the ray class field of K modulo $\mathfrak{p}$ in terms of the $\mathfrak{p}$-adic properties of Hurwitz numbers. We shall extend their result to provide criteria for determining whether $\mathfrak{p}$ is irregular for any Galois extension of K contained in $K_{0,0}$.

We write $\mathrm{L}(\bar{\psi}^k, s)$ for the primitive Hecke L-function attached to $\bar{\psi}^k$ for each integer $k \geq 1$. Since $\mathrm{L}(\bar{\psi}^k, s)$ differs from $L(\bar{\psi}^k, s)$ only by a finite number of Euler factors, it follows from our earlier results that the numbers

$$\left(2\pi/\sqrt{d_K}\right)^j \Omega_\infty^{-(k+j)} \mathrm{L}\left(\bar{\psi}^{k+j}, k\right), \quad k \geq 1, \quad j \geq 0, \tag{59}$$

belong to $K_{\mathfrak{p}}$.

In order to state which of the numbers (59) determine whether $\underline{\underline{p}}$ is irregular for a given field F, we introduce the following notion. Let F be any Galois extension of K contained in $K_{0,0}$. We shall say that a character χ of $\mathrm{Gal}(K_{0,0}/K)$ belongs to F if $\mathrm{Gal}(K_{0,0}/F)$ is contained in the kernel of χ. Then, our result is as follows.

THEOREM 32. *Let F be any Galois extension of K contained in $K_{0,0}$. Then the prime $\underline{\underline{p}}$ is irregular for F if and only if there exist integers k and j with $0 \le j < p-1$, $1 < k \le p$ such that $\chi_1^k \chi_2^{-j}$ is a non-trivial character belonging to F and the number $(2\pi/\sqrt{d_K})^j \Omega_\infty^{-(k+j)} L(\bar{\psi}^{k+j}, k)$ is not a unit in $\mathcal{O}_{\underline{\underline{p}}}$.*

As a numerical example, consider the field $K = \mathbb{Q}(i)$ and the elliptic curve $E : y^2 = 4x^3 - 4x$. If p is a prime congruent to 1 modulo 4, and $\underline{\underline{p}}$ is a prime lying above p, then the characters belonging to $R_{\underline{\underline{p}}}$, the ray class field of K modulo $\underline{\underline{p}}$, are the characters $\chi_1^k \chi_2^{-j}$ for which $j \equiv 0 \bmod (p-1)$ and $k \equiv 0 \bmod 4$, while the characters belonging to R_p, the ray class field of K modulo p, are the characters $\chi_1^k \chi_2^{-j}$ for which $k + j \equiv 0 \bmod 4$. Using the table in Hurwitz [5], together with the formulae in Weil [13] p. 45, it is easy to calculate the following table of values for $(2\pi/\sqrt{d_K})^j (k-1)!\Omega_\infty^{-(k+j)} L(\bar{\psi}^{k+j}, k)$.

It follows from Theorem 32 that $\underline{\underline{p}}$ is regular for both $R_{\underline{\underline{p}}}$ and R_p when $p = 5$, but that while $\underline{\underline{p}}$ is regular for $R_{\underline{\underline{p}}}$, it is irregular for R_p when $p = 29$, since 29 divides $\pi\Omega_\infty^{-20} L(\bar{\psi}^{20}, 19)$.

Values of $\pi^{j}(k-1)!\Omega_{\infty}^{-(k+j)}L(\bar{\psi}^{k+j}, k)$ for the curve $y^2 = 4x^3 - 4x$

	j			
$k+j$	0	1	2	3
4	$2^{-1}.5^{-1}$	$2^{-2}.3^{-1}$	$2^{-2}.3^{-1}$	$2^{-1}.5^{-1}$
8	$2^{2}.3.5^{-1}$	$2^{3}.7^{-1}$	2.3^{-1}	2^{-1}
12	$2^{7}.3^{3}.5^{-1}.7.13^{-1}$	$2^{7}.3^{2}.11^{-1}$	2^{5}	$2^{5}.3^{-1}$
16	$2^{9}.3^{4}.5^{-1}.7^{2}.11.17^{-1}$	$2^{11}.3^{3}$	$2^{9}.3^{2}.7^{-1}.19$	$2^{10}.3$
20	$2^{15}.3^{6}.5^{-2}.7^{2}.11$	$2^{15}.3^{5}.7.19^{-1}.29$	$2^{13}.3^{3}.67$	$2^{13}.3^{2}.37$
24	$2^{18}.3^{6}.5^{-1}.7^{3}.11^{2}.13^{-1}.19$	$2^{19}.3^{6}.7^{2}.23^{-1}.389$	$2^{17}.3^{5}.11^{-1}.15629$	

