Annals of Mathematics, **104** (1976), 459-571

p-adic interpolation of real analytic Eisenstein series

By NICHOLAS M. KATZ

TABLE OF CONTENTS

Introduction

The first half of this paper is devoted to working out a correspondence between real analytic Eisenstein series on congruence subgroups of $\mathrm{SL}_2(\mathbf{Z})$ and Ramanujan series [27], the latter viewed as p-adic modular forms. To give the simplest non-trivial example, let, k and l be strictly positive integers, with $k+1 \geqq l+3$, and $k+1-l$ even. Then the real analytic Eisenstein series on $\mathrm{SL}_2(\mathbf{Z})$ of weight $k+l+1$

$$\Phi_{k,l}^{\infty}(\tau) \overset{\mathrm{dfn}}{=} \frac{k!\,\pi^l}{2y^l} \sum\nolimits_{(n,m)\neq(0,0)} \frac{(n+m\bar{\tau})^l}{(n+m\tau)^{k+1}}, \qquad \tau = x + iy,$$

corresponds to the Ramanujan series

$$\Phi_{k,l}(q) = \sum\nolimits_{n\geq 1} q^n \sum\nolimits_{n=dd'} d^k (d')^l .$$

What gives substance to this correspondence is the fact that both sides agree on all complex-multiplication curves on which both are defined. Let us try to make this precise.

To begin, we view $\Phi_{k,l}^{\infty}$ homogeneously, as a function of lattices $M \subset \mathbf{C}$. For any lattice $M \subset \mathbf{C}$, we denote by $a(M)$ the area of a fundamental parallelogram. (Thus $a(\mathbf{Z} + \mathbf{Z}\tau) = y$ if $\tau = x + iy$). Then we define

$$\Phi_{k,l}^{\infty}(M) = \frac{k!\,\pi^l}{2(a(M))^l} \sum\nolimits_{\substack{m \in M \\ m\neq 0}} \frac{\bar{m}^l}{m^{k+1}} .$$

If we are given a complex elliptic curve E with a non-zero invariant differential ω, we can form the lattice $M(E, \omega)$ of all periods of ω over elements of $H_1(E, \mathbf{Z})$. This allows us to view $\Phi_{k,l}^{\infty}$ as a function of pairs (E, ω), by defining

$$\Phi_{k,l}^{\infty}(E, \omega) = \Phi_{k,l}^{\infty}(M(E, \omega)) .$$

Suppose now that (E, ω) is defined over a finite algebraic number-field $K \subset \mathbf{C}$, and that it has complex multiplication which is defined over the same field. Let $\mathfrak{p}$ be any prime of K such that (E, ω) has "good reduction" at $\mathfrak{p}$, and such that the underlying rational prime p splits in the multiplication field. Then E has *ordinary* reduction at $\mathfrak{p}$, and so it makes sense to evaluate any *p-adic modular form*, e.g., $\Phi_{k,l}$, at (E, ω) viewed $\mathfrak{p}$-adically: the value $\Phi_{k,l}(E, \omega)$ will be a $\mathfrak{p}$-adic integer in the $\mathfrak{p}$-adic completion $K_{\mathfrak{p}}$. The precise result (cf 4.1, 4.8) is that the complex number $\Phi_{k,l}^{\infty}(E, \omega)$ lies in K, the $\mathfrak{p}$-adic number $\Phi_{k,l}(E, \omega)$ lies in K, and the two are *equal*. (That $\Phi_{k,l}^{\infty}(E, \omega)$ lies in K is a fundamental result of Damerell [2]).

In the second half of the paper, we use this correspondence to develop a fairly complete theory of the p-adic L-functions (*including* the Γ factor) attached to a quadratic imaginary field K_0 in which p splits. We obtain the L-functions as the "Mellin transforms" in the sense of Mazur-Swinnerton-Dyer of a p-adic measure in two variables, whose moments are essentially the values of the Ramanujan series $\Phi_{k,l}$ on suitable "trivialized elliptic curves" with complex multiplication by K_0.

Construction of such p-adic L-functions amounts to a problem of p-adic interpolation of special values of Hecke L-series attached to grossencharacters of type A_0 of the field K_0 (cf. [31], p. 262–263). In this form, the problem had already been solved by Manin-Vishik [22] (except that their p-adic L-functions exist only as p-adically continuous functions of two variables, but not as the Mellin transforms of measures in two variables). In fact, their solution of the problem, by techniques quite different from those used here, was the psychological starting point of this work.

Here is a brief description of the various chapters. The first chapter is devoted to the study of the Halphen-Fricke differential operator on analytic and C^∞ modular forms. It was very strongly influenced by Weil's Fall 1974 lectures "Elliptic Funtions According to Eisenstein" at the Institute for Advanced Study. The second chapter reviews the interplay between the algebraic and analytic approaches to modular forms. The third chapter constructs real analytic Eisenstein series as special values of Epstein zeta functions. Following Hecke ([10], pp. 450–453 and 468–476), we give a fairly thorough account of holomorphic Eisenstein series in weights one and two. The formulas in this chapter show that in passing from the additive form of Eisenstein series with level (a sum over the lattice) to their q-expansions, an intrinsic partial Fourier transform takes place. Keeping track of this will plague us in later chapters, especially VIII, because our whole technique of studying Eisenstein series is through their q-expansions, while their number-theoretic interest (their relation to Hecke L-series with grossen-character of type A_0) is apparent only when they are written in additive form.

Chapter IV gives a mild generalization of Damerell's theorem. The proof we give shows that Damerell's theorem is "also" true for elliptic curves over number fields whose de Rham cohomology *looks* as though the curve has complex multiplication (cf. 4.0.8 for a precise statement). The fifth chapter reviews the p-adic theory of modular forms. The last five chapters are devoted to the construction and over-detailed explication of the p-adic L-functions attached to quadratic imaginary fields in which p splits. The last chapter, giving a Kronecker "second limit formula" for our p-adic L-functions, was directly inspired by conversations with Lichtenbaum. This formula is a generalization to quadratic imaginary fields of Leopoldt's p-adic $L(1, \chi)$ formula for the rational field. In fact, our modular proof also provides a simple proof of Leopoldt's formula.

Chapter I. Review of the classical theory

1.0. *The space* GL^+. We will work with the space GL^+ of all oriented $\mathbf{R}$-bases of $\mathbf{C}$. Thus

1.01 $$\mathrm{GL}^+ = \{(\omega_1, \omega_2) \in \mathbf{C}^2 \mid \mathrm{Im}(\omega_2/\omega_1) > 0\}$$

is also the space of all "lattices with oriented bases" in C. A point $(\omega_1, \omega_2) \in \mathrm{GL}^+$ may also be viewed as a triple $(E, \omega; \gamma_1, \gamma_2)$ consisting of a complex elliptic curve $E/\mathbf{C}$ together with a nowhere-vanishing invariant differential ω and an oriented basis γ_1, γ_2 of $H_1(E, \mathbf{Z})$. The correspondence between the last two points of view is given by the mutually inverse constructions

1.0.2 $$\begin{cases} (\omega_1, \omega_2) \longmapsto (\mathbf{C}/\mathbf{Z}\omega_1 + \mathbf{Z}\omega_2, dz; \omega_1, \omega_2)\,, \\ \left(\int_{\gamma_1}\omega, \int_{\gamma_2}\omega\right) \longleftarrow\!\!\dashv (E, \omega; \gamma_1, \gamma_2)\,. \end{cases}$$

The group $\mathrm{SL}(2, \mathbf{Z})$ acts freely on the right on GL^+, by

1.0.3 $$(\omega_1, \omega_2) \longmapsto (\omega_1, \omega_2)\begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

The quotient space $\mathfrak{L} \stackrel{\text{def}}{=} \mathrm{GL}^+/\mathrm{SL}(2, \mathbf{Z})$ is the space of all lattices in C. A point $L \in \mathfrak{L}$ is a lattice $L \subset \mathbf{C}$, and may be viewed as a pair (E, ω) consisting of a complex elliptic curve $E/\mathbf{C}$ together with a nowhere-vanishing invariant differential ω. The correspondence is given by the mutually inverse constructions

1.0.4 $$\begin{cases} L \longmapsto (\mathbf{C}/L, dz)\,, \\ \left\{\int_{\gamma}\omega \,\middle|\, \gamma \in H_1(E, \mathbf{Z})\right\} \longleftarrow\!\!\dashv (E, \omega)\,. \end{cases}$$

Weierstrass theory gives us a pair of global coordinates g_2, g_3 on $\mathfrak{L}$ in the well-known manner: to the lattice $L \in \mathfrak{L}$ we attach the elliptic curve with differential $(y^2 = 4x^3 - g_2x - g_3, dx/y)$ where

1.0.5 $$\begin{cases} x = \wp(z, L) = \dfrac{1}{z^2} + \sum_{l \in L, l \neq 0}\left\{\dfrac{1}{(z-l)^2} - \dfrac{1}{l^2}\right\}\,, \\ y = \wp'(z; L)\,, \\ g_2 = 60\sum_{l \in L, l \neq 0} 1/l^4\,, \\ g_3 = 140\sum_{l \in L, l \neq 0} 1/l^6\,. \end{cases}$$

Thus $\mathfrak{L}$ becomes the open set of $\mathbf{C}^2$ defined by

1.0.6 $$\mathfrak{L} \xrightarrow{\sim} \{(g_2, g_3) \in \mathbf{C}^2 \mid g_3^2 - 27g_2^3 \neq 0\}$$

over which $(y^2 = 4x^3 - g_2x - g_3, dx/y)$ sits as the universal elliptic curve with (nowhere-vanishing invariant) differential.

The action of $\mathbf{C}^\times$ on GL^+ by homothety, $(\omega_1, \omega_2) \mapsto (\lambda\omega_1, \lambda\omega_2)$, commutes with the action of $\mathrm{SL}(2, \mathbf{Z})$. For the elliptic-curve point of view, it is the action $(E, \omega; \gamma_1, \gamma_2) \mapsto (E, \lambda\omega; \gamma_1, \gamma_2)$. On the space $\mathfrak{L}$ it is the action $L \mapsto \lambda L$, or $(g_2, g_3) \mapsto (\lambda^{-4}g_2, \lambda^{-6}g_3)$.

1.1. *Functions on GL^+.* A function $F(\omega_1, \omega_2)$ is said to be of weight $k \in \mathbf{Z}$ if it satisfies the functional equation

1.1.1 $$F(\lambda\omega_1, \lambda\omega_2) = \lambda^{-k}F(\omega_1, \omega_2) \qquad \text{for all } \lambda \in \mathrm{C}^\times .$$

More generally, it is said to be of weight $(k, s) \in \mathbf{Z}\times\mathrm{C}$ if it satisfies

1.1.2 $$F(\lambda\omega_1, \lambda\omega_2) = \lambda^{-k}|\lambda|^{-2s}F(\omega_1, \omega_2) \qquad \text{for all } \lambda \in \mathrm{C}^\times .$$

Suppose $F(\omega_1, \omega_2)$ is a holomorphic function on GL^+ which for some integer $N \geqq 1$ is invariant by $\begin{pmatrix}1 & N\\ 0 & 1\end{pmatrix}$, i.e., satisfies $F(\omega_1, \omega_2+N\omega_1)=F(\omega_1, \omega_2)$. Then the function on the upper half-plane

1.1.3 $$\tau \longrightarrow F(2\pi i, 2\pi i N\tau)$$

is invariant by $\tau \to \tau + 1$, so is an analytic function of $q = e^{2\pi i\tau}$ for $0 < |q| < 1$. Its Laurent series development

1.1.4 $$F(2\pi i, 2\pi i N\tau) = \textstyle\sum_{n\in\mathbf{Z}} a_n q^n$$

is called the q-expansion of F (relative to N). If we too generously replace N by its multiple $N\cdot M$, then we make a change of variable $q \mapsto q^M$ in the q-expansion. Notice that if F is of weight $k \in \mathbf{Z}$, then it is completely determined by its q-expansion:

1.1.5 $$\begin{aligned} F(\omega_1, \omega_2) = \omega_1^{-k}F(1, \omega_2/\omega_1) &= \left(\frac{2\pi i}{\omega_1}\right)^k F\left(2\pi i, 2\pi i N\left(\frac{\omega_2}{N\omega_1}\right)\right) \\ &= \left(\frac{2\pi i}{\omega_1}\right)^k \textstyle\sum_{n\in\mathbf{Z}} a_n \exp(2\pi i n\omega_2/N\omega_1) . \end{aligned}$$

For example, the function ω_1 has weight -1, and q-expansion $2\pi i$.

A holomorphic function F on GL^+ is said to be a modular form of weight k on $\Gamma(N)$ = the kernel of $\mathrm{SL}(2, \mathbf{Z}) \twoheadrightarrow \mathrm{SL}(2, \mathbf{Z}/N\mathbf{Z})$ if it is invariant by $\Gamma(N)$, of weight k, and if it and all of its transforms by $\mathrm{SL}(2, \mathbf{Z})/\Gamma(N) \xrightarrow{\sim} \mathrm{SL}(2, \mathbf{Z}/N\mathbf{Z})$ have meromorphic (i.e., finite-tailed) q-expansions. For example, the j-invariant is a modular form of weight zero on $\Gamma(1) = \mathrm{SL}(2, \mathbf{Z})$, but $\exp(j)$ is not.

A C^∞-function on GL^+ which is of weight $(k, s) \in \mathbf{Z} \times \mathrm{C}$ and invariant by $\Gamma(N)$ will be called a C^∞-modular form of weight (k, s) on $\Gamma(N)$. For example the function on $\mathfrak{L}$,

1.1.6 $$a(L) = \text{area of } \mathrm{C}/L = \mathrm{Im}(\bar{\omega}_1\omega_2) = \frac{1}{2i}(\bar{\omega}_1\omega_2 - \omega_1\bar{\omega}_2) ,$$

is a C^∞-modular form of weight $(0, -1)$ on $\Gamma(1)$.

1.2. *H^1, periods of the second kind, and Ramanujan's series P.* Let (E, ω) be a complex elliptic curve with differential, corresponding to the period lattice $L = \left\{\int_\gamma \omega \,\middle|\, \gamma \in H_1(E, \mathbf{Z})\right\}$. The first complex cohomology group $H^1(E, \mathbf{C})$ may be viewed transcendentally as $\mathrm{Hom}_{\mathbf{Z}}(L, \mathbf{C})$, or algebraically as $H^1_{\mathrm{DR}}(E/\mathbf{C})$ = meromorphic differentials of the second kind (d.s.k.), modulo exact ones. Let us recall how a d.s.k. ξ on E gives rise to a cohomology class in $\mathrm{Hom}_{\mathbf{Z}}(L, \mathbf{C})$. By definition, ξ becomes exact on the universal covering $\mathbf{C}$ of E, say $\xi = df$ for some meromorphic function f on $\mathbf{C}$. Since $\xi = df$ is invariant by L-translation, f itself can only transform by a constant:

1.2.1 $$f(z + l) - f(z) = \text{constant} .$$

The cohomology class of ξ is the element of $\mathrm{Hom}_{\mathbf{Z}}(L, \mathbf{C})$ given by

1.2.2 $$l \longmapsto f(z + l) - f(z) = \int_z^{z+l} \xi = \int_l \xi .$$

In terms of the Weierstrass form ($y^2 = 4x^3 - g_2x - g_3$, dx/y) of (E, ω), a standard basis of $H^1_{\mathrm{DR}}(E/\mathbf{C})$ is given by $\omega = dx/y$ and $\eta = xdx/y$. The cohomology class of $\omega = dz$ is the given inclusion $L \hookrightarrow \mathbf{C}$, while thecohomology class of $\eta = xdx/y = \wp(z; L)dz$ arises from translating the negative of the Weierstrass zeta function

1.2.3 $$\zeta(z, L) = \frac{1}{z} + \sum_{l \neq 0} \left\{\frac{1}{z + l} + \frac{z}{l^2} - \frac{1}{l}\right\} ,$$

which integrates $\eta = -d\zeta$. Thus the cohomology class of η is

1.2.4 $$l \longmapsto \zeta(z; L) - \zeta(z + l; L) \overset{\mathrm{dfn}}{=} \eta(l; L) .$$

The Legendre period relation asserts that if (ω_1, ω_2) is any positively oriented basis of L, then

1.2.5 $$\det\begin{pmatrix} \omega_1 & \omega_2 \\ \eta(\omega_1; L) & \eta(\omega_2; L) \end{pmatrix} = 2\pi i .$$

In terms of the topological cup-product $\langle\ ,\ \rangle_{\mathrm{top}}$ on H^1, defined by

1.2.6 $$\langle \xi_1, \xi_2 \rangle_{\mathrm{top}} = \det\begin{pmatrix} \int_{\omega_1} \xi_1 & \int_{\omega_2} \xi_1 \\ \int_{\omega_1} \xi_2 & \int_{\omega_2} \xi_2 \end{pmatrix} ,$$

this says simply $\langle \omega, \eta \rangle_{\mathrm{top}} = 2\pi i$. In terms of the De Rham cup-product $\langle\ ,\ \rangle_{\mathrm{DR}} = (1/2\pi i)\langle\ ,\ \rangle_{\mathrm{top}}$, it says $\langle \omega, \eta \rangle_{\mathrm{DR}} = 1$.

The "periods of the second kind" $\eta(\omega_1; L)$ and $\eta(\omega_2; L)$ are holomorphic functions on GL^+, of weight one. Indeed, from their definition in terms of translating the Weierstrass zeta function, we easily obtain the series representations

1.2.7
$$\begin{cases} \eta(\omega_1; \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2) = -\omega_1 \sum_m \sum_{n; n\neq 0 \text{ if } m=0} \dfrac{1}{(m\omega_2 + n\omega_1)^2}, \\ \eta(\omega_2; \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2) = -\omega_2 \sum_m \sum_{n; n\neq 0 \text{ if } m=0} \dfrac{1}{(m\omega_1 + n\omega_2)^2}. \end{cases}$$

Let us define two holomorphic functions of weight one on GL^+

1.2.8
$$\begin{cases} \eta_1 = \eta_1(\omega_1, \omega_2) \overset{\text{dfn}}{=} \eta(\omega_1; \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2) \\ \eta_2 = \eta_2(\omega_1, \omega_2) \overset{\text{dfn}}{=} \eta(\omega_2; \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2) \end{cases}$$

and a function of weight two

1.2.9
$$A_2(\omega_1, \omega_2) = \sum_m \sum_{n; n\neq 0 \text{ if } m=0} \frac{1}{(m\omega_2 + n\omega_1)^2}.$$

Thus

1.2.10
$$\begin{cases} \eta_1(\omega_1, \omega_2) = -\omega_1 A_2(\omega_1, \omega_2) \\ \eta_2(\omega_1, \omega_2) = -\omega_2 A_2(-\omega_2, \omega_1) \end{cases}$$

and Legendre's period relation

1.2.11
$$\det\begin{pmatrix} \omega_1 & \omega_2 \\ -\omega_1 A_2(\omega_1, \omega_2) & -\omega_2 A_2(-\omega_2, \omega_1) \end{pmatrix} = 2\pi i$$

is equivalent to the *functional equation*

1.2.12
$$A_2(\omega_1, \omega_2) - A_2(-\omega_2, \omega_1) = \frac{2\pi i}{\omega_1 \omega_2}.$$

The series definition of A_2 makes it obvious that A_2 is invariant by $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, i.e., $A_2(\omega_1, \omega_2) = A_2(\omega_1, \omega_2 + \omega_1)$. Its q-expansion is given explicitly by

1.2.13
$$\begin{aligned} A_2(2\pi i, 2\pi i\tau) &= \frac{-1}{12} + 2\sum_{n\geq 1} q^n \sum_{d\mid n} d \\ &= \frac{-1}{12} P(q), \end{aligned}$$

where $P(q)$ is Ramanujan's series $P(q) = 1 - 24\sum_{n\geq 1} q^n \sum_{d\mid n} d$.

1.3. *The function S, and the position of the antiholomorphic subspace* $H^{0,1} \subset H^1_{\mathrm{DR}}$. It follows from the functional equation

1.3.1
$$A_2(\omega_1, \omega_2) - A_2(-\omega_2, \omega_1) = \frac{2\pi i}{\omega_1 \omega_2}$$

that the C^∞ function $S(\omega_1, \omega_2)$, defined by

1.3.2
$$\frac{-1}{12} S(\omega_1, \omega_2) \overset{\text{dfn}}{=} A_2(\omega_1, \omega_2) - \frac{\pi\bar{\omega}_1}{\omega_1 a(L)} = A_2(\omega_1, \omega_2) - \frac{\pi\bar{\omega}_1}{\omega_1(\bar{\omega}_1\omega_2 - \omega_1\bar{\omega}_2)},$$

is invariant under $(\omega_1, \omega_2) \mapsto (\omega_2, -\omega_1)$. As it is also invariantun der $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, it is invariant under all of SL(2, Z), hence is a C^∞-modular form of weight two on SL(2, Z).

We now wish to relate S to the position of the subspace $H^{0,1} \subset H^1$ spanned by the antiholomorphic differential $\bar{\omega}$. As an element of $\mathrm{Hom}_{\mathbf{Z}}(L, \mathbf{C})$, $\bar{\omega}$ is the map $l \to \bar{l}$. The cup-product $\langle \bar{\omega}, \omega \rangle_{\text{top}}$ is thus equal to

1.3.3 $$\langle \bar{\omega}, \omega \rangle_{\text{top}} \overset{\text{dfn}}{=} \det \begin{pmatrix} \bar{\omega}_1 & \bar{\omega}_2 \\ \omega_1 & \omega_2 \end{pmatrix} = 2i \,\mathrm{Im}\,(\bar{\omega}_1 \omega_2) = 2i\, a(L) .$$

In particular, $\langle \bar{\omega}, \omega \rangle_{\text{top}}$ is always non-zero.

In terms of the basis ω, η of H^1, we can express $\bar{\omega}$:

1.3.4 $$\bar{\omega} = a\omega + b\eta .$$

Because $\langle \omega, \omega \rangle = 0$ and $\langle \omega, \eta \rangle_{\text{top}} = 2\pi i$, we can solve for a and b:

1.3.5 $$\begin{cases} 2\pi i a = \langle \bar{\omega}, \eta \rangle_{\text{top}} , \\ 2\pi i b = \langle \omega, \bar{\omega} \rangle_{\text{top}} = -\langle \bar{\omega}, \omega \rangle_{\text{top}} . \end{cases}$$

Thus b can never be zero, and the direction of the line $\mathbf{C} \cdot \bar{\omega}$ in H^1, measured with respect to the basis ω, η, is completely determined by its slope $a/b = -\langle \bar{\omega}, \eta \rangle_{\text{top}} / \langle \bar{\omega}, \omega \rangle_{\text{top}}$.

LEMMA 1.3.6. *The direction of $H^{0,1}$ in H^1, measured relative to the basis ω, η, is given by* $-(1/12)S$, *in the sense that*

1.3.7 $$-\frac{1}{12} S(\omega_1, \omega_2) = -\frac{\langle \bar{\omega}, \eta \rangle_{\text{top}}}{\langle \bar{\omega}, \omega \rangle_{\text{top}}} = -\frac{\langle \bar{\omega}, \eta \rangle_{\text{DR}}}{\langle \bar{\omega}, \omega \rangle_{\text{DR}}} .$$

Proof. The last equality holds simply because $\langle\ ,\ \rangle_{\text{DR}} = (1/2\pi i)\langle\ ,\ \rangle_{\text{top}}$. To verify the first, we simply compute the cup-product expression, using the functional equation 1.3.1 of A_2:

1.3.8 $$\begin{aligned} -\langle \bar{\omega}, \eta \rangle_{\text{top}} &= -\det \begin{pmatrix} \bar{\omega}_1 & \bar{\omega}_2 \\ -\omega_1 A_2(\omega_1, \omega_2) & -\omega_2 A_2(-\omega_2, \omega_1) \end{pmatrix} \\ &= \bar{\omega}_1 \omega_2 A_2(-\omega_2, \omega_1) - \omega_1 \bar{\omega}_2 A_2(\omega_1, \omega_2) \\ &= \bar{\omega}_1 \omega_2 \left(A_2(\omega_1, \omega_2) - \frac{2\pi i}{\omega_1 \omega_2} \right) - \omega_1 \bar{\omega}_2 A_2(\omega_1, \omega_2) \\ &= (\bar{\omega}_1 \omega_2 - \omega_1 \bar{\omega}_2) A_2(\omega_1, \omega_2) - \frac{2\pi i \bar{\omega}_1}{\omega_1} , \end{aligned}$$

while

1.3.9 $$\langle \bar{\omega}, \omega \rangle = \det \begin{pmatrix} \bar{\omega}_1 & \bar{\omega}_2 \\ \omega_1 & \omega_2 \end{pmatrix} = \bar{\omega}_1 \omega_2 - \omega_1 \bar{\omega}_2 ,$$

so that

1.3.10 $$-\frac{\langle\bar{\omega}, \eta\rangle_{\text{top}}}{\langle\bar{\omega}, \omega\rangle_{\text{top}}} = A_2(\omega_1, \omega_2) - \frac{2\pi i\bar{\omega}_1}{\omega_1(\bar{\omega}_1\omega_2 - \omega_1\bar{\omega}_2)} \overset{\text{dfn}}{=} -\frac{1}{12}S(\omega_1, \omega_2)\,.$$

Q.E.D.

Remark 1.3.11. Another proof of the modular invariance of S is due to Hecke ([9]) who showed that in fact

1.3.12 $$-\frac{1}{12}S(\omega_1, \omega_2) = \lim_{s\to 0}\sum\nolimits_{(n,m)\neq(0,0)} \frac{1}{(n\omega_1 + m\omega_2)^2|n\omega_1 + m\omega_2|^{2s}}\,.$$

For full details, see Rademacher [26], pp. 126–131.

1.4. *The Halphen-Fricke operator D* (compare [7], Ch. IX, pp. 300 ff). It is the holomorphic derivation on GL^+ defined by

1.4.1 $$D = \eta_1(\omega_1, \omega_2)\frac{\partial}{\partial\omega_1} + \eta_2(\omega_1, \omega_2)\frac{\partial}{\partial\omega_2}\,.$$

For any of the functions $l = n\omega_1 + m\omega_2 \in \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2$, we have

1.4.2 $$D(l) = \eta(l; L),\ D(\bar{l}) = 0\,.$$

We will develop the basic properties of D in a series of lemmas.

LEMMA 1.4.3. *D is $\mathrm{SL}(2, \mathbf{Z})$-invariant in the sense that it commutes with the action of $\mathrm{SL}(2, \mathbf{Z})$ on functions defined by*

1.4.4 $$([g]F)(\omega_1, \omega_2) = F((\omega_1, \omega_2)g) = F\left((\omega_1, \omega_2)\begin{pmatrix} a & b \\ c & d\end{pmatrix}\right) \text{ for } g = \begin{pmatrix} a & b \\ c & d\end{pmatrix}\,.$$

Proof. For fixed $g \in \mathrm{SL}(2, \mathbf{Z})$, both D and $[g^{-1}]\cdot D\cdot[g]$ are holomorphic derivations, so it suffices to check that they agree on the coordinate functions $F(\omega_1, \omega_2) = \omega_1$ or $F(\omega_1, \omega_2) = \omega_2$. We carry out the computation only for $F(\omega_1, \omega_2) = \omega_1$; the other case is similar.

$$\begin{aligned} D([g]F)(\omega_1, \omega_2) &= D(F(a\omega_1 + c\omega_2, b\omega_1 + d\omega_2)) \\ &= D(a\omega_1 + c\omega_2) \\ &= \eta(a\omega_1 + c\omega_2; L) \\ &= ([g]\eta_1)(\omega_1, \omega_2) \\ &= [g](DF)(\omega_1, \omega_2)\,. \end{aligned}$$

Q.E.D.

LEMMA 1.4.4. *D is of weight two in the sense that under the action of $\lambda \in \mathbf{C}^\times$ on functions defined by*

$$([\lambda]F)(\omega_1, \omega_2) = F(\lambda^{-1}\omega_1, \lambda^{-1}\omega_2)$$

we have

$$\begin{cases} [\lambda]\cdot D\cdot[\lambda^{-1}] = \lambda^2 D & \textit{for all } \lambda \in \mathbf{C}^\times, \\ \text{i.e., } [\lambda](DF) = \lambda^2 D([\lambda]F) & \textit{for all } \lambda \in \mathbf{C}^\times, \textit{ all } F\,. \end{cases}$$

Proof. As in the previous lemma, it suffices to chek the coordinate functions $F = \omega_1$ or $F = \omega_2$. We carry out the computation only for $F(\omega_1, \omega_2) = \omega_1$; the other case is similar.

$$\begin{aligned}[\lambda](DF) &= [\lambda]\eta_1(\omega_1, \omega_2) = \eta_1(\lambda^{-1}\omega_1, \lambda^{-1}\omega_2) \\ &= \lambda \cdot \eta_1(\omega_1, \omega_2) \\ &= \lambda^2 \cdot \lambda^{-1}D(F) \\ &= \lambda^2 D(\lambda^{-1}F) \\ &= \lambda^2 D([\lambda]F) . \end{aligned}$$

Q.E.D.

The next lemma identifies D with the operator ∂ of Serre [30].

LEMMA 1.4.5 (q-expansion of D). *Let $F(\omega_1, \omega_2)$ be a holomorphic function on* GL^+ *of weight $k \in \mathbf{Z}$, which is invariant under $\begin{pmatrix} 1 & N \\ 0 & 1 \end{pmatrix}$. Let $F(q)$ denote its q-expansion* (relative to N):

1.4.6 $$F(q) = F(2\pi i, 2\pi i N\tau) = \textstyle\sum_{n \in \mathbf{Z}} a_n q^n , \qquad q = e^{2\pi i\tau}$$

Then DF, which by the two previous lemmas is a holomorphic function of weight $k+2$ invariant by $\begin{pmatrix} 1 & N \\ 0 & 1 \end{pmatrix}$, has q-expansion given by

1.4.7 $$(DF)(q) = DF(2\pi i, 2\pi i N\tau) = \frac{1}{N} q \frac{d}{dq}(F(q)) - \frac{k}{12} P(q^N) \cdot F(q) .$$

Proof. We first express F via its q-expansion:

1.4.8 $$\begin{aligned} F(\omega_1, \omega_2) &= (2\pi i)^k F(2\pi i\omega_1, 2\pi i\omega_2) = \left(\frac{2\pi i}{\omega_1}\right)^k F(2\pi i, 2\pi i\omega_2/\omega_1) \\ &= \left(\frac{2\pi i}{\omega_1}\right)^k \textstyle\sum_n a_n \exp(2\pi i n\omega_2/N\omega_1) . \end{aligned}$$

Thus

1.4.9 $$\begin{aligned} DF(\omega_1, \omega_2) &= \left(\frac{2\pi i}{\omega_1}\right)^k \textstyle\sum_n a_n \cdot \dfrac{2\pi i n}{N} D(\omega_2/\omega_1) \cdot \exp(2\pi i n\omega_2/N\omega_2) \\ &\quad - k \cdot \frac{(2\pi i)^k}{(\omega_1)^{k+1}} \eta_1(\omega_1, \omega_2) \cdot \textstyle\sum a_n \exp(2\pi i n\omega_2/N\omega_1) . \end{aligned}$$

We simplify the first sum by using Legendre's period relation:

1.4.10 $$D(\omega_2/\omega_1) = \frac{\omega_1 D(\omega_2) - \omega_2 D(\omega_1)}{(\omega_1)^2} = \frac{\omega_1\eta_2 - \omega_2\eta_1}{(\omega_1)^2} = \frac{2\pi i}{(\omega_1)^2}$$

and in the second sum we substitute $\eta_1(\omega_1, \omega_2) = -\omega_1 A_2(\omega_1, \omega_2)$. Thus we get

$$\begin{aligned} DF(\omega_1, \omega_2) &= \frac{1}{N}\left(\frac{2\pi i}{\omega_1}\right)^{k+2} \textstyle\sum_n n \cdot a_n \exp(2\pi i n\omega_2/N\omega_1) \\ &\quad + k\left(\frac{2\pi i}{\omega_1}\right)^k \cdot A_2(\omega_1, \omega_2) \cdot \textstyle\sum a_n \exp(2\pi i n\omega_2/N\omega_1) . \end{aligned}$$

Recalling (1.2.13) that the q-expansion with respect to 1 of A_2 is $-(1/12)P(q)$, we see that

$$DF(q) = (DF)(2\pi i, 2\pi i N\tau) = \frac{1}{N} q \frac{d}{dq} F(q) - \frac{k}{12} P(q^N) \cdot F(q) . \qquad \text{Q.E.D.}$$

COROLLARY 1.4.11. *The operator D maps modular forms of weight k on $\Gamma(N)$ to modular forms of weight $k+2$ on $\Gamma(N)$, and the q-expansion coefficients of $12NDF$ lie in the $\mathbf{Z}$-submodule of $\mathbf{C}$ generated by the q-expansion coefficients of F.*

The operator D, being $\mathrm{SL}(2, \mathbf{Z})$-invariant, necessarily "descends" to a derivation on $\mathfrak{L} = \mathrm{GL}^+/\mathrm{SL}(2, \mathbf{Z})$.

LEMMA 1.4.12. *The expression of D in the coordinates (g_2, g_3) on $\mathfrak{L}$ is*

1.4.13 $$D = 6g_3 \frac{\partial}{\partial g_2} + \frac{1}{3}(g_2)^2 \cdot \frac{\partial}{\partial g_3} .$$

Proof. Up to constant factors, the forms g_2, g_3, $(g_2)^2$ are the unique modular forms of weights 4, 6, and 8 on $\mathrm{SL}(2, \mathbf{Z})$, whose q-expansions are holomorphic. Therefore, we necessarily have $D(g_2) = \text{constant} \times g_3$, and $D(g_3) = \text{constant} \times (g_2)^2$. Using the q-expansions (with respect to $N = 1$)

1.4.14 $$\begin{cases} g_2(q) = \dfrac{1}{12}\left(1 + 240 \sum_{n \geq 1} q^n \sum_{d/n} d^3\right) , \\ g_3(q) = \dfrac{-1}{216}\left(1 - 504 \sum_{n \geq 1} q^n \sum_{d/n} d^5\right) , \end{cases}$$

and Lemma 1.4.5, we see that

1.4.15 $$\begin{cases} (Dg_2)(q) = q \dfrac{d}{dq}(g_2(q)) - \dfrac{4}{12} P(q) g_2(q) = \dfrac{-1}{36} + \cdots , \\ (Dg_3)(q) = q \dfrac{d}{dq}(g_3(q)) - \dfrac{6}{12} P(q) g_3(q) = \dfrac{1}{432} + \cdots . \end{cases}$$

Thus we conclude that

1.4.16 $$\begin{cases} Dg_2 = 6g_3 \\ Dg_3 = \dfrac{1}{3}(g_2)^2 . \end{cases} \qquad \text{Q.E.D.}$$

To relieve the aridity, we recall one of the standard applications of this last lemma (compare [17], p. 301).

COROLLARY 1.4.17 (q-expansion of Δ). *The q-expansions of $\Delta \overset{\mathrm{dfn}}{=} (g_2)^3 - 27(g_3)^2$ is given by*

1.4.18 $$\Delta(q) = q \prod_{n \geq 1} (1 - q^n)^{24} .$$

Proof. From the expressions of D in terms of g_2, g_3, we see that $D\big((g_2)^3 - 27(g_3)^2\big) = 0$. Interpreting this in q-expansion, we find

1.4.19 $$0 = q\frac{d}{dq}\Delta(q) - P(q)\Delta(q)\,,$$

i.e.,

1.4.20 $$q\frac{d}{dq}\log\Delta(q) = 1 - 24\sum_{n\geq 1} q^n \sum_{d\mid n} d$$
$$= 1 - 24\sum_{d\geq 1}\frac{dq^d}{1-q^d}\,,$$

which integrates to give

1.4.21 $$\Delta(q) = \text{constant} \times q\prod_{n\geq 1}(1-q^n)^{24}\,.$$

The constant is one, because $\big(g_2(q)\big)^3 - 27\big(g_3(q)\big)^2 = q + \cdots$, as follows immediately from 1.4.15. Q.E.D.