Similarly, $\underline{\underline{p}}$ is irregular for R_p when $p = 37$, 389 or 15629, since these primes divide $\pi^3\Omega_{\infty}^{-20}L(\bar{\psi}^{20}, 17)$, $\pi\Omega_{\infty}^{-24}L(\bar{\psi}^{24}, 23)$ and $\pi^2\Omega_{\infty}^{-24}L(\bar{\psi}^{24}, 22)$ respectively.

Proof of Theorem 32. Let M denote the maximal abelian p-extension of F unramified outside the primes of F dividing $\underline{\underline{p}}$, and let F denote the composition of F and K. It can be shown that for F as in our theorem, $\mathrm{Gal}(M/\mathsf{F})$ is finite, and it is easy to deduce from this that $\underline{\underline{p}}$ is irregular for F if and only if $\mathrm{Gal}(M/\mathsf{F})$ is non-trivial. Thus, the idea of our proof is to relate the formula given in Theorem 11 of Coates and Wiles [1] for the order of $\mathrm{Gal}(M/\mathsf{F})$ to the numbers (59).

It will be convenient to do this in two parts. The first part is to prove the $\underline{\underline{p}}$-adic analogue of the well known formula which gives the product of the regulator and the class number of an abelian extension of K in terms of logarithms of Robert's elliptic units. The $\underline{\underline{p}}$-adic logarithms of these elliptic units arise in the work of Lichtenbaum [8] as special values of certain Iwasawa functions which he constructs and which, as we shall show, are related to the functions which Katz produced interpolating the numbers (59). The congruences which arise from this observation will yield Theorem 32.

For the moment, let us suppose only that F is a finite abelian extension of K of degree d and conductor $\underline{\underline{g}}$. For each character χ of $\mathrm{Gal}(F/K)$, we let F_χ denote the fixed field of the kernel of χ and we write $\underline{\underline{g}}_\chi$ for the conductor of F_χ . If we denote by $R_{\underline{\underline{g}}_\chi}$ the ray class field of K modulo $\underline{\underline{g}}_\chi$, it is clear that we may regard χ as a character of $\mathrm{Gal}(R_{\underline{\underline{g}}_\chi}/K)$, and hence, *via* the reciprocity map, as a primitive character of the ray class modulo $\underline{\underline{g}}_\chi$ which we shall denote by $\mathrm{Cl}(\underline{\underline{g}}_\chi)$. Let n_χ be the smallest positive rational integer in $\underline{\underline{g}}_\chi$ and let $w_{\underline{\underline{g}}_\chi}$ be the number of roots of unity in K which are congruent to 1 modulo $\underline{\underline{g}}_\chi$. Let w and w_F be the number of roots of unity in K and F respectively, and let h denote the class number of F . Then, if $\varphi_{\underline{\underline{g}}_\chi}(C)$, $C \in \mathrm{Cl}(\underline{\underline{g}}_\chi)$ is the invariant defined by Robert [10] p. 14, we have the following lemma.

LEMMA 33. *With a suitable choice of the sign of the regulator* R *of* F *,*

$$\prod_{\chi\neq 1}\left\{\sum_{C\in \mathrm{Cl}(\underline{\underline{g}}_\chi)}\chi^{-1}(C)\log\left|\varphi_{\underline{\underline{g}}_\chi}(C)\right|\right\}/n_\chi w_{\underline{\underline{g}}_\chi} = 6^{d-1}whR/w_F\ , \tag{60}$$

where the product on the left is taken over all non-trivial characters of $\mathrm{Gal}(F/K)$.