LEMMA 1.4.22. *For any of the functions $l = m\omega_1 + m\omega_2$, $n, m \in \mathbf{Z}$, we have*

1.4.23 $$D^2(l) = -\frac{1}{12}g_2 l\,,\ \text{i.e.,}\ D\big(\eta(l; L)\big) = -\frac{1}{12}g_2 l\,.$$

Proof. By additivity, it suffices to prove that

1.4.24 $$\begin{cases} D\eta_1 = -\dfrac{1}{12}g_2\omega_1\,, \\[2ex] D\eta_2 = -\dfrac{1}{12}g_2\omega_2\,. \end{cases}$$

Notice that if we apply D to Legendre's period relation $\omega_1\eta_2 - \omega_2\eta_1 = 2\pi i$, we obtain

1.4.25 $$\begin{cases} \omega_1 D(\eta_2) + \eta_1\eta_2 - \eta_2\eta_1 + \omega_2 D(\eta_1) = 0\,, \quad \text{i.e.,} \\[1ex] \dfrac{D(\eta_1)}{\omega_1} = \dfrac{D(\eta_2)}{\omega_2}\,. \end{cases}$$

If follows that the ratio

1.4.26 $$\frac{D^2(l)}{l} = \frac{D(n\eta_1 + m\eta_2)}{n\omega_1 + m\omega_2}$$

is independent of $(m, m) \neq (0, 0)$. We next conclude that the ratio $D^2\omega_1/\omega_1 = D\eta_1/\omega_1$ is invariant by $\mathrm{SL}(2, \mathbf{Z})$. For if $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2, \mathbf{Z})$, we have

$$\begin{aligned}([g]\eta_1)(\omega_1, \omega_2) &= \eta_1(a\omega_1 + c\omega_2, b\omega_1 + d\omega_2) \\ &= \eta(a\omega_1 + c\omega_2, \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2) = a\eta_1 + c\eta_2\,,\end{aligned}$$

while $[g](\omega_1) = a\omega_1 + c\omega_2$, and thus

1.4.27 $$[g]\left(\frac{D^2(\omega_1)}{\omega_1}\right) = [g]\left(\frac{D\eta_1}{\omega_1}\right) = \frac{D([g]\eta_1)}{[g]\omega_1} = \frac{D(a\eta_1 + c\eta_2)}{a\omega_1 + c\omega_2}$$

is independent of the choice of g. Thus $D^2(\omega_1)/\omega_1$ is $\mathrm{SL}_2(\mathbf{Z})$-invariant, and of weight four. To identify it as $-(1/12)g_2$, we compute its q-expansion. The function ω_1 is $\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$-invariant and of weight -1, and its q-expansion is $2\pi i$. So by 1.4.5, we have

1.4.28 $$(D\omega_1)(q) = q\frac{d}{dq}(2\pi i) + \frac{1}{12}P(q)2\pi i = \frac{2\pi i}{12}P(q)\,.$$

Now $D\omega_1$ is $\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$-invariant of weight $1 = -1 + 2$, so again by 1.4.5 we have

1.4.29 $$(D^2(\omega_1))(q) = q\frac{d}{dq}\left(\frac{2\pi i}{12}P(q)\right) - \frac{1}{12}P(q)\frac{2\pi i}{12}P(q)\,.$$

Thus $D^2(\omega_1)/\omega_1$ has q-expansion

1.4.30 $$\left(\frac{D^2(\omega_1)}{\omega_1}\right)(q) = \frac{1}{12}q\frac{d}{dq}P(q) - \frac{1}{144}(P(q))^2 = -\frac{1}{144} + \cdots\,.$$

Thus $D^2(\omega_1)/\omega_1$ is a weight four modular form on $\mathrm{SL}(2, \mathbf{Z})$ with holomorphic q-expansion, so a multiple of g_2, and comparing constant terms in the q-expansions 1.4.14 and 1.4.30 shows that it is $-(1/12)g_2$. Q.E.D.

Looking at the q-expansion formula 1.4.30, we obtain

COROLLARY 1.4.31. *Ramanujan's series P satisfies the differential equation*

1.4.32 $$12q\frac{d}{dq}P(q) - (P(q))^2 = -12g_2(q)\,.$$

1.5. *The Weil operator W, and the function S.* W is the C^∞ derivation on GL^+ defined by

1.5.1 $$W = -\frac{\pi}{a(L)}\left(\bar\omega_1\frac{\partial}{\partial\omega_1} + \bar\omega_2\frac{\partial}{\partial\omega_2}\right)$$

where $a(L)$ is the area function (1.1.6). For any of the functions $l = n\omega_1 + m\omega_2$, $n, m \in \mathbf{Z}$, we have

1.5.2 $$\begin{cases} W(l) = -\dfrac{\pi}{a(L)}\,\bar l\,, \\ W(\bar l) = 0\,, \end{cases}$$

and these formulas uniquely determine W.

Notice that

1.5.3 $$W(a(L)) = W\left(\frac{1}{2i}(\bar{\omega}_1\omega_2 - \omega_1\bar{\omega}_2)\right) = 0$$

and hence

1.5.4 $$W^2(l) = 0 .$$

We will develop the basic properties of W in a series of lemmas, analogous to those concerning D.

LEMMA 1.5.5 (analog of 1.4.3). *W is* SL(2, **Z**)*-invariant.*

Proof. Since the function $-\pi/a(L)$ is itself SL(2, **Z**)-invariant, the formulas 1.5.2 which characterize W are themselves SL(2, **Z**)-invariant.

Q.E.D.

LEMMA 1.5.6 (analog of 1.4.4). *W is of weight two.*

Proof. We simply compute

$$W([\lambda]l) = W(\lambda^{-1}l) = \lambda^{-1}\left(\frac{-\pi}{a(L)}\,\bar{l}\,\right),$$

while

$$[\lambda](W(l)) = [\lambda]\left(\frac{-\pi}{a(L)}\right)\overline{(\lambda^{-1}l)} = \frac{-\pi\bar{l}}{\bar{\lambda}|\lambda|^{-2}a(L)} = \lambda\left(\frac{-\pi\bar{l}}{a(L)}\right) = \lambda^2 W([\lambda]l)$$

and

$$[\lambda](W(\bar{l})) = \lambda^2 W([\lambda]\bar{l}\,) = 0 .$$ Q.E.D.

1.5.7. Thus W maps C^∞ modular forms of weight (k, s) on $\Gamma(N)$ to C^∞ modular forms of weight $(k+2, s)$ on $\Gamma(N)$.

Let us denote by H the holomorphic homogeneity operator

1.5.8 $$H \overset{\text{dfn}}{=} -\omega_1\frac{\partial}{\partial\omega_1} - \omega_2\frac{\partial}{\partial\omega_2} .$$

The operator H is SL(2, **Z**)-invariant and of weight zero, characterized by the conditions

1.5.9 $$H(l) = -l,\ H(\bar{l}\,) = 0 .$$

If F is a C^∞ function on GL^+ of weight (k, s), then

1.5.10 $$H(F) = (k + s)F .$$

More generally, if X is any differential operator (of any order) on GL^+ which is of weight (k, s), then

1.5.11 $$[H, X] = (k + s)X .$$

LEMMA 1.5.12 (analog of 1.4.5). *The Halphen-Fricke operator D is expressed in terms of the operators W, H, and* (multiplication by) S *by the formula*

1.5.13
$$D = W - \frac{1}{12} S \cdot H\,.$$

Proof. Comparing coefficients of $\partial/\partial\omega_1$ and $\partial/\partial\omega_2$, we reduce this to the assertion

1.5.14
$$\eta_i(\omega_1, \omega_2) = \frac{-\pi}{a(L)}\bar{\omega}_i + \frac{\omega_i}{12} S(\omega_1, \omega_2) \qquad \text{for } i = 1, 2,$$

or equivalently to the assertions

1.5.15
$$\begin{cases} A_2(\omega_1, \omega_2) = \dfrac{\pi\bar{\omega}_1}{\omega_1 a(L)} - \dfrac{1}{12} S(\omega_1, \omega_2)\,, \\[2ex] A_2(-\omega_2, \omega_1) = \dfrac{\pi\bar{\omega}_1}{\omega_2 a(L)} - \dfrac{1}{12} S(\omega_1, \omega_2)\,. \end{cases}$$

The first is the definition 1.3.2 of S, and the second is its invariance under $(\omega_1, \omega_2) \mapsto (\omega_2, -\omega_1)$. Q.E.D.

Heuristic 1.5.16. It is perhaps more enlightening to explain the cohomological apparatus which underlies such identities as 1.5.13. Over GL^+ sits the universal elliptic curve $E_{\mathrm{univ}} \xrightarrow{f} \mathrm{GL}^+$, whose "$H^1$ along the fibre" $R^1 f_* \mathbf{C}$ is a canonically trivialized flat holomorphic vector bundle. The cohomology classes ω and η define homomorphic (but not flat) cross-sections, while $\bar{\omega}$ defines only a C^∞ cross-section. In terms of the canonical trivialization, a section ξ is just a pair (ξ_1, ξ_2) of functions on GL^+, namely the periods of ξ,

1.5.17
$$\xi_i = \int_{\omega_i} \xi\,.$$

The Gauss-Manin connection ∇ is the action of the derivations of GL^+ on the cross-sections, defined by differentiating the periods

1.5.18
$$\int_{\omega_i} \nabla(X)(\xi) = X\left(\int_{\omega_i} \xi\right)\,.$$

Formulas 1.4.2, 1.4.22, 1.6.2, 1.5.9-10 reappear in this context as

1.5.19
$$\nabla(D)(\omega) = \eta, \quad \nabla(D)(\eta) = -\frac{1}{12} g_2 \omega, \quad \nabla(D)(\bar{\omega}) = 0\,,$$

1.5.20
$$\nabla(W)(\omega) = \frac{-\pi}{a(L)}\bar{\omega}, \quad \nabla(W)(\bar{\omega}) = 0\,,$$

1.5.21
$$\nabla(H)(\omega) = -\omega, \quad \nabla(H)(\eta) = \eta, \quad \nabla(H)(\bar{\omega}) = 0\,.$$

The cup-product of two sections ξ, ξ' is the function on GL^+ defined by

1.5.22 $$\langle \xi, \xi' \rangle_{\mathrm{top}} = \det \begin{pmatrix} \xi_1 \, \xi_2 \\ \xi_1' \, \xi_2' \end{pmatrix} .$$

In terms of this, Legendre's period relation reappears as

1.5.23 $$\langle \omega, \eta \rangle_{\mathrm{top}} = \langle \omega, \nabla(D)(\omega) \rangle_{\mathrm{top}} = 2\pi i \; .$$

Remembering that

1.5.24 $$\langle \bar{\omega}, \omega \rangle_{\mathrm{top}} = 2ia(L) \; ,$$

we obtain

1.5.25 $$\langle \omega, \nabla(W)(\omega) \rangle_{\mathrm{top}} = \left\langle \omega, \frac{-\pi}{a(L)} \bar{\omega} \right\rangle_{\mathrm{top}} = 2\pi i \; .$$

Comparing 1.5.23 and 1.5.25, we see that

1.5.26 $$\langle \omega, \nabla(D)(\omega) - \nabla(W(\omega)) \rangle_{\mathrm{top}} = 0$$

which implies that $\nabla(W)(\omega) - \nabla(D)(\omega)$ is a *multiple* of ω, i.e.,

1.5.27 $$\frac{-\pi}{a(L)} \bar{\omega} = \eta + ?\, \omega \; .$$

Taking the cup-product with η, we find

1.5.28 $$2\pi i ? = \left\langle \frac{-\pi}{a(L)} \bar{\omega}, \eta \right\rangle_{\mathrm{top}} = \frac{-2\pi i \langle \bar{\omega}, \eta \rangle_{\mathrm{top}}}{\langle \bar{\omega}, \omega \rangle_{\mathrm{top}}} \; .$$

Comparing this with the cohomological expression 1.3.7 for S, we see that $? = -(1/12)S$, whence

1.5.29 $$\begin{cases} \dfrac{-\pi}{a(L)} \bar{\omega} = \eta - \dfrac{1}{12} S\omega, \text{ i.e.,} \\ \nabla(W)(\omega) = \nabla(D)(\omega) + \dfrac{1}{12} S \nabla(H)(\omega) \; . \end{cases}$$

This shows that D and $W - (1/12)S \cdot H$ have the same effect, under ∇, on both ω and $\bar{\omega}$. But because the periods of ω and $\bar{\omega}$ *are* global C^∞-coordinates on GL^+, we certainly know a C^∞ derivation when we know its effect, under ∇, on both ω and $\bar{\omega}$. Therefore we again conclude that $D = W - (1/12)S \cdot H$.

LEMMA 1.5.30 (analog of 1.4.31). *The function S satisfies the differential equation*

1.5.31 $$12W(S) - S^2 = -12g_2 \; ,$$

or equivalently,

1.5.32 $$12D(S) = -S^2 - 12g_2 \; .$$

Proof. The two formulations are equivalent by 1.5.12, since S has weight two. To prove the second, we apply D to the cohomological expression for S.

1.5.33
$$\begin{aligned} D(S) &= D\left(12\frac{\langle\bar{\omega}, \eta\rangle}{\langle\bar{\omega}, \omega\rangle}\right) \\ &= 12\frac{\langle\bar{\omega}, \nabla(D)\eta\rangle}{\langle\bar{\omega}, \omega\rangle} - 12\frac{\langle\bar{\omega}, \eta\rangle}{(\langle\bar{\omega}, \omega\rangle)^2}\langle\bar{\omega}, \nabla(D)\rangle \end{aligned}$$

because $\nabla(D)(\bar{\omega}) = 0$.

Remembering that $\nabla(D)(\omega) = \eta$, and $\nabla(D)(\eta) = -(1/12)g_2\omega$, this becomes

$$D(S) = -g_2 - \frac{1}{12}S^2 . \qquad \text{Q.E.D.}$$

1.6. *Interpretation in terms of a certain algebra of operators $\mathcal{Z}$.* Let $\mathcal{Z}$ denote the associative $\mathbf{Z}[1/12]$-algebra generated by symbols

1.6.1
$$\boldsymbol{g}_2, \boldsymbol{g}_3, \mathbf{D}, \mathbf{H}, \mathbf{W}, \mathbf{S}$$

subject only to the relations

1.6.2
$$\begin{aligned} \mathbf{D} &= \mathbf{W} - \frac{1}{12}\mathbf{SH} , \\ [\mathbf{S}, \boldsymbol{g}_2] &= [\mathbf{S}, \boldsymbol{g}_3] = [\boldsymbol{g}_2, \boldsymbol{g}_3] = 0 , \\ [\mathbf{D}, \mathbf{S}] &= -\boldsymbol{g}_2 - \frac{1}{12}\mathbf{S}^2 , \\ [\mathbf{D}, \boldsymbol{g}_2] &= 6\boldsymbol{g}_3 , \\ [\mathbf{D}, \boldsymbol{g}_3] &= \frac{1}{3}(\boldsymbol{g}_2)^2 , \\ [\mathbf{H}, \mathbf{S}] &= 2\mathbf{S} , \\ [\mathbf{H}, \boldsymbol{g}_2] &= 4\boldsymbol{g}_2 , \\ [\mathbf{H}, \boldsymbol{g}_3] &= 6\boldsymbol{g}_3 , \\ [\mathbf{H}, \mathbf{D}] &= 2\mathbf{D} . \end{aligned}$$

If we assign the weights 4, 6, 2, 0, 2, 2 to $\boldsymbol{g}_2$, $\boldsymbol{g}_3$, $\mathbf{D}$, $\mathbf{H}$, $\mathbf{W}$, and $\mathbf{S}$ respectively, then $\mathcal{Z}$ becomes a graded algebra, whose graded pieces are the eigenspaces of $\operatorname{ad}(\mathbf{H})$. As a $\mathbf{Z}[1/12]$-module, $\mathcal{Z}$ is free, with basis the monomials

1.6.3
$$\mathbf{S}^a\boldsymbol{g}_2^b\boldsymbol{g}_3^c\mathbf{D}^d\mathbf{H}^e , \quad a, b, c, d, e \text{ integers} \geqq 0 .$$

Our previous computations may be summarized by saying that the ring of C^∞ functions on GL^+ has the structure of a $\mathcal{Z}$-module, in which the symbols $\boldsymbol{g}_2$, $\boldsymbol{g}_3$, $\mathbf{D}$, $\mathbf{H}$, $\mathbf{W}$, $\mathbf{S}$ operate as g_2, g_3, D, H, W, S.

Chapter II. Review of the algebraic theory

2.0. *Level N structures.* Let E be an elliptic curve over a ring B. For each integer $N \geqq 1$, we denote by ${}_N E$ the (scheme-theoretic) kernel of multiplication by N. It is a finite and flat commutative group-scheme over B, of rank N^2. The e_N pairing is a canonical alternating pairing

2.0.1 $$e_N\colon {}_N E \times {}_N E \longrightarrow \mu_N$$

which identifies ${}_N E$ with its own Cartier dual.

When $B = \mathbf{C}$, and we view E transcendentally as being $\mathbf{C}/L$, then ${}_N E$ "is" the group $(1/N)L/L$, and the e_N-pairing is given by the explicit formula

2.0.2 $$e_N\left(\frac{l_1}{N}, \frac{l_2}{N}\right) = \exp\left(\frac{\pi}{N} \cdot \frac{\bar{l}_1 l_2 - l_1 \bar{l}_2}{a(L)}\right).$$

Over any ground-ring B, a *naive* level N structure on E/B is an isomorphism of B-group-schemes

2.0.3 $$\alpha\colon \mathbf{Z}/N\mathbf{Z} \times \mathbf{Z}/N\mathbf{Z} \xrightarrow{\sim} {}_N E .$$

Its very existence implies that N is invertible in B. Its *determinant* $\det(\alpha)$ is the primitive N'th root of unity $e_N(\alpha(1, 0), \alpha(0, 1))$. We will refer to a pair (E, α) as a naive level N curve, or as a $\Gamma(N)^{\text{naive}}$-curve.

2.0.4 For arithmetic purposes, it is convenient to define an *arithmetic* level N structure on E/B to be an isomorphism

2.0.5 $$\beta\colon \mu_N \times \mathbf{Z}/N\mathbf{Z} \xrightarrow{\sim} {}_N E$$

under which the e_N pairing becomes the standard symplectic autoduality of $\mu_N \times \mathbf{Z}/N\mathbf{Z}$ defined by

2.0.6 $$\langle(\zeta_1, n), (\zeta_2, m)\rangle_{\text{std}} = \zeta_1^m/\zeta_2^n .$$

A pair (E, β) will be referred to as an arithmetic level N curve, or as a $\Gamma(N)^{\text{arith}}$-curve.

When N is invertible in B, then a *naive* level N structure α gives rise to both a primitive N'th root of unity $\det(\alpha)$ and to an *arithmetic* level N structure β_α, defined by

2.0.7 $$\beta_\alpha(\det(\alpha)^m, n) = \alpha(m, n) .$$

This construction establishes a bijection

2.0.8 $$\left\{\begin{matrix}\text{naive level } N \\ \text{structures on } E/B\end{matrix}\right\} \xrightarrow{\sim} \mu_N^{\text{prim}}(B) \times \left\{\begin{matrix}\text{arithmetic level } N \\ \text{structures on } E/B\end{matrix}\right\},$$
$$\alpha \longmapsto (\det(\alpha), \beta_\alpha),$$

whenever $B \ni 1/N$.

We can think of an arithmetic level N structure β as being a pair of inclusions $\beta_1\colon \boldsymbol{\mu}_N \hookrightarrow {}_NE$, $\beta_2\colon \mathbf{Z}/N\mathbf{Z} \hookrightarrow {}_NE$ such that

2.0.9 $$e_N(\beta_1(\zeta), \beta_2(n)) = \zeta^n .$$

So it is natural to define a $\Gamma_{00}(N)^{\text{arith}}$-structure on E/B to be an inclusion

2.0.10 $$i\colon \boldsymbol{\mu}_N \hookrightarrow {}_NE ,$$

and a $\Gamma_{00}(N)^{\text{naive}}$-structure on E/B to be an inclusion

2.0.11 $$j\colon \mathbf{Z}/N\mathbf{Z} \hookrightarrow {}_NE .$$

2.1. *Level N test objects, and modular forms.*

2.1.1. A $\Gamma(N)^{\text{arith}}$-test object over a ring B is a triple (E, ω, β) consisting of an elliptic curve E/B, a nowhere-vanishing invariant differential ω on E, and a $\Gamma(N)^{\text{arith}}$-structure β on E/B; similarly for $\Gamma(N)^{\text{naive}}$, $\Gamma_{00}(N)^{\text{arith}}$, or $\Gamma_{00}(N)^{\text{naive}}$.

A $\Gamma(N)^{\text{arith}}$ modular form of weight $k \in \mathbf{Z}$ defined over a ring B is a "function" F which assigns to any $\Gamma(N)^{\text{arith}}$-test object (E, ω, β), defined over a B-algebra B', a value $F(E, \omega, \beta) \in B'$. This value is to depend only on the B'-isomorphism class of the test object. It is to depend on the choice of ω, which is indeterminate up to a unit $\lambda \in (B')^\times$, by the rule

2.1.2 $$F(E, \lambda^{-1}\omega, \beta) = \lambda^k F(E, \omega, \beta) .$$

Finally, its formation is to be compatible with extension of scalars of B-algebras. Similarly for $\Gamma(N)^{\text{naive}}$, or $\Gamma_{00}(N)^{\text{arith}}$, or $\Gamma_{00}(N)^{\text{naive}}$.

2.1.3. We denote by $R^{\cdot}(B, \Gamma(N)^{\text{arith}})$ the graded ring of $\Gamma(N)^{\text{arith}}$ modular forms defined over B. Similarly for $\Gamma(N)^{\text{naive}}$, $\Gamma_{00}(N)^{\text{arith}}$, or $\Gamma_{00}(N)^{\text{naive}}$.

2.2. *q-expansions.*

2.2.1. The Tate curve Tate (q^N) over $\mathbf{Z}((q))$, viewed as "$\mathbf{G}_m/q^{N\mathbf{Z}}$", carries a canonical invariant differential ω_{can}, deduced from "dx/x" on $\mathbf{G}_m$, and a canonical arithmetic level N structure β_{can}, defined by

2.2.2 $$\beta_{\text{can}}(\zeta, n) = \zeta q^n \quad \text{"mod } q^{N\mathbf{Z}}\text{"} .$$

Thus $(\text{Tate}(q^N), \omega_{\text{can}}, \beta_{\text{can}})$ is a $\Gamma(N)^{\text{arith}}$-test object over $\mathbf{Z}((q))$. We denote by $j_{\text{can}}\colon \mathbf{Z}/N\mathbf{Z} \to {}_N\text{Tate}(q^N)$ the canonical $\Gamma_{00}(N)^{\text{naive}}$ structure defined by

2.2.3 $$j_{\text{can}}(n) = q^n \quad \text{"mod } q^{N\mathbf{Z}}\text{"} ,$$

so that $(\text{Tate}(q^N), \omega_{\text{can}}, j_{\text{can}})$ is a $\Gamma_{00}(N)^{\text{naive}}$-test object over $\mathbf{Z}((q))$.

Finally, we denote by $i_{\text{can}}\colon \boldsymbol{\mu}_N \hookrightarrow {}_N\text{Tate}(q)$ the canonical $\Gamma_{00}(N)^{\text{arith}}$ structure on Tate (q) defined by

2.2.4 $$i_{\text{can}}(\zeta) = \zeta \quad \text{"mod } q^{\mathbf{Z}}\text{"} .$$

Notice that $\text{Tate}(q) = \text{Tate}(q^N)/j_{\text{can}}(\mathbf{Z}/N\mathbf{Z})$, and i_{can} is the composite

$$\begin{tikzcd} \mu_N \arrow[r, hook, "\beta_{\text{can}}"] \arrow[rr, bend left, "i_{\text{can}}"] & \text{Tate}(q^N) \arrow[r, two heads] & \text{Tate}(q^N)/j_{\text{can}}(\mathbf{Z}/N\mathbf{Z}) . \end{tikzcd}$$

Thus $(\text{Tate}(q), \omega_{\text{can}}, i_{\text{can}})$ is a $\Gamma_{00}(N)^{\text{arith}}$ test object over $\mathbf{Z}((q))$.

Evaluation at the relevant Tate curve defines q-expansion homomorphisms

2.2.5 $$\begin{cases} R^{\cdot}(B, \Gamma(N)^{\text{arith}}) \\ R^{\cdot}(B, \Gamma_{00}(N)^{\text{naive}}) \\ R^{\cdot}(B, \Gamma_{00}(N)^{\text{arith}}) \end{cases} \longrightarrow B \otimes \mathbf{Z}((q)) \subset B((q)) .$$

According to the *q-expansion principle* [16], we have

2.2.6 If we fix the weight $k \in \mathbf{Z}$, each of the q-expansion maps

2.2.7 $$\begin{cases} R^{k}(B, \Gamma(N)^{\text{arith}}) \\ R^{k}(B, \Gamma_{00}(N)^{\text{naive}}) \\ R^{k}(B, \Gamma_{00}(N)^{\text{arith}}) \end{cases} \hookrightarrow B((q))$$

is *injective*.

2.2.8 If $B \subset B'$, then $R^k(B, \Gamma(N)^{\text{arith}}) \hookrightarrow R^k(B', \Gamma(N)^{\text{arith}})$ (and similarly for $\Gamma_{00}(N)^{\text{naive}}$ and $\Gamma_{00}(N)^{\text{arith}}$), and an element $f \in R^k(B', \Gamma(N)^{\text{arith}})$ lies in $R^k(B, \Gamma(N)^{\text{arith}})$ if and only if its q-expansion lies in $B((q))$ (and similarly for $\Gamma_{00}(N)^{\text{arith}}$, $\Gamma_{00}(N)^{\text{naive}}$).

2.3. *Some interrelations.* We first define a natural map (of stacks)

2.3.1 $$\{\Gamma(N)^{\text{arith}}\text{-test objects}\} \longmapsto \{\Gamma_{00}(N)^{\text{naive}}\text{-test objects}\}$$

by sending

2.3.2 $$(E, \omega, \beta) \longmapsto (E, \omega, \beta \mid \mathbf{Z}/N\mathbf{Z}) .$$

It carries $(\text{Tate}(q^N), \omega_{\text{can}}, \beta_{\text{can}})$ to $(\text{Tate}(q^N), \omega_{\text{can}}, j_{\text{can}})$.

We next describe a pair of mutually inverse equivalences

2.3.3 $$\{\Gamma_{00}(N)^{\text{naive}}\text{-test objects}\} \rightleftarrows \{\Gamma_{00}(N)^{\text{arith}}\text{-test objects}\} .$$

Beginning with a $\Gamma_{00}(N)^{\text{naive}}$-test object $(E, \omega, j\colon \mathbf{Z}/N\mathbf{Z} \hookrightarrow {}_NE)$, we let $E' = E/j(\mathbf{Z}/N\mathbf{Z})$, and denote by $\pi\colon E \to E'$ the projection. Because π is étale (its kernel being $\mathbf{Z}/N\mathbf{Z}$), there is a unique invariant differential ω' on E' such that $\pi^*(\omega') = \omega$. By Cartier-Nishi duality, the kernel of the dual map $\check{\pi}\colon E' \to E$ is dual to $\ker(\pi) \simeq \mathbf{Z}/N\mathbf{Z}$, hence "is" μ_N. We normalize $i\colon \mu_N \hookrightarrow E'$ by decreeing that $i(\zeta) = \pi(t)$, where t is any section of ${}_NE$ (defined over some f.p.p.f. overring) such that $e_N(t, j(n))_E = \zeta^n$ for all $n \in \mathbf{Z}/N\mathbf{Z}$. This construction

$$(E, \omega, j) \longrightarrow (E', \omega', i)$$

is the upper of the maps 2.3.3. It carries $(\mathrm{Tate}(q^N), \omega_{\mathrm{can}}, j_{\mathrm{can}})$ to $(\mathrm{Tate}(q), \omega_{\mathrm{can}}, i_{\mathrm{can}})$.

The inverse map is quite similarly defined. Starting with a $\Gamma_{00}(N)^{\mathrm{arith}}$-test object (E, ω, i), we define $E' = E/i(\mu_N)$, and denote by $\pi: E \to E'$ the projection. Since $\ker(\pi) \simeq \mu_N$, we have $\ker(\check{\pi}: E' \to E) \simeq \mathbf{Z}/N\mathbf{Z}$. Thus $\check{\pi}$ is étale, and we may define $\omega' = \check{\pi}^*(\omega)$. Finally, we normalize the inclusion j of $\mathbf{Z}/N\mathbf{Z} \simeq \ker(\check{\pi}) \hookrightarrow E'$ by decreeing that $j(n) = \pi(t)$, where t is any section of ${}_N E$ such that $e_N(i(\zeta), t)_E = \zeta^n$ for all $\zeta \in \mu_N$. This construction

$$(E, \omega, i) \longmapsto (E', \omega', j)$$

defines the lower of the maps 2.3.3. It carries $(\mathrm{Tate}(q), \omega_{\mathrm{can}}, i_{\mathrm{can}})$ to $(\mathrm{Tate}(q^N), \omega_{\mathrm{can}}, j_{\mathrm{can}})$.

Finally we combine 2.3.1 with the upper arrow of 2.3.3 to define a map

2.3.4 $$\{\Gamma(N)^{\mathrm{arith}}\text{-test objects}\} \longrightarrow \{\Gamma_{00}(N)^{\mathrm{arith}}\text{-test objects}\}$$

defined by

$$(E, \omega, \beta) \longmapsto (E/\beta(\mathbf{Z}/N\mathbf{Z}), \omega', \pi \circ \beta \,|\, \mu_N) .$$

The maps thus sit in a commutative diagram

2.3.5
$$\begin{tikzcd}
 & \{\Gamma(N)^{\mathrm{arith}} \text{ test objects}\} \arrow[dl, "\text{divide by } \mathbf{Z}/N\mathbf{Z}"'] \arrow[d, "\text{forget half of } \beta"] \\
\{\Gamma_{00}(N)^{\mathrm{arith}} \text{ test objects}\} \arrow[r, shift left, "\text{divide by } \mu_N"] & \{\Gamma_{00}(N)^{\mathrm{naive}} \text{ test objects}\} \arrow[l, shift left, "\text{divide by } \mathbf{Z}/N\mathbf{Z}"]
\end{tikzcd}$$,

which by transposition yields a commutative diagram of ring homomorphisms

2.3.6
$$\begin{tikzcd}
 & R^{\cdot}(B, \Gamma(N)^{\mathrm{arith}}) \\
R^{\cdot}(B, \Gamma_{00}(N)^{\mathrm{arith}}) \arrow[ur, "\text{``exotic inclusion''}"] \arrow[r, shift right, "\sim"'] & R^{\cdot}(B, \Gamma_{00}(N)^{\mathrm{naive}}) \arrow[u, "\text{``natural inclusion''}"'] \arrow[l, shift right, "\sim"']
\end{tikzcd}$$,

which all *preserve q-expansions*.

LEMMA 2.3.7. *When $N = p^r$ is a prime power, and p is nilpotent in the ring B, the "natural inclusion"* (2.3.6) $R^{\cdot}(B, \Gamma_{00}(p^r)^{\mathrm{naive}}) \to R^{\cdot}(B, \Gamma(p^r)^{\mathrm{arith}})$ *is an isomorphism* (and hence so is the "exotic inclusion" by 2.3.6).

Proof. In fact, we will show that the map 2.3.1 on test objects is an equivalence. Given a B-algebra B', and a $\Gamma_{00}(p^r)^{\mathrm{naive}}$-test object $(E, \omega, j: \mathbf{Z}/p^r\mathbf{Z} \hookrightarrow {}_{p^r}E)$, we must show that there exists a unique

$$i: \mu_{p^r} \hookrightarrow {}_{p^r}E \text{ such that } e_{p^r}(i(\zeta), j(n)) = \zeta^n \text{ for } \zeta \in \mu_{p^r} \text{ and } n \in \mathbf{Z}/p^r\mathbf{Z} .$$

Unicity is clear, for the *difference* of two such i's is a map of $\mu_{p^r} \hookrightarrow {}_{p^r}E$ whose image is orthogonal under e_{p^r} to $j(\mathbf{Z}/p^r\mathbf{Z})$, hence whose image *lies* in $j(\mathbf{Z}/p^r\mathbf{Z})$. But over any ring B' where p is nilpotent, $\mathrm{Hom}_{B'}(\mu_{p^r}, \mathbf{Z}/p^r\mathbf{Z}) = \{0\}$. As for existence, notice that the *existence* of j implies that E/B is fibre by fibre *ordinary*, and therefore that ${}_{p^r}E$ sits in an auto-dual short exact sequence

2.3.8 $$0 \longrightarrow {}_{p^r}\hat{E} \longrightarrow {}_{p^r}E \longrightarrow ({}_{p^r}E)^{\text{étale}} \longrightarrow 0 ,$$

where ${}_{p^r}\hat{E}$ is the kernel of p^r in the *formal group* of E. We know that ${}_{p^r}\hat{E}$ is a *twisted* form of μ_{p^r}, and that $({}_{p^r}E)^{\text{étale}}$ is the dual twisted form of $\mathbf{Z}/p^r\mathbf{Z}$. But the inclusion $\mathbf{Z}/p^r\mathbf{Z} \overset{j}{\hookrightarrow} {}_{p^r}E$ necessarily projects to give an isomorphism $\mathbf{Z}/p^r\mathbf{Z} \xrightarrow{\sim} ({}_{p^r}E)^{\text{et}}$, whose Cartier dual is the inverse of the required isomorphism $i\colon \mu_{p^r} \xrightarrow{\sim} {}_{p^r}\hat{E}$.

2.4. *Comparison with the transcendental situation, and applications.* Let (E, ω, β) be a $\Gamma(N)^{\text{arith}}$-test object over C. Using the primitive N'th root of unity $e^{2\pi i/N}$, we may identify (cf. 2.0.8) β with a *naive* level N structure α of determinant $e^{2\pi i/N}$. Transcendentally, this datum (E, ω, α) corresponds to a lattice $L \subset \mathrm{C}$ together with a basis l_1/N, l_2/N of $(1/N)L/L$ such that

2.4.0 $$\exp\left(\frac{\pi}{N}\frac{\bar{l}_1 l_2 - l_1 \bar{l}_2}{a(L)}\right) = \exp(2\pi i/N) .$$

Now if the vectors $l_1, l_2 \in L$ formed an oriented basis of L, the above condition 2.4.0 would be automatic. Because $\mathrm{SL}(2, \mathbf{Z})$ maps onto $\mathrm{SL}(2, \mathbf{Z}/N\mathbf{Z})$, we can in fact choose an oriented basis ω_1, ω_2 of L such that $\omega_i/N \equiv l_i/N \bmod L$ for $i = 1, 2$.

2.4.1. If $F \in R^k(\mathrm{C}, \Gamma(N)^{\text{arith}})$, then the function on GL^+

2.4.2 $$F^{an}(\omega_1, \omega_2) = F\left(\mathrm{C}/\mathbf{Z}\omega_1 + \mathbf{Z}\omega_2, dz, \beta(e^{2\pi i a/N}, b) = \frac{a\omega_1 + b\omega_2}{N}\right)$$

is a "modular form of weight k on $\Gamma(N)$" in the sense of (1.1). The key GAGA-type result is that a "modular form of weight k on $\Gamma(N)$" in the sense of (1.1) is always of the form F^{an} for a unique element $F \in R^k(\mathrm{C}, \Gamma(N)^{\text{arith}})$. This correspondence $F \leftrightarrow F^{an}$ preserves q-expansion:

2.4.3 $$F^{an}(2\pi i, 2\pi i N\tau) = F(\mathrm{Tate}(q^N), \omega_{\text{can}}, \beta_{\text{can}}),\ q = e^{2\pi i\tau} .$$

If we combine this with the q-expansion principle, we see that if B is any subring of C, then elements of $R^k(B, \Gamma(N)^{\text{arith}})$ are just those "modular forms of weight k on $\Gamma(N)$" in the sense of (1.1) whose q-expansion coefficients happen to lie in B. Further, if (E, ω, β) is any $\Gamma(N)^{\text{arith}}$-test object over B, whose complexification $(E_{\mathbf{C}}, \omega_{\mathbf{C}}, \beta_{\mathbf{C}})$ corresponds to the point $(\omega_1, \omega_2) \in \mathrm{GL}^+/\Gamma(N)$, then for any $F \in R^k(B, \Gamma(N)^{\text{arith}})$ we have the equality of values

2.4.4 $$F(E, \omega, \beta) = F^{an}(\omega_1, \omega_2)$$

(which shows that $F^{an}(\omega_1, \omega_2)$ lies in B, the characteristic rationality property of a modular form defined over B).

2.4.5. As another application, we see by 1.4.11 that if B is any subring of $\mathbf{C}$, then this Halphen-Fricke operator D maps $R^k(B, \Gamma(N)^{\text{arith}})$ to $(1/12N)R^{k+2}(B, \Gamma(N)^{\text{arith}})$. Of course this last fact is also a (more elementary) consequence of the expression 1.4.13 of D in terms of g_2 and g_3, at least when 12 is invertible.

2.5. *A remark.* We formulated the algebraic definition of modular form in terms of "test objects" to avoid technical questions of representability. In fact, for $N \geqq 3$, the functor "isomorphism classes of $\Gamma(N)^{\text{arith}}$ elliptic curves" is *represented* by a smooth affine curve $M(\Gamma(N)^{\text{arith}})$ over $\mathbf{Z}$, with *geometrically irreducible* fibres, and the corresponding $\Gamma(N)^{\text{naive}}$ functor is *represented* by $\mathbf{Z}[1/N, \zeta_N] \otimes_{\mathbf{Z}} M(\Gamma(N)^{\text{arith}})$. Similarly, for $N \geqq 4$, the functor "isomorphism classes of $\Gamma_{00}(N)^{\text{naive}}$ (resp. $\Gamma_{00}(N)^{\text{arith}}$)-elliptic curves" is represented by a smooth affine curve $M(\Gamma_{00}(N)^{\text{naive}})$ (resp. $M(\Gamma_{00}(N)^{\text{arith}})$) over $\mathbf{Z}$, with geometrically irreducible fibres. The q-expansion principle 2.2.6 is a consequence of the *irreducibility* (cf. [16]). Each of these modular curves M carries an invertible sheaf $\underline{\omega}$, defined in terms of the universal elliptic curve $f: E \to M$ as $\underline{\omega} = f_*(\Omega^1_{E/M})$. The corresponding ring of modular forms $R^{\cdot}(B, ?)$ is the graded ring $\bigoplus_{k \in \mathbf{Z}} H^0(M(?) \otimes_{\mathbf{Z}} B, \underline{\omega}^{\otimes k})$.

Over $\mathbf{Z}[1/12]$, the functor "isomorphism classes of $\Gamma(N)^{\text{arith}}$ (resp. $\Gamma(N)^{\text{naive}}$, resp. $\Gamma_{00}(N)^{\text{arith}}$, resp. $\Gamma_{00}(N)^{\text{naive}}$)-test objects" is itself representable by a smooth affine surface $M^{\text{diff}}(?)$ over $\mathbf{Z}[1/12]$, for *any* $N \geqq 1$. The *coordinate rings* of these surfaces are just the corresponding rings of modular forms over $\mathbf{Z}[1/12]$. So in those cases where the scheme $M(?)$ exists (i.e., $N \geqq 3$ for $\Gamma(N)$, $N \geqq 4$ for $\Gamma_{00}(N)$), its coordinate ring, over $\mathbf{Z}[1/12]$ is the subring of the above ring consisting of modular functions (= modular forms of weight *zero*).

For example, when $N = 1$, $M^{\text{diff}}(\Gamma(1))$ is (the spectrum of) the ring $\mathbf{Z}[1/12, g_2, g_3, 1/\Delta]$, with universal test object $(E_{\text{univ}}, \omega) = (y^2 = 4x^3 - g_2x - g_3, dx/y)$. The surface $M^{\text{diff}}(\Gamma(N)^{\text{arith}})$ is then obtained as the affine quasi-finite covering of $M^{\text{diff}}(\Gamma(1))$ given by

$$M^{\text{diff}}(\Gamma(N)^{\text{arith}}) = ISOM_{M^{\text{diff}}(\Gamma(1));\, e_N}(\mu_N \times \mathbf{Z}/N\mathbf{Z},\, {}_NE)\,,$$

the "scheme of arithmetic level N structures on the curve E_{univ}" and similarly for $\Gamma(N)^{\mathrm{naive}}$. The surface $M^{\mathrm{diff}}(\Gamma_{00}(N)^{\mathrm{arith}})$ is the fppf quotient of $M^{\mathrm{diff}}(\Gamma(N)^{\mathrm{arith}})$ by $\mu_N = \mathrm{Hom}(\mathbf{Z}/N\mathbf{Z}, \mu_N)$, the indeterminacy in completing a $\Gamma_{00}(N)^{\mathrm{arith}}$ structure to a $\Gamma(N)^{\mathrm{arith}}$ structure. From this surface we obtain the (isomorphic) surface $M^{\mathrm{diff}}(\Gamma_{00}(N)^{\mathrm{naive}})$ by 2.3.3.

Chapter III. Review of the Epstein zeta function and Eisenstein series

3.0. *The Epstein zeta function; definition and functional equation.* Fix an integer $N \geqq 1$. Given a function f on $\mathbf{Z}/N\mathbf{Z} \times \mathbf{Z}/N\mathbf{Z}$, we define its symplectic Fourier transform $\hat{f}$ on $\mathbf{Z}/N\mathbf{Z} \times \mathbf{Z}/N\mathbf{Z}$ by the formula

3.0.1 $$\hat{f}(c, d) = \frac{1}{N}\sum_{a,b \bmod N} f(a, b) \exp\left(\frac{2\pi i}{N}(ad - bc)\right).$$

Notice that

3.0.2 $$\hat{\hat{f}} = f$$

as an immediate computation shows.

Let $(\omega_1, \omega_2) \in \mathrm{GL}^+$, and $k \in \mathbf{Z}$. The k'th Epstein zeta function $\zeta_k(s; \omega_1, \omega_2, f)$ is defined for $\mathrm{Re}(s) > 1$ by the series

3.0.3 $$N^{2s}\sum_{(n,m)\neq(0,0)} \frac{f(n, m)}{(n\omega_1 + m\omega_2)^k |n\omega_1 + m\omega_2|^{2s-k}}.$$

It is known (cf. [34], pp. 70–72) that

3.0.4. $\zeta_k(s; \omega_1, \omega_2, f)$ extends to the whole s-plane as a meromorphic function of s. For $k \neq 0$, it is an entire function of s, while for $k = 0$, it has (at worst) a first-order pole at $s = 1$ with residue $N\pi/a(L)\cdot\hat{f}(0, 0)$, ($a(L)$ denoting as before (1.1.6) the *area* of $\mathbf{C}/\mathbf{Z}\omega_1 + \mathbf{Z}\omega_2$).

In order to state the functional equation, it is convenient to introduce the auxiliary meromorphic function

3.0.5 $$\varphi_k(s; \omega_1, \omega_2, f) \overset{\mathrm{dfn}}{=} \Gamma\left(s + \frac{k}{2}\right)\left(\frac{a(L)}{N\pi}\right)^{s-k/2} \zeta_k(s; \omega_1, \omega_2, f).$$

It is known (cf. [34], pp. 70–72) that

3.0.6. For $k > 0$, $\varphi_k(s; \omega_1, \omega_2, f)$ is an entire function of s.

3.0.7. For $k = 0$, $\varphi_0(s; \omega_1, \omega_2, f) = \dfrac{\hat{f}(0, 0)}{s - 1} - \dfrac{f(0, 0)}{s} +$ an entire fct.

3.0.8. For $k < 0$, the function $\dfrac{\Gamma\left(s - \frac{k}{2}\right)}{\Gamma\left(s + \frac{k}{2}\right)}\varphi_k$ is entire.

The functional equation has the simple form

3.0.9 $$\varphi_k(s;\,\omega_1,\,\omega_2,\,f) = \varphi_k(1-s;\,\omega_1,\,\omega_2,\,\hat{f})\,.$$

Remark 3.0.10. To give a more intrinsic description, let L be any lattice in $\mathbf{C}$, and f a function on $(1/N)L/L$. The e_N-pairing

3.0.11 $$e_N(l_1/N,\,l_2/N) = \exp\Big(\frac{\pi}{Na(L)}(\bar{l}_1 l_2 - l_1\bar{l}_2)\Big)$$

makes the group $(1/N)L/L$ into its own dual. We define the Fourier transform $\hat{f}$ on $(1/N)L/L$ by the formula

3.0.12 $$\hat{f}(l_1/N) = \frac{1}{N}\sum\nolimits_{l \bmod NL} f(l/N)e_N(l/N,\,l_1/N)$$

and define

3.0.13 $$\zeta_k(s;\,L,\,f) = \sum\nolimits_{l\neq 0}\frac{f(l/N)}{(l/N)^k\,|\,l/N\,|^{2s-k}}\,;$$
$$\varphi_k(s;\,L,\,f) = \Gamma\Big(s+\frac{k}{2}\Big)\Big(\frac{a(L)}{N\pi}\Big)^{s-k/2}\zeta_k(s;\,L,\,f)\,.$$

The asymmetry in 3.0.6–3.0.8 between k and $-k$ comes about because of a *symmetry* in ζ_k, as follows. Given a function f on $(1/N)L/L$, consider the complex conjugate lattice $\bar{L}$ and the function Tf on $(1/N)\bar{L}/\bar{L}$ defined by

3.0.14 $$Tf(\bar{l}/N) = f(l/N)\,.$$

Then we have

3.0.15 $$\zeta_k(s;\,L,\,f) = \zeta_{-k}(s;\,\bar{L},\,Tf)$$

as results immediately from the definition 3.0.3.

3.1. *The Epstein zeta function: special values.* The functions

3.1.0 $$\begin{cases}\zeta_k(s;\,\omega_1,\,\omega_2,\,f)\,, & k\neq 0\,,\\ (s-1)\zeta_0(s;\,\omega_1,\,\omega_2,\,f)\end{cases}$$

are entire functions of s. Viewed as functions on $\mathbf{C}\times\mathrm{GL}^+$, they are C^∞ functions of the three complex variables s, ω_1, ω_2, which are holomorphic in the first variable s. For fixed s, they are $\Gamma(N)$-invariant functions on GL^+ of weight $(k,\,s-k/2)$. We are interested in special values of s, for which we obtain analytic functions on GL^+. Since an analytic function can have weight $(k,\,s-k/2)$ only if $s=k/2$, our only hope is to put $s=k/2$. This usually works.

LEMMA 3.1.1 (3.1.1.1). *For $k\neq 2$, $\zeta_k(k/2;\,\omega_1,\,\omega_2,\,f)$ is an analytic function on GL^+. For $k<0$, it vanishes identically, and for $k=0$, it is the constant $-f(0,\,0)$.*

(3.1.1.2) *For $k=2$, $\zeta_k(k/2;\,\omega_1,\,\omega_2,\,f)$ is analytic if and only if $\hat{f}(0,\,0)=0$.*

Proof. In terms of the C^∞ coordinates $\omega_1, \omega_2, \bar{\omega}_1, \bar{\omega}_2$, we define

3.1.2
$$\begin{cases} D_1 = \bar{\omega}_1 \dfrac{\partial}{\partial \bar{\omega}_1} + \bar{\omega}_2 \dfrac{\partial}{\partial \bar{\omega}_2} , \\ D_2 = \omega_1 \dfrac{\partial}{\partial \bar{\omega}_1} + \omega_2 \dfrac{\partial}{\partial \bar{\omega}_2} , \end{cases}$$

whose simultaneous kernel consists of the analytic functions. If follows immediately from the series definition 3.0.3 that

3.1.3
$$\begin{cases} D_1 \zeta_k(s; \omega_1, \omega_2, f) = -\left(s - \dfrac{k}{2}\right) \zeta_k(s; \omega_1, \omega_2, f) , \\ D_2 \zeta_k(s; \omega_1, \omega_2, f) = -\left(s - \dfrac{k}{2}\right) \zeta_{k-2}(s; \omega_1, \omega_2, f) , \end{cases}$$

first for $\mathrm{Re}(s) > 1$, then for all s by analytic continuation. Now for $k \neq 2$, both ζ_k and ζ_{k-2} are entire functions of s, and so 3.1.3, evaluated at $s = k/2$, gives the desired analyticity. For $k = 2$, we still get $D_1(\zeta_2(1; \omega_1, \omega_2, f)) = 0$, while

3.1.4
$$D_2(\zeta_2(1; \omega_1, \omega_2, f)) = -(s-1)\zeta_0(s; \omega_1, \omega_2, f)|_{s=1} = \frac{-N\pi}{a(L)} \hat{f}(0, 0) .$$

It remains to see that $\zeta_k(k/2; \omega_1, \omega_2, f)$ is constant for $k = 0$, and vanishes for $k < 0$. For $k = 0$, the functional equation is the statement

3.1.5
$$\Gamma(s)\left(\frac{a(L)}{N\pi}\right)^s \zeta_0(s; \omega_1, \omega_2, f) = \Gamma(1-s)\left(\frac{a(L)}{N\pi}\right)^{1-s} \zeta_0(1-s; \omega_1, \omega_2, \hat{f}) .$$

Multiplying both sides by s gives

3.1.6
$$\Gamma(s+1)\left(\frac{a(L)}{N\pi}\right)^s \zeta_0(s, \omega_1, \omega_2, f) = \Gamma(1-s)\left(\frac{a(L)}{N\pi}\right)^{1-s} s\zeta_0(1-s, \omega_1, \omega_2, \hat{f}).$$

Letting $s \to 0$ gives

3.1.7
$$\begin{aligned} \zeta_0(0; \omega_1, \omega_2, f) &= -\frac{a(L)}{N\pi} \times (\text{residue at } s = 1 \text{ of } \zeta_0(s; \omega_1, \omega_2, \hat{f})) \\ &= -f(0, 0) \qquad \text{by 3.0.4} . \end{aligned}$$

For $k < 0$, the vanishing of $\zeta_k(k/2; \omega_1, \omega_2, f)$ will result from the Γ factors. To simplify matters, let us use the trick 3.0.15 to shift to $k > 0$. Then the assertion becomes

3.1.8
$$\zeta_k\left(-\frac{k}{2}; \omega_1, \omega_2, f\right) = 0 \qquad \text{for } k > 0 .$$

But the *product*

$$\Gamma\left(s + \frac{k}{2}\right) \zeta_k(s; \omega_1, \omega_2, f)$$

is an entire function of s for $k > 0$, which shows that in fact ζ_k has "trivial zeroes" at $s = -k/2, -k/2 - 1, \cdots$. Q.E.D.

Remark 3.1.9. Under the Weil operator W, the φ_k satisfy the pleasing equation

3.1.10 $$N \cdot W(\varphi_k(s; \omega_1, \omega_2, f)) = \varphi_{k+2}(s; \omega_1, \omega_2, f) .$$

3.2. *q-expansions of special values: the easy case $k \geqq 3$.* Given a function f on $\mathbf{Z}/N\mathbf{Z} \times \mathbf{Z}/N\mathbf{Z}$, we define its *partial* Fourier transform Pf on $\mathbf{Z}/N\mathbf{Z} \times \mathbf{Z}/N\mathbf{Z}$ by the formula

3.2.1 $$(Pf)(n, m) = \sum\nolimits_{a \bmod N} f(a, m) e^{2\pi i a n/N} .$$

The *inverse* partial Fourier transform is defined by the formula

3.2.2 $$(P^{-1}f)(n, m) = \frac{1}{N} \sum\nolimits_{a \bmod N} f(a, m) e^{-2\pi i a n/N} .$$

The *flipped* function f^t on $\mathbf{Z}/N\mathbf{Z} \times \mathbf{Z}/N\mathbf{Z}$ is defined by the formula

3.2.3 $$f^t(n, m) = f(m, n) .$$

LEMMA 3.2.4. *For any function f on $\mathbf{Z}/N\mathbf{Z} \times \mathbf{Z}/N\mathbf{Z}$, we have*

$$P\hat{f} = (Pf)^t .$$

Proof. Write ζ for $e^{2\pi i/N}$, and compute:

$$\begin{aligned}(P\hat{f})(n, d) &= \sum\nolimits_c \hat{f}(c, d)\zeta^{cn} = \frac{1}{N}\sum\nolimits_c \zeta^{cn} \sum\nolimits_{a,b} f(a, b)\zeta^{ad-bc} \\ &= \sum\nolimits_{a,b} f(a, b)\zeta^{ad} \frac{1}{N}\sum\nolimits_c \zeta^{c(n-b)} \\ &= \sum\nolimits_a f(a, n)\zeta^{ad} = Pf(d, n) \\ &= (Pf)^t(n, d) .\end{aligned}$$

Q.E.D.

LEMMA 3.2.5. *Let $k \geqq 3$, f a function on $\mathbf{Z}/N\mathbf{Z} \times \mathbf{Z}/N\mathbf{Z}$. Then the q-expansion (with respect to N) of*

$$(-1)^k \varphi_k\Big(\frac{k}{2}; \omega_1, \omega_2, f\Big) = (-1)^k (k-1)! \sum\nolimits_{(n,m) \neq (0,0)} \frac{f(n, m)}{\Big(\dfrac{n\omega_1}{N} + \dfrac{m\omega_2}{N}\Big)^k}$$

is given by

3.2.6 $$\begin{cases} 0 & \textit{if } f(-n, -m) = (-1)^{k+1} f(n, m) , \\ L(1-k, Pf(n, 0)) + 2\sum_{n \geq 1} q^n \sum_{n=dd'} d^{k-1}(Pf)(d, d') & \\ & \textit{if } f(-n, -m) = (-1)^k f(n, m) . \end{cases}$$

Proof. When we replace $f(n, m)$ by $f^-(n, m) \overset{\text{dfn}}{=} f(-n, -m)$, we get $\varphi_k(s, \omega_1, \omega_2, f^-) = (-1)^k \varphi_k(s; \omega_1, \omega_2, f)$. So we get 0 when f has the "wrong" parity. It remains to treat the case when $f(-n, -m) = (-1)^k f(n, m)$. By definition, the q-expansion in level N is evaluation on $(2\pi i, 2\pi i N\tau)$. So we must compute

$$\frac{(-1)^k(k-1)!}{(2\pi i)^k}\sum_{(n,m)\neq(0,0)}\frac{f(n,m)}{\left(\frac{n}{N}+m\tau\right)^k}$$

$$=\frac{2(-1)^k(k-1)!}{(2\pi i)^k}\sum_{n\geqq 1}\frac{f(n,0)}{\left(\frac{n}{N}\right)^k}+\frac{2(-1)^k(k-1)!}{(2\pi i)^k}\sum_{m\geqq 1}\sum_{n\in\mathbf{Z}}\frac{f(n,m)}{\left(\frac{n}{N}+m\tau\right)^k}$$

$$=\frac{2(-N)^k(k-1)!}{(2\pi i)^k}\sum_{n\geqq 1}\frac{f(n,0)}{n^k}$$

$$+\frac{2(-1)^k(k-1)!}{(2\pi i)^k}\sum_{m\geqq 1}\sum_{j=0}^{N-1}\sum_{n\in\mathbf{Z}}\frac{f(j,m)}{(n+j/N+m\tau)^k}\,.$$

Invoking the Lipschitz formula, valid for $\mathrm{Im}(z)>0$ and $k\geqq 2$,

3.2.7 $$\frac{(-1)^k(k-1)!}{(2\pi i)^k}\sum_{n\in\mathbf{Z}}\frac{1}{(n+z)^k}=\sum_{d\geqq 1}d^{k-1}e^{2\pi i d z}\,,$$

we obtain

$$\frac{2(-N)^k(k-1)!}{(2\pi i)^k}L(k, f(n,0))+\sum_{m\geqq 1}\sum_{j=0}^{N-1}f(j,m)\sum_{d\geqq 1}d^{k-1}\zeta^{jd}q^{dm}$$

$$=\frac{2(-N)^k(k-1)!}{(2\pi i)^k}L(k, f(n,0))+\sum_{m\geqq 1}\sum_{d\geqq 1}(Pf)(d,m)d^{k-1}q^{dm}\,.$$

That the constant term is correct results from the functional equation of L-series (cf. [15], A. 15). Q.E.D.

3.3. *q-expansions; the case $k=2$.* Here we must suppose $\hat{f}(0,0)=0$ to get an analytic function, but to get a nice formula we must also assume $f(0,0)=0$.

LEMMA 3.3.1 *Let f be a function on $\mathbf{Z}/N\mathbf{Z}\times\mathbf{Z}/N\mathbf{Z}$, which satisfies*

$$f(0,0)=\hat{f}(0,0)=0\,.$$

Then the q-expansion of

$$(-1)^2\varphi_2(1;\omega_1,\omega_2,f)=\lim_{s\to 1}\sum_{(n,m)\neq(0,0)}\frac{f(n,m)}{\left(\frac{n\omega_1}{N}+\frac{m\omega_2}{N}\right)^2\left|\frac{n\omega_1+m\omega_2}{N}\right|^{2s-2}}$$

is still given by the formula 3.2.6.

Proof. The first step is to prove that $\varphi_2(1;\omega_1,\omega_2,f)$ may be expressed in terms of the $\wp$-function by the formula

3.3.2 $$\varphi_2(1;\omega_1,\omega_2,f)=\sum_{n,m \bmod N}f(n,m)\wp\left(\frac{n\omega_1+m\omega_2}{N};L\right),$$

a formula which makes sense because $f(0, 0) = 0$. To prove it, let x denote a non-zero element of $(1/N)L/L$. Then by definition

3.3.3 $$\varphi_2(1; \omega_1, \omega_2, f) = \lim_{s\to 1} \sum_{l\in L} \left\{\sum_x \frac{f(x)}{(l+x)^2|l+x|^{2s-2}}\right\}$$

while, remembering that $\sum_x f(x) = N\hat{f}(0, 0) = 0$, we have

3.3.4 $$\sum_x f(x)\wp(x; L) = \sum_x f(x)\left(\frac{1}{x} + \sum_{\substack{l\in L\\ l\neq 0}}\left(\frac{1}{(x+l)^2} - \frac{1}{l^2}\right)\right) = \sum_{l\in L}\left\{\sum_x \frac{f(x)}{(x+l)^2}\right\}.$$

So we must show that

3.3.5 $$0 = \lim_{s\to 1} \sum_{l\in L}\left\{\sum_x f(x)\left[\frac{1}{(l+x)^2|l+x|^{2s-2}} - \frac{1}{(l+x)^2}\right]\right\}.$$

It suffices to treat the case when f is the *difference* of two characteristic functions of points x and y; then the claim is that

3.3.6 $$0 = \lim_{s\to 1} \sum_{l\in L}\left\{\frac{1}{(l+x)^2|l+x|^{2s-2}} - \frac{1}{(l+y)^2|l+y|^{2s-2}} + \frac{1}{(l+y)^2} - \frac{1}{(l+x)^2}\right\}.$$

This will certainly be established if we can establish an estimate for the general term of the shape

3.3.7 $$\left|\frac{1}{(l+x)^2|l+x|^{2s-2}} - \frac{1}{(l+y)|l+y|^{2s-2}} + \frac{1}{(l+y)^2} - \frac{1}{(l+x)^2}\right| = O\left(\frac{(\log|l|)(s-1)}{|l|^3}\right)$$

for s near 1, $\mathrm{Re}(s) > 1$, and $|l| \gg 0$. By the mean value theorem, it suffices to show that the *derivative* with respect to s satisfies an estimate

3.3.8 $$\left|-\frac{2\log|l+x|}{(l+x)^2|l+x|^{2s-2}} + \frac{2\log|+y|}{(l+y)^2|+y|^{2s-2}}\right| = O\left(\frac{\log|l|}{l^3}\right)$$

for s near 1, $(\mathrm{Re}(s) > 1$, and $|l| \gg 0)$.

To simplify, let us check separately for x and y that

3.3.9 $$\left|\frac{\log|l|}{l^2|l|^{2s-2}} - \frac{\log|l+x|}{(l+x)^2|l+x|^{2s-2}}\right| = O\left(\frac{\log|l|}{l^3}\right),$$

i.e.,

3.3.10 $$\left|1 - \frac{1 + \dfrac{\log\left|1+\dfrac{x}{l}\right|}{\log|l|}}{\left(1+\dfrac{x}{l}\right)^2\left|1+\dfrac{x}{l}\right|^{2s-2}}\right| = O\left(\frac{|l|^{2s-2}}{l}\right).$$

But for $|l| \gg 0$ and $\mathrm{Re}(s) > 1$, s near one, we obviously have

3.3.11 $$1 + \frac{\log\left|1 + \frac{x}{l}\right|}{\log|l|} = 1 + \frac{O\left(\left|\frac{x}{l}\right|\right)}{\log|l|} = 1 + O\left(\left|\frac{x}{l}\right|\right),$$

and

3.3.12 $$\left(1 + \frac{x}{l}\right)^2 \left|1 + \frac{x}{l}\right|^{2s-2} = 1 + O\left(\left|\frac{x}{l}\right|\right),$$

which proves 3.3.11, even with an $O(1/|l|)$ estimate.

Now that we have the $\wp$-expression 3.3.4 for $\varphi_2(1; \omega_1, \omega_2, f)$, we compute as before. As in the proof of 3.2.5, we may limit attention to the case when f is an *even* function.

$$\begin{aligned}
\varphi_2(1; 2\pi i, 2\pi i N\tau, f) &= \frac{1}{(2\pi i)^2}\sum_{n,m}\left\{\sum_{j,\, l \bmod N}\frac{f(j, l)}{(j/N + n + (l + Nm)\tau)^2}\right\} \\
&= \frac{1}{(2\pi i)^2}\sum_{j,\, l \bmod N}\sum_m \sum_n \frac{f(j, l)}{\left(\dfrac{j + Nn}{N} + (l + Nm)\tau\right)^2} \\
&= \frac{1}{(2\pi i)^2}\sum_m \sum_n \frac{f(n, m)}{\left(\dfrac{n}{N} + m\tau\right)^2} \\
&= \frac{1}{(2\pi i)^2}\sum_n \frac{f(n, 0)}{\left(\dfrac{n}{N}\right)^2} + \frac{2}{(2\pi i)^2}\sum_{m\geq 1}\sum_n \frac{f(n, m)}{\left(\dfrac{n}{N} + m\tau\right)^2}.
\end{aligned}$$

From this point on, the proof is identical to the proof of 3.2.5. Q.E.D.

3.4. *q-expansions; the case $k = 1$: reductions via the Weierstrass zeta function.* We will eventually prove

LEMMA 3.4.1. *Let f be a function on $\mathbf{Z}/N\mathbf{Z} \times \mathbf{Z}/N\mathbf{Z}$. The q-expansion of*

$$(-1)\varphi_1\left(\frac{1}{2}; \omega_1, \omega_2, f\right) = -\sum_{(n,m)\neq(0,0)} \left.\frac{f(n, m)}{\left(\dfrac{n\omega_1 + m\omega_2}{N}\right)\left|\dfrac{n\omega_1 + m\omega_2}{N}\right|^{2s-1}}\right|_{s=1/2}$$

is given by the formula

$$\begin{cases} 0 & \textit{if } f \textit{ is even} \\ L(0, (Pf)(n, 0) + (Pf)(0, n)) + 2\sum_{n\geq 1} q^n \sum_{n=dd'}(Pf)(d, d') & \textit{if } f \textit{ is odd}. \end{cases}$$

Proof. Clearly $\varphi_1(s, \omega_1, \omega_2, f) = 0$ for f even. However, we will not immediately suppose f odd, but we will suppose that $f(0, 0) = 0$. In fact, let us begin by supposing that f is the characteristic function of a non-zero element $x \in (1/N)L/L$, and write $\varphi_1(s; L, x)$ instead.

3.4.3 $$\varphi_1(s; L, x) \overset{\text{dfn}}{=} \varphi_1(s; \omega_1, \omega_2, \text{the char. fct. of } x).$$

Thus

3.4.4 $$\varphi_1(s; L, x) = \sum_{l \in L} \frac{1}{(l + x)|l + x|^{2s-1}} \quad \text{for } \operatorname{Re}(s) > 1\,,$$

and for *any* $x \in \mathbf{C}$, $x \notin L$, the series 3.4.4 above extends to an *entire* function of s.

We will begin by comparing the *value* $\varphi_1(1/2; L, x)$ to the value of the Weierstrass zeta function

3.4.5 $$\zeta(x; L) \overset{\text{dfn}}{=} \frac{1}{x} + \sum_{l \neq 0} \left(\frac{1}{x + l} - \frac{1}{l} + \frac{x}{l^2} \right).$$

KEY LEMMA 3.4.6. *For variable $x \in \mathbf{C}$, $x \notin L$, the difference*

$$A(x) \overset{\text{dfn}}{=} \zeta(x, L) - \varphi_1\left(\frac{1}{2}; L, x\right)$$

is additive:

$$A(x + y) = A(x) + A(y) \quad \textit{if } x \notin L,\ y \notin L,\ x + y \notin L\,.$$

Proof. Fix $x \in \mathbf{C}$, $x \notin L$. To simplify, we make a change of variable $t = s - 1/2$. Let us define some series:

3.4.7 $$\varphi(t; x) = \frac{1}{x|x|^{2t}} + \sum_{l \neq 0} \frac{1}{(l + x)|l + x|^{2t}} \qquad \text{for } \operatorname{Re}(t) > \frac{1}{2}\,,$$

3.4.8 $$\zeta(t, x) = \frac{1}{x} + \sum_{l \neq 0} \left(\frac{1}{x + l} - \frac{1}{l} + \frac{x}{l^2} \right) \frac{1}{|l|^{2t}} \qquad \text{for } \operatorname{Re}(t) > -\frac{1}{2}\,,$$

3.4.9 $$g(t, x) = \frac{1}{x} + \sum_{l \neq 0} \left(\frac{1}{x + l} - \frac{1}{l} \right) \frac{1}{|l|^{2t}} \qquad \text{for } \operatorname{Re}(t) > 0\,.$$

3.4.10 $$h(t, x) = \frac{1}{x} + \sum_{l \neq 0} \left(\frac{1}{(x + l)|l|^{2t}} \right) \qquad \text{for } \operatorname{Re}(t) > \frac{1}{2}\,,$$

3.4.11 $$j(t) = \sum_{l \neq 0} \frac{1}{l|l|^{2t}} \qquad \text{for } \operatorname{Re}(t) > \frac{1}{2}\,,$$

3.4.12 $$k(t) = \sum_{l \neq 0} \frac{1}{l^2|l|^{2t}} \qquad \text{for } \operatorname{Re}(t) > 0\,.$$

We know that

3.4.13 $$\begin{cases} \varphi(t; x),\ j(t), \text{ and } k(t) \text{ extend to entire functions of } t, \text{ and } j(t) = 0, \\ g(t, x) \text{ has an analytic continuation to } \operatorname{Re}(t) > -\frac{1}{2}, \text{ namely} \\ \qquad \zeta(t, x) - xk(t)\,, \\ h(t; x) \text{ has an analytic continuation to } \operatorname{Re}(t) > -\frac{1}{2}, \text{ namely} \\ \qquad g(t; x) + j(t)\ (= g(t, x), \text{ because } j(t) = 0). \end{cases}$$

We now compute

3.4.14
$$\begin{aligned}\zeta(t, x) - \varphi(t; x) &= h(t;x) - j(t) + xk(t) - \varphi(t, x)\\ &= h(t; x) - \varphi(t, x) + xk(t)\,,\end{aligned}$$

an equality of functions *analytic* for $\mathrm{Re}(t) > -1/2$. Therefore,

3.4.15
$$A(x) \overset{\text{dfn}}{=} \zeta(x, L) - \varphi(0, x) = \lim_{\substack{t\to 0\\ t>0}} \big(h(t, x) - \varphi(t, x) + xk(0)\big)\,.$$

We next derive a series for $h(t; x) - \varphi(t; x)$, valid for $t > 0$: For $\mathrm{Re}(t) > 1/2$, we can write

3.4.16
$$\begin{aligned} &h(t; x) - \varphi(t; x)\\ &= \sum_{l\neq 0}\left(\frac{1}{(x + l)|l|^{2t}} - \frac{1}{(x + l)|x + l|^{2t}}\right) + \left(\frac{1}{x} - \frac{1}{x|x|^{2t}}\right).\end{aligned}$$

The general term of this series may be estimated for $\mathrm{Re}(t) > 0$, $|t| < 3/4$, by

3.4.17
$$\begin{aligned} &\frac{1}{(x + l)|l|^{2t}} - \frac{1}{(x + l)|x + l|^{2t}}\\ &= \frac{1}{l|l|^{2t}}\left[\frac{1}{1 + \frac{x}{l}} - \frac{1}{\left(1 + \frac{x}{l}\right)\left|1 + \frac{x}{l}\right|^{2t}}\right]\\ &= \frac{1}{l|l|^{2t}}\left(1 + \frac{x}{l}\right)^{-1}\left[1 - \left(1 + \frac{x}{l}\right)^{-t}\left(1 + \frac{\bar{x}}{\bar{l}}\right)^{-t}\right]\\ &= \frac{1}{l|l|^{2t}}\left[1 + O\left(\frac{x}{l}\right)\right]\left[1 - \left(1 - \frac{tx}{l} + O\left(\frac{t^2x^2}{l^2}\right)\right)\left(1 - \frac{t\bar{x}}{\bar{l}} + O\left(\frac{t^2\bar{x}^2}{\bar{l}^2}\right)\right)\right]\\ &= \frac{1}{l|l|^{2t}}\left[1 + O\left(\frac{x}{l}\right)\right]\left[\frac{tx}{l} + \frac{t\bar{x}}{\bar{l}} + O\left(\frac{t^2}{|l|^2}\right)\right]\\ &= \frac{1}{l|l|^{2t}}\left[\frac{tx}{l} + \frac{t\bar{x}}{\bar{l}} + O\left(\frac{|t|}{|l|^2}\right)\right]\\ &= \frac{tx}{l^2|l|^{2t}} + \frac{t\bar{x}}{|l|^{2t+2}} + O\left(\frac{|t|}{|l|^3}\right).\end{aligned}$$

This shows that the series 3.4.16 converges for $\mathrm{Re}(t) > 0$, and so provides an explicit analytic continuation of $h(t; x) - \varphi(t; x)$ to $\mathrm{Re}(t) > 0$, $|t| > 3/4$. Because the *series*

3.4.18
$$\begin{cases} k(t) = \sum_{l\neq 0}\dfrac{1}{l^2|l|^{2t}}\,,\\[2ex] n(t) = \sum_{l\neq 0}\dfrac{1}{|l|^{2t+2}}\,,\end{cases}$$

themselves converge absolutely and uniformly in $\mathrm{Re}(t) > \varepsilon > 0$, we can write, for $\mathrm{Re}(t) > 0$, $|t| < 3/4$,

3.4.19 $$h(t, x) - \varphi(t, x) = \frac{1}{x} - \frac{1}{x|x|^{2t}} + xtk(t) + \bar{x}tn(t) + O(t) .$$

Now the function $k(t)$ prolongs to an entire function of t, therefore

3.4.20 $$\lim_{t\to 0} tk(t) = 0 .$$

The function $n(t)$ prolongs to a meromorphic function of t, with only a simple pole at $t = 0$; therefore

3.4.21 $$\lim_{t\to 0} tn(t) \text{ exists} .$$

So taking the limit as $t \to 0$ in 3.4.19 gives

3.4.22 $$h(0, x) - \varphi(0, x) = \bar{x} \lim_{t\to 0} \sum_{l\neq 0} \frac{t}{|l|^{2t+2}} .$$

Combining this with 3.4.14, we even obtain an *explicit formula* for $A(x)$.