Proof. This is Theorem 3 (ii) of Robert [10], if we note that the numbers Robert denotes by $\rho(\chi')$ satisfy $\left(\prod_{\chi\neq 1} \rho(\chi')\right)^2 = 1$.

From now on, we fix our choice of the regulator R of F so that equation (60) holds, and we shall now prove a $\underline{\underline{p}}$-adic analogue of this formula. We denote by $\mathbb{C}_{\underline{\underline{p}}}$ an algebraic closure of $K_{\underline{\underline{p}}}$, and let $\log_{\underline{\underline{p}}}$ be an extension of the $\underline{\underline{p}}$-adic logarithm to the whole of $\mathbb{C}_{\underline{\underline{p}}}$. Let Δ be the group of values taken by the characters of $\mathrm{Gal}(F/K)$. By fixing an embedding of $\overline{K}$, the algebraic closure of K , in $\mathbb{C}_{\underline{\underline{p}}}$, we may regard the elements of Δ both as elements of $\mathbb{C}$ and of $\mathbb{C}_{\underline{\underline{p}}}$. Naturally, our results will be independent of this choice.

Recall that $R_{\underline{\underline{g}}}$ is the ray class field of K modulo $\underline{\underline{g}}$, and we extend $\log|\ |$ and $\log_{\underline{\underline{p}}}$ to $R_{\underline{\underline{g}}}^{\times} \otimes \mathbb{Z}[\Delta]$ by defining

$$\log|\alpha \otimes a| = a \log|\alpha| \tag{61}$$

and

$$\log_{\underline{\underline{p}}} \alpha \otimes a = a \log_{\underline{\underline{p}}} \alpha \quad \text{for} \quad \alpha \in R_{\underline{\underline{g}}}^{\times} \quad \text{and} \quad a \in \mathbb{Z}[\Delta] . \tag{62}$$

Let φ_χ denote the expression $\prod_{C\in \mathrm{Cl}(\underline{\underline{g}}_\chi)} \left(\varphi_{\underline{\underline{g}}_\chi}(C) \otimes \chi^{-1}(C)\right)$, and observe that if $\sigma \in \mathrm{Gal}(F/K)$, then

$$\varphi_\chi^\sigma = \varphi_\chi \otimes \chi(\sigma) .$$

It follows that

$$\det\left(\log\left|\varphi_\chi^\sigma\right|\right)_{\chi\neq 1,\sigma\neq 1} = \det\left(\chi(\sigma)\right)_{\chi\neq 1,\sigma\neq 1}\cdot\prod_{\chi\neq 1}\left(\sum_{C\in \mathrm{Cl}(\underline{\underline{g}}_\chi)}\chi^{-1}(C)\log\left|\varphi_{\underline{\underline{g}}_\chi}(C)\right|\right) \tag{63}$$

and that

$$\det\left(\log_{\underline{\underline{p}}}\varphi_\chi^\sigma\right)_{\chi\neq 1,\sigma\neq 1} = \det\left(\chi(\sigma)\right)_{\chi\neq 1,\sigma\neq 1}\cdot\prod_{\chi\neq 1}\left(\sum_{C\in \mathrm{Cl}(\underline{\underline{g}}_\chi)}\chi^{-1}(C)\log_{\underline{\underline{p}}}\varphi_{\underline{\underline{g}}_\chi}(C)\right). \tag{64}$$

Choose units $e_1, \ldots, e_{d-1}$ in F which generate a subgroup of index w_F in the group of units of F so that

$$R = 2^{d-1}\det\left(\log\left|e_j^\sigma\right|\right)_{\sigma\neq 1, 1\leq j<d}.$$

We define the $\underline{\underline{p}}$-adic regulator of F, $R_{\underline{\underline{p}}}$ by

$$R_{\underline{\underline{p}}} = \det\left(\log_{\underline{\underline{p}}} e_j^\sigma\right)_{\sigma\neq 1, 1\leq j<d}.$$

(This definition fixes the sign of $R_{\underline{\underline{p}}}$, but otherwise agrees with that used by Coates and Wiles [1].)

Now, if C_0 is a fixed element of $\mathrm{Cl}(\underline{\underline{g}}_\chi)$, $\varphi_{\underline{\underline{g}}_\chi}(C)/\varphi_{\underline{\underline{g}}_\chi}(C_0)$ is a unit in $R_{\underline{\underline{g}}}$ for all $C\in \mathrm{Cl}(\underline{\underline{g}}_\chi)$, and it is clear that

$$\varphi_\chi = \prod_{C\in \mathrm{Cl}(\underline{\underline{g}}_\chi)}\left(\varphi_{\underline{\underline{g}}_\chi}(C)/\varphi_{\underline{\underline{g}}_\chi}(C_0)\right)\otimes\chi^{-1}(C).$$

Moreover, since φ_χ is fixed by $\mathrm{Gal}(R_{\underline{\underline{g}}}/F)$, it follows that if W denotes the group of roots of unity in F, there are elements $a_{\chi,j}\in Z[\Delta]$ and

$\mu_\chi \in W \otimes \mathbb{Z}[\Delta]$ such that

$$\varphi_\chi = \mu_\chi \prod_{j=1}^{d-1} e_j \otimes a_{\chi,j} .$$

Thus, if $\sigma \in \mathrm{Gal}(F/K)$,

$$\varphi_\chi^\sigma = \mu_\chi^\sigma \prod_{j=1}^{d-1} e_j^\sigma \otimes a_{\chi,j} ,$$

and so we conclude that

$$\det\left(\log\left|\varphi_\chi^\sigma\right|\right)_{\chi\neq 1,\sigma\neq 1} = \det\left(a_{\chi,j}\right)_{\chi\neq 1, 1\leq j<d} \cdot R/2^{d-1} \tag{65}$$

and

$$\det\left(\log_{\underline{\underline{p}}} \varphi_\chi^\sigma\right)_{\chi\neq 1,\sigma\neq 1} = \det\left(a_{\chi,j}\right)_{\chi\neq 1,1\leq j<d} \cdot R_{\underline{\underline{p}}} . \tag{66}$$

But, it is easy to see that $\det(\chi(\sigma))_{\chi\neq 1,\sigma\neq 1}$ is non-zero (see, for instance, Lemma 10.9 of Lichtenbaum [8]), and so, since $R \neq 0$, we conclude from Lemma 33 and equations (63)-(66) that we have the following $\underline{\underline{p}}$-adic analogue of Lemma 33.

THEOREM 34. *With our given choice of the sign of* $R_{\underline{\underline{p}}}$,

$$\prod_{\chi\neq 1}\left\{\sum_{C\in \mathrm{Cl}(\underline{\underline{g}}_\chi)} \chi^{-1}(C) \log_{\underline{\underline{p}}} \varphi_{\underline{\underline{g}}_\chi}(C)\right\}/n_\chi w_{\underline{\underline{g}}_\chi} = 12^{d-1} whR_{\underline{\underline{p}}}/w_F , \tag{67}$$

where the product on the left is taken over all non-trivial characters of $\mathrm{Gal}(F/K)$.

Recall that if χ is any character of $\mathrm{Gal}(F/K)$, we may regard χ as a character of the ray class modulo $\underline{\underline{g}}_\chi$, and hence as a primitive Dirichlet character of conductor $\underline{\underline{g}}_\chi$. Suppose $\underline{\underline{g}}_\chi = \underline{\underline{p}}^{m_\chi}\underline{\underline{c}}_\chi$, where $\underline{\underline{c}}_\chi$ is prime to $\underline{\underline{p}}$. Then we may express χ uniquely as the product of two primitive Dirichlet characters χ_0 and $\chi_{\underline{\underline{p}}}$ of conductor $\underline{\underline{c}}_\chi$ and $\underline{\underline{p}}^{m_\chi}$ respectively. Choose a generator γ_χ of $\underline{\underline{c}}_\chi$, and let P_χ be the point of exact order $\underline{\underline{g}}_\chi$ on the curve E given by $P_\chi = P_{\chi_0} + P_{\chi_{\underline{\underline{p}}}}$ where $P_{\chi_0} = \xi(\Omega_\infty/\gamma_\chi)$ and $P_{\chi_{\underline{\underline{p}}}} = \xi(\Omega_\infty/\pi^{m_\chi})$. The point $P_{\chi_{\underline{\underline{p}}}}$ may be regarded as a point of order p^{m_χ} on the formal group $\hat{E}$, and so, if η denotes our chosen isomorphism of formal groups $\eta : \hat{E} \xrightarrow{\sim} G_m$ as usual, $\zeta_\chi = \eta(P_{\chi_{\underline{\underline{p}}}}) + 1$ is a p^{m_χ}-th root of unity. We write C_χ for the Gauss sum