3.4.23 $$A(x) = \zeta(x; L) - \varphi(0, x) = x \lim_{t\to 0} \sum_{l\neq 0} \frac{1}{l^2|l|^{2t}} + \bar{x} \lim_{t\to 0} \sum_{l\neq 0} \frac{t}{|l|^{2t+2}} .$$

Q.E.D.

COROLLARY 3.4.24. *In the notations of* 3.4.4, *suppose* $x \in (1/N)L$, $x \notin L$. *Then for any* $z \in \mathbf{C}$, $z \notin L$, *we have the formula*

3.4.25 $$\varphi_1\Big(\frac{1}{2}; L, x\Big) = \zeta(x; L) + \frac{1}{N}(\zeta(z; L) - \zeta(z + Nx; L)) .$$

Proof. Notice that for any $l \in L$, $\varphi_1(s; L, z + l) = \varphi_1(s; L, z)$; this is clear for $\mathrm{Re}(s) > 1$ from the series, and so follows for all s by analytic continuation. In particular,

3.4.26 $$\varphi_1\Big(\frac{1}{2}; L, z + Nx\Big) = \varphi_1\Big(\frac{1}{2}; L, z\Big) .$$

Now simply compute

$$\begin{cases} \zeta(x; L) = \varphi_1\Big(\dfrac{1}{2}; L, x\Big) + A(x) , \\ \dfrac{1}{N}\zeta(z; L) = \dfrac{1}{N}\varphi_1\Big(\dfrac{1}{2}; L, z\Big) + \dfrac{1}{N}A(z) , \\ -\dfrac{1}{N}\zeta(z + Nx; L) = -\dfrac{1}{N}\varphi_1\Big(\dfrac{1}{2}; L, z + Nx\Big) - \dfrac{1}{N}A(z + Nx) . \end{cases}$$

Adding vertically and using 3.4.26 and the additivity of A give 3.4.25.

Q.E.D.

3.5. *q-expansion for* $k = 1$; *the end of the proof.* We have already remarked that the double series

3.5.1 $$A_2(\omega_1, \omega_2) = \sum_m \sum_{n;\ n\neq 0 \text{ if } m=0} \frac{1}{(m\omega_2 + n\omega_1)^2}$$

converges. Since the Weierstrass zeta function

3.5.2 $$\zeta(z; L) = \frac{1}{z} + \sum_{l\neq 0}\left(\frac{1}{z+l} - \frac{1}{l} + \frac{z}{l^2}\right)$$

is absolutely and uniformly convergent on compact subsets of $\mathbf{C} - L$, it follows that the double series

3.5.3 $$F(z; \omega_1, \omega_2) \overset{\text{dfn}}{=} \frac{1}{z} + \sum_m \sum_{n;\ n\neq 0 \text{ if } m=0}\left(\frac{1}{z + m\omega_2 + n\omega_1} - \frac{1}{m\omega_2 + n\omega_1}\right)$$

converges uniformly on compact subsets of $\mathbf{C} - L$, to $\zeta(z, L) - zA_2(\omega_1, \omega_2)$.

LEMMA 3.5.4. *$F(z; \omega_1, \omega_2)$ satisfies the functional equation*

$$F(z + n\omega_1 + m\omega_2; \omega_1, \omega_2) = F(z; \omega_1, \omega_2) - \frac{2\pi i m}{\omega_1}$$

Proof. Since the terms in the formula are all of "weight one," it is equivalent to prove

3.5.5 $$F(z + n + m\tau; 1, \tau) = F(z; 1, \tau) - 2\pi i m$$

for $\operatorname{Im}(\tau) > 0$. For translation by 1, this is easy. For convenience, we will write $F(z)$ for $F(z; 1, \tau)$.

$$\begin{aligned} &F(z+1) - F(z) \\ &\quad = \frac{1}{z+1} - \frac{1}{z} + \sum_m \sum_{\substack{n \\ n\neq 0 \text{ if } m=0}}\left(\frac{1}{z+n+1+m\tau} - \frac{1}{z+n+m\tau}\right) \\ &\quad = \sum_m \lim_{N\to\infty} \sum_{-N}^{N}\left(\frac{1}{z+m\tau+n+1} - \frac{1}{z+m\tau+n}\right) \\ &\quad = \sum_m \lim_{N\to\infty}\left(\frac{1}{z+m\tau+N+1} - \frac{1}{z+m\tau-N}\right) \\ &\quad = \sum_m 0 = 0\,. \end{aligned}$$

For translation by τ, we must use the cotangent identity

3.5.6 $$\lim_{N\to\infty} \sum_{n=-N}^{N} \frac{1}{z+n} = \pi\cot(\pi z) = \pi i \frac{e^{2\pi i z} + 1}{e^{2\pi i z} - 1}$$

valid for $z \notin \mathbf{Z}$.

We compute

$$\begin{aligned} &F(z+\tau) - F(z) \\ &\quad = \frac{1}{z+\tau} - \frac{1}{z} + \sum_m \sum_{\substack{n \\ n\neq 0 \text{ if } m=0}}\left(\frac{1}{z+n+(m+1)\tau} - \frac{1}{z+n+m\tau}\right) \end{aligned}$$

$$= \sum_m \sum_n \left(\frac{1}{z+n+(m+1)\tau} - \frac{1}{z+n+m\tau}\right)$$
$$= \sum_m (\pi\cot(\pi(z+(m+1)\tau)) - \pi\cot(\pi(z+m\tau)))$$
$$= \lim_{M\to\infty} \sum_{-M}^{M} (\pi\cot(\pi z+(m+1)\tau) - \pi\cot(\pi(z+m\tau)))$$
$$= \lim_{M\to\infty} (\pi\cot(\pi z+\pi(M+1)\tau) - \pi\cot(\pi z-\pi M\tau))$$
$$= \lim_{M\to\infty}\left(\pi i\frac{e^{2\pi iz}q^{M+1}+1}{e^{2\pi iz}q^{M+1}-1} - \pi i\frac{e^{2\pi iz}q^{-M}+1}{e^{2\pi iz}q^{-M}-1}\right)$$
$$= \lim_{M\to\infty}\left(\pi i\frac{q^{M+1}e^{2\pi iz}+1}{q^{M+1}e^{2\pi iz}-1}\right) - \lim_{M\to\infty}\left(\pi i\frac{e^{2\pi iz}+q^M}{e^{2\pi iz}-q^M}\right)$$
$$= -\pi i - \pi i = -2\pi i \text{ because } |q|<1 .$$
Q.E.D.

COROLLARY 3.5.7. *In the notations of* 3.4.4, *let* $x \in (1/N)L$, $x \notin L$; *then for any oriented basis* (ω_1, ω_2) *of* L, *we have*

$$\varphi_1\left(\frac{1}{2}; L, x\right) = F(x;\omega_1,\omega_2) + \frac{1}{N}(F(z;\omega_1,\omega_2) - F(z+Nx;\omega_1,\omega_2)) .$$

Proof. This follows from 3.4.25, simply because ζ and F differ by an *additive* function (in this case $zA_2(\omega_1, \omega_2)$).

Thus if we write

$$x = \frac{n\omega_1 + m\omega_2}{N} ,$$

then 3.5.4 gives the "explicit formula"

3.5.8
$$\varphi_1\left(\frac{1}{2}; L, \frac{n\omega_1+m\omega_2}{N}\right) = F\left(\frac{n\omega_1+m\omega_2}{N};\omega_1,\omega_2\right) + \frac{2\pi i m}{N\omega_1} .$$

In view of this, we next compute the q-expansion of $F(n\omega_1+m\omega_2/N;\omega_1,\omega_2)$ (which makes sense because, by 3.5.8, it is invariant under $(\omega_1,\omega_2)\to(\omega_1,\omega_2+N\omega_1)$).

LEMMA 3.5.9. *Let* $0 \leqq j,\ l \leqq N-1$, *and assume* $(j, l) \neq (0, 0)$. *Write* $\zeta = e^{2\pi i/N}$.

The q-expansion of $F((j\omega_1 + l\omega_2)/N; \omega_1, \omega_2)$ *is given by the series*

3.5.10
$$\begin{Bmatrix} \frac{1}{2}\frac{\zeta^j+1}{\zeta^j-1} & \text{if } l=0 \\ -\frac{1}{2} & \text{if } l\neq 0 \end{Bmatrix} - \sum_{n\geq 1} q^n \Big(\sum_{\substack{n=dd' \\ d'\equiv l \bmod N}} \zeta^{jd} - \sum_{\substack{n=dd' \\ d'\equiv -l \bmod N}} \zeta^{-id}\Big) .$$

Proof. We simply compute :

$$F\left(\frac{2\pi ij}{N} + 2\pi il\tau; 2\pi i, 2\pi iN\tau\right)$$
$$= \frac{1}{2\pi i}F\left(\frac{j}{N} + l\tau; 1, N\tau\right)$$

$$= \frac{1}{2\pi i}\left[\frac{1}{\frac{j}{N}+l\tau} + \sum_m \sum_{\substack{n \\ n\neq 0 \text{ if } m=0}} \left(\frac{1}{\frac{j}{N}+l\tau+n+mN\tau} - \frac{1}{n+mN\tau}\right)\right]$$

$$= \frac{1}{2\pi i}\left[\frac{1}{\frac{j}{N}+l\tau} + \sum_{n\neq 0}\left(\frac{1}{\frac{j}{N}+l\tau+n} - \frac{1}{n}\right)\right]$$

$$+ \frac{1}{2\pi i}\left[\sum_{m\neq 0}\sum_n \left(\frac{1}{\frac{j}{N}+l\tau+n+mN\tau} - \frac{1}{n+mN\tau}\right)\right].$$

Using symmetric ($\lim_{N\to\infty}\sum_{-N}^{N}$) summation on the inner sums allows us to use the cotangent identity 3.5.6, and rewrite this as

$$= \frac{1}{2\pi i}\left(\pi \cot\left(\pi\left(\frac{j}{N}+l\tau\right)\right) + \lim_{N\to\infty}\sum_{\substack{-N \\ n\neq 0}}^{N}\frac{1}{n}\right)$$

$$+ \frac{1}{2\pi i}\sum_{m\neq 0}\left(\pi\cot\left(\pi\left(\frac{j}{N}+l\tau+mN\tau\right)\right) - \pi\cot(\pi(mN\tau))\right).$$

Now using symmetric summation ($\lim_{M\to\infty}\sum_{-M}^{M}$) once again, the fact that the cotangent is an *odd* function gives

3.5.11 $$= \frac{1}{2\pi i}\lim_{M\to\infty}\sum_{m=-M}^{M}\pi\cot\left(\pi\left(\frac{j}{N}+l\tau+mN\tau\right)\right).$$

If $l = 0$, this is

3.5.12 $$\frac{1}{2\pi i}\left[\pi\cot\left(\frac{\pi j}{N}\right) + \lim_{M\to\infty}\sum_{m=1}^{M}\left(\pi\cot\left(\frac{\pi j}{N}+\pi mN\tau\right) - \pi\cot\left(\frac{-\pi j}{N}+\pi mN\tau\right)\right)\right].$$

If $l\neq 0$, we would like to run the *inner* sum from $-M-1$ to M. This involves *adding* a term:

3.5.13 $$\pi\cot\left(\pi\left(\frac{j}{N}+l\tau-(M+1)N\tau\right)\right) = \pi i\frac{e^{2\pi i(j/N+l\tau)}q^{-(M+1)N}+1}{e^{2\pi i(j/N+l\tau)}q^{-(M+1)N}-1}$$

$$= \pi i\frac{e^{2\pi i(j/N+l\tau)}+q^{(M+1)N}}{e^{2\pi i(j/N+l\tau)}-q^{(M+1)N}}$$

which tends to πi as $M\to\infty$ (since $|q|<1$).

So for $l\neq 0$, we add the term 3.5.12, and subtract its limit, to get

3.5.14 $$= -\frac{1}{2} + \frac{1}{2\pi i}\lim_{M\to\infty}\sum_{m=-M-1}^{M}\pi\cot\left(\pi\left(\frac{j}{N}+(l+mN)\tau\right)\right)$$

3.5.15 $$= -\frac{1}{2} + \frac{1}{2\pi i}\lim_{M\to\infty}\sum_{m=0}^{M}\left\{\pi\cot\left(\frac{\pi j}{N}+\pi(l+mN)\tau\right) - \pi\cot\left(\frac{-\pi j}{N}+\pi(N-l+mN)\tau\right)\right\}.$$

Writing $\pi\cot(\pi z)$ in terms of $e^{2\pi iz}$, we have

3.5.16 $$\pi\cot(\pi z) = \pi i\frac{e^{2\pi iz}+1}{e^{2\pi iz}-1} = \pi i - \frac{2\pi i}{1-e^{2\pi iz}},$$

and abbreviating $e^{2\pi i/N}$ as ζ, we can rewrite 3.5.12 and 3.5.15 as

3.5.17 $$\begin{cases} \dfrac{1}{2}\dfrac{\zeta^j+1}{\zeta^j-1} - \sum_{m\geq 1}\left(\dfrac{1}{1-\zeta^j q^{mN}} - \dfrac{1}{1-\zeta^{-j}q^{mN}}\right) & \text{if } l = 0\,, \\ -\dfrac{1}{2} - \sum_{m\geq 0}\left(\dfrac{1}{1-\zeta^j q^{l+mN}} - \dfrac{1}{1-\zeta^{-j}q^{N-l+mN}}\right) & \text{if } l \neq 0\,. \end{cases}$$

The desired formula 3.5.10 follows immediately upon expanding the individual terms as power series in q and collecting terms (the resulting double series in powers of q converges absolutely in $|q|<1$, so there is no subtlety in doing this!). Q.E.D.

It now only remains to combine 3.5.8 and 3.5.9, in order to prove 3.4.1. We may and will suppose f *odd*. By definition,

3.5.18 $$\begin{aligned}&(-1)\varphi_1\left(\frac{1}{2}, \omega_1, \omega_2, f\right)\\ &= -\sum_{j,l=0}^{N-1} f(j,l)\varphi_1\left(\frac{1}{2}; \omega_1, \omega_2, \frac{j\omega_1+l\omega_2}{N}\right)\\ &= -\sum_{j,l=0}^{N-1} f(j,l)\left[\frac{2\pi il}{N\omega_1} + F\left(\frac{j\omega_1+l\omega_2}{N}; \omega_1, \omega_2\right)\right] \quad \text{(by 3.5.8)}\,.\end{aligned}$$

Passing to q-expansion, we obtain from 3.5.10,

3.5.19 $$\begin{aligned}&(-1)\varphi_1\left(\frac{1}{2}; 2\pi i, 2\pi iN\tau, f\right)\\ &= -\frac{1}{N}\sum_{j,l=0}^{N-1} lf(j,l) - \frac{1}{2}\sum_{j=0}^{N-1} f(j,0)\frac{\zeta^j+1}{\zeta^j-1}\\ &\quad + \frac{1}{2}\sum_{\substack{j,l=0\\ l\neq 0}}^{N-1} f(j,l)\\ &\quad + \sum_{n\geq 1} q^n \sum_{n=dd'}\left(\sum_{j=0}^{N-1} f(j,d')\zeta^{jd} - \sum_{j=0}^{N-1} f(j,-d')\zeta^{-jd}\right)\,.\end{aligned}$$

Since f is odd, we have

3.5.20 $$\sum_{\substack{j,l\\ l\neq 0}} f(j,l) = 0$$

and we can rewrite 3.5.19 in terms of Pf (cf. 3.2.1):

3.5.21 $$\begin{aligned}&= -\frac{1}{N}\sum_{l=0}^{N-1} lPf(0,l)\\ &\quad - \frac{1}{2}\sum_{l=0}^{N-1} f(j,0)\frac{\zeta^j+1}{\zeta^j-1} + 2\sum_{N\geq 1} q^n \sum_{n=dd'} Pf(d,d')\,.\end{aligned}$$

To conclude, we must check that the constant term is correct, i.e., that for f odd, we have

3.5.22
$$\begin{cases} L(0, Pf(0, n)) = -\dfrac{1}{N}\sum_{l=0}^{N-1} l(Pf)(0, l)\,, \\ L(0, (Pf)(n, 0)) = -\dfrac{1}{2}\sum_{l=0}^{N-1} f(j, 0)\dfrac{\zeta^j + 1}{\zeta^j - 1}\,. \end{cases}$$

Recall that for *any* odd function $g(n)$ on $\mathbf{Z}/N\mathbf{Z}$, we have

3.5.23
$$L(0, g) = \text{“}\textstyle\sum_{n\geq 1} g(n)\text{”} = \sum_{n\geq 1} g(n)T^n\Big|_{T=1} = \dfrac{\sum_{n=1}^{N} g(n)T^n}{1 - T^N}\Big|_{T=1}$$
$$= \frac{-1}{N}\sum_{n=1}^{N} ng(n) \qquad \text{(by l'Hôpital).}$$

This formula, applied to $Pf(0, n)$, gives the first part of 3.5.22. Applied to $Pf(n, 0)$, it gives

3.5.24
$$\begin{aligned} L(0, Pf(n, 0)) &= -\frac{1}{N}\sum_{n=1}^{N-1} nPf(n, 0) \\ &= -\frac{1}{N}\sum_{n=1}^{N} n \sum_{j=0}^{N-1} f(j, 0)\zeta^{nj} \\ &= \frac{-1}{2N}\Big(\sum_{n=1}^{N} n\Big[\sum_{j \bmod N} f(j, 0)\zeta^{nj} + f(-j, 0)\zeta^{-nj}\Big]\Big) \\ &= \frac{-1}{2N}\sum_{j \bmod N} f(j, 0)\sum_{n=1}^{N} n(\zeta^{nj} - \zeta^{-nj}) \end{aligned}$$

(because f is odd),

and it remains only to check that for $j = 1, \cdots, N-1$

3.5.25
$$-\frac{1}{2}\frac{\zeta^j + 1}{\zeta^j - 1} = \frac{-1}{2N}\sum_{n=1}^{N-1} n(\zeta^{nj} - \zeta^{-nj})\,,$$

i.e.,

$$N(\zeta^j + 1) = \sum_{n=1}^{N-1} n(\zeta^{nj} - \zeta^{-nj})(\zeta^j - 1)\,.$$

We compute

$$\begin{aligned} N(\zeta^j + 1) &\overset{?}{=} \sum_{n=1}^{N-1} n(\zeta^{(n+1)j} - \zeta^{nj} + \zeta^{-nj} - \zeta^{(1-n)j}) \\ &= \sum_{n=2}^{N} (n-1)\zeta^{nj} - \sum_{1}^{N-1} n\zeta^{nj} + \sum_{n=1}^{N-1} n\zeta^{-nj} \\ &\quad - \sum_{n=0}^{N-2}(n+1)\zeta^{-nj} \\ &= -\sum_{n=2}^{N} \zeta^{nj} + N - \zeta^j - \sum_{n=0}^{N-2} \zeta^{-nj} + (N-1)\zeta^{-(N-1)j} \\ &= \zeta^j + N - \zeta^j + \zeta^{-(N-1)j} + (N-1)\zeta^{-(N-1)j} \\ &= N + \zeta^j + (N-1)\zeta^j = N(1 + \zeta^j)\,. \end{aligned}$$

Q.E.D.

3.6. *Algebrifying the Eisenstein series $\varphi_k(k/2; \omega_1, \omega_2, f)$; the forms $G_{k,s,f}$.* As already remarked (3.0.10), it is more natural to think of $\varphi_k(s; L, f)$, where L is a lattice in C and f is a function on $(1/N)L/L$. It is even better to think of this as $\varphi_k(s; E, \omega, f)$, where (E, ω) is an elliptic curve with differential over C, and f is a function on the group ${}_N E$.

Now intrinsically, we can view the *partial* Fourier transforms P^{-1} and P (3.2.1, 3.2.2) as carrying functions on $\mathbf{Z}/N\mathbf{Z} \times \mathbf{Z}/N\mathbf{Z}$ to functions on $\boldsymbol{\mu}_N \times \mathbf{Z}/N\mathbf{Z}$, and inversely: given f on $\mathbf{Z}/N\mathbf{Z} \times \mathbf{Z}/N\mathbf{Z}$, $P^{-1}f$ is the function on $\boldsymbol{\mu}_N \times \mathbf{Z}/N\mathbf{Z}$,

3.6.1 $$(P^{-1}f)(\zeta, m) = \frac{1}{N}\sum\nolimits_{n \bmod N} f(n, m)\zeta^{-n} ,$$

and given g on $\boldsymbol{\mu}_N \times \mathbf{Z}/N\mathbf{Z}$, Pg is the function on $\mathbf{Z}/N\mathbf{Z} \times \mathbf{Z}/N\mathbf{Z}$

3.6.2 $$(Pg)(n, m) = \sum\nolimits_{\zeta \in \boldsymbol{\mu}_N} g(\zeta, m)\zeta^{n} .$$

Now suppose (E, ω, β) is a $\Gamma(N)^{\text{arith}}$-test object over C, and f is a function on $\mathbf{Z}/N\mathbf{Z} \times \mathbf{Z}/N\mathbf{Z}$. Then $P^{-1}f$ is a function on $\boldsymbol{\mu}_N \times \mathbf{Z}/N\mathbf{Z}$, which we transport by $\beta\colon \boldsymbol{\mu}_N \times \mathbf{Z}/N\mathbf{Z} \xrightarrow{\sim} {}_N E$ to a function on ${}_N E$. This allows us to form

3.6.3 $$\varphi_k(s; E, \omega, P^{-1}f \circ \beta^{-1}) .$$

If we think of the test object (E, ω, β) over C as varying, it is natural to view the construction

3.6.4 $$(E, \omega, \beta) \longmapsto \varphi_k(s; E, \omega, P^{-1}f \circ \beta^{-1})$$

as providing a sort of "C^∞ modular form of weight k on $\Gamma(N)^{\text{arith}}$."

At the risk of deranging the reader, it will also be convenient to make a shift in the variable s, so that $s = 0$ rather than $s = k/2$ becomes the "good" point.

Definition 3.6.5.

$$G_{k,s,f}(E, \omega, \beta) \overset{\text{dfn}}{=} \frac{(-1)^k}{2}\varphi_k\Big(s + \frac{k}{2}; E, \omega, (P^{-1}f)\circ\beta^{-1}\Big) .$$

In terms of the lattice L corresponding to (E, ω), $(P^{-1}f)\circ\beta^{-1}$ becomes a function $g(l/N)$ on $(1/N)L/L$, and for $\operatorname{Re}(s) > 1 - k/2$, we have the series representation

3.6.6 $$G_{k,s,f}(E, \omega, \beta) = \frac{(-1)^k}{2}\Gamma(s + k)\Big(\frac{a(L)}{N\pi}\Big)^s \sum\nolimits_{l \neq 0} \frac{g(l/N)}{(l/N)^k |l/N|^{2s}} .$$

The functional equation 3.0.9 becomes

3.6.7 $$G_{k,s,f} = G_{k,1-s-k,f^t} .$$

The differentiation formula 3.1.10 becomes

3.6.8 $$NW(G_{k,s,f}) = G_{k+2,s-1,f} .$$

We may sum up the main results of Sections 3.2–3.5 in the following theorem.

THEOREM 3.6.9. *Let $k \geqq 1$. Let f be a complex-valued function on $\mathbf{Z}/N\mathbf{Z} \times \mathbf{Z}/N\mathbf{Z}$. In the exceptional case $k = 2$, suppose also that $\sum_j f(j, 0) = \sum_l f(0, l) = 0$. Then the value $G_{k,0,f} = G_{k,s,f}|_{s=0}$ is a modular form of weight k on $\Gamma(N)^{\text{arith}}$, defined over $\mathbf{Q}$ [the values of f], whose q-expansion is given by the formulas:*

3.6.10 $$G_{1,0,f}(\mathrm{Tate}(q^N), \omega_{\mathrm{can}}, \beta_{\mathrm{can}}) = \begin{cases} 0 & f \textit{ even}, \\ \frac{1}{2}L(0, f(n, 0) + f(0, n)) + \sum_{n \geqq 1} q^n \sum_{n=dd'} f(d, d') & f \textit{ odd}, \end{cases}$$

and for $k \geqq 2$,

3.6.11 $$G_{k,0,f}(\mathrm{Tate}(q^N), \omega_{\mathrm{can}}, \beta_{\mathrm{can}}) = \begin{cases} 0 & \textit{if } f \textit{ is of parity } k-1, \\ \frac{1}{2}L(1-k, f(n, 0)) + \sum_{n \geqq 1} q^n \sum_{n=dd'} d^{-1} f(d, d') & \\ & \textit{if } f \textit{ is of parity } k. \end{cases}$$

Proof. Given the q-expansion computations of 3.2–3.5, everything follows from the q-expansion principle and GAGA (cf. 2.4). (The restrictions on f in case $k = 2$ are just the partial Fourier transforms of those occurring in 3.3.1.)

Remark 3.6.12. In the case $k = 2$, the two forbidden functions are $f_1 =$ the characteristic function of $\mathbf{Z}/N\mathbf{Z} \times \{0\}$, and $f_2 = (f_1)^t$. Their partial transforms $P^{-1}f_1$ and $P^{-1}f_2$ are respectively the characteristic function of $(0, 0)$ and the constant function $1/N$. Referring to the series definition 3.6.6, we see that in terms of the lattice L corresponding to (E, ω), we have

3.6.13 $$\begin{cases} G_{2,0,\,\text{char. fct. of } \mathbf{Z}/N\mathbf{Z} \times \{0\}}(E, \omega, \beta) = \frac{1}{2}\lim_{s \to 0} \sum_{l \neq 0} \frac{2}{l^2 |l|^{2s}} = -\frac{1}{24} S(L), \\ G_{2,0,\,\text{char. fct. of } \{0\} \times \mathbf{Z}/N\mathbf{Z}}(E, \omega, \beta) = \frac{1}{2}\lim_{s \to 0} \sum_{l \neq 0} \frac{1/N}{(l/N)^2 |l/N|^{2s}} = -\frac{N}{24} S(L), \end{cases}$$

where $S(L)$ is the "position of $H^{0,1}$" C^∞ modular form (cf. 1.3).

Chapter IV. Damerell's theorem

4.0. *Formulation and proof the theorem.*

4.0.1. Let $N \geqq 1$ be an integer, K a finite extension of $\mathbf{Q}$, and (E, ω, β) a $\Gamma(N)^{\text{arith}}$-test object over K. We assume that the curve E has complex multiplication, and that all of its complex multiplications are defined over K. The representation of $\mathrm{End}(E)$ on $H^0(E, \Omega^1_{E/K})$ allows us to view $\mathrm{End}(E)$ as an *order* in a subfield $K_0 \subset K$, which we know to be quadratic imaginary over $\mathbf{Q}$. We denote by $\alpha \mapsto \bar{\alpha}$ the unique non-trivial automorphism of K_0.

Given an element $\alpha \in \operatorname{End}(E) \subset K_0$, we denote by $[\alpha]$ the corresponding endomorphism of E, but we think of α itself as an element of $K_0 \subset K$. Thus $[\alpha]^*(\omega) = \alpha\omega$.

4.0.2 If we choose an embedding $K \hookrightarrow \mathbf{C}$, we obtain by extension of scalars a $\Gamma(N)^{\text{arith}}$-test object $(E_{\mathbf{C}}, \omega_{\mathbf{C}}, \beta_{\mathbf{C}})$ over $\mathbf{C}$, which we may view transcendentally as being a point $(\omega_1, \omega_2) \in \mathrm{GL}^+$, well defined mod $\Gamma(N)$ (cf. 2.4). We also obtain inclusions of rings of modular forms

4.0.3 $$R^\cdot(K, \Gamma(N)^{\text{arith}}) \hookrightarrow R^\cdot(\mathbf{C}, \Gamma(N)^{\text{arith}}) \hookrightarrow C^\infty(\mathrm{GL}^+/\Gamma(N)) .$$

The $\mathbf{Z}[1/12]$ algebra of operators $\mathcal{Z}$ introduced in 1.6 operates on the ring $C^\infty(\mathrm{GL}^+/\Gamma(N))$, but of course it does *not* leave stable the subring $R^\cdot(K, \Gamma(N)^{\text{arith}})$. We denote by $\mathcal{Z}R^\cdot(K, \Gamma(N))$ the smallest $\mathcal{Z}$-submodule of $C^\infty(\mathrm{GL}^+/\Gamma(N))$ which contains $R^\cdot(K, \Gamma(N)^{\text{arith}})$.

THEOREM 4.0.4. *Hypotheses and notations as above, let F be an element of $\mathcal{Z}R^\cdot(K, \Gamma(N)^{\text{arith}})$. Then the complex number*

$$F(\omega_1, \omega_2) = F(E_{\mathbf{C}}, \omega_{\mathbf{C}}, \beta_{\mathbf{C}})$$

lies in K, and, as an element of K, is independent of the choice of the embedding $K \hookrightarrow \mathbf{C}$.

Proof. According to 1.6.3, any element of $\mathcal{Z}$ is a $\mathbf{Z}[1/12]$ linear combination of the monomials $\mathbf{S}^a \boldsymbol{g}_2^b \boldsymbol{g}_3^c \mathbf{D}^d \mathbf{H}^e$. Since the operators H, D, and (multiplication by) g_2, g_3 are all stable on $R^\cdot(K, \Gamma(N)^{\text{arith}})$, it follows that any element of $\mathcal{Z}R^\cdot(K, \Gamma(N)^{\text{arith}})$ is a sum of elements of the form

$$S^n \times \text{an element of } R^\cdot(K, \Gamma(N)^{\text{arith}}) , \qquad n = 0, 1, 2, \cdots .$$

The assertion of the theorem is essentially tautologous for $F \in R^\cdot(K, \Gamma(N)^{\text{arith}})$ (compare 2.4), so we are reduced to checking its truth for the function S. It is at this point that we use the hypothesis of complex multiplication. The chosen embedding $K \hookrightarrow \mathbf{C}$ allows us to speak of the usual singular cohomology group $H^1_{\text{sing}}(E_{\mathbf{C}}, \mathbf{C})$, which we can also view as algebraic de Rham cohomology:

4.0.5 $$H^1_{\text{sing}}(E_{\mathbf{C}}, \mathbf{C}) \xrightarrow{\sim} H^1_{\text{DR}}(E_{\mathbf{C}}/\mathbf{C}) \xrightarrow{\sim} H^1_{\text{DR}}(E/K) \otimes_K \mathbf{C} .$$

The subspace $H^1_{\text{DR}}(E/K)$ sits in $H^1_{\text{sing}}(E_{\mathbf{C}}, \mathbf{C})$ as the K-span of the cohomology classes of $\omega = dx/y$ and $\eta = xdx/y$ (compare 1.2). The de Rham cup-product $\langle , \rangle_{\text{DR}} = (1/2\pi i)\langle , \rangle_{\text{top}}$ on $H^1_{\text{sing}}(E_{\mathbf{C}}, \mathbf{C})$ takes values in K on the subspace $H^1_{\text{DR}}(E/K)$ (in fact it is the unique alternating form satisfying $\langle \omega, \eta \rangle_{\text{DR}} = 1$). The cohomological expression (1.3.6) for S

4.0.6 $$S(L) = 12 \frac{\langle \bar{\omega}, \eta \rangle_{\text{DR}}}{\langle \bar{\omega}, \omega \rangle_{\text{DR}}}$$

does not change if we replace $\bar{\omega}$ by *any* non-zero element of $H^{0,1}(E_{\mathbf{C}})$. So we need only see that there is a non-zero element $\xi \in H^1_{\mathrm{DR}}(E/K)$ which, for any embedding $K \hookrightarrow \mathbf{C}$, lands in $H^{0,1}(E_{\mathbf{C}})$ under the isomor phism 4.0.5. This results from the following lemma.

LEMMA 4.0.7. *Hypotheses as above, the subspace*

$$H^{0,1}(E_{\mathbf{C}}) \cap H^1_{\mathrm{DR}}(E/K) \subset H^1_{\mathrm{DR}}(E/K)$$

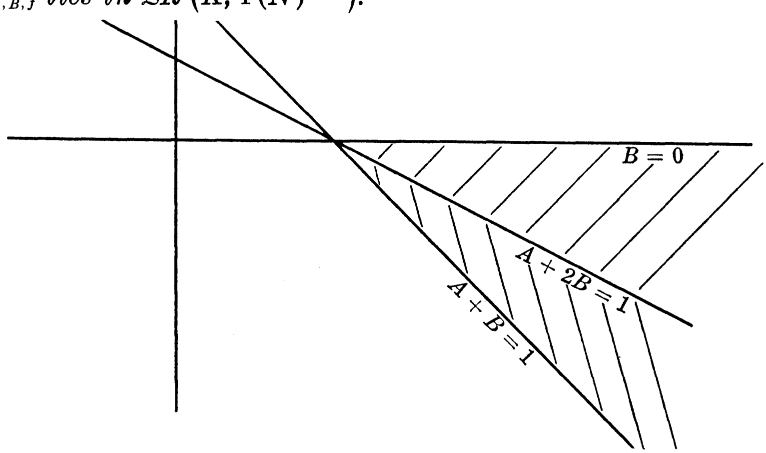
is non-zero, and it is independent of the choice of embedding $K \hookrightarrow \mathbf{C}$. *In fact, for any* $[\alpha] \in \mathrm{End}(E)$ *with* $\alpha \notin \mathbf{Z}$, *it is the* $\bar{\alpha}$-*eigenspace of* $[\alpha]^*$ *acting on* $H^1_{\mathrm{DR}}(E/K)$.

Proof. The endomorphism $[\alpha]$ acts (as $[\alpha]^*$) on both $H^1_{\mathrm{DR}}(E/K)$ and on $H^1_{\mathrm{sing}}(E_{\mathbf{C}}, \mathbf{C})$, compatibly with isomorphism 4.0.5. It has the distinct eigenvalues α and $\bar{\alpha}$. Because the action of $[\alpha]$ on $H^1_{\mathrm{sing}}(E_{\mathbf{C}}, \mathbf{C})$ respects $H^1_{\mathrm{sing}}(E_{\mathbf{C}}, \mathbf{Z})$; it commutes with complex conjugation. So from the tautological relation $[\alpha]^*(\omega) = \alpha\omega$ we deduce that $[\alpha]^*(\bar{\omega}) = \bar{\alpha}\bar{\omega}$. Thus the Hodge decomposition $H^1_{\mathrm{sing}}(E_{\mathbf{C}}, \mathbf{C}) = H^{1,0}(E_{\mathbf{C}}) \oplus H^{0,1}(E_{\mathbf{C}})$ is simply the eigenspace decomposition of $[\alpha]^*$. In particular, the subspace $H^{0,1}(E_{\mathbf{C}}) \cap H^1_{\mathrm{DR}}(E/K)$ is just the $\bar{\alpha}$-eigenspace of $[\alpha]^*$ on $H^1_{\mathrm{DR}}(E/K)$. An explicit rational projector onto it is $(1/(\bar{\alpha} - \alpha))([\alpha]^* - \alpha)$. Q.E.D.

4.0.8. *Question.* The proof we have given actually shows that Damerell's theorem is true for any lattice $L \subset \mathbf{C}$ such that $g_2(L)$, $g_3(L)$, and $S(L)$ are simultaneously algebraic. Does any such lattice L have complex multiplication? Equivalently, if an elliptic curve E over a number field K has the Hodge decomposition of its complex H^1 induced from a splitting of its algebraic de Rham H^1 over K, does E have complex multiplication?

4.1. *Concrete applications.*

LEMMA 4.1.0. *Let* (A, B) *be a pair of integers satisfying* $A + B \geqq 1$, $B \leqq 0$. *Then for any* K-*valued function* f *on* $\mathbf{Z}/N\mathbf{Z} \times \mathbf{Z}/N\mathbf{Z}$, *the* C^∞ *modular form* $G_{A,B,f}$ *lies in* $\mathcal{Z}R^\cdot(K, \Gamma(N)^{\mathrm{arith}})$.



Proof. For $k \geqq 1$, we know that $G_{k,0,f}$ is either itself an element of $R^{\cdot}(K, \Gamma(N)^{\mathrm{arith}})$, if $k \neq 2$, or is the sum of such an element and a K-multiple of S (cf. 3.6.12). Thus $G_{k,0,f}$ lies in $\mathcal{Z}R^{\cdot}(K, \Gamma(N)^{\mathrm{arith}})$ for $k \geqq 1$. For each integer $r \geqq 0$, the differentiation formula (cf. 3.6.8)

4.1.1 $$N^r W^r(G_{k,0,f}) = G_{k+2r,-r,f}$$

shows that $G_{k+2r,-r,f}$ lies in $\mathcal{Z}R^{\cdot}(K, \Gamma(N)^{\mathrm{arith}})$ for $k \geqq 1$, $r \geqq 0$. The functional equation (3.6.7) gives

4.1.2 $$G_{k+2r,-r,f} = G_{k+2r,1-k-r,f^t}$$

which shows that $G_{k+2r,1-k-r,f}$ lies in $\mathcal{Z}R_{\cdot}(K, \Gamma(N)^{\mathrm{arith}})$ for $k \geqq 1$, $r \geqq 0$. If we put $(A, B) = (k + 2r, -r)$, the conditions $k \geqq 1$, $r \geqq 0$ become the conditions $A + 2B \geqq 1$, $B \leqq 0$. If we put $(A, B) = (k + 2r, 1 - k - r)$, the conditions $k \geqq 1$, $r \geqq 0$ become the conditions $A + 2B \leqq 1$, $A + B \geqq 1$. Q.E.D.

Applying 4.0.4 to the $G_{A,B,f}$, we find

COROLLARY 4.1.3. *Hypotheses as in* 4.0, *let* A, B *be integers satisfying* $A + B \geqq 1$, $B \leqq 0$. *Then for any K-valued function f on* $\mathbf{Z}/N\mathbf{Z} \times \mathbf{Z}/N\mathbf{Z}$, *the complex numbers* $G_{A,B,f}(E_{\mathbf{C}}, \omega_{\mathbf{C}}, \beta_{\mathbf{C}})$ *lie in* K, *and there they are independent of the chosen embedding* $K \hookrightarrow \mathbf{C}$.

We now turn to the explicit transcendental expression of the functions $G_{A,B,f}$. Let L denote the period lattice of $(E_{\mathbf{C}}, \omega_{\mathbf{C}})$. Because E has complex multiplication, the two-dimensional $\mathbf{Q}$-space $L \otimes_{\mathbf{Z}} \mathbf{Q}$ is a one-dimensional K_0-space, with basis any *period* $\Omega = \int_{\gamma} \omega$ of $\omega_{\mathbf{C}}$ over a non-zero element $\gamma \in \pi_1(E_{\mathbf{C}})$. Thus

4.1.4 $$L = \Omega M$$

where M is a lattice which lies in the subfield $K_0 \subset \mathbf{C}$.

Now suppose in addition that $K \ni \zeta_N$, a primitive N'th root of unity. Then as f runs over all K-valued functions on $\mathbf{Z}/N\mathbf{Z} \times \mathbf{Z}/N\mathbf{Z}$, $g = P^{-1}f \circ \beta^{-1}$ runs over all K-valued functions on ${}_N(E_{\mathbf{C}}) \simeq (1/N)L/L \simeq M/NM$. The transcendental expression for $G_{A,B,f}(E_{\mathbf{C}}, \omega_{\mathbf{C}}, \beta_{\mathbf{C}})$ (cf. 3.6.6)

4.1.5 $$\frac{(-1)^A}{2}(A + B - 1)!\left(\frac{a(\Omega M)}{N\pi}\right)^B \left(\sum_{\substack{m \in M \\ m \neq 0}} \frac{g(m)}{\left(\dfrac{\Omega m}{N}\right)^A \left|\dfrac{\Omega m}{N}\right|^{2B} \left|\dfrac{\Omega m}{N}\right|^{2s}}\right)\Bigg|_{s=0}$$

may be rewritten as

4.1.6 $$\frac{(-1)^A(A + B - 1)!\, N^{A+B} a(M)^B}{2\Omega^A \pi^B}\left(\sum_{\substack{m \in M \\ m \neq 0}} \frac{g(m)}{m^A \mathbf{N}(m)^{B+s}}\right)\Bigg|_{s=0}$$

where $\mathbf{N}\colon K_0 \to \mathbf{Q}$ denotes the *norm* mapping.

Conversely, it is well known that any collection of data

4.1.7
$$\begin{cases} \text{a quadratic imaginary field } K_0 \\ \text{an embedding } K_0 \hookrightarrow \mathbf{C} \\ \text{a lattice } M \subset K_0 \\ \text{a function } g\colon M/NM \to \mathbf{C} \text{ with algebraic values} \end{cases}$$

arises from a suitable $\Gamma(N)^{\text{arith}}$-test object (E, ω, β) over a finite extension K of K_0, whose underlying elliptic curve has complex multiplication ring $\operatorname{End}(E) = \{\alpha \in K_0 \mid \alpha M \subset M\}$. There is of course a great deal of indeterminacy in choosing the Ω such that the lattice ΩM will define the complexification $(E_{\mathbf{C}}, \omega_{\mathbf{C}})$ of the putative (E, ω): *any* complex number $\Omega \in \mathbf{C}$ such that *both* the numbers

4.1.8
$$g_2(\Omega M) = \frac{60}{\Omega^4}\sum_{\substack{m \in M \\ m \neq 0}} \frac{1}{m^4}, \quad g_3(\Omega M) = \frac{140}{\Omega^6}\sum_{\substack{m \in M \\ m \neq 0}} \frac{1}{m^6}$$

are *algebraic* will do.

COROLLARY 4.1.9. *Given data 4.1.7 as above, let $\Omega \in \mathbf{C}$ be such that both $g_2(\Omega M)$ and $g_3(\Omega M)$ are algebraic. Then for any integers A, B satisfying $A + B \geqq 1$, $B \leqq 0$, the value*

$$\frac{1}{\Omega^A \pi^B}\sum_{\substack{m \in M \\ m \neq 0}} \frac{g(m)}{m^A \mathbf{N}(m)^{B+s}}\bigg|_{s=0}$$

is an algebraic number.

Chapter V. Review of the p-adic theory

5.0. *Trivializations.*

5.0.0. Fix a prime number p. A ring which is complete and separated in its p-adic topology will be called a p-adic ring. Given an elliptic curve E over a p-adic ring B, a trivialization of E/B is by definition an isomorphism of formal groups over B,

5.0.1
$$\varphi\colon \hat{E} \xrightarrow{\sim} \hat{\mathbf{G}}_m .$$

For *any* integer $N \geqq 1$, we say that a $\Gamma(N)^{\text{arith}}$-structure β on E/B is *compatible* with φ if, when we write $N = N_0 p^r$ with $(p, N_0) = 1$, the composite map

5.0.2
$$\boldsymbol{\mu}_{p^r} \xhookrightarrow{\beta} \hat{E} \xrightarrow[\sim]{\varphi} \hat{\mathbf{G}}_m$$

is the inclusion. Similary, we say that a $\Gamma_{00}(N)^{\text{arith}}$-structure

5.0.3
$$i\colon \boldsymbol{\mu}_N \hookrightarrow {}_N E$$

is compatible with φ if the composite

5.0.4 $$\mu_{p^r} \overset{i}{\hookrightarrow} \hat{E} \overset{\varphi}{\xrightarrow{\sim}} \hat{\mathbf{G}}_m$$

is the inclusion. (Thus for any $r \geqq 0$, a trivialized curve (E, φ) admits a *unique* $\Gamma_{00}(p^r)^{\text{arith}}$-structure compatible with φ, and in fact φ itself if precisely a compatible system of $\Gamma_{00}(p^r)^{\text{arith}}$-structures on E/B for all $r \geqq 0$.) Finally, we say that a $\Gamma_{00}(N)^{\text{naive}}$-structure

5.0.5 $$j \colon \mathbf{Z}/N\mathbf{Z} \hookrightarrow {}_N E$$

is compatible with φ if, once again with $N = p^r N_0$, $(p, N) = 1$, the underlying $\Gamma_{00}(p^r)^{\text{naive}}$ structure $j \mid N_0\mathbf{Z}/N\mathbf{Z}$ satisfies

5.0.6 $$e_{p^r}(\varphi^{-1}(\zeta), j(N_0)) = \zeta \qquad \text{for all } \zeta \in \mu_{p^r} .$$

5.1. *Generalized p-adic modular functions* (compare 2.1 and 2.5).

5.1.0. The functor "isomorphism classes of trivialized $\Gamma(N)^{\text{arith}}$-elliptic curves (E, φ, β)" is *represented* by a p-adic ring $V(\mathbf{Z}_p, \Gamma(N)^{\text{arith}})$. For any p-adic ring B, the same functor restricted to B-algebras is represented by $V(\mathbf{Z}_p, \Gamma(N)^{\text{arith}}) \hat{\otimes}_{\mathbf{Z}_p} B$, sometimes denoted $V(B, \Gamma(N)^{\text{arith}})$. For example, if $N = 1$, we have

5.1.1 $$V(\mathbf{Z}_p, \Gamma(1)) \xrightarrow{\sim} \varprojlim V(\mathbf{Z}/p^n\mathbf{Z}, \Gamma(1))$$

and, viewing φ as a compatible system of $\Gamma_{00}(p^n)^{\text{arith}}$-structures,

5.1.2 $$\begin{aligned} V(\mathbf{Z}/p^n\mathbf{Z}, \Gamma(1)) &= \varinjlim_r \left(\text{the coordinate ring of } M(\Gamma_{00}(p^r)^{\text{arith}}) \otimes_{\mathbf{Z}} \mathbf{Z}/p^n\mathbf{Z}\right) \\ &= \varinjlim_r R^0(\mathbf{Z}/p^n\mathbf{Z}, \Gamma_{00}(p^r)^{\text{arith}}) ; \end{aligned}$$

similarly for $\Gamma_{00}(N)^{\text{arith}}$ and $\Gamma_{00}(N)^{\text{naive}}$.

5.1.3. An element $F \in V(B, \Gamma(N)^{\text{arith}})$ is called a $\Gamma(N)^{\text{arith}}$ generalized p-adic modular function. On any trivialized $\Gamma(N)^{\text{arith}}$ "test object" (E, φ, β) over a p-adic B-algebra B', such an F has a *value* $F(E, \varphi, \beta) \in B'$, which depends only on the isomorphism class of (E, φ, β), and whose formation commutes with extension of scalars of p-adic B-algebras. In this optic, F "is" its value on the universal trivialized $\Gamma(N)^{\text{arith}}$-curve $(E_{\text{univ}}, \varphi_{\text{univ}}, \beta_{\text{univ}})$, defined over $V(B, \Gamma(N)^{\text{arith}})$; similarly for $\Gamma_{00}(N)^{\text{arith}}$ and $\Gamma_{00}(N)^{\text{naive}}$.

Remark 5.1.4. If we restrict N to be prime to p, we also have the notion of trivialized $\Gamma(N)^{\text{naive}}$-elliptic curves, and the corresponding rings $V(B, \Gamma(N)^{\text{naive}})$. As explained in 2.0.8, we have

5.1.4.0 $$V(B, \Gamma(N)^{\text{naive}}) \xrightarrow{\sim} V(B, \Gamma(N)^{\text{naive}}) \otimes_{\mathbf{Z}} \mathbf{Z}[1/N, \zeta_N] \quad \text{if } (p, N) = 1,$$

so that there is nothing essentially "new" here.

5.2. *q-expansions: the q-expansion principle.*

5.2.0. The Tate curve Tate (q^N), viewed over $\widehat{\mathbf{Z}_p((q))} \overset{\text{dfn}}{=}$ the p-adic completion of $\mathbf{Z}((q))$, has a canonical trivialization φ_{can} (think of Tate (q^N) as the quotient of $\mathbf{G}_m$ by the discrete subgroup $q^{N\mathbf{Z}}$; its formal group "is" $\hat{\mathbf{G}}_m$), with which β_{can} is compatible. *Evaluation* on $(\text{Tate}(q^N), \varphi_{\text{can}}, \beta_{\text{can}})$ defines an injective q-expansion homomorphism

5.2.1 $$V(B, \Gamma(N)^{\text{arith}}) \hookrightarrow B((\hat{q}))$$

such that the cokernel $B((\hat{q}))/V(B, \Gamma(N)^{\text{arith}})$ is B-flat.

5.2.2. If $B \subset B'$, then $V(B, \Gamma(N)^{\text{arith}}) \subset V(B', \Gamma(N)^{\text{arith}})$, and an element $F \in V(B', \Gamma(N)^{\text{arith}})$ lies in $V(B, \Gamma(N)^{\text{arith}})$ if and only if its q-expansion lies in $B((\hat{q}))$.

5.2.3. The corresponding q-expansions for $\Gamma_{00}(N)^{\text{naive}}$ and $\Gamma_{00}(N)^{\text{arith}}$ are defined by evaluating at $(\text{Tate}(q^N), \varphi_{\text{can}}, j_{\text{can}})$ and at $(\text{Tate}(q), \varphi_{\text{can}}, i_{\text{can}})$ respectively. The analogues of 5.2.1 and 5.2.2. hold.

5.3. *The action of the group $G(N)$; weight and nebentypus.*

5.3.0. The group $\mathbf{Z}_p^\times$ acts on $V(B, \Gamma(N)^{\text{arith}})$ through its action on the trivialization φ and its "correcting" action on the p-part of β. More generally, consider the subgroup

5.3.1 $$G(N) \subset \mathbf{Z}_p^\times \times (\mathbf{Z}/N\mathbf{Z})^\times$$

of all elements $(a, b) \in \mathbf{Z}_p^\times \times (\mathbf{Z}/N\mathbf{Z})^\times$ such that, writing $N = p^r N_0$, $(p, N_0) = 1$, we have $b \bmod p^r \equiv a \bmod p^r$. Thus $G(N) \xrightarrow{\sim} \mathbf{Z}_p^\times \times (\mathbf{Z}/N_0\mathbf{Z})^\times$.

5.3.2. We define the action of $G(N)$ on the rings $V(B, \Gamma(N)^{\text{arith}})$, resp. $\Gamma_{00}(N)^{\text{arith}}$ and $\Gamma_{00}(N)^{\text{naive}}$, by the formulas

5.3.3 $$\begin{cases} [a, b]F(E, \varphi, \beta) = F(E, a^{-1}\varphi, \beta \circ (b, b^{-1})) & \text{for } \Gamma(N)^{\text{arith}}, \\ [a, b]F(E, \varphi, i) = F(E, a^{-1}\varphi, bi) & \text{for } \Gamma_{00}(N)^{\text{arith}}, \\ [a, b]F(E, \varphi, j) = F(E, a^{-1}\varphi, b^{-1}j) & \text{for } \Gamma_{00}(N)^{\text{naive}}. \end{cases}$$

Given a continuous character

5.3.4 $$\chi\colon G(N) \longrightarrow B^\times,$$

we say that an element $F \in V(B, \Gamma(N)^{\text{arith}})$ is of *weight* χ if

5.3.5 $$[a, b]F = \chi(a, b)F \qquad \text{for all } (a, b) \in G(N);$$

similarly for $\Gamma_{00}(N)^{\text{arith}}$ and $\Gamma_{00}(N)^{\text{naive}}$. If the character χ happens to be a product $\chi = \chi_k \cdot \rho$ where

5.3.6 $$\begin{cases} k \in \mathbf{Z}, \text{ and } \chi_k \text{ is the character } \chi_k(a, b) = a^k, \\ \rho \text{ is a character of } \textit{finite order} \text{ of } G(N), \end{cases}$$

then we sometimes say "weight k and nebentypus ρ" instead.

5.4. *Relation to true modular forms, via magic differentials.*

5.4.0. Given a trivialization $\varphi: \hat{E} \xrightarrow{\sim} \hat{\mathbf{G}}_m$ on E/B, we can use it to pull back the standard invariant differential $dT/(1+T)$ on $\hat{\mathbf{G}}_m$, thus obtaining a nowhere vanishing invariant differential $\varphi^*(dT/(1+T))$ on $\hat{E}$, which is necessarily the restriction to $\hat{E}$ of a unique nowhere vanishing invariant differential ω_φ on all of E.

Notice that if B is *flat* over $\mathbf{Z}_p$, i.e., $B \subset B \otimes \mathbf{Q}$, then φ is uniquely determined by the differential ω_φ. Given *any* nowhere vanishing invariant differential ω on E, one can *determine* if it is magic by picking a formal parameter, say u, for $\hat{E}$, integrating ω formally over $B \otimes \mathbf{Q}$,

5.4.1 $$\omega = d\psi(u), \quad \psi(u) = \textstyle\sum_{n \geq 1} a_n u^n \text{ with } a_n \in B \otimes \mathbf{Q} ,$$

and "checking" to see whether the series

5.4.2 $$\varphi(u) \overset{\text{dfn}}{=} \exp\left(\psi(u)\right) ,$$

a priori in $(B \otimes \mathbf{Q})[[u]]$, actually has coefficients laying in B. If it does, then $u \mapsto \varphi(u)$ is the trivialization, and $\omega = \varphi^*(dT/(1+T))$.

5.4.3. For example, if B is the ring of integers in a finite extension of $\mathbf{Q}_p$, with residue field $\mathbf{F}_q$, and E/B is an ordinary elliptic curve with differential ω, then there exists a unit $c \in$ the completion of the maximal unramified extension B_∞ of B such that $c\omega$ is magic. Furthermore, if we denote by σ the Frobenius automorphism of B_∞/B, then, according to Tate [5]

5.4.4 $c^\sigma/c =$ the p-adic unit eigenvalue of Frobenius relative to $\mathbf{F}_q$ on the elliptic curve $E \otimes \mathbf{F}_q$,

and if $B = \mathbf{Z}_p$ itself, then the magic differentials over B_∞ are *exactly* the differentials $c\omega$, where $c \in B_\infty^\times$ satisfies 5.4.4.

The construction

5.4.5 $$(E, \varphi, \beta) \longmapsto (E, \varphi^*(dT/(1+T)), \beta)$$

allows us to define by transposition a ring homomorphism $F \mapsto \tilde{F}$:

5.4.6 $$\begin{cases} R^\cdot(B, \Gamma(N)^{\text{arith}}) \longrightarrow V(B, \Gamma(N)^{\text{arith}}) \\ \tilde{F}(E, \varphi, \beta) \overset{\text{dfn}}{=} F(E, \varphi^*(dT/1+T), \beta) , \end{cases}$$

which preserves q-expansions:

5.4.7 $$\begin{array}{ccc} R^\cdot(E, \Gamma(N)^{\text{arith}}) & \longrightarrow & V(B, \Gamma(N)^{\text{arith}}) \\ {\scriptstyle q\text{-expansion}} \big\downarrow & & \big\downarrow {\scriptstyle q\text{-expansion}} \\ B((q)) & \hookrightarrow & \widehat{B((q))} \end{array} \quad ;$$

similarly for $\Gamma_{00}(N)^{\text{arith}}$ and $\Gamma_{00}(N)^{\text{naive}}$.

Before stating the next compatibility, let us recall the action of $b \in (\mathbf{Z}/N\mathbf{Z})^{\times}$ on the rings $R^{\cdot}(B, \Gamma(N)^{\text{arith}})$, resp. $\Gamma_{00}(N)^{\text{arith}}$ and $\Gamma_{00}(N)^{\text{naive}}$, defined by

5.4.8
$$\begin{cases} [b]F(E, \omega, \beta) = F(E, \omega, \beta \circ (b, b^{-1})) & \text{for } \Gamma(N)^{\text{arith}}\,, \\ [b]F(E, \omega, i) = F(E, \omega, bi) & \text{for } \Gamma_{00}(N)^{\text{arith}}\,, \\ [b]F(E, \omega, j) = F(E, \omega, b^{-1}j) & \text{for } \Gamma_{00}(N)^{\text{naive}}\,. \end{cases}$$

An element F in one of these rings is said to be of *nebentypus* ρ for $\rho \in \operatorname{Hom}((\mathbf{Z}/N\mathbf{Z})^{\times}, B^{\times})$, if it satisfies

5.4.9
$$[b]F = \rho(b)F \qquad \text{for all } b \in (\mathbf{Z}/N\mathbf{Z})^{\times}.$$

LEMMA 5.4.10. *Under the homomorphisms* 5.4.6 *for* $\Gamma(N)^{\text{arith}}$, $\Gamma_{00}(N)^{\text{arith}}$ *and* $\Gamma_{00}(N)^{\text{naive}}$, *if F is a true modular form of weight k and nebentypus ρ, then $\tilde{F}$ is of "weight k and nebentypus ρ_0" in the sense of* 5.3.6, *where ρ_0 is the character of $G(N)$ defined by $\rho_0(a, b) = \rho(b)$.*

Proof. This follows from the definitions 5.3.3, 5.3.6, and 5.4.9. Q.E.D.

Remark 5.4.11. If $F \in R^k(B, \Gamma(N)^{\text{arith}})$ is not of nebentypus, we can only assert that $\tilde{F} \in V(B, \Gamma(N)^{\text{arith}})$ has weight k over the open subgroup $\mathbf{Z}_p \times \{1\} \cap G(N)$ in $G(N)$, in the sense that, writing $N = p^r N_0$ with $(p, N_0) = 1$ we have

5.4.12
$$[a, l]\tilde{F} = a^k \tilde{F} \quad \text{if } a \in \mathbf{Z}_p^{\times},\ a \equiv 1(p^r)\,.$$

5.5. *The Frobenius endomorphism.*

5.5.0. Let (E, φ, β) be a trivialized $\Gamma(N)^{\text{arith}}$ elliptic curve. We wish to define its Frobenius transform (E', φ', β'). We define

5.5.1
$$E' = E/\varphi^{-1}(\mu_p)$$

and denote by $\pi\colon E \to E'$ the projection. Its dual $\check{\pi}\colon E' \to E$ is étale, so we can define $\varphi' = \varphi \circ \check{\pi}$. We view β as a pair (β_1, β_2) consisting of compatible $\Gamma_{00}(N)^{\text{arith}}$ and $\Gamma_{00}(N)^{\text{naive}}$ structures (cf. 2.0.9), which are both compatible with φ (5.0). Writing $N = p^r N_0$ with $(p, N_0) = 1$, we treat separately the two cases $(p, N) = 1$ and $N = p^r$. In the first case $(p, N) = 1$, both π and $\check{\pi}$ are of degree prime to p, so induce isomorphisms $\pi\colon {}_N E \xrightarrow{\sim} {}_N E'$ and $\check{\pi}\colon {}_N E' \xrightarrow{\sim} {}_N E$. We define β_1', β_2' by requiring commutativity in the diagrams

5.5.2
$$\begin{tikzcd} & {}_N E \\ \mu_N \arrow[ur, "\beta_1"] \arrow[dr, "\beta_1'"'] & \\ & {}_N E' \arrow[uu, "\check{\pi}"', "\wr"] \end{tikzcd} , \qquad \begin{tikzcd} & {}_N E \arrow[dd, "\pi", "\wr"'] \\ \mathbf{Z}/N\mathbf{Z} \arrow[ur, "\beta_2"] \arrow[dr, "\beta_2'"'] & \\ & {}_N E' \end{tikzcd} .$$

In the second case $N = p^r$, the β_1' is already determined; it is $(\varphi')^{-1}$ restricted to $\boldsymbol{\mu}_{p^r}$:

5.5.3
$$\begin{tikzcd}
 & \hat{E} \arrow[dr, "\varphi", "\sim"'] & \\
\boldsymbol{\mu}_{p^r} \arrow[ur, hook, "\beta_1"] \arrow[dr, "\beta_1'"'] & & \hat{\mathbf{G}}_m ; \\
 & \hat{E}' \arrow[uu, "\check{\pi}"', "\wr"] \arrow[ur, "\varphi'"', "\sim"] &
\end{tikzcd}$$

and β_2' is simply the composite $\pi \cdot \beta_2$:

5.5.4
$$\begin{tikzcd}
 & E \arrow[dd, "\pi"] \\
\mathbf{Z}/p^r\mathbf{Z} \arrow[ur, hook, "\beta_2"] \arrow[dr, hook, "\beta_2'"'] & \\
 & E' .
\end{tikzcd}$$

Reassembling $N = p^r N_0$, we see that $\beta' = \beta_1', \beta_2'$ is *characterized* by the equations $\beta_1 = \check{\pi}\beta_1'$, $\beta_2' = \pi\beta_2$.

5.5.5. This construction carries

$$\big(\mathrm{Tate}(q^N), \varphi_{\mathrm{can}}, \beta_{\mathrm{can}}\big) \text{ to } \mathrm{Tate}\big(q^{pN}, \varphi_{\mathrm{can}}, \beta_{\mathrm{can}}\big) ,$$

and by transposition, defines the Frobenius endomorphism of $V\big(B, \Gamma(N)^{\mathrm{arith}}\big)$:

5.5.6
$$(\mathrm{Frob}\, F)(E, \varphi, \beta) \overset{\mathrm{dfn}}{=} F(E', \varphi', \beta') .$$

By 5.5.5, its effect upon q-expansion is simply

5.5.7
$$(\mathrm{Frob}\, F)(q) = F(q^p) ;$$

similarly for $\Gamma_{00}(N)^{\mathrm{arith}}$ and $\Gamma_{00}(N)^{\mathrm{naive}}$.

LEMMA 5.5.8. *The Frobenius endomorphism of* $V\big(B, \Gamma(N)^{\mathrm{arith}}\big)$ *commutes with the operation of the group* $G(N)$; *similarly for* $\Gamma_{00}(N)^{\mathrm{arith}}$, $\Gamma_{00}(N)^{\mathrm{naive}}$.

Proof. We must check that the two values

$$\begin{aligned} \mathrm{Frob}\,\big([a, b]F\big)(E, \varphi, \beta) &= \big([a, b]F\big)(E', \varphi', \beta') \\ &= F\big(E', a^{-1}\varphi', \beta' \circ (b, b^{-1})\big) \end{aligned}$$

and

$$\begin{aligned} [a, b](\mathrm{Frob}\, F)(E, \varphi, \beta) &= (\mathrm{Frob}\, F)\big(E, a^{-1}\varphi, \beta \circ (b, b^{-1})\big) \\ &= F\big(E', (a^{-1}\varphi)', \big(\beta \circ (b, b^{-1})\big)'\big) \end{aligned}$$

agree, for any test object (E, φ, β). The defining equation $\varphi' = \varphi \circ \check{\pi}$ shows that $(a^{-1}\varphi)' = a^{-1}\varphi'$. Viewing β as (β_1, β_2) (5.5.2), we see from the defining equations $\beta_1 = \check{\pi} \circ \beta_1'$ and $\beta_2' = \pi \circ \beta_2$, that $(b\beta_1)' = b\beta_1'$ and $(b^{-1}\beta_2)' = b^{-1}\beta_2'$.

Q.E.D.

5.6. *Some "exotic" isomorphisms.*

5.6.0. We can recopy Section 2.3, once we tell how to "push" a trivialization when we divide by a subgroup μ_N or $\mathbf{Z}/N\mathbf{Z}$. Given (E, φ) and a subgroup $\mu_N \hookrightarrow E$, let $\pi: E \to E/\mu_N$ denote the projection, and take as trivialization on E/μ_N the composite $\varphi \circ \check{\pi}$. Given (E, φ) and a subgroup $\mathbf{Z}/N\mathbf{Z} \hookrightarrow E$, let $\pi: E \to E/\mathbf{Z}/N\mathbf{Z}$ denote the projection, and take as trivialization φ' on $E/\mathbf{Z}/N\mathbf{Z}$ the unique one such that $\varphi = \varphi' \circ \pi$. With these rules, the isomorphisms 2.3.6 may be transcribed in the p-adic case as inverse isomorphisms

5.6.1 $$V(B, \Gamma_{00}(N)^{\text{arith}}) \rightleftarrows V(B, \Gamma_{00}(N)^{\text{naive}})$$

which arise by transposition from the inverse equivalences

5.6.2
$$\{\text{trivialized } \Gamma_{00}(N)^{\text{arith}} \text{ curves}\} \underset{\text{divide by } \mu_N}{\overset{\text{divide by } \mathbf{Z}/N\mathbf{Z}}{\rightleftarrows}} \{\text{trivialized } \Gamma_{00}(N)^{\text{naive}} \text{ curves}\} .$$

The isomorphisms 5.6.1 preserve q-expansion.

Another exotic isomorphism worth noting arises whenever $N = p^r N_0$ with $r \geqq 1$. It is *characteristic* of the p-adic theory.

LEMMA 5.6.3. *Let $N = p^r N_0$, with $r \geqq 1$ and $(p, N_0) = 1$. There is an "exotic", $(G(N) \simeq G(N_0)$ equivariant, q-expansion-preserving isomorphism*

5.6.4 $$V(B, \Gamma(p^r N_0)^{\text{arith}}) \xrightarrow{\sim} V(B, \Gamma(N_0)^{\text{arith}}) .$$

Proof-construction. We will in fact construct an equivalence

5.6.5 $$\{\text{trivialized } \Gamma(N_0)^{\text{arith}} \text{ curves}\} \xmapsto{\sim} \{\text{trivialized } \Gamma(p^r N_0)^{\text{arith}} \text{ curves}\} .$$

Given a trivialized $\Gamma(N_0)^{\text{arith}}$ curve (E, φ, β), we can iterate the Frobenius construction (5.5.1) r times (which amounts to dividing E by $\varphi^{-1}(\mu_{p^r})$), and obtain another $\Gamma(N_0)^{\text{arith}}$ curve $(E^{(r)}, \varphi^{(r)}, \beta^{(r)})$. It remains to endow $E^{(r)} = E/\mu_{p^r}$, with a canonical $\Gamma(p^r)^{\text{arith}}$ structure, or what is the same for a trivialized curve, with a $\Gamma_{00}(p^r)^{\text{naive}}$ structure. For this we simply invoke the equivalence 5.6.2, in the case $N = p^r$.

The *inverse* construction

5.6.6 $$\{\text{trivialized } \Gamma(p^r N_0)^{\text{arith}} \text{ curves}\} \longmapsto \{\text{trivialized } \Gamma(N_0)^{\text{arith}} \text{ curves}\}$$

does *not* depend on the fact that we have trivializations, and is just the "trivialized" version of a modular construction in which p^r could be *any* integer N_1, and in which the fact that N_0 is prime to p plays no role:

5.6.7 $$\{\Gamma(N_1 N_0)^{\text{arith}}\text{-test objects}\} \longmapsto \{\Gamma(N_0)^{\text{arith}} \text{ test objects}\} .$$

Given a $\Gamma(N_1 N_0)^{\text{arith}}$-test object of either sort (E, ω or φ, β), E contains a subgroup $\mathbf{Z}/N_1\mathbf{Z}$, namely the subgroup $N_0\mathbf{Z}/N_0N_1\mathbf{Z} \subset \mathbf{Z}/N_1N_0\mathbf{Z} \overset{\beta}{\hookrightarrow} E$. We define $E' = E/\mathbf{Z}/N_1\mathbf{Z}$, and denote by π the étale projection. There is a unique differential ω' on E' such that $\pi^*(\omega') = \omega$, and a unique trivialization φ' on E' such that $\varphi = \varphi' \circ \pi$. The quotient curve E' isomorphically receives $\mathbf{Z}/N_0\mathbf{Z}$, through the composite of β_2 with π:

5.6.8
$$\begin{array}{ccc} \mathbf{Z}/N_0N_1\mathbf{Z} & \xhookrightarrow{\beta_2} & E \\ \downarrow & & \downarrow{\scriptstyle \pi} \\ \mathbf{Z}/N_0\mathbf{Z} & \xhookrightarrow{\beta_2'} & E'. \end{array}$$

The inclusion of $\mu_{N_0N_1}$ into E' is defined by

5.6.9
$$\begin{array}{ccc} \mu_{N_0N_1} & \xhookrightarrow{\beta_1} & E \\ \cup & & \downarrow{\scriptstyle \pi} \\ \mu_{N_0} & \xhookrightarrow[\beta_1']{} & E'. \end{array}$$

This construction $(E, \omega \text{ or } \varphi, \beta) \mapsto (E', \omega' \text{ or } \varphi', \beta')$ carries Tate curve to Tate curve, and so defines by transposition a commutative diagram of q-expansion-preserving ring homomorphisms

5.6.10
$$\begin{array}{ccc} R\big(B, \Gamma(N_0)^{\text{arith}}\big) & \xrightarrow{\text{(divide by } \mathbf{Z}/N_1\mathbf{Z})^*} & R\big(B, \Gamma(N_1N_0)^{\text{arith}}\big) \\ \downarrow{\scriptstyle F \mapsto \tilde{F}} & & \downarrow{\scriptstyle F \mapsto \tilde{F}} \\ V\big(B, \Gamma(N)^{\text{arith}}\big) & \xrightarrow{\text{(divide by } \mathbf{Z}/N_1\mathbf{Z})^*} & V\big(B, \Gamma(N_1N_0)^{\text{arith}}\big)\,. \end{array}$$

In case $N_1 = p^r$, this construction 5.6.6 is easily checked to be *inverse* to that of 5.6.5. Q.E.D.

Remark 5.6.11. The isomorphisms 5.6.4 for r and $r+1$ "differ" by an isomorphism (which necessarily preserves q-expansions)

5.6.12
$$V\big(B, \Gamma(pN)^{\text{arith}}\big) \xrightarrow{\sim} V\big(B, \Gamma(N)^{\text{arith}}\big)$$

whose *inverse* is none other than the map 5.6.10 (for $N_1 = p$, $N_0 = N$).

Because a $\Gamma(pN)^{\text{arith}}$-structure determines, by restriction to the subgroup $\mu_N \times p\mathbf{Z}/pN\mathbf{Z}$, a $\Gamma(N)^{\text{arith}}$-structure, we have a "natural inclusion" of $V\big(B, \Gamma(N)^{\text{arith}}\big) \hookrightarrow V\big(B, \Gamma(pN)^{\text{arith}}\big)$ which has the effect $q \mapsto q^p$ on q-expansion. The composite

5.6.13
$$\begin{array}{ccccc} & & V\big(B, \Gamma(pN)^{\text{arith}}\big) & & \\ & {\scriptstyle \text{nat'l incl.}} \nearrow & & \searrow {\scriptstyle \text{the isom. 5.6.12}} & \\ V\big(B, \Gamma(N)^{\text{arith}}\big) & & \xrightarrow{\text{Frob}} & & V\big(B, \Gamma(N)^{\text{arith}}\big) \end{array}$$

is, as labeled, the Frobenius (just check the effect on q-expansion!).