$$C_\chi = p^{-m_\chi} \sum_{a=1}^{p^{m_\chi}} \chi_{\underline{\underline{p}}}(a)\zeta_\chi^a \ .$$

Let $\mathcal{E}$ denote the triple $(E,\ 2dx/y,\ \eta^{-1})$ as in §6 of Lichtenbaum [8] and let $L(\mathcal{E},\ \chi,\ P_\chi)$ be the function he defines in §8.1. Then we have the following theorem.

THEOREM 35. *Let* $d_{F/K}$ *be the relative discriminant of* F *over* K *. Then* $\prod_{\chi\neq 1} L(\mathcal{E},\ \chi,\ P_\chi)(1)$ *, with the product taken over all non-trivial characters of* Gal(F/K) *, has the same* $\underline{\underline{p}}$*-adic valuation as*

$$\frac{phR_{\underline{\underline{p}}}}{w_F\sqrt{d_{F/K}}} \cdot \prod_{\underline{\underline{q}}|\underline{\underline{p}}} \left(1-(N\underline{\underline{q}})^{-1}\right) ,$$

where the product is taken over the prime ideals of F *lying above* $\underline{\underline{p}}$ *and* $N\underline{\underline{q}}$ *denotes the norm to* K *of* $\underline{\underline{q}}$ *.*

Proof. It is easy to see from Corollary 9.4 of Lichtenbaum that, if χ is non-trivial

$$L(E, \chi, P_\chi)(1) = \frac{\bar{C}_\chi}{6n_\chi \Omega_{\underline{\underline{p}}}} \left(1-\chi(\pi)/p\right)\chi\left(\gamma_\chi + \pi^{m_\chi}\right)$$

$$\cdot\, w \sum_{C \in Cl(\underline{\underline{g}}_\chi)} \chi^{-1}(C) \log_{\underline{\underline{p}}} \varphi_{\underline{\underline{g}}_\chi}(C) \,. \tag{68}$$

Since $\underline{\underline{p}}$ is prime to 2 and 3, and $\gamma_\chi + \pi^{m_\chi}$ is prime to $\underline{\underline{g}}_\chi$, it is clear from equations (67) and (68) that it will suffice to prove that $\prod_{\chi\neq 1} C_\chi\left(1-\chi(\pi)/p\right)$ has the same $\underline{\underline{p}}$-adic valuation as $pd_{F/K}^{-\frac{1}{2}} \cdot \prod_{\underline{\underline{q}}|\underline{\underline{p}}} \left(1-(N\underline{\underline{q}})^{-1}\right)$.

Now, it is well known that $\pi^{m_\chi} C_\chi C_{\chi^{-1}}$ is a unit in $C_{\underline{\underline{p}}}$, and so the conductor-discriminant theorem shows that $\prod_{\chi\neq 1} C_\chi$ has the same $\underline{\underline{p}}$-adic valuation as $d_{F/K}^{-\frac{1}{2}}$. Moreover, if H denotes the maximal abelian extension of K contained in F in which $\underline{\underline{p}}$ is unramified, it is easy to see that only those characters χ which belong to H contribute to $\prod_{\chi\neq 1} \left(1-\chi(\pi)/p\right)$. We conclude that $\prod_{\chi\neq 1} \left(1-\chi(\pi)/p\right)$ has the same $\underline{\underline{p}}$-adic valuation as $p^{1-[H:K]}$, which is also the same as the $\underline{\underline{p}}$-adic valuation of $p \cdot \prod_{\underline{\underline{q}}|\underline{\underline{p}}} \left(1-(N\underline{\underline{q}})^{-1}\right)$.

From now on we suppose, as in Theorem 32, that F is a Galois extension of K contained in $K_{0,0}$. The importance of the previous theorem can be seen from the following corollary.

COROLLARY 36. *Let* F *be a Galois extension of* K *contained in* $K_{0,0}$. *Then* $\mathfrak{p}$ *is regular for* F *if and only if the number*

$\prod_{\chi \neq 1} L(\mathrm{E}, \chi, P_\chi)(1)$ *, where the product is taken over all non-trivial characters of* $\mathrm{Gal}(F/K)$ *, is a unit in* $\mathrm{C}_{\mathfrak{p}}$.

Proof. Recall that M denotes the maximal abelian p-extension of F unramified outside the primes of F lying above $\mathfrak{p}$, and that F denotes the composition of F and K. Since the $\mathfrak{p}$-adic regulator $R_{\mathfrak{p}}$ is non-zero, it follows from Theorem 11 of Coates and Wiles [1] that $\mathrm{Gal}(M/\mathrm{F})$ is finite, and that it is trivial if and only if $\prod_{\chi \neq 1} L(\mathrm{E}, \chi, P_\chi)(1)$ is a unit in $\mathrm{C}_{\mathfrak{p}}$. But since $\mathrm{Gal}(\mathrm{F}/F)$ has no torsion, we conclude that $\mathfrak{p}$ is regular for F if and only if $\mathrm{Gal}(M/\mathrm{F})$ is trivial, and the assertion of the corollary is now plain.

To conclude the proof of Theorem 32, we need to relate the numbers (59) to the values of $L(\mathrm{E}, \chi, P_\chi)$. Let ρ be the Dirichlet character of conductor $\mathfrak{f}$ given by

$$\rho(\alpha) = \psi\big((\alpha)\big)/\alpha\ , \quad (\alpha, \mathfrak{f}) = 1\ , \tag{69}$$

and observe that the character $\chi_1^k \chi_2^{-j}$, when viewed as primitive Dirichlet character, is given by

$$\chi_1^k \chi_2^{-j}(\alpha) = \omega^k(\alpha)\omega^{-j}(\bar{\alpha})\rho^{k+j}(\alpha)\ , \tag{70}$$

where ω is the usual Teich-Muller character on $Z_p^\times$ (and hence a Dirichlet character of conductor $\underline{\underline{p}}$ under our identification of $\mathcal{O}_{\underline{\underline{p}}}$ with Z_p). By the characters on the right hand side of equation (70) we mean, of course, the associated primitive characters.

THEOREM 37. *For each integer* i *modulo* w , *there is an* $\hat{I}_\infty$*-valued measure* μ_i *supported on* $Z_p^{\times 2}$ *such that*

$$\int_{Z_p^2} x^{k-1}y^j d\mu_i = (-1)^{k+j}(k-1)!\left(2\pi/\sqrt{d_K}\right)^j\left(\Omega_{\underline{\underline{p}}}\Omega_\infty\right)^{-(k+j)}\left(1-\psi^{k+j}(\underline{\underline{p}})/N\underline{\underline{p}}^{j+1}\right)$$

$$\cdot\left(1-\overline{\psi}^{k+j}(\underline{\underline{p}}^*)/N\underline{\underline{p}}^{*k}\right)\omega L\left(\overline{\psi}^{k+j}, k\right)$$

$$\textit{for all } k \geq 1 \text{ , } j \geq 0 \textit{ satisfying } k+j \equiv i \bmod w \quad (71)$$

and

$$\int_{Z_p^2} x^{k-1}\omega^j(y)d\mu_i = (-1)^k(k-1)!\left(\Omega_{\underline{\underline{p}}}\Omega_\infty\right)^{-k}\left(1-\omega^{-j}\left(\overline{\psi}(\underline{\underline{p}})\right)\psi^k(\underline{\underline{p}})/p\right)\sum_{\substack{\alpha\in\mathcal{O}\\ \alpha\neq 0}}\frac{\rho^{-i}(\alpha)\omega^j(\bar{\alpha})}{\alpha^k}$$

$$\textit{for all } k \geq 3 \textit{ and } j \not\equiv 0 \bmod p-1 \text{ .} \quad (72)$$