Interpretation 5.6.14. If we combine 5.4.7 with 5.6.4 and 5.6.10, we get a commutative diagram of q-expansion-preserving ring homomorphisms

$$\begin{tikzcd} R^{\bullet}(B, \Gamma(p^r N_0)^{\mathrm{arith}}) \arrow[r, "F \mapsto \tilde{F}"] & V(B, \Gamma(p^r N_0)^{\mathrm{arith}}) \arrow[d, shift right, "\text{(divide by } \mu_{p^r})^*"', "\wr"] \\ R^{\bullet}(B, \Gamma(N_0)^{\mathrm{arith}}) \arrow[u, "\text{(divide by } \mathbf{Z}/p^r\mathbf{Z})^*"] \arrow[r, "F \mapsto \tilde{F}"] & V(B, \Gamma(N_0)^{\mathrm{arith}}) \arrow[u, shift right, "\text{(divide by } \mathbf{Z}/p^r\mathbf{Z})^*"', "\wr"] \end{tikzcd} .$$

We can sum this up in the catch phrase "a true modular form of level $p^r N_0$ is p-adically modular of level N_0."

5.7. *Ramanujan's series P as the direction of the unit root subspace* (*compare* 1.3).

5.7.0. This series is the q-expansion of a (necessarily unique) element $P \in V(\mathbf{Z}_p, \Gamma(1)^{\mathrm{arith}})$ which has weight two. It is defined modularly as follows. Over the ring $V_1 \overset{\mathrm{dfn}}{=} V(\mathbf{Z}_p, \Gamma(1)^{\mathrm{arith}})$, we have the universal trivialized elliptic curve $(E_{\mathrm{univ}}, \varphi_{\mathrm{univ}})$. Its Frobenius transform (E', φ'), formed by dividing E_{univ} by its "canonical subgroup" (cf. [13]) $\varphi_{\mathrm{univ}}^{-1}(\mu_p)$, is *another* trivialized elliptic curve over V_1. The ring homomorphism $V_1 \to V_1$ which classifies it is just the Frobenius endomorphism of V_1:

$$E' = E_{\mathrm{univ}}^{(\mathrm{Frob})} .$$

5.7.1. The free rank-two V_1-module $H^1_{\mathrm{DR}}(E_{\mathrm{univ}}/V_1)$ undergoes a Frob-linear endomorphism as follows. The projection map

5.7.2 $$\pi: E_{\mathrm{univ}} \longrightarrow E'$$

induces by functoriality a V_1-linear map F

5.7.3 $$\begin{tikzcd} \pi^*: H^1_{\mathrm{DR}}(E'/V_1) \arrow[r] \arrow[d, equal] & H^1_{\mathrm{DR}}(E_{\mathrm{univ}}/V_1) \\ H^1_{\mathrm{DR}}(E_{\mathrm{univ}}^{(\mathrm{Frob})}/V_1) & \\ H^1_{\mathrm{DR}}(E_{\mathrm{univ}}/V_1)^{(\mathrm{Frob})} \arrow[u, "\wr"'] \arrow[uur, dashed, "F"'] & \end{tikzcd}$$

which we view as a Frob-linear endomorphism of $H^1_{\mathrm{DR}}(E_{\mathrm{univ}}/V_1)$.

Consider the F-stable Hodge filtration of $H^1_{\mathrm{DR}}(E_{\mathrm{univ}}/V_1)$,

5.7.4 $$0 \longrightarrow H^0(\Omega^1) \longrightarrow H^1_{\mathrm{DR}} \longrightarrow H^0(\mathcal{O}_E) \longrightarrow 0 .$$

The endomorphism F is divisible by p on $H^0(\Omega^1)$, but induces a Frob-linear automorphism on $H^1(\mathcal{O}_E)$. From this it follows that there is a unique F-stable splitting of the Hodge filtration

5.7.5 $$H^1_{\mathrm{DR}} = H^0(\Omega^1) \oplus U ,$$

where F induces a Frob-linear automorphism of U (the "unit root part") (cf. [13], A2).

On the purely algebraic side, we are given a basis $\omega = \varphi^*(dT/(1+T))$ of $H^0(\Omega^1)$, so that after extending scalars from V_1 to $V_1[1/6]$, we can write a Weierstrass equation $y^2 = 4x^3 - g_2 x - g_3$ for E_{univ}, under which $\omega = dx/y$. The differential of the second kind $\eta \overset{\mathrm{dfn}}{=} xdx/y$ forms, with ω, a *basis* of $H^1_{\mathrm{DR}}(E_{\mathrm{univ}}/V_1) \otimes_{\mathbf{Z}} \mathbf{Z}[1/12]$, and we know that $\langle \omega, \eta \rangle_{\mathrm{DR}} = 1$.

In complete analogy with 1.3.6, we can *measure* the direction of the unit root subspace $U \subset H^1_{\mathrm{DR}}$ by choosing an arbitrary invertible section $u \in U$, and considering the ratio

5.7.6 $$\frac{-\langle u, \eta \rangle_{\mathrm{DR}}}{\langle u, \omega \rangle_{\mathrm{DR}}} \in V_1\left[\frac{1}{12}\right]$$

(the denominator $\langle u, \omega \rangle_{\mathrm{DR}}$ is necessarily a *unit* in V_1, because ω and u are invertible sections of $H^0(\Omega^1)$ and U respectively, which the alternating form $\langle\ ,\ \rangle_{\mathrm{DR}}$ necessarily puts into duality).

This said, we could *define* an element $P \in V_1[1/12]$ by the formula

5.7.7 $$P(E, \varphi) = 12 \frac{\langle u, \eta \rangle_{\mathrm{DR}}}{\langle u, \omega \rangle_{\mathrm{DR}}} .$$

LEMMA 5.7.8. *The element* $P \in V(\mathbf{Z}_p, \Gamma(1)^{\mathrm{arith}}) \otimes_{\mathbf{Z}} \mathbf{Z}[1/12]$ *of weight two defined by* 5.7.7 *above actually lies in* $V(\mathbf{Z}_p, \Gamma(1)^{\mathrm{arith}})$. *It q-expansion is given by Ramanujan's series*

5.7.9 $$P(q) = 1 - 24 \sum\nolimits_{n \geq 1} q^n \sum\nolimits_{d \mid n} d .$$

Proof. The q-expansion computation is carried out in ((13), A2.4). It shows that in fact P lies in $V(\mathbf{Z}_p, \Gamma(1))$ even for $p = 2$ or 3, by the q-expansion principle. That P is of weight two follows from the cohomological expression 5.7.7: Changing φ to $a^{-1}\varphi$ changes ω to $a^{-1}\omega$, and η to $a\eta$, and thus carries P to $a^2 P$.

Remark 5.7.10. The fact that P lies in V_1 means that 12η is actually a section of $H^1_{\mathrm{DR}}(E_{\mathrm{univ}}/V_1)$. Explicitly, we have

5.7.11 $$12\eta = P\omega + \frac{12}{\langle \omega, u \rangle_{\mathrm{DR}}} u .$$

For any $N \geq 1$, we can consider P as an element of $V(\mathbf{Z}_p, \Gamma(N)^{\mathrm{arith}})$, by defining $P(E, \varphi, \beta) = P(E, \varphi)$. Its level N q-expansion is

5.7.12 $$P(q^N) = 1 - 24\sum_{n\geq 1} q^{Nn}\sum_{d|n} d\ .$$

In the notation of 3.6.11, we have the formulas

5.7.13 $$\begin{cases} -\dfrac{1}{24}P(q^N) = G_{2,0,\ \text{char. fct of } \mathbf{Z}/N\mathbf{Z}\times\{0\}} \\ \dfrac{-N}{24}P(q^N) = G_{2,0,\ \text{char. fct of } \{0\}\times\mathbf{Z}/N\mathbf{Z}}\ , \end{cases}$$

which should be viewed as the p-adic analogue of the C^∞ formulas 3.6.13.

5.8. *The derivation θ.*

LEMMA 5.8.1. *For each integer $N \geqq 1$, there is a derivation "$N\theta$" of $V(\mathbf{Z}_p(N)^{\text{arith}})$, whose effect upon level N q-expansion is $q(d/dq)$, in the sense that the diagram below commutes*

5.8.2 $$\begin{array}{ccc} V(\mathbf{Z}_p,\ \Gamma(N)^{\text{arith}}) & \xrightarrow{N\theta} & V(\mathbf{Z}_p,\ \Gamma(N)^{\text{arith}}) \\ \Big\downarrow q\text{-expansion} & & \Big\downarrow q\text{-expansion} \\ \widehat{\mathbf{Z}_p((q))} & \xrightarrow{q\frac{d}{dq}} & \widehat{\mathbf{Z}_p((q))}\ . \end{array}$$

It is of weight two in the sense that for any element $(a, b) \in G(N)$ (cf. 5.3), *we have*

5.8.3 $$[a, b]\circ N\theta = a^2 N\theta\circ[a, b]\ .$$

Proof-construction. The notation "$N\theta$" is simply to emphasize the dependence upon N: under the natural inclusion $V(B, \Gamma(N)^{\text{arith}}) \subset (B, \Gamma(NM)^{\text{arith}})$, the subring is stable by "$NM\theta$," and "$NM\theta$" $= M$"$N\theta$" on it.

To prove it, we can use the isomorphism 5.6.4 to reduce to the case where N is prime to p. In that case, the $\Gamma(N)^{\text{arith}}$ moduli problem is *étale* over the $\Gamma(1)^{\text{arith}}$ moduli problem, so it suffices to treat the case $N = 1$. Deformation theory gives us an isomorphism of $V(\mathbf{Z}_p, \Gamma(1)^{\text{arith}})$ modules

5.8.4 $$(\underline{\omega}_{E_{\text{univ}}/V})^{\otimes 2} \simeq \Omega^1_{V/\mathbf{Z}_p}\ .$$

Now $\omega = \varphi^*(dT/(1 + T))$ is a canonical *basis* of $\underline{\omega}$, so its square gives a canonical basis of $\underline{\omega}^{\otimes 2}$, which by 5.8.4 gives a canonical basis of $\Omega^1_{V/\mathbf{Z}_p}$. The *dual* basis of $\operatorname{Der}(V, V)$ is defined to be θ. In concrete terms, this means that θ is the unique derivation of $V(\mathbf{Z}_p, \Gamma(1)^{\text{arith}})$ such that under the Gauss-Manin connection ∇ on $H^1_{\text{DR}}(E_{\text{univ}}/V(\mathbf{Z}_p, \Gamma(1)))$, we have the cup-product formula

5.8.5 $$\langle\varphi^*(dT/(1 + T)),\ \nabla(\theta)(\varphi^*(dT/(1 + T)))\rangle_{\text{DR}} = 1\ .$$

That this derivation has the effect $q(d/dq)$ on q-expansions is equivalent to the assertion that on the Tate curve Tate(q), we have

5.8.6
$$\left\langle \omega_{\text{can}}, \nabla\left(q\frac{d}{dq}\right)(\omega_{\text{can}})\right\rangle_{\text{DR}} = 1$$

a formula which is verified in ([13], A1.3.18).

That θ has weight two is obvious from its cohomological definition: an element $[a] \in \mathbf{Z}_p^\times$ carries φ to $a^{-1}\varphi$, so carries $\omega = \varphi^*(dT/(1+T))$ to $a^{-1}\omega$, and hence carries $\theta \mapsto [a]\theta[a]^{-1} = a^2\theta$, as required. Q.E.D.

5.9. *A p-adic graded $\mathcal{Z}$-module* (compare 1.6). Let us denote by $GV^\cdot(\mathbf{Z}_p, \Gamma(N)^{\text{arith}})$ the *graded* subring of the non-graded ring $V(\mathbf{Z}_p, \Gamma(N)^{\text{arith}})$ whose elements in degree k are the elements of $V(\mathbf{Z}_p, \Gamma(N)^{\text{arith}})$ which are of weight k under the open subgroup $\mathbf{Z}_p^\times \times \{1\} \cap G(N)$ of $G(N)$. Thus an element $F \in V$ lies in GV^k if and only if, writing $N = p^r N_0$ with $(p, N_0) = 1$, we have

5.9.1
$$a \in \mathbf{Z}_p^\times,\ a \equiv 1(p^r) \Longrightarrow [a, 1]F = a^k F\ .$$

The homogeneity derivation $H\colon GV^\cdot \to GV^\cdot$ is defined by

5.9.2
$$H(\textstyle\sum f_i) = \sum i f_i\ .$$

LEMMA 5.9.3. *The graded ring $GV^\cdot(\mathbf{Z}_p, \Gamma(N)^{\text{arith}}) \otimes_{\mathbf{Z}} \mathbf{Z}[1/12N]$ becomes a graded $\mathcal{Z}$ module under the assignment*

5.9.4
$$\begin{cases} g_2 \longmapsto (\textit{multiplication by}) g_2 \\ g_3 \longmapsto (\textit{multiplication by}) g_3 \\ \mathbf{S} \longmapsto (\textit{multiplication by}) P \\ \mathbf{H} \longmapsto H \\ \mathbf{W} \longmapsto \theta \\ \mathbf{D} \longmapsto \theta - \dfrac{1}{12} P\cdot H\ . \end{cases}$$

Proof. Since the operators g_2, g_2, $\theta - (1/12)PH$, H, θ, P are homogeneous of weight 4, 6, 2, 0, 2, 2 respectively, the commutation relations between H and any other are satisfied. Since $GV^\cdot$ is a commutative ring, the commutation relations among g_2, g_3, P are satisfied. Since the operator $\theta - (1/12)P\cdot H$ acts stably on the subring $R^\cdot(\mathbf{Z}_p[1/12N], \Gamma(N)^{\text{arith}})$ of "true" modular forms as the Halphen-Fricke operator D (cf. 1.5.12), the commutation relations between it and g_2 or g_3 are satisfied. It remains to check that

$$\left[\theta - \frac{1}{12}P\cdot H, P\right] = -g_2 - \frac{1}{12}P^2\ ,$$

i.e., that
$$\theta(P) - \frac{1}{12}P\cdot H(P) = -g_2 - \frac{1}{12}P^2\ ,$$

i.e., that $$\theta(P) - \frac{2}{12}P^2 = -g_2 - \frac{1}{12}P^2 ,$$

i.e., that $$\theta(P) - \frac{1}{12}P^2 = -g_2 ,$$

i.e., that $$q\frac{d}{dq}(P(q)) - \frac{1}{12}P(q)^2 = -g_2(q) ,$$

which is the differential equation established in 1.4.31. Q.E.D.

5.10. *Another modular description of* $GV^{\cdot}(\mathbf{Z}_p, \Gamma(N)^{\mathrm{arith}})$.

5.10.0. Let B be a p-adic ring, and (E, ω, β) a $\Gamma(N)^{\mathrm{arith}}$-test object (cf. 2.1) defined over B. Assume in addition that the underlying curve E/B is fibre by fibre *ordinary*. (This last condition is *automatic* if p divides N.) Then over a pro-ind-étale over-ring B_∞ (meaning that B_∞ is a p-adic ring, and for each $n \geqq 1$, B_∞/p^nB_∞ is an increasing union of finite étale over-rings of B/p^nB) there exists a trivialization φ on $E\otimes B_\infty/B_\infty$ with which β is compatible. Furthermore, the *indeterminacy* in the choice of such a φ is the group $\mathbf{Z}_p^\times \times \{1\} \cap G(N)$, i.e., with $N = p^rN_0$ where $(p, N_0) = 1$, the given inclusion of $\mu_{p^r} \hookrightarrow E$ by β determines the "beginning" of φ, so we can only change it by an element $a \in \mathbf{Z}_p^\times$ which is $\equiv 1 \bmod p^r$.

Suppose we are given an element $F \in GV^k(\mathbf{Z}_p, \Gamma(N)^{\mathrm{arith}})$. We want to give it a *value* $F(E, \omega, \beta) \in B$ on such a test object. First we will define this value as an element of B_∞. *Choose* a trivialization φ over B_∞ with which β is compatible. Then we can write $\omega = \lambda\varphi^*(dT/(1+T))$ for some unit $\lambda \in B_\infty^\times$. We tentatively define

5.10.1 $$F(E, \omega, \beta) = \lambda^{-k}F(E, \varphi, \beta) \in B_\infty \text{ if } \omega = \lambda\varphi^*(dT/(1+T)) .$$

This is *well defined* independent of the choice of φ, for if we change φ to $a^{-1}\varphi$, with $a \in \mathbf{Z}_p^\times$, $a \equiv 1(p^r)$, we have $\omega = a\lambda(a^{-1}\varphi)^*(dT/(1+T))$, and the "definition" 5.10.1 would yield

$$F(E, \omega, \beta) = (a\lambda)^{-k}F(E, a^{-1}\varphi, \beta) = \lambda^{-k}F(E, \varphi, \beta) ,$$

because F lies in GV^k. It follows by a standard étale descent argument that this value, being independent of the auxiliary choice of φ, must itself lie in B, rather than B_∞. Notice that we have lost no information, for when we are given a trivialized $\Gamma(N)^{\mathrm{arith}}$ curve (E, φ, β) over B, we have the the tautological equality:

5.10.2 $$F(E, \varphi, \beta) = F(E, \varphi^*(dT/(1+T)), \beta) .$$

Thus we have

LEMMA 5.10.3. *The above construction establishes an isomorphism between* $GV^k(\mathbf{Z}_p, \Gamma(N)^{\mathrm{arith}})$ *and the p-adic* $\mathbf{Z}_p$*-module of "functions"* F *which* *to any fibre-by-fibre ordinary $\Gamma(N)^{\text{arith}}$-test object (E, ω, β) over any p-adic ring B, assign a value $F(E, \omega, \beta) \in B$, such that (compare* 2.1.1 *and* [13], *Ch.* 2)

5.10.4
$$\begin{cases} F(E, \omega, \beta) \text{ depends only on the } B\text{-isomorphism class of } (E, \omega, \beta) \\ F(E, \lambda^{-1}\omega, \beta) = \lambda^k F(E, \omega, \beta) \text{ for all } \lambda \in B^\times \\ \text{formation of } F(E, \omega, \beta) \text{ commutes with extension of scalars of} \\ \qquad p\text{-adic rings .} \end{cases}$$

In the language of [13], this lemma says that $GV^k(\mathbf{Z}_p, \Gamma(N)^{\text{arith}})$ is the module of all "p-adic modular forms on $\Gamma(N)^{\text{arith}}$ of weight k."

Remark 5.10.4.1. If we *fix* a p-adic ground-ring B_0, we have an analogous modular interpretation of the ring $GV^\bullet(B_0, \Gamma(N)^{\text{arith}}) \overset{\text{dfn}}{=} \bigoplus GV^k(\mathbf{Z}_p, \Gamma(N)^{\text{arith}}) \hat{\otimes} B_0$.

5.10.5. *An example*: P (compare 5.4.3). Suppose B is the ring of integers in a finite extension K of $\mathbf{Q}_p$ with residue field $\mathbf{F}_q$, and (E, ω) is an ordinary elliptic curve with nowhere vanishing differential. The 2-dimensional K-space $H^1_{\text{DR}}(E_K/K)$ undergoes a canonical "q^{th} power Frobenius endomorphism" F_q, exactly one of whose eigenvalues is a unit $a \in \mathbf{Z}_p^\times$, the other being q/a. (The characteristic polynomial $(1 - aT)(1 - (q/a)T)$ is the numerator of the zeta function of $E \otimes \mathbf{F}_q/\mathbf{F}_q$.) If we choose any nonzero eigenvector u in the (unit) a-eigenspace, then we have

5.10.6
$$P(E, \omega) = 12\frac{\langle u, \eta\rangle_{\text{DR}}}{\langle u, \omega\rangle_{\text{DR}}}$$

Tautology 5.10.7. Suppose that B is a p-adic ring, and that (E, ω, β) is a fibre-by-fibre ordinary $\Gamma(N)^{\text{arith}}$-test object over B. A necessary and sufficient condition that ω be a *magic differential* (i.e., of the form $\varphi^*(dT/(1+T))$ for some trivialization φ defined over B) is that the evaluation homomorphism

5.10.8
$$GV^\bullet(\mathbf{Z}_p, \Gamma(N)^{\text{arith}}) \xrightarrow{\text{eval. at } (E, \omega, \beta)} B$$

be prolongable to a ring homomorphism

5.10.9
$$\begin{tikzcd} V(\mathbf{Z}_p, \Gamma(N)^{\text{arith}}) \arrow[r, "?"] & B \\ \cup & \\ GV^\bullet(\mathbf{Z}_p, \Gamma(N)^{\text{arith}}) \arrow[uur, "\text{eval. at } (E, \omega, \beta)"'] & \end{tikzcd}$$

It is a tautology in view of the functorial description (5.1.0) of the ring $V(\mathbf{Z}_p, \Gamma(N)^{\text{arith}})$. But in view of the known explicit generators for V as a

$GV^{\bullet}$-algebra (cf. [14]), it is also a congruence criterion on the coefficient of the power series expansion of ω, at least when B is flat over $\mathbf{Z}_p$!

5.11. *Construction of the p-adic Eisenstein-Ramanujan series* $G_{k,r,f}$ *and* $\Phi_{k,r,f}$ (compare 3.6).

LEMMA 5.11.0. *Let f be a $\mathbf{Z}_p$-valued function on $\mathbf{Z}/N\mathbf{Z} \times \mathbf{Z}/N\mathbf{Z}$, and $k \geqq 1$ an integer. The q-series*

5.11.1
$$2G_{k,0,f} = \begin{cases} \frac{1}{2}L\big(0,\, f(n,\, 0) + f(0,\, n) - f(-n,\, 0) - f(0,\, -n)\big) & \text{if } k = 1 \\ \frac{1}{2}L\big(1 - k,\, f(n,\, 0) - (-1)^{k-1}f(-n,\, 0)\big) & \text{if } k \geqq 2 \end{cases}$$
$$+ \textstyle\sum_{n \geqq 1} q^n \sum_{dd'=n} \big(d^{k-1}f(d,\, d') - (-d)^{k-1}f(-d,\, -d')\big)$$
is the q-expansion of an element $2G_{k,0,f} \in GV^k\big(\mathbf{Z}_p,\, (\Gamma(N)^{\mathrm{arith}}\big) \otimes \mathbf{Q}_p$.

Proof. For $k \neq 2$ and any f, and for $k = 2$ and f's satisfying the extra conditions $\sum f(j,\, 0) = \sum f(0,\, l) = 0$, the element $G_{k,0,f}$ even lies in $R^k\big(\mathbf{Q}_p,\, \Gamma(N)^{\mathrm{arith}}\big)$. In the two remaining cases, $k = 2$ and the functions $f_1 =$ the characteristic function of $\mathbf{Z}/N\mathbf{Z} \times \{0\}$ and $f_2 = f_1^t$, these are the q-expansions of $(-1/24)P$ and $(-N/24)P$ respectively (cf. 5.7.13). Q.E.D.

Definition 5.11.2. Let k and r be non-negative integers, and f a $\mathbf{Z}_p$-valued function on $\mathbf{Z}/N\mathbf{Z} \times \mathbf{Z}/N\mathbf{Z}$. We define the q-series $2\Phi_{k,r,f}$ by the formulas

5.11.3
$$2\Phi_{k,r,f} = \begin{cases} 2G_{k+1,0,f} & \text{if } r = 0 \\ 2G_{r+1,0,f^t} & \text{if } k = 0 \\ \sum_{n \geqq 1} q^n \sum_{n=dd'} \big(d^k(d')^r f(d,\, d') - (-d)^k(-d')^r f(-d,\, -d')\big) & \\ & \text{if } k,\, r \geqq 1\,. \end{cases}$$

Notice that no ambiguity is caused by the overlapping case $k = r = 0$, because $G_{1,0,f} = G_{1,0,f^t}$, as is visible from 5.11.1.

LEMMA 5.11.4. *For $k,\, r \geqq 0$, and f a $\mathbf{Z}_p$-valued function on $\mathbf{Z}/N\mathbf{Z} \times \mathbf{Z}/N\mathbf{Z}$, the series $2\Phi_{k,r,f}$ is the q-expansion on an element*

$$2\Phi_{k,r,f} \in GV^{k+r+1}\big(\mathbf{Z}_p,\, \Gamma(N)^{\mathrm{arith}}\big) \otimes \mathbf{Q}_p\,.$$

If both $k,\, r \geqq 1$, then $2\Phi_{k,r,f}$ lies in $GV^{k+r+1}\big(\mathbf{Z}_p,\, \Gamma(N)^{\mathrm{arith}}\big)$.

Proof. If $k = 0$ or $r = 0$, there is nothing to prove. If $k \geqq r \geqq 1$, we have the q-series equality

5.11.5
$$\Phi_{k,r,f} = \left(q\frac{d}{dq}\right)^r (2G_{k+1-r,0,f})$$

so that we can *modularly* define $2\Phi_{k,r,f}$ by

5.11.6 $$2\Phi_{k,r,f} \overset{\text{dfn}}{=} (N\theta)^r(2G_{k+1-r,0,f}) \qquad \text{if } k \geqq r \geqq 1 .$$

Similarly, if $r \geqq k \geqq 1$, we have the q-series equality

5.11.7 $$2\Phi_{k,r,f} = \left(q\frac{d}{dq}\right)^k (G_{r+1-k,0,f^t}) \qquad \text{if } r \geqq k \geqq 1 ,$$

so that we can *modularly* define

5.11.8 $$2\Phi_{k,r,f} \overset{\text{dfn}}{=} (N\theta)^k(2G_{r+1-k,0,f^t}) \qquad \text{if } r \geqq k \geqq 1 .$$

Since $N\theta$ increases weight by two, we have $\Phi_{k,r,f} \in GV^{k+r+1}(\mathbf{Z}_p, \Gamma(N)^{\text{arith}}) \otimes \mathbf{Q}_p$. If $k, r \geqq 1$, then $2\Phi_{k,r,f}$ has *integral* q-expansion, so by the q-expansion principle it lies in $GV^{k+r+1}(\mathbf{Z}_p, \Gamma(N)^{\text{arith}})$. Q.E.D.

Definition 5.11.9. Let A, B be integers satisfying $B \leqq 0$, $A + B \geqq 1$, and f a $\mathbf{Z}_p$-valued function on $\mathbf{Z}/N\mathbf{Z} \times \mathbf{Z}/N\mathbf{Z}$. We define an element $2G_{A,B,f} \in GV^A(\mathbf{Z}_p, \Gamma(N)^{\text{arith}}) \otimes \mathbf{Q}_p$ by setting

5.11.10 $$2G_{A,B,f} = 2\Phi_{A+B-1,-B,f} ,$$

i.e., $$2\Phi_{k,r,f} = 2G_{k+r+1,-r,f} .$$

Notice that if $B < -1$ and $A + B \geqq 2$, then $2G_{A,B,f} \in GV^A(\mathbf{Z}_p, \Gamma(N)^{\text{arith}})$. The functional equation for Φ,

5.11.11 $$2\Phi_{k,r,f} = 2\Phi_{r,k,f^t} , \qquad k, r \geqq 0$$

(which is obvious from 5.11.3) becomes one for G:

5.11.12 $$2G_{A,B,f} = 2G_{A,1-A-B,f^t} , \qquad B \leqq 0,\ A + B \geqq 1 .$$

The differentiation relation

5.11.13 $$N\theta(2\Phi_{k,r,f}) = 2\Phi_{k+1,r+1,f} , \qquad k, r \geqq 0$$

(also obvious from 5.11.3, cf. 5.11.6–8) becomes

5.11.14 $$N\theta(2G_{A,B,f}) = 2G_{A+2,B-1,f} , \qquad B \leqq 0,\ A + B \geqq 1 .$$

To give the transformation properties under the group $G(N)$, it is convenient to introduce a notation. Given $b \in (\mathbf{Z}/N\mathbf{Z})^\times$ and a function f on $\mathbf{Z}/N\mathbf{Z} \times \mathbf{Z}/N\mathbf{Z}$, the function $[b]f$ is defined by

5.11.15 $$[b]f(u, v) = f(bu, bv) .$$

LEMMA 5.11.16. *The transformation property of the Φ and the G under the group $G(N)$ is given by the formulas*

5.11.17 $$\begin{cases} [a, b](2\Phi_{k,r,f}) = a^{k+r+1}2\Phi_{k,r,[b]f} , & k, r \geqq 0 \\ [a, b](2G_{A,B,f}) = a^A 2G_{A,B,[b]f} , & B \leqq 0,\ A + B \geqq 1 . \end{cases}$$

Proof. By 5.11.10, the two formulas are equivalent. We will prove the first. By 5.11. 13 and the fact that θ is of weight two, we may assume that either $k = 0$ or $r = 0$. By 5.11.11, we may assume $r = 0$. Thus we are reduced to showing

5.11.18 $$[a, b]G_{k,0,f} = a^k G_{k,0,[b]f} \qquad \text{for } k \geqq 1 .$$

If $k = 2$ and f is either the characteristic function of $\mathbf{Z}/N\mathbf{Z} \times \{0\}$, or $\{0\} \times \mathbf{Z}/N\mathbf{Z}$, then $f = [b]f$ and $G_{2,0,f}$ is a multiple of P, which indeed satisfies $[a, b]P = a^2P$.

So we may assume that, if $k = 2$, the function f satisfies $\sum f(j, 0) = \sum f(0, l) = 0$, whence $G_{k,0,f}$ lies in $R^k(\mathbf{Q}_p, \Gamma(N)^{\text{arith}})$. The entire group $\mathbf{Q}_p^\times \times (\mathbf{Z}/N\mathbf{Z})^\times$ acts on $R^k(\mathbf{Q}_p, \Gamma(N)^{\text{arith}})$, by the rule

5.11.19 $$[a, b]F(E, \omega, \beta) = F\big(E, a^{-1}\omega, \beta\circ(b, b^{-1})\big) .$$

Under this action, resticted to the subgroup $G(N)$, the map

$$R^k\big(\mathbf{Q}_p, \Gamma(N)^{\text{arith}}\big) \longrightarrow GV^k\big(\mathbf{Z}_p, \Gamma(N)^{\text{arith}}\big) \otimes \mathbf{Q}_p$$

is $G(N)$-equivariant. Now since $G_{k,0,f} \in R^k$, we certainly have

5.11.20 $$\begin{aligned}[a, b]G_{k,0,f}(E, \omega, \beta) &= G_{k,0,f}\big(E, a^{-1}\omega, \beta\circ(b, b^{-1})\big) \\ &= a^k G_{k,0,f}\big(E, \omega, \beta\circ(b, b^{-1})\big) \\ &= a^k[1, b]G_{k,0,f}(E, \omega\beta) .\end{aligned}$$

Thus it suffices to check that

5.11.21 $$[1, b]G_{k,0,f} = G_{k,0,[b]f} .$$

Since the assertion is linear in f, we may suppose f to have values in, say, $\mathbf{Z}$, then extend scalars to $\mathbf{C}$ and view $G_{k,0,f}$ as lying in $R^k(\mathbf{C}, \Gamma(N)^{\text{arith}})$. By (2.4), we may view $G_{k,0,f}$ as a function on $\mathrm{GL}^+/\Gamma(N)$, and for fixed $(\omega_1, \omega_2) \in \mathrm{GL}^+$, the value $G_{k,0,f}(\omega_1, \omega_2)$ is the value at $s = 0$ of the entire function $s \mapsto G_{k,s,f}(\omega_1, \omega_2)$. So by analytic continuation, it suffices to check that

5.11.22 $$[1, b]G_{k,s,f} = G_{k,s,[b]f} \qquad \text{for } \mathrm{Re}(s) \gg 0.$$

In view of the definition (3.6.5) of $G_{k,s,f}$ in terms of φ_k,

5.11.23 $$G_{k,s,f}(E, \omega, \beta) = \frac{(-1)^k}{2}\varphi_k\Big(s + \frac{k}{2}, E, \omega, (P^{-1}f)\circ\beta^{-1}\Big) ,$$

we must check that

5.11.24 $$P^{-1}\big([b]f\big)\circ\beta^{-1} = (P^{-1}f)\circ\big(\beta\circ(b, b^{-1})\big)^{-1} ,$$

i.e., $$P^{-1}\big([b]f\big) = (P^{-1}f)\circ(b^{-1}, b) .$$

By definition, we have

$$\begin{aligned}P^{-1}([b]f)(\zeta, m) &= \frac{1}{N}\sum_n([b]f)(n, m)\zeta^{-n}\\ &= \frac{1}{N}\sum_n f(bn, bm)\zeta^{-n}\\ &= \frac{1}{N}\sum_n f(n, bm)\zeta^{-b^{-1}n}\\ &= (P^{-1}f)(\zeta^{b^{-1}}, bm)\\ &= (P^{-1}f)\circ(b^{-1}, b)(\zeta, m)\,. \qquad \text{Q.E.D.}\end{aligned}$$

Chapter VI. Construction of the Eisenstein-Ramanujan measures $\mu_N^{(a,b)}$ and μ_N

6.0. *Review of p-adic measures.* Let X be a compact topological space, and denote by Contin $(X, \mathbf{Z}_p)$ the ring of all continuous $\mathbf{Z}_p$-valued functions on X. For any p-adic ring B, a $\mathbf{Z}_p$-linear map (not assumed to be a ring homomorphism)

6.0.1 $$\mu\colon \text{Contin}\,(X, \mathbf{Z}_p) \longrightarrow B$$

is called a B-valued measure on X. We can also view μ as a B-linear map Contin $(X, B) \to B$, since Contin $(X, B) \simeq$ Contin $(X, \mathbf{Z}_p)\,\hat{\otimes}\, B$. For $f\colon X \to \mathbf{Z}_p$ a continuous function on X, its image $\mu(f) \in B$ is denoted symbolically

6.0.2 $$\int_X f d\mu, \quad \text{or} \quad \int f(x)d\mu(x)\,.$$

Notice that μ is automatically *continuous* for the p-adic topologies.

Let us specialize now to the case when X is the product of a *finite* space T with a finite number n of copies of $\mathbf{Z}_p$. By Mahler's theorem [19], any continuous function $f\colon (\mathbf{Z}_p)^n \times T \to B$ has a unique interpolation series

6.0.3 $$f(x_1, \cdots, x_n, t) = \sum_{i_1,\cdots,i_n\geq 0} a_{i_1,\cdots,i_n}(t)\binom{x_1}{i_1}\cdots\binom{x_n}{i_n}$$

where the $a_{i_1,\cdots,i_n}$ are $\mathbf{Z}_p$-valued functions on T which tend uniformly to zero as $\sum_{j=1}^n i_j \to \infty$, and where the $\binom{x}{n}$ are the binomial-coefficient functions

6.0.4 $$\binom{x}{n} = \frac{(x-1)\cdots(x-(n-1))}{n!}$$

which take $\mathbf{Z}_p$-values on $\mathbf{Z}_p$. Thus a measure μ on $(\mathbf{Z}_p)^n \times T$ is uniquely determined by the sequence of values

6.0.5 $$b(i_1, \cdots, i_n, t, \mu) \overset{\text{dfn}}{=} \int\binom{x_1}{i_1}\cdots\binom{x_n}{i_n} \times (\text{the char. fct. of a point } t \in T)d\mu,$$

and <u>any</u> collection $\{b_{i_1,\cdots,i_n,t}\}$ of elements of B, indexed by $\mathbf{N}^n \times T$, arises via

6.0.5 from a unique measure on $(\mathbf{Z}_p)^n \times T$.