Furthermore, if $a \in Z_p^\times$, *there is another* $\hat{I}_\infty$*-valued measure* $\mu_i^{(a)}$ *on* $Z_p^\times$ *such that*

$$\int_{Z_p} x^{k-1}d\mu_i^{(a)} = \left(1-a^k\right)(-1)^k(k-1)!\left(\Omega_{\underline{\underline{p}}}\Omega_\infty\right)^{-k}\left(1-\psi^k(\underline{\underline{p}})/p\right)\omega L\left(\overline{\psi}^k, k\right)$$

$$\textit{for all } k \geq 1 \textit{ such that } k \equiv i \bmod w \text{ .} \quad (73)$$

Proof. Let N be a positive rational integer belonging to the conductor of ρ^{-i} which is prime to p . We regard ρ^{-i} as a function

$\rho^{-i} : \mathcal{O}/N\mathcal{O} \to \mathcal{O}$ and let $\mu_{\rho^{-i}}$ be the corresponding measure defined in Appendix 1. It is easy to check that the measure μ_i defined by

$$\int \phi(x, y)d\mu_i = \frac{1}{N}\int \phi\left(\frac{x}{N}, y\right)d\mu_{\rho^{-i}}$$

has all the required properties. Similarly, if we define $\mu_i^{(a)}$ by

$$\int \phi(x)d\mu_i^{(a)} = \frac{1}{N}\int_{Z_p^\times \times Z_p} \phi\left(\frac{x}{N}\right)d\mu_{\rho^{-i}}^{(a)}$$

it is a simple matter to verify that it satisfies equation (73).

We are now in a position to prove the following theorem, from which we will be able to deduce Theorem 32.

THEOREM 38. *Let* χ *be a non-trivial character of* Gal(F/K) *, and let* i_1 *and* i_2 *be integers modulo* $(p-1)$ *such that* $\chi = \chi_1^{i_1}\chi_2^{i_2}$ *. Then* $\chi_0 = \chi\omega^{-i_1}$ *and* $\chi_{\underline{p}} = \omega^{i_1}$ *. Choose a generator* γ_χ *of the conductor* $\underline{\underline{c}}_\chi$ *of* χ_0 *as before, and let* P_χ *be the corresponding primitive* $\underline{\underline{g}}_\chi$*-division point of* E *. Then* $L(E, \chi, P_\chi)$ *is an Iwasawa function, and if* a *is a primitive* $(p-1)$th *root of unity and* $u \equiv 1-i_1$ mod $p-1$ *,*

$$L(E, \chi, P_\chi)(u) = \begin{cases} -\gamma_\chi\Omega_{\underline{p}}\displaystyle\int (\gamma_\chi x)^{-u}\omega^{-i_2}(y)d\mu_{i_1-i_2}\ , & i_2 \not\equiv 0 \bmod (p-1)\ , \\ \dfrac{-\gamma_\chi\Omega_{\underline{p}}}{1-a^{i_1}}\displaystyle\int (\gamma_\chi x)^{-u}d\mu_{i_1}^{(a)}\ , & i_2 \equiv 0 \bmod (p-1)\ . \end{cases}$$

Proof. Since $L(E, \chi, P_\chi)$ is a continuous function, it will suffice to prove that if $k \geq 3$ and $k \equiv i_1 \bmod (p-1)$, $L(E, \chi, P_\chi)(1-k)$ is given by the formula in the theorem, since this is a dense subset of $\mathbb{Z}_p$. But, for such k, Theorem 8.2 of Lichtenbaum [8] shows that

$$L(E, \chi, P_\chi)(1-k) = -\Omega_{\underline{\underline{p}}}^{1-k}\left(1-\chi_0(\pi)\pi^k/p\right)E_{k,\chi_0}/k$$

where E_{k,χ_0} is given by Theorem 7.2 and

$$E_{k,\chi_0} = (-1)^k k!\left(\gamma_\chi/\Omega_\infty\right)^k \sum_{\substack{\alpha\in\mathcal{O}\\ \alpha\neq 0}} \frac{\rho^{i_2-i_1}(\alpha)\omega^{-i_2}(\bar{\alpha})}{\alpha^k}.$$

Since $\chi_0(\pi)\pi^k = \omega^{-i_2}(\bar{\psi}(\underline{\underline{p}}))\psi^k(\underline{\underline{p}})$, the theorem follows immediately from equations (72) and (73).