6.0.6 If B is flat over $\mathbf{Z}_p$, then μ is also uniquely determined by its *moments*

6.0.7 $$m(i_1, \cdots, i_n, t; \mu) = \int (x_1)^{i_1} \cdots (x_n)^{i_n} \times (\text{char. fct. of } t \in T) d\mu .$$

However, these moments cannot be prescribed arbitrarily. Let us introduce the rational numbers $c(j_1, \cdots, j_n; i_1, \cdots, i_n)$ defined by

6.0.8 $$\binom{x_1}{i_1} \cdots \binom{x_n}{i_n} = \sum_{0 \leqq j_\nu \leqq i_\nu} c(j_1, \cdots, j_n; i_1, \cdots, i_n)(x_1)^{i_1} \cdots (x_n)^{i_n} .$$

In terms of these, we have

LEMMA 6.0.9. *If B is a p-adic ring flat over $\mathbf{Z}_p$, then a collection $m(i_1, \cdots, i_n, t)$ of elements of B, indexed by $\mathbf{N}^n \times T$, arises as the moments of a (necessarily unique) measure on $(\mathbf{Z}_p)^n \times T$ if and only if the quantities*

6.0.10 $$b(i_1, \cdots, i_n, t) \overset{\text{dfn}}{=} \sum_{0 \leqq j_\nu \leqq i_\nu} c(j_1, \cdots, j_n; i_1, \cdots, i_n) m(j_1, \cdots, j_n, t) ,$$

which a priori are elements of $B[1/p]$, all lie in B.

6.1. *Construction of the measure $\mu_N^{(a,b)}$.*

THEOREM 6.1.1. *Let $N \geqq 1$ be an integer, and (a, b) an element of the group $G(N)$. There exists a $V(\mathbf{Z}_p, \Gamma(N)^{\text{arith}})$-valued measure $\mu_N^{(a,b)}$ on $\mathbf{Z}_p \times \mathbf{Z}_p \times \mathbf{Z}/N\mathbf{Z} \times \mathbf{Z}/N\mathbf{Z}$ whose moments are given by*

6.1.2 $$\begin{aligned} \int x^k y^r f(u, v) d\mu_N^{(a,b)} &= 2\Phi_{k,r,f} - 2[a, b]\Phi_{k,r,f} \\ &= 2\Phi_{k,r,f} - 2a^{k+r+1}\Phi_{k,r,[b]f} \end{aligned}$$

where $f(u, v)$ is any $\mathbf{Z}_p$-valued function on $\mathbf{Z}/N\mathbf{Z} \times \mathbf{Z}/N\mathbf{Z}$.

For any continuous $\mathbf{Z}_p$-valued function $\psi(x, y)$ on $\mathbf{Z}_p \times \mathbf{Z}_p$, the q-expansion of $\int \psi(x, y) f(u, v) d\mu_N^{(a,b)}$ has the form

6.1.3 $$\textit{constant} + \sum_{n \geq 1} q^n \sum_{n = dd'} \begin{pmatrix} \psi(d, d')f(d, d') - \psi(-d, -d')f(-d, -d') \\ -a\psi(ad, ad')f(bd, bd') \\ +a\psi(-ad, -ad')f(-bd, -bd') \end{pmatrix} .$$

The transformation property of $\int \psi(x, y) f(u, v) d\mu_N^{(a,b)}$ under an element $[a', b'] \in G(N)$ is given by

6.1.4 $$[a', b'] \int \psi(x, y) f(u, v) d\mu_N^{(a,b)} = \int a' \psi(a'x, a'y) f(b'u, b'v) d\mu_N^{(a,b)} .$$

The functional equation may be expressed in terms of the functions $\psi^t(x, y) \overset{\text{dfn}}{=} \psi(y, x)$ and $f^t(u, v) \overset{\text{dfn}}{=} f(v, u)$ by the relation

6.1.5 $$\int \psi(x, y) f(u, v)\, d\mu_N^{(a,b)} = \int \psi^t(x, y) f^t(u, v)\, d\mu_N^{(a,b)} .$$

Proof-construction. Suppose that we already know the existence of a measure $\mu_N^{(a,b)}$ satisfying 6.1.2. Then 6.1.3–5 are visibly true when the function ψ is a monomial $x^k y^r$, thanks to 5.11.3 and 5.11.16. By linearity, 6.1.3–5 will remain true when $\psi(x, y)$ is a finite $\mathbf{Z}_p$-linear combination of binomial coefficient functions $\binom{x}{i}\binom{y}{j}$, and hence, by Mahler's theorem and the p-adic continuity of $\mu_N^{(a,b)}$, when ψ is an arbitrary $\mathbf{Z}_p$-valued continuous function.

To show the *existence* of $\mu_N^{(a,b)}$, we use the integrality criterion 6.0.9. We must show that for any $\mathbf{Z}_p$-valued function f on $\mathbf{Z}/N\mathbf{Z} \times \mathbf{Z}/N\mathbf{Z}$, whenever we write

6.1.6 $$\binom{x}{k}\binom{y}{r} = \sum_{\substack{0 \leqq n \leqq k \\ 0 \leqq m \leqq r}} c(n, m; k, r) x^n y^m ,$$

the corresponding sum

$$\begin{aligned} &\sum_{n\, m} c(n, m; k, r)(2\Phi_{n,m,f} - 2[a, b]\Phi_{n,m,f}) \\ &\quad = (1 - [a, b])\Big(2\sum_{n,m} c(n, m; k, r)\Phi_{n,m,f}\Big) , \end{aligned}$$

a priori an element of $V(\mathbf{Z}_p, \Gamma(N)^{\mathrm{arith}}) \otimes \mathbf{Q}_p$, actually lies in $V(\mathbf{Z}_p, \Gamma(N)^{\mathrm{arith}})$. Notice that by 5.11.3, the inner sum

6.1.7 $$2\sum_{n,m} c(n, m; k, r)\Phi_{n,m,f}$$

has a q-expansion which is *integral* except possibly for its constant term: the coefficient of q^n for $n \geqq 1$ is given by

6.1.8 $$\begin{aligned} \sum_{n=dd'} \Bigg(&\binom{d}{k}\binom{d'}{r} f(d, d') - \binom{-d}{k}\binom{-d'}{r} f(-d, -d') \\ &- a\binom{ad}{k}\binom{ad'}{r} f(bd, bd') + a\binom{-ad}{k}\binom{-ad'}{k} f(-bd, -bd')\Bigg) . \end{aligned}$$

Thus to conclude the proof, it suffices to apply to this element 6.1.7 the following basic lemma (cf. [15], 1.2.1).

KEY LEMMA 6.1.9. *Let F be any element of $V(\mathbf{Z}_p, \Gamma(N)^{\mathrm{arith}}) \otimes \mathbf{Q}_p$, whose q-expansion has all of its coefficients in $\mathbf{Z}_p$ except possibly for the constant term. Then for any element (a, b) in $G(N)$, the difference $F - [a, b]F$ lies in $V(\mathbf{Z}_p, \Gamma(N)^{\mathrm{arith}})$.*

Proof. Let $c \in \mathbf{Q}_p$ be the constant term. The difference $F - c$ lies in $V(\mathbf{Z}_p, \Gamma(N)^{\mathrm{arith}}) \otimes \mathbf{Q}_p$, but has *integral* q-expansion by hypothesis, so must be in fact an element of $V(\mathbf{Z}_p, \Gamma(N)^{\mathrm{arith}})$ (lest it give a p-power torsion element of $\widehat{\mathbf{Z}_p((q))}/V(\mathbf{Z}_p, \Gamma(N)^{\mathrm{arith}})$, cf. 5.2.1 and [15], 1.2). If we extend by linearity the action of $G(N)$ to $V(\mathbf{Z}_p, \Gamma(N)^{\text{arith}}) \otimes \mathbf{Q}_p$, then any *constant* $c \in \mathbf{Q}_p$ is certainly fixed by all of $G(N)$. Therefore

6.1.10 $$F - [a, b]F = (F - c) - [a, b](F - c) \in V(\mathbf{Z}_p, \Gamma(N)^{\text{arith}}) . \qquad \text{Q.E.D.}$$

6.2. *Relation to the Kubota-Leopoldt measure, and to the "Eisenstein measure"* $2\mathbf{H}^{a,b}$ *of* [15]. Given a continuous map $\pi: X \to Y$ of compact topological spaces, and a B-valued measure μ on X, we obtain a B-valued measure $\pi_*\mu$ on Y, defined by

6.2.0 $$\int_Y f(y) d\pi_*\mu(y) = \int_X f(\pi(x)) d\mu(x) .$$

In particular, if we take the map

$$pr_1: \mathbf{Z}_p \times \mathbf{Z}_p \times \mathbf{Z}/N\mathbf{Z} \times \mathbf{Z}/N\mathbf{Z} \longrightarrow \mathbf{Z}_p \times \mathbf{Z}/N\mathbf{Z} ,$$
$$(x, y, u, v) \longmapsto (x, u) ,$$

we obtain a measure $pr_{1*}\mu_N^{(a,b)}$ on $\mathbf{Z}_p \times \mathbf{Z}/N\mathbf{Z}$, defined by

6.2.1 $$\int_{\mathbf{Z}_p \times \mathbf{Z}/N\mathbf{Z}} \psi(x) f(u) d(pr_{1*}\mu_N^{(a,b)}) = \int_{(\mathbf{Z}_p)^2 \times (\mathbf{Z}/N\mathbf{Z})^2} \psi(x) f(u) d\mu_N^{(a,b)}$$

where, on the right, "$\psi(x)$" is the function $(x, y) \mapsto \psi(x)$, and "$f(u)$" is $(u, v) \mapsto f(u)$. The moments of this measure are the Eisenstein series $G_{k+1,0,f}$ of 5.11.0

6.2.2 $$\int_{\mathbf{Z}_p \times \mathbf{Z}/N\mathbf{Z}} x^k f(u) dpr_{1*}\mu_N^{(a,b)} = (1 - [a, b])(2G_{k+1,0,f})$$

(where "f" is the function $(u, v) \mapsto f(u)$). Their q-expansions are given by

6.2.3 $$\int_{\mathbf{Z}_p \times \mathbf{Z}/N\mathbf{Z}} x^k f(u) dpr_{1*}\mu_N^{(a,b)}$$
$$= \begin{cases} 0 & \text{if } f \text{ is of parity } (-1)^k \\ L(-k, f(u)) - a^{k+1}L(-k, f(bu)) & \\ \quad + 2\sum_{n \geq 1} q^n \sum_{d/n} d^k(f(d) - a^{k+1}f(bd)) & \text{if } f \text{ is of parity } (-1)^{k-1} . \end{cases}$$

These q-expansions are the *same* as those of the moments of $V(\mathbf{Z}_p, \Gamma_{00}(N)^{\text{arith}})$-valued "Eisenstein measure" which was denoted $2\mathbf{H}^{a,b}$ in [15]. To clarify this apparent discrepancy (between considering a given q-series as being on $\Gamma(N)^{\text{arith}}$ or on $\Gamma_{00}(N)^{\text{arith}}$), recall that the construction "divide by $\mathbf{Z}/N\mathbf{Z}$" (cf. 2.3.5, the diagonal arrow) gives by transposition an "exotic inclusion"

6.2.4 $$V(\mathbf{Z}_p, \Gamma_{00}(N)^{\text{arith}}) \xrightarrow{(\text{divide by } \mathbf{Z}/N\mathbf{Z})^*} V(\mathbf{Z}_p, \Gamma(N)^{\text{arith}})$$

which preserves q-expansions. Thus we have

Compatibility 6.2.5. *The following diagram is commutative.*

6.2.6
$$\begin{tikzcd} \mathrm{Contin}(\mathbf{Z}_p \times \mathbf{Z}/N\mathbf{Z}, \mathbf{Z}_p) \arrow[r, "2\mathbf{H}^{a,b}"] \arrow[d, "pr_1^*"'] \arrow[dr, "pr_{1*}\mu_N^{(a,b)}"] & V(\mathbf{Z}_p, \Gamma_{00}(N)^{\mathrm{arith}}) \arrow[d, "(\text{divide by } \mathbf{Z}/N\mathbf{Z})^*"] \\ \mathrm{Contin}((\mathbf{Z}_p)^2 \times (\mathbf{Z}/N\mathbf{Z})^2, \mathbf{Z}_p) \arrow[r, "\mu_N^{(a,b)}"] & V(\mathbf{Z}_p, \Gamma(N)^{\mathrm{arith}}) . \end{tikzcd}$$

6.2.7. Let us denote by $\mu_{K.\text{-}L.}^{(a,b)}$ the $\mathbf{Z}_p$-valued Kubota-Leopoldt measure on $\mathbf{Z}_p \times \mathbf{Z}/N\mathbf{Z}$, defined to be the *constant term* in the q-expansion of $pr_{1*}\mu_N^{(a,b)} = 2\mathbf{H}^{a,b}$. Thus

6.2.8
$$\int_{\mathbf{Z}_p \times \mathbf{Z}/N\mathbf{Z}} x^k f(u) d\mu_{K.\text{-}L.}^{(a,b)} = L(-k, f(u)) - a^{k+1} L(-k, f(bu)) .$$

In terms of the Kubota-Leopoldt measure $\mu_{K.\text{-}L.}^{(a,b)}$, we can give a formula for the "missing" constant (cf. 6.1.3) in the q-expansion of $\mu_N^{(a,b)}$.

LEMMA 6.2.9. *For any continuous $\mathbf{Z}_p$-valued function $\psi(x, y)$ on $\mathbf{Z}_p \times \mathbf{Z}_p$, and any $\mathbf{Z}_p$-valued function f on $\mathbf{Z}/N\mathbf{Z} \times \mathbf{Z}/N\mathbf{Z}$, the constant term of the q-expansion of $\int \psi(x, y) f(u, v) d\mu_N^{(a,b)}$ is equal to*

6.2.10
$$\int_{\mathbf{Z}_p \times \mathbf{Z}/N\mathbf{Z}} (\psi(x, 0) f(u, 0) + \psi(0, x) f(0, u)) d\mu_{K.\text{-}L.}^{(a,b)} .$$

Proof. It suffices to check when $\psi(x, y)$ is a monomial $x^k y^r$. When $k \geqq 1$ and $r \geqq 1$, both sides vanish. Since both sides are invariant under $\psi f \mapsto \psi^t f^t$, it suffices to check the case $r = 0$, $k \geqq 0$, which is taken care of by comparing the formulas 6.2.8 and 5.11.1. Q.E.D.

6.3. *Restricting $\mu_N^{(a,b)}$ to $\mathbf{Z}_p^\times \times \mathbf{Z}_p \times (\mathbf{Z}/N\mathbf{Z})^2$, and its relation to Frobenius.* Given a compact open set U in a space X, the characteristic function of U, χ_U, is continuous. If X is compact, and μ is a B-valued measure on X, we define its *restriction* to U as the measure *on* X defined by

6.3.1
$$f \longmapsto \int_X \chi_U(x) f(x) d\mu(x) \overset{\mathrm{dfn}}{=} \int_U f(x) d\mu(x) .$$

Of course, we can also view it as the measure *on* U defined by

6.3.2
$$\int_U g(u) d\mu(u) \overset{\mathrm{dfn}}{=} \int_X (g \text{ extended to be zero outside } U) d\mu(x) .$$

This should never lead to any confusion.

LEMMA 6.3.3. *For any continuous $\mathbf{Z}_p$-valued functions ψ on $\mathbf{Z}_p \times \mathbf{Z}_p$, f on $\mathbf{Z}/N\mathbf{Z} \times \mathbf{Z}/N\mathbf{Z}$, we have the integration formula*

6.3.4
$$\int_{\mathbf{Z}_p^\times \times \mathbf{Z}_p \times (\mathbf{Z}/N\mathbf{Z})^2} \psi(x, y) f(u, v) d\mu_N^{(a,b)} = \int_{(\mathbf{Z}_p)^2 \times (\mathbf{Z}/N\mathbf{Z})^2} \psi(x, y) f(u, v) d\mu_N^{(a,b)}$$
$$- \mathrm{Frob} \int_{(\mathbf{Z}_p)^2 \times (\mathbf{Z}/N\mathbf{Z})^2} \psi(px, y) f(pu, v) d\mu_N^{(a,b)} .$$

Proof. First of all, notice that both sides have the *same* q-expansion coefficients, except possibly for their constant terms, as an immediate computation using 6.1.3 shows. Secondly, notice that it suffices to treat the case when ψ is a monomial $x^k y^r$, in which case, by 6.1.4, both sides are of weight $k + r + 1 \geqq 1$ under the subgroup $\mathbf{Z}_p^\times \times \{1\} \cap G(N)$ of $G(N)$. So their *difference* is then a *constant* which is of weight $\neq 0$, hence is zero. Q.E.D.

Remark 6.3.6. Combining the *definition* 6.3.1 with the formula 6.2.10 for the *constant term*, we see that the constant term in the q-expansion of

$$\int_{\mathbf{Z}_p^\times \times \mathbf{Z}_p \times (\mathbf{Z}/N\mathbf{Z})^2} \psi(x, y) f(u, v) d\mu_N^{(a, b)}$$

is equal to

6.3.7 $$\int_{\mathbf{Z}_p^\times \times \mathbf{Z}/N\mathbf{Z}} \psi(x, 0) f(u, 0) d\mu_{K.\text{-}L.}^{(a,b)}$$

Combining this with 6.3.3, we obtain a well-known integration formula for $\mu_{K.\text{-}L.}$

COROLLARY 6.3.8. *For any continuous* $\mathbf{Z}_p$*-valued functions* ψ *on* $\mathbf{Z}_p$ *and* f *on* $\mathbf{Z}/N\mathbf{Z}$, *we have*

6.3.9 $$\int_{\mathbf{Z}_p^\times \times \mathbf{Z}/N\mathbf{Z}} \psi(x) f(u) d\mu_{K.\text{-}L.}^{(a,b)} = \int_{\mathbf{Z}_p \times \mathbf{Z}/N\mathbf{Z}} (\psi(x) f(u) - \psi(px) f(pu)) d\mu_{K.\text{-}L.}^{(a,b)} .$$

Proof. View ψ and f as functions on $\mathbf{Z}_p \times \mathbf{Z}_p$ and $\mathbf{Z}/N\mathbf{Z} \times \mathbf{Z}/N\mathbf{Z}$ respectively, through projection on the first variable: $\psi(x, y) = \psi(x)$, $f(u, v) = f(u)$. If we equate the constant terms in 6.3.4, and use 6.3.7, we get an identity,

6.3.10 $$\begin{aligned} &\int_{\mathbf{Z}_p^\times \times \mathbf{Z}/N\mathbf{Z}} \psi(x, 0) f(u, 0) d\mu_{K.\text{-}L.}^{(a,b)} \\ &\quad = \int_{\mathbf{Z}_p \times \mathbf{Z}/N\mathbf{Z}} (\psi(x, 0) f(u, 0) + \psi(0, x) f(0, u)) d\mu_{K.\text{-}L.}^{(a,b)} \\ &\quad\quad - \int_{\mathbf{Z}_p \times \mathbf{Z}/\mathbf{Z}N} (\psi(px, 0) f(pu, 0) + \psi(p0, x) f(p0, u)) d\mu_{K.\text{-}L.}^{(a,b)} , \end{aligned}$$

in which the $\psi(0, x) f(0, u)$ term cancels the $\psi(p0, x) f(p0, u)$ term to give the assertion. Q.E.D.

Remark 6.3.11. We can use the functional equation 6.1.5 of the measure $\mu_N^{(a, b)}$ to deduce analogues of 6.3.4 and 6.3.7 for restriction to $\mathbf{Z}_p \times \mathbf{Z}_p^\times \times (\mathbf{Z}/N\mathbf{Z})^2$. The result is

6.3.12 $$\begin{aligned} &\int_{\mathbf{Z}_p \times \mathbf{Z}_p^\times \times (\mathbf{Z}/N\mathbf{Z})^2} \psi(x, y) f(u, v) d\mu_N^{(a, b)} \\ &= \int_{(\mathbf{Z}_p)^2 \times (\mathbf{Z}/N\mathbf{Z})^2} \psi(x, y) f(u, v) d\mu_N^{(a,b)} - \operatorname{Frob} \int_{(\mathbf{Z}_p)^2 \times (\mathbf{Z}/N\mathbf{Z})} \psi(x, py) f(u, pv) d\mu_N^{(a,b)} \\ &= \int_{\mathbf{Z}_p^\times \times \mathbf{Z}/N\mathbf{Z}} (\psi(0, x) f(0, u)) d\mu_{K.\text{-}L.}^{(a, b)} + \text{higher terms (in } q\text{-expansion)} . \end{aligned}$$

If we *combine* 6.3.4 and 6.3.12, we get a formula for restricting $\mu_N^{(a,b)}$ to $(\mathbf{Z}_p^\times)^2 \times (\mathbf{Z}/N\mathbf{Z})^2$. The result is

$$\begin{aligned}6.3.13 \qquad \int_{(\mathbf{Z}_p^\times)^2 \times (\mathbf{Z}/N\mathbf{Z})} \psi(x, y) f(u, v) d\mu_N^{(a,b)} &= \int \psi(x, y) f(u, v) d\mu_N^{(a,b)} - \operatorname{Frob} \int \psi(px, y) f(du, v) d\mu_N^{(a,b)} \\ &\quad - \operatorname{Frob} \int \psi(x, py) f(u, pv) d\mu_N^{(a,b)} \\ &\quad + \operatorname{Frob}^2 \int \psi(px, py) f(pu, pv) d\mu_N^{(a,b)} .\end{aligned}$$

If we apply these formulas to functions ψ on $\mathbf{Z}_p$ and f on $\mathbf{Z}/N\mathbf{Z}$, pulled up to functions on $\mathbf{Z}_p \times \mathbf{Z}_p$ and $\mathbf{Z}/N\mathbf{Z} \times \mathbf{Z}/N\mathbf{Z}$ respectively by pr_1, i.e., $\psi(x, y) = \psi(x)$, $f(u, v) = f(u)$, we get the integration formulas

$$6.3.14 \qquad \int_{(\mathbf{Z}_p)^2 \times (\mathbf{Z}/N\mathbf{Z})^2} \psi(x) f(u) d\mu_N^{(a,b)} = \int_{\mathbf{Z}_p \times \mathbf{Z}/N\mathbf{Z}} \psi(x) f(u) d(2\mathbf{H}^{a,b}) ,$$

$$6.3.15 \qquad \int_{\mathbf{Z}_p^\times \times \mathbf{Z}_p \times (\mathbf{Z}/N\mathbf{Z})^2} \psi(x) f(u) d\mu_N^{(a,b)} = \int_{\mathbf{Z}_p^\times \times \mathbf{Z}/N\mathbf{Z}} \psi(x) f(u) d(2\mathbf{H}^{a,b}) ,$$

$$6.3.16 \qquad \int_{\mathbf{Z}_p \times \mathbf{Z}_p^\times \times (\mathbf{Z}/N\mathbf{Z})^2} \psi(x) f(u) d\mu_N^{(a,b)} = (1 - \operatorname{Frob}) \int_{\mathbf{Z}_p \times \mathbf{Z}/N\mathbf{Z}} \psi(x) f(u) d(2\mathbf{H}^{a,b}) ,$$

$$6.3.17 \qquad \int_{\mathbf{Z}_p^\times \times \mathbf{Z}_p^\times \times (\mathbf{Z}/N\mathbf{Z})^2} \psi(x) f(u) d\mu_N^{(a,b)} = (1 - \operatorname{Frob}) \int_{\mathbf{Z}_p^\times \times \mathbf{Z}/N\mathbf{Z}} \psi(x) f(u) d(2\mathbf{H}^{a,b}) .$$

6.4. *Restriction to $(\mathbf{Z}_p^\times)^2 \times (\mathbf{Z}/N\mathbf{Z})^2$; the measure μ_N.*

6.4.0. Let k and r be non-negative integers, and f a $\mathbf{Z}_p$-valued function on $\mathbf{Z}/N\mathbf{Z} \times \mathbf{Z}/N\mathbf{Z}$. We define the q-series $2\Phi_{k,r,f}^*$ by the formula

$$6.4.1 \qquad 2\Phi_{k,r,f}^* = \sum_{\substack{n \geqq 1 \\ (p,n)=1}} \sum_{n=dd'} \left(d^k (d')^r f(d, d') - (-d)^k (-d')^r f(-d, -d')\right) .$$

LEMMA 6.4.2. *For k, r non-negative integers, and f a $\mathbf{Z}_p$-valued function on $\mathbf{Z}/N\mathbf{Z} \times \mathbf{Z}/N\mathbf{Z}$, the series $2\Phi_{k,r,f}^*$ is the q-expansion of an element of $GV^{k+r+1}(\mathbf{Z}_p, \Gamma(N)^{\text{arith}})$. For any element $(a_0, 1) \in G(N) \cap (\mathbf{Z}_p \times \{1\})$, we have*

$$6.4.3 \qquad (1 - a_0^{k+r+1}) 2\Phi_{k,r,f}^* = \int_{(\mathbf{Z}_p^\times)^2 \times (\mathbf{Z}/N\mathbf{Z})^2} x^k y^r f(u, v) d\mu_N^{(a_0,1)} .$$

The transformation property of $2\Phi_{k,r,f}^*$ under $(a, b) \in G(N)$ is given by

$$6.4.4 \qquad [a, b](2\Phi_{k,r,f}^*) = a^{k+r+1} 2\Phi_{k,r,[b]f}^* .$$

Proof. From 6.2.10, we see that $\int_{(\mathbf{Z}_p^\times)^2 \times (\mathbf{Z}/N\mathbf{Z})^2} \psi(x, y) f(u, v) d\mu_N^{(a,b)}$ always has constant term *zero* in its q-expansion. The truth of 6.4.3 as an identity of q-series then follows from 6.1.3. Choosing any $a_0 \in \mathbf{Z}_p^\times$ so that $(a_0, 1) \in G(N)$ and $a_0^{k+r+1} \neq 1$, we can read 6.4.3 as defining $2\Phi_{k,r,f}^*$ as an element of $GV^{k+r+1}(\mathbf{Z}_p, \Gamma(N)^{\text{arith}}) \otimes \mathbf{Q}_p$, which by 6.1.4 will enjoy the transformation law

6.4.4. Finally, the fact that $2\Phi^*_{k,r,f}$ has integral q-expansion shows that in fact it lies in $GV^{k+r+1}(\mathbf{Z}_p, \Gamma(N)^{\text{arith}})$. Q.E.D.

The functional equation

6.4.5 $$2\Phi^*_{k,r,f} = 2\Phi^*_{r,k,f^t}$$

results immediately from its q-expansion formula 6.4.1, as does the differentiation formula

6.4.6 $$N\theta(2\Phi^*_{k,r,f}) = 2\Phi^*_{k+1,r+1,f}$$

THEOREM 6.4.7. *Let $N \geqq 1$ be an integer. There exists a $V(\mathbf{Z}_p, \Gamma(N)^{\text{arith}})$-valued measure μ_N on $(\mathbf{Z}_p^\times)^2 \times (\mathbf{Z}/N\mathbf{Z})^2$, whose moments are given by*

6.4.8 $$\int x^k y^r f(u, v)\, d\mu_N = 2\Phi^*_{k,r,f}\ .$$

where $f(u, v)$ is any $\mathbf{Z}_p$-valued function on $\mathbf{Z}/N\mathbf{Z} \times \mathbf{Z}/N\mathbf{Z}$.

For any continuous function $\psi(x, y)$ on $\mathbf{Z}_p \times \mathbf{Z}_p$, we have the q-expansion formula

6.4.9 $$\begin{aligned}&\int \psi(x, y) f(u, v)\, d\mu_N \\ &= \sum_{\substack{n \geqq 1 \\ (p,n)=1}} q^n \sum_{n=dd'} \big(\psi(d, d') f(d, d') - \psi(-d, -d') f(-d, -d')\big)\ .\end{aligned}$$

The transformation property under $(a, b) \in G(N)$ is

6.4.10 $$[a, b]\int \psi(x, y) f(u, v)\, d\mu_N = \int a\psi(ax, ay) f(bu, bv)\, d\mu_N\ .$$

The relation between μ_N and the restriction of $\mu_N^{(a,b)}$ to $(\mathbf{Z}_p^\times)^2 \times (\mathbf{Z}/N\mathbf{Z})^2$ is given by the formula

6.4.11 $$(1 - [a, b])\int \psi(x, y) f(u, v)\, d\mu_N = \int_{(\mathbf{Z}_p^\times)^2 \times (\mathbf{Z}/N\mathbf{Z})^2} \psi(x, y) f(u, v)\, d\mu_N^{(a,b)}\ .$$

Proof. The *existence* of a measure μ_N on $\mathbf{Z}_p \times \mathbf{Z}_p \times \mathbf{Z}/N\mathbf{Z} \times \mathbf{Z}/N\mathbf{Z}$ satisfying 6.4.8 follows immediately from the integrality criterion 6.0.9 and the simple q-expansion formula for $2\Phi^*_{k,r,f}$ much as in the proof of 6.1.1, except that here there is no constant term to worry over. The formula 6.4.9 is valid for ψ of the form $x^k y^r$, so by linearity for ψ of the form $\binom{x}{k}\binom{y}{r}$, and then by Mahler for all continuous ψ; similarly for 6.4.10. To prove 6.4.11, we check it in q-expansion, using 6.4.9 and 6.4.10 to compute the left side, and using 6.1.3 and 6.2.10 to compute the right. Q.E.D.

COROLLARY 6.4.12. *For any $(a, b) \in G(N)$, we have the integration formula*

6.4.13 $$\left(1-[a, b]\right)\int\psi(x, y)f(u, v)\,d\mu_N$$
$$= \int\psi(x, y)f(u, v)\,d\mu_N^{(a,b)} - \mathrm{Frob}\int\psi(px, y)f(pu, v)\,d\mu_N^{(a,b)}$$
$$- \mathrm{Frob}\int\psi(x, py)f(u, pv)\,d\mu_N^{(a,b)}$$
$$+ \mathrm{Frob}^2\int\psi(px, py)f(pu, pv)\,d\mu_N^{(a,b)} .$$

Proof. Combine 6.4.11 with 6.3.13.

COROLLARY 6.4.14. *For k, r non-negative integers, and f any $\mathbf{Z}_p$-valued function on $\mathbf{Z}/N\mathbf{Z} \times \mathbf{Z}/N\mathbf{Z}$, we have an equality in $GV^{\cdot}(\mathbf{Z}_p, \Gamma(N)^{\mathrm{arith}}) \otimes Q_p$:*

6.4.15 $$\Phi^*_{k,r,f} = \Phi_{k,r,f} - p^k\,\mathrm{Frob}\,(\Phi_{k,r,f(pu,v)}) - p^r\,\mathrm{Frob}\,(\Phi_{k,r,f(u,pv)}) + p^{k+r}\,\mathrm{Frob}^2(\Phi_{k,r,f(pu,pv)}) .$$

Proof. This is 6.4.13, if we take $x^k y^r$ for ψ, $(a, b) = (a, 1) \in G(N) \cap (\mathbf{Z}_p^\times \times \{1\})$, and divide through by the common factor $2(1 - a^{k+r+1})$ which occurs.

Oversight 6.4.16. The behaviour of μ_N under the derivation $N\theta$ is given by

6.4.17 $$N\theta\int\psi(x, y)f(u, v)\,d\mu_N = \int xy\psi(x, y)f(u, v)\,d\mu_N ,$$

as follows immediately from 6.4.9.

The analogue of 6.3.17 is the formula

6.4.18 $$(1-[a, b])\int_{(\mathbf{Z}_p^\times)^2\times(\mathbf{Z}/N\mathbf{Z})^2}\psi(x)f(u)\,d\mu_N = (1-\mathrm{Frob})\int_{\mathbf{Z}_p^\times\times\mathbf{Z}/N\mathbf{Z}}\psi(x)f(u)\,d(2\mathbf{H}^{a,b}) ,$$

Chapter VII. Construction of p-adic L-functions: generalities

7.1. *Definition of $\mathfrak{L}(\chi, f)$.* Let W be a complete rank one valuation ring with residue field of characteristic p, and fraction field of characteristic zero. We take "rank one" instead of "discrete" to allow, for instance, the ring of integers in the completion of the algebraic closure of Q_p.

The measures $\mu_N^{(a,b)}$ and μ_N allow us to integrate W-valued continuous functions on $(\mathbf{Z}_p)^2 \times (\mathbf{Z}/N\mathbf{Z})^2$ and $(\mathbf{Z}_p^\times)^2 \times (\mathbf{Z}/N\mathbf{Z})^2$ respectively; their integrals will be elements of $V(W, \Gamma(N)^{\mathrm{arith}}) = V(\mathbf{Z}_p, \Gamma(N)^{\mathrm{arith}})\,\hat{\otimes}_{\mathbf{Z}_p} W$, cf. 6.0.1 and 5.1.0. In particular, if $\chi \in \mathrm{Hom}_{\mathrm{contin}}(\mathbf{Z}_p^\times \times \mathbf{Z}_p^\times, W^\times)$ is any continuous character (i.e., multiplicative homomorphism) of the group $\mathbf{Z}_p^\times \times \mathbf{Z}_p^\times$, and f is any W-valued function on $\mathbf{Z}/N\mathbf{Z} \times \mathbf{Z}/N\mathbf{Z}$, we can consider the integral

7.1.1 $$\int\chi(x, y)f(u, v)\,d\mu_N \in V(W, \Gamma(N)^{\mathrm{arith}}) .$$

We denote this integral $\mathfrak{L}(\chi, f)$, and view the construction $(\chi, f) \mapsto \mathfrak{L}(\chi, f)$ as a $V(W, \Gamma(N)^{\text{arith}})$-valued *function* on the space $\mathrm{Hom}_{\text{contin}}(\mathbf{Z}_p^\times \times \mathbf{Z}_p^\times, W^\times) \times \mathrm{Maps}(\mathbf{Z}/N\mathbf{Z} \times \mathbf{Z}/N\mathbf{Z}, W)$. This function $\mathfrak{L}(\chi, f)$ we call the ("two variable") p-adic L function. It is essentially the Mellin transform of the measure μ_N.

Knowledge of $\mathfrak{L}(\chi, f)$ is *equivalent* to knowledge of the measure μ_N, viewed as a measure on $(\mathbf{Z}_p)^2 \times (\mathbf{Z}/N\mathbf{Z})^2$ which is *supported* in $(\mathbf{Z}_p^\times)^2 \times (\mathbf{Z}/N\mathbf{Z})^2$. Indeed, if we denote by $\chi_{k,r}$ the character

7.1.2 $$\chi_{k,r}(x, y) = x^k y^r \qquad k, r \in \mathbf{Z},$$

then the L-values $\{\mathfrak{L}(\chi_{k,r}, f\}_{k,r \geq 0}$ are precisely the *moments* of the measure μ_N.

The fact that $\mathfrak{L}(\chi, f)$ *is* the Mellin transform of a measure implies a number of striking congruences between the values of $\mathfrak{L}$ at different characters (and conversely, by 6.0.9). Let us pause briefly to recall one such congruence.

LEMMA 7.1.3. *If (k, r) and (k', r') are pairs of integers satisfying*

$$(k, r) \equiv (k', r') \mod (p-1)p^n ,$$

then for any W-valued function f on $\mathbf{Z}/N\mathbf{Z} \times \mathbf{Z}/N\mathbf{Z}$, we have

$$\mathfrak{L}(\chi_{k,r}, f) \equiv \mathfrak{L}(\chi_{k',r'}, f) \mod p^{n+1} .$$

Proof. Because $(\mathbf{Z}/p^{n+1}\mathbf{Z})^\times$ has order $(p-1)p^n$, the hypothesis on the indices implies that the characters $\chi_{k,r}$ and $\chi_{k',r'}$ are congruent modulo p^{n+1} as functions on $\mathbf{Z}_p^\times \times \mathbf{Z}_p^\times$. This congruence of functions in turn implies the same congruence between their integrals.

In fact, the original point of view of Kubota-Leopoldt [17] when confronted with a function $f(k, r)$ on, say, $\mathbf{Z}_{\geq 0} \times \mathbf{Z}_{\geq 0}$, which satisfies the congruence of 7.1.3 (i.e., $f(k, r) \equiv f(k', r') \mod p^{n+1}$ if $(k, r) \equiv (k', r')$, mod $(p-1)p^n$), was this. For each of the $(p-1)^2$ residue classes (a, b) of $\mathbf{Z}^2 \mod p - 1$, let $S(a, b)$ denote the subset of $\mathbf{Z} \times \mathbf{Z}$ consisting of pairs (k, r) with $k \geqq 0$, $r \geqq 0$, and $(k, r) \equiv (a, b) \mod (p-1)$. Then $S(a, b)$ is uniformly dense in $\mathbf{Z}_p \times \mathbf{Z}_p$, and the function $f(k, r)$ extends to a (very) continuous function on all of $\mathbf{Z}_p \times \mathbf{Z}_p$. We will not pursue this point of view.

7.2. *Relation to the "one-variable" p-adic L-function* [15]. In [15], we constructed a p-adic L-function, which we will denote $\mathbf{L}$ temporarily to distinguish it from $\mathfrak{L}$. It is the function

7.2.1 $$\mathrm{Hom}_{\text{contin}}(G(N), W^\times) - \{\text{trivial character}\} \longrightarrow V(W, \Gamma_{00}(N)^{\text{arith}}) \otimes W\left[\frac{1}{p}\right]$$

defined by

7.2.2 $$\mathbf{L}(\psi\cdot\rho)=\frac{1}{1-\psi(a)\rho(b)}\int_{\mathbf{Z}_p^\times\times(\mathbf{Z}/N\mathbf{Z})^\times}\frac{\psi(x)}{x}\rho(u)d(\mathbf{H}^{a,b})\,.$$

Remark. The apparent ambiguity between the insistence on $G(N)$ in 7.2.1, and the integration over all of $\mathbf{Z}_p^\times\times(\mathbf{Z}/N\mathbf{Z})^\times$ is actually harmless, because when the measure $2\mathbf{H}^{a,b}$ is restricted to $\mathbf{Z}_p^\times\times(\mathbf{Z}/N\mathbf{Z})^\times$, it is in fact *supported* on the open subgroup $G(N)$. This last fact is obvious for the coefficients of q^n with $n\geqq 1$, which are sums of point evaluations at points $(d,d')\in G(N)$; it then follows for the constant term by a consideration of the transformation property of $\mathbf{L}$ under $G(N)$.

The q-expansion of $\mathbf{L}(\psi\cdot\rho)$ was given explicitly by

7.2.3 $$\frac{1}{1-\psi(a)\rho(b)}\left[\int\frac{\psi(x)}{x}\rho(u)d\mu_{K.-L.}^{(a,b)}\right] + \sum_{n\geqq 1}q^n\sum_{\substack{n=dd'\\(p,d)=1}}\left(\frac{\psi(d)}{d}\rho(d)+\frac{\psi(-d)}{d}\rho(-d)\right).$$

Applying 6.2.5, we can express $\mathbf{L}(\psi\cdot\rho)$, viewed as an element of $V(W,\Gamma(N)^{\mathrm{arith}})\otimes W[1/p]$ by means of the "exotic inclusion" 6.2.4, by an integral over $\mathbf{Z}_p^\times\times\mathbf{Z}_p\times(\mathbf{Z}/N\mathbf{Z})^2$:

7.2.4 $$\int_{\mathbf{Z}_p^\times\times\mathbf{Z}_p\times(\mathbf{Z}/N\mathbf{Z})^2}\frac{\psi(x)}{d}\rho(u)d\mu_N^{(a,b)}=2\int_{\mathbf{Z}_p^\times\times\mathbf{Z}/N\mathbf{Z}}\frac{\psi(x)}{x}\rho(u)d(\mathbf{H}^{a,b}) = 2(1-\psi(a)\rho(b))\mathbf{L}(\psi\cdot\rho)\,.$$

(In the second integral, we can integrate over all $\mathbf{Z}_p^\times\times\mathbf{Z}/N\mathbf{Z}$ instead of just $\mathbf{Z}_p^\times\times(\mathbf{Z}/N\mathbf{Z})^\times$, because by convention ρ is *extended by zero* to all of $\mathbf{Z}/N\mathbf{Z}$.)

Our two-variable $\mathfrak{L}$, however, is obtained by integrating over $(\mathbf{Z}_p^\times)^2\times(\mathbf{Z}/N\mathbf{Z})^2$, or, what is the same for the function $(x,y)\to\psi(x)/x$ which is already supported in $\mathbf{Z}_p^\times\times\mathbf{Z}_p$, only over $\mathbf{Z}_p\times\mathbf{Z}_p^\times\times(\mathbf{Z}/N\mathbf{Z})^2$. Applying 6.3.12, we see that

7.2.5 $$\int_{(\mathbf{Z}_p^\times)^2\times(\mathbf{Z}/N\mathbf{Z})^2}\frac{\psi(x)}{x}\rho(u)d\mu_N^{(a,b)}=(1-\mathrm{Frob})\int_{\mathbf{Z}_p^\times\times\mathbf{Z}_p\times(\mathbf{Z}/N\mathbf{Z})^2}\frac{\psi(x)}{x}\rho(u)d\mu_N^{(a,b)}\,.$$

Comparing 7.2.4 with 7.2.5, and remembering 6.4.11, we find

7.2.6 $$(1-[a,b])\int\frac{\psi(x)}{x}\rho(u)d\mu_N=2(1-\psi(a)\rho(b))(1-\mathrm{Frob})\,\mathbf{L}(\psi\cdot\rho)$$

which gives

LEMMA 7.2.7. $$\mathfrak{L}\left(\frac{\psi(x)}{x}\rho(u)\right)=2(1-\mathrm{Frob})\,\mathbf{L}(\psi\rho)\,.$$

A caution 7.2.8. The moral is that we should not be too quick to forget entirely the one variable L function $\mathbf{L}$, since when it "applies" it gives a more sensitive tool than the restriction of $\mathfrak{L}$. For example, the constant term in the q-expansion of **L** is the highly non-trivial Kubota-Leopoldt p-adic Dirichlet L-series, for abelian extensions of $\mathbf{Q}$. The passage to $\mathfrak{L}$ by applying $(1 - \mathrm{Frob})$ obliterates this constant term!

7.3. *Useful $\mathfrak{L}$-identites.* These are all immediate consequences of the definition (7.1) of $\mathfrak{L}$, and the properties (6.4.7–18) of μ_N. We list them for ease of reference.

7.3.1 (transformation under $G(N)$) $\quad [a, b]\mathfrak{L}(\chi, f) = a\chi(a, a)\mathfrak{L}(\chi, [b]f)$;

7.3.2 (functional equation) $\quad \mathfrak{L}(\chi, f) = \mathfrak{L}(\chi^t, f^t)$, where $\begin{cases} \chi^t(x, y) = \chi(y, x) \\ f^t(u, v) = f(v, u) \end{cases}$;

7.3.3 (action of $N\theta$) $\quad N\theta\,\mathfrak{L}(\chi, f) = \mathfrak{L}(xy\chi, f)$;

7.3.4 (moments) $\quad \mathfrak{L}(\chi_{k,r}, f) = \Phi^*_{k,r,f}$ for $k, r \geqq 0$;

7.3.5 (q-expansion)

$$\mathfrak{L}(\chi, f) = \sum_{n \geqq 1} q^n \sum_{n = dd'} \bigl(\chi(d, d')f(d, d') - \chi(-d, -d')f(-d, -d')\bigr)$$

(where χ is extended by zero to all of $\mathbf{Z}_p \times \mathbf{Z}_p$) .

Chapter VIII. p-adic L-functions for quadratic imaginary fields where p splits

8.0. *The p-adic analogue of Damerell's theorem.*

8.0.1. We return to the situation of 4.0.1. Thus K is a finite extension of $\mathbf{Q}$ and (E, ω, β) is a $\Gamma(N)^{\mathrm{arith}}$-test object over K, such that E has complex multiplication, which we assume defined over K. The action of $\mathrm{End}(E)$ on $H^0(E, \Omega^1_{E/K})$ allows us to view $\mathrm{End}(E)$ as an order in a subfield $K_0 \subset K$, which must be quadratic imaginary over $\mathbf{Q}$. The non-trivial automorphism of K_0 is written $\alpha \mapsto \bar{\alpha}$. Given an element $\alpha \in \mathrm{End}(E) \subset K_0 \subset K$, we denote by $[\alpha]$ the corresponding endomorphism of E, but think of α itself as an element of $K_0 \subset K$. Thus $[\alpha]^*(\omega) = \alpha w$.

Now choose any place $\mathfrak{p}$ of K which satisfies the following conditions:

8.0.2. (E, ω, β) has *good reduction* at $\mathfrak{p}$, in the sense that there exists a $\Gamma(N)^{\mathrm{arith}}$-test object over the ring $\mathcal{O}_\mathfrak{p}$ of $\mathfrak{p}$-integers in K which gives (E, ω, β) by extension of scalars $\mathcal{O}_\mathfrak{p} \to K$.

8.0.3. The curve E has *ordinary reduction* at $\mathfrak{p}$. (This is equivalent to the hypothesis that the rational prime p under $\mathfrak{p}$ splits completely in the multiplication field K_0.)

If we choose such a $\mathfrak{p}$ we can pass from $\mathcal{O}_\mathfrak{p}$ to its *completion* $\hat{\mathcal{O}}_\mathfrak{p}$. We have a corresponding inclusion of the ring of true modular forms into the ring of p-adic ones:

8.0.4 $$R^{\cdot}(K, \Gamma(N)^{\text{arith}}) \subset R^{\cdot}(\hat{K}_{\mathfrak{p}}, \Gamma(N)^{\text{arith}}) = R^{\cdot}(\mathbf{Z}_p, \Gamma(N)^{\text{arith}}) \otimes \hat{K}_{\mathfrak{p}} \subset GV^{\cdot}(\mathbf{Z}_p, \Gamma(N)^{\text{arith}}) \otimes \hat{K}_{\mathfrak{p}} .$$

The algebra $\mathcal{Z}$ acts on $GV^{\cdot} \otimes \hat{K}_{\mathfrak{p}}$ (cf. 5.9), but does not act stably on the sub-ring $R^{\cdot}(K, \Gamma(N)^{\text{arith}})$. As explained in 5.10, an element of $GV^{\cdot}(\mathbf{Z}_p, \Gamma(N)^{\text{arith}})$ has a *value*, in $\hat{\mathcal{O}}_{\mathfrak{p}}$, on the test object (E, ω, β), and therefore any element of $GV^{\cdot} \otimes \hat{K}_{\mathfrak{p}}$ has a *value*, in $\hat{K}_{\mathfrak{p}}$, on (E, ω, β).

Suppose we *also* choose a complex embedding $K \hookrightarrow \mathbf{C}$. The inclusions 8.0.4 are the p-adic analogues of the inclusions (cf. 4.0.3),

8.0.5 $$R^{\cdot}(K, \Gamma(N)^{\text{arith}}) \subset R^{\cdot}(\mathbf{C}, \Gamma(N)^{\text{arith}}) \subset C^{\infty}(\mathrm{GL}^{+}/\Gamma(N)) .$$

The action of $\mathcal{Z}$ on $GV^{\cdot}(\mathbf{Z}_p, \Gamma(N)^{\text{arith}}) \otimes \hat{K}_{\mathfrak{p}}$ not respecting $R^{\cdot}(K, \Gamma(N)^{\text{arith}})$ is the p-adic analogue of its action on $C^{\infty}(\mathrm{GL}^{+}/\Gamma(N))$, not respecting $R^{\cdot}(K, \Gamma(N)^{\text{arith}})$. For complex multiplication curves, the analogy is perfect, as we shall see below.

Let $F \in R^{k}(K, \Gamma(N)^{\text{arith}})$ be a true modular form defined over K, and let $Z \in \mathcal{Z}$ be an element of $\mathcal{Z}$. Let us denote by

8.0.7 $$(ZF)_{\mathfrak{p}} \in GV^{\cdot}(\mathbf{Z}_p, \Gamma(N)^{\text{arith}}) \otimes \hat{K}_{\mathfrak{p}}$$

the image under Z of F, viewed as itself lying in $GV^{\cdot}(\mathbf{Z}_p, \Gamma(N)^{\text{arith}}) \otimes \hat{K}_{\mathfrak{p}}$, using the $\mathcal{Z}$-module structure 5.9.3. Let us denote by

8.0.8 $$(ZF)_{C^{\infty}} \in C^{\infty}(\mathrm{GL}^{+}/\Gamma(N))$$

the image under Z of F, viewed as itself lying in $C^{\infty}(\mathrm{GL}^{+}/\Gamma(N))$, with the $\mathcal{Z}$-module structure 1.6. Let $(\omega_1, \omega_2) \in \mathrm{GL}^{+}$ represent the test object $(E, \omega, \beta)_{\mathbf{C}}$ (cf. 4.0.2). We have already proved (4.0.4) that the complex value $(ZF)_{C^{\infty}}(\omega_1, \omega_2)$ lies in K, and that, considered as an element of K, it is independent of the choice of the embedding $K \mapsto \mathbf{C}$.

COMPARISON THEOREM 8.0.9. *With hypotheses and notations as above, for any place $\mathfrak{p}$ of K satisfying* 8.0.2 *and* 8.0.3, *the value*

$$(ZF)_{\mathfrak{p}}(E, \omega, \beta) \in \hat{K}_{\mathfrak{p}}$$

in fact lies in K, and, as an element K, it is independent of the choice of $\mathfrak{p}$ satisfying 8.0.2 *and* 8.0.3. *This common value is none other than the "complex" value*

$$(ZF)_{C^{\infty}}(\omega_1, \omega_2)$$

for any embedding of $K \hookrightarrow \mathbf{C}$.

Proof (compare that of 4.0.4). By linearity and 1.6.3, we may assume that the operator Z is a monomial $\mathbf{S}^{a} \boldsymbol{g}_2^{b} \boldsymbol{g}_3^{c} \mathbf{D}^{d} \mathbf{H}^{e}$. The operators $\mathbf{H}$, $\mathbf{D}$, $\boldsymbol{g}_2$, and $\boldsymbol{g}_3$ are *stable* on $R^{\cdot}(K, \Gamma(N)^{\text{arith}})$ in both the "classical" and the $\mathfrak{p}$-adic actions, and when restricted to $R^{\cdot}(K, \Gamma(N)^{\text{arith}})$, they act the *same* in both the classical and $\mathfrak{p}$-adic actions. So replacing F by $g_2^b g_3^c D^d(k^e F) \in R^{4b+6c+2d+k}(K, \Gamma(N)^{\text{arith}})$, we may assume that the operator Z is a power of S, say S^n. Then

8.0.10 $$\begin{cases} (ZF)_\infty = S^n F \in C^\infty(\mathrm{GL}^+/\Gamma(N)) \\ (ZF)_\mathfrak{p} = P^n F \in GV^{\cdot}(\mathbf{Z}_p, \Gamma(N)^{\text{arith}}) \otimes \hat{K}_\mathfrak{p} . \end{cases}$$

The assertion of the theorem is essentially tautologous for F itself, so we are reduced to "comparing" P and S. It is at this point that the hypothesis "complex multiplication with good and ordinary reduction at $\mathfrak{p}$" will be used.

We have already seen (4.0.6–7) how to compute the value of S on $(E, \omega, \beta)_\mathbf{C}$: simply choose any $[\alpha] \in \mathrm{End}(E)$ with $\alpha \notin \mathbf{Z}$, and any non-zero vector $v \in H^1_{\mathrm{DR}}(E/K)$ such that $[\alpha]^*(v) = \bar{\alpha} v$. Then in terms of the basis $\omega = dx/y$ and $\eta = x dx/y$ of $H^1_{\mathrm{DR}}(E/K)$, the cohomological expression for S is

8.0.11 $$S((E, \omega, \beta)_\mathbf{C}) = 12 \frac{\langle v, \eta \rangle_{\mathrm{DR}}}{\langle v, \omega \rangle_{\mathrm{DR}}} .$$

What about P? After the extension of scalars $K \hookrightarrow \hat{K}_\mathfrak{p}$, the q^{th} power Frobenius endomorphism F_q ($q = \# \mathcal{O}_\mathfrak{p}/\mathfrak{p}$) operates on

$$H^1_{\mathrm{DR}}(E \otimes \hat{\mathcal{O}}_\mathfrak{p}/\hat{\mathcal{O}}_\mathfrak{p}) \otimes \hat{K}_\mathfrak{p} \simeq H^1_{\mathrm{DR}}(E/K) \otimes_K \hat{K}_\mathfrak{p} ,$$

with distinct eigenvalues, one a unit $a \in \mathbf{Z}_p^\times$, the other q/a. If we choose a non-zero vector $u \in H^1_{\mathrm{DR}}(E/K) \otimes \hat{K}_\mathfrak{p}$ lying in the (unit) a-eigenspace $U_\mathfrak{p} \subset H^1_{\mathrm{DR}}(E/K) \otimes \hat{K}_\mathfrak{p}$, we have the cohomological formula (cf. 5.10.5)

8.0.12 $$P((E, \omega, \beta)\hat{\mathcal{O}}_\mathfrak{p}) = 12 \frac{\langle u, \eta \rangle_{\mathrm{DR}}}{\langle u, \omega \rangle_{\mathrm{DR}}} .$$

So it remains only to see that the vector v figuring in 8.0.11 can serve as our u. This results from the following lemma, analogue of 4.0.7.

LEMMA 8.0.13. *With hypotheses as above, the subspace*

$$U_\mathfrak{p} \cap H^1_{\mathrm{DR}}(E/K) \subset H^1_{\mathrm{DR}}(E/K)$$

is non-zero, and is independent of the choice of place $\mathfrak{p}$ *satisfying* 8.0.2–3. *In fact, for any* $[\alpha] \in \mathrm{End}(E)$, *it is the* $\bar{\alpha}$*-eigenspace of* $[\alpha]^*$ *on* $H^1_{\mathrm{DR}}(E/K)$, *and for any embedding* $K \hookrightarrow \mathbf{C}$, *it coincides with the antiholomorphic subspace*

$$H^{0,1}(E_\mathbf{C}) \cap H^1_{\mathrm{DR}}(E/K).$$

Proof. Let $\mathfrak{p}_0$ denote the place of K_0 induced by $\mathfrak{p}$. It is thus one of the two places of K_0 which lie over p. As a prime ideal in $\mathcal{O}_{K_0}$, $\mathfrak{p}_0$ may not be principal, but certainly its h^{th} power (h = class number of K_0) is. Let $\pi \in \mathcal{O}_{K_0}$ be a generator of $(\mathfrak{p}_0)^h$. The element π may not lie in the order $\mathrm{End}(E) \subset \mathcal{O}_{K_0}$, but there exists an integer $f \geqq 1$ (the conductor) such that $\mathrm{End}(E) = \mathbf{Z} + f\mathcal{O}_{K_0}$. So we can consider π as an element of $\mathrm{End}_K(E) \otimes \mathbf{Q}$, and we can speak of its *reduction* mod $\mathfrak{p}$ as an element of $\mathrm{End}_{\mathbf{F}_q}(E \otimes_{\mathcal{O}_\mathfrak{p}} \mathbf{F}_q) \otimes_{\mathbf{Z}} \mathbf{Q}$. According to complex multiplication theory, some *power* π^n of π is equal to some *power* F_q^m of the Frobenius endomorphism F_q of $E \otimes_{\mathcal{O}_\mathfrak{p}} \mathbf{F}_q$: the equality takes place in $\mathrm{End}_{\mathbf{F}_q}(E \otimes_{\mathcal{O}_\mathfrak{p}} \mathbf{F}_q) \otimes \mathbf{Q}$. Clearing denominators, we find an equality of endomorphisms

8.0.14 $$f\pi^n = fF_q^m \quad \text{for some integers } f,\, n,\, m \geqq 1.$$

The endomorphism F_q of $H^1_{\mathrm{DR}}(E/K) \otimes \hat{K}_\mathfrak{p}$ had two distinct eigenvalues, $a \in \mathbf{Z}_p^\times$ and q/a. Let

$$H^1_{\mathrm{DR}}(E/K) \otimes \hat{K}_\mathfrak{p} = U_\mathfrak{p} \oplus U'_\mathfrak{p}$$

be the corresponding decomposition into eigenspaces ($U_\mathfrak{p}$ the unit root eigenspace). Then $f(F_q)^m$ respects this eigendecomposition, it acts as fa^m on $U_\mathfrak{p}$, and as fq^m/a^m on $U'_\mathfrak{p}$. Thus $U_\mathfrak{p}$ is the eigenspace of $f(F_q)^m$ corresponding to the eigenvalue of $f(F_q)^m$ of smaller ordinal.

The equality 8.0.14 then allows us to characterize the intersection $U_\mathfrak{p} \cap H^1_{\mathrm{DR}}(E/K)$ as the eigenspace of $[f\pi^n]$ on $H^1_{\mathrm{DR}}(E/K)$ whose eigenvalue has smallest $\mathfrak{p}$-adic value. The eigenvalues of $[f\pi^n]$ on $H^1_{\mathrm{DR}}(E/K)$ are $f\pi^n$ and $f\bar{\pi}^n$ respectively; $\mathfrak{p}$-adically, π is a power of a uniformizing parameter, while $\bar{\pi}$ is a $\mathfrak{p}$-adic unit. Thus $U_\mathfrak{p} \cap H^1_{\mathrm{DR}}(E/K)$ is the $f\bar{\pi}^n$-eigenspace of $[f\pi^n]$ on $H^1_{\mathrm{DR}}(E/K)$. Since $f\pi^n \notin \mathbf{Z}$, we have $K_0 = \mathbf{Q}[f\pi^n]$, and hence $U_\mathfrak{p} \cap H^1_{\mathrm{DR}}(E/K)$ is also the $\bar{\alpha}$-eigenspace of any $[\alpha] \in \mathrm{End}(E)$, $\alpha \notin \mathbf{Z}$. The final assertion of the theorem is just a reminder of what we already proved (4.0.7). Q.E.D.

8.1. *Concrete applications; the $G_{A,B,f}$.*

LEMMA 8.1.0. *Let (A, B) be a pair of integers satisfying $A + B \geqq 1$, $B \leqq 0$, and f a K-valued function on $\mathbf{Z}/N\mathbf{Z} \times \mathbf{Z}/N\mathbf{Z}$. The C^∞ modular form $G^{\mathrm{cl}}_{A,B,f}$ constructed in* 3.6.5 *"corresponds," via* 8.0.9, *to the p-adic modular form $G^{\mathfrak{p}}_{A,B,f}$ constructed in* 5.11.9.

Proof. If $B=0$, and $A \neq 2$, we have $G^{\mathrm{cl}}_{A,B,f} = G^{\mathfrak{p}}_{A,B,f}$ is a true modular form belonging to $R^A(K, \Gamma(N)^{\mathrm{arith}})$. If $B=0$ and $A=2$, then $G^{\mathrm{cl}}_{2,0,f}$ and $G^{\mathfrak{p}}_{2,0,f}$ are the sum of a common element of $R^2(K, \Gamma(N)^{\mathrm{arith}})$ and of a common K-multiple of S (resp. P) (cf. 3.6.9, 3.6.13 and 5.7.13). If $A + 2B \geqq 1$ and $B \leqq 0$, then

8.1.1 $$\begin{cases} G^{\mathrm{cl}}_{A,B,f} = (NW)^{-B}(G_{A+2B,0,f}) & \text{by } 4.1.1 \\ G^{\mathfrak{p}}_{A,B,f} = (N\theta)^{-B}(G_{A+2B,0,f}) & \text{by } 5.11.13 \end{cases} \quad \text{if } A + 2B \geqq 1,\ B \leqq 0\,,$$

while if $A + 2B \leqq 1$, $A + B \geqq 1$, we apply the functional equation (3.6.7, 5.11.12) to obtain

8.1.2 $$\begin{cases} G^{\mathrm{cl}}_{A,B,f} = G^{\mathrm{cl}}_{A,1-A-B,f^t} = (NW)^{A+B-1}(G^{\mathrm{cl}}_{2-A-2B,0,f^t}) \\ G^{\mathfrak{p}}_{A,B,f} = G^{\mathfrak{p}}_{A,1-A-B,f^t} = (N\theta)^{A+B-1}(G^{\mathfrak{p}}_{2-A-2B,0,f^t})\,. \end{cases}$$

Since the p-adic operators θ and P correspond to the C^∞ operators W and S under 8.0.9, the result follows. Q.E.D.

COROLLARY 8.1.3. *With the hypotheses and notations of* 8.0, *we have an equality in* K *between the "complex" number* $G^{\mathrm{cl}}_{A,B,f}((E, \omega, \beta)_{\mathrm{C}})$ *and the "p-adic" number* $G^{\mathrm{p}}_{A,B,f}((E, \omega, \beta)_{\hat{\mathcal{O}}_{\mathrm{p}}})$, *whenever* $A + B \geqq 1$, $B \leqq 0$, *and* f *is a K-valued function on* $(\mathbf{Z}/N\mathbf{Z})^2$ (*cf.* 4.1.6 *for the explicit transcendental formula for* $G^{\mathrm{cl}}_{A,B,f}((E, \omega, \beta)_{\mathrm{C}})$ *in terms of "the" period* Ω *and a period lattice* $\subset K_0$.)

8.2. *Interlude*: *a minor compatibility*.

8.2.0. Up to now, we have worked exclusively with *arithmetic*, rather than *naive*, level N structures, even when $N = N_0$ is prime to p. The chief benefits were an irreducible moduli problem, and the attendant pleasures of level-N q-expansions with $\mathbf{Z}$ coefficients. However, when we study complex-multiplication elliptic curves via their period lattices, the notion of *arithmetic* level N structure appears much *less* natural than the naive notion. Strictly speaking, the arithmetic notion remains reasonable provided that *all* the primes dividing N are split in the multiplication field. But this last condition is first of all highly unnatural in a p-adic theory, and secondly, even the simplest examples, such as $\mathbf{Q}(i)$, show the practical need for considering worse N's ($N = 4$ for $\mathbf{Q}(i)$ arises naturally, cf. [15]).

8.2.1. As we have already explained in 2.0, once we are given a naive level N structure $\alpha: (\mathbf{Z}/N\mathbf{Z})^2 \xrightarrow{\sim} {}_N E$, we can deduce from it both a primitive N^{th} root of unity $\det(\alpha)$, and an *arithmetic* level N structure $\beta_\alpha(\det(\alpha)^n, m) = \alpha(n, m)$.

An isogeny $\pi: E \to E'$ of degree *prime* to N, π induces an isomorphism ${}_N E \xrightarrow{\sim} {}_N E'$. This allows us to define a naive level N structure $\alpha' = \pi \cdot a$ on E':

8.2.2
$$\begin{tikzcd} (\mathbf{Z}/N\mathbf{Z})^2 \arrow[r, "\alpha", "\sim"'] \arrow[rr, bend right, "\alpha' = \pi\alpha"'] & {}_N E \arrow[r, "\pi", "\sim"'] & {}_N E' \end{tikzcd} .$$

This construction does *not* preserve determinants, but rather

8.2.3
$$\det(\pi\alpha) = \det(\alpha)^{\deg(\pi)} .$$

Compatibility 8.2.4. Let B be a p-adic ring, $N_0 \geqq 1$ an integer prime to p, (E, φ, α) a trivialized $\Gamma(N)^{\text{naive}}$ elliptic curve over B, and $(E, \varphi, \beta_\alpha)$ the trivialized $\Gamma(N)^{\text{arith}}$ curve over B deduced from (E, φ, α) by the construction $\alpha \mapsto \beta_\alpha$. Let $\pi: E \to E' \overset{\text{dfn}}{=} E/\varphi^{-1}(\mu_p)$ be the projection, let $(E', \varphi' = \varphi \circ \check{\pi}, (\beta_\alpha)')$ be the Frobenius transform of $(E, \varphi, \beta_\alpha)$. Then

8.2.5 $$(\beta_\alpha)' = \beta_{\pi\cdot\alpha}\ ,$$

i.e., under the construction $\alpha \mapsto \beta_\alpha$, the operation $\alpha \longrightarrow \pi\cdot\alpha$ goes over into the operation $\beta \mapsto \beta'$ defined by Frobenius.

Proof. By definition, $\check{\pi}\beta'(\zeta, 0) = \beta(\zeta, 0)$, and $\beta'(1, m) = \pi\beta(1, m)$. Since $p = \deg\pi = \pi\check{\pi}$ is prime to N_0, this first equation can be rewritten $p\beta'(\zeta, 0) = \pi\beta(\zeta, 0)$, or, better yet, $\beta'(\zeta^{\det\pi}, 0) = \pi\beta(\zeta, 0)$. Thus $\beta'(\zeta^{\deg\pi}, m) = \pi\beta(\zeta, m)$. Taking $\zeta = \det(\alpha)^n$, this becomes $\beta'(\det(\pi\alpha)^n, m)$. When β is β_α,

$$\pi\beta_\alpha(\det(\alpha)^n, m) \overset{\text{dfn}}{=} \pi\alpha(n, m) = \beta_{\pi\alpha}(\det(\pi\alpha)^n, m)\ . \qquad \text{Q.E.D.}$$

8.2.6. *A final word.* For the rest of this chapter, any "π" occurring in a formula is 3.1415. . . .

8.3. *The setting for the L-function: a review of the relevant class-field theory* (*cf.* [32]). Fix

8.3.1 $$\begin{cases} \text{a quadratic imaginary field } K_0\text{, given with complex embedding } K_0 \hookrightarrow \mathbf{C}. \\ \text{a prime ideal } \mathfrak{p} \subset \mathcal{O}_{K_0} \text{ of norm } p \text{ (i.e., we assume that } p \text{ splits in } K_0\text{, and we \textit{choose} one of the primes lying over it, the other being } \bar{\mathfrak{p}}). \\ \text{an integer } N_0 \geqq 1\text{, prime to } p. \end{cases}$$

We will consider triples $(M, \check{\varphi}, \alpha)$ where

8.3.2 $$\begin{cases} M \subset K_0 \text{ is an invertible } \mathcal{O}_{K_0}\text{-module, i.e., a fractional ideal of } K_0. \\ \check{\varphi} \text{ is an isomorphism } \mathbf{Q}_p/\mathbf{Z}_p \xrightarrow{\sim} \bigcup_{n\geq 1} \bar{\mathfrak{p}}^{-n}M/M \text{ (such } \check{\varphi} \text{ exist because } \bar{\mathfrak{p}} \text{ is unramified and of norm } p). \\ \alpha \text{ is an isomorphism } (\mathbf{Z}/N_0\mathbf{Z})^2 \xrightarrow{\sim} (1/N_0)M/M. \end{cases}$$

Notice that if $\mathfrak{A} \subset \mathcal{O}_{K_0}$ is an integral ideal which is prime to $N_0\bar{\mathfrak{p}}$, then the natural inclusion $\mathcal{O}_{K_0} \subset \mathfrak{A}^{-1}$ may be tensored with M to give an inclusion $M \subset \mathfrak{A}^{-1}M$ which induces isomorphisms

8.3.3 $$\begin{cases} \bigcup_n \bar{\mathfrak{p}}^{-n}M/M \xrightarrow{\sim} \bigcup \bar{\mathfrak{p}}^{-n}\mathfrak{A}^{-1}M/\mathfrak{A}^{-1}M \\ \dfrac{1}{N_0}M/M \xrightarrow{\sim} \dfrac{1}{N_0}\mathfrak{A}^{-1}M/\mathfrak{A}^{-1}M\ . \end{cases}$$

If we compose $\check{\varphi}$ and α respectively with these isomorphisms, we obtain composite isomorphisms

8.3.4 $$\begin{cases} \begin{tikzcd} \mathbf{Q}_p/\mathbf{Z}_p \arrow[r, "\check{\varphi}", "\sim"'] \arrow[rr, bend right, "\mathfrak{A}^{-1}\check{\varphi}"'] & \bigcup \bar{\mathfrak{p}}^{-n}M/M \arrow[r, "\sim"] & \bigcup \bar{\mathfrak{p}}^{-n}\mathfrak{A}^{-1}M/\mathfrak{A}^{-1}M \end{tikzcd} \\ \begin{tikzcd} (\mathbf{Z}/N\mathbf{Z})^2 \arrow[r, "\sim"] \arrow[rr, bend right, "\mathfrak{A}^{-1}\alpha"'] & \dfrac{1}{N_0}M/M \arrow[r, "\sim"] & \dfrac{1}{N_0}\mathfrak{A}^{-1}M/\mathfrak{A}^{-1}M\ . \end{tikzcd} \end{cases}$$

The construction $(M, \check{\varphi}, \alpha) \mapsto (\mathfrak{A}^{-1}M, \mathfrak{A}^{-1}\check{\varphi}, \mathfrak{A}^{-1}\alpha)$ is a multiplicative action of integral ideals prime to $N_0\bar{\mathfrak{p}}$ on the space of all triples $(M, \check{\varphi}, \alpha)$.

For any integral ideal $\mathfrak{A}$ of K_0, we let $K(\mathfrak{A})$ denote the corresponding ray class field of conductor $\mathfrak{A}$ over K_0, and write simply K for the Hilbert class field. We will be particularly interested in the field $\bigcup_{n\geq 1} K(N_0\bar{\mathfrak{p}}^n)$, which we denote simply $K(N_0\bar{\mathfrak{p}}^\infty)$. According to the theory of complex multiplication, any triple $(M, \check{\varphi}, \alpha)$ determines (a complex embedding of) the field $K(N_0\bar{\mathfrak{p}}^\infty)$ as follows: Consider the complex elliptic curve $\mathbf{C}/M$, which is endowed with a $\Gamma_{00}(p^\infty)^{\text{naive}}$-structure $\check{\varphi}$, and a $\Gamma(N_0)^{\text{naive}}$-structure α. Then $K(N_0\bar{\mathfrak{p}}^\infty)$ is the smallest overfield (in $\mathbf{C}$) of K_0 over which $(\mathbf{C}/M, \check{\varphi}, \alpha)$ can be defined.

More precisely, consider the sub-ring of $\mathbf{C}$ generated by the values of all the modular functions

8.3.5 $$F \in \bigcup_{n\geq 1} R^0(\mathcal{O}_{K_0}[1/N_0], \Gamma(N_0)^{\text{naive}} \cap \Gamma_{00}(p^n)^{\text{naive}})$$

on the complex test object $(\mathbf{C}/M, \check{\varphi}, \alpha)$. This ring is the ring of all "integers outside of $N_0\bar{\mathfrak{p}}$" in the field $K(N_0\bar{\mathfrak{p}}^\infty)$. It is the *smallest sub-ring* of $\mathbf{C}$ over which there exists a $\Gamma(N_0)^{\text{naive}} \cap \Gamma_{00}(p^\infty)^{\text{naive}}$-elliptic curve $(E, \check{\varphi}, \alpha)$ plus an action of $\mathcal{O}_{K_0}$ which gives back $(\mathbf{C}/M, \check{\varphi}, \alpha)$ after extension of scalars. Of course the embedding $K(N_0\bar{\mathfrak{p}}^\infty) \hookrightarrow \mathbf{C}$ depends upon the choice of triple $(M, \check{\varphi}, \alpha