Let χ be a non-trivial character of $\mathrm{Gal}(F/K)$ and choose integers k and j with $0 \leq j < p-1$ and $1 < k \leq p$ such that $\chi = \chi_1^k\chi_2^{-j}$. Since $L(E, \chi, P_\chi)$ is an Iwasawa function, $L(E, \chi, P_\chi)(1)$ is an integer in $\mathbb{C}_{\underline{\underline{p}}}$ (in $\hat{I}_\infty$, in fact), and it is a unit if and only if $L(E, \chi, P_\chi)(1-k)$ is a unit. Now, if $j = 0$,

$$L(E, \chi, P_\chi)(1-k) = (-1)^{k-1}(k-1)!\Omega_{\underline{\underline{p}}}^{1-k}\left(\gamma_\chi/\Omega_\infty\right)^k\left(1-\psi^k(\underline{\underline{p}})/p\right)w\mathrm{L}\left(\bar{\psi}^k, k\right)$$

and so we conclude that $L(E, \chi, P_\chi)(1)$ is a unit if and only if $\Omega_\infty^{-k}\mathrm{L}(\bar{\psi}^k, k)$ is a unit in $\mathcal{O}_{\underline{\underline{p}}}$.

On the other hand, if $j \neq 0$, it follows from the fact that

$y^j \equiv \omega^j(y) \bmod p$ for all $y \in \mathbb{Z}_p$ and Theorem 38, that $L(E, \chi, P_\chi)(1-k)$ is a unit if and only if $\int x^{1-k} y^j d\mu_{k+j}$ is a unit. Again, we deduce from equation (71) that this is the case if and only if $(2\pi/\sqrt{d_K})^j \Omega_\infty^{-(k+j)} L(\bar{\psi}^{k+j}, k)$ is a unit in $\underline{\underline{O}}_{\mathfrak{p}}$.

These facts, together with Corollary 36, yield Theorem 32.

REFERENCES

[1] Coates, J., Wiles, A., Kummer's criterion for Hurwitz numbers. *Algebraic Number Theory.* Papers contributed for the International Symposium, Kyoto 1976, Japan Society for the Promotion of Science, 9-23 (1977).

[2] Coates, J., Wiles, A., On the conjecture of Birch and Swinnerton-Dyer, *Invent. Math.* **39**, 223-251 (1977).

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

[4] Coleman, R., Division values in local fields, *Invent. Math.* **53**, 91-116 (1979).

[5] Hurwitz, A., Über die Entwicklungskoeffizienten der lemniskatischen Funktionen, *Math. Ann.* **51**, 196-226 (1899) (= *Werke II*, 342-373).

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

[7] Leopoldt, H., Eine p-adische Theorie der Zetawerte II, *J. reine agnew. Math.* **274-275**, 224-239 (1975).

[8] Lichtenbaum, S., On p-adic L-functions associated to elliptic curves, *Invent. Math.* **56**, 19-55 (1980).

[9] Lubin, J., Tate, J., Formal complex multiplication in local fields, *Ann. Math.* **81**, 380-387 (1965).

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

[11] Tate, J., p-divisible groups. *Proceedings of a Conference on Local Fields* (Driebergen 1966), Springer-Verlag, 158-183 (1967).

[12] Вишик, М.М., Манин, Ю.И. [Visik, M., Manin, J.], p-адические ряды Гекке мнимых квадратичных полей [p-adic Hecke series of imaginary quadratic fields], *Mat. Sb.* **95** (**137**), 357-383 (1974). English Transl: *Math. USSR-Sb.* **24**, 345-371 (1974).

[13] Weil, A., *Elliptic Functions According to Eisenstein and Kronecker*, Springer-Verlag, 1976.

[14] Wintenberger, J-P., Structure galoisienne de limites projectives d'unités locals (to appear in *Compositio Mathematica*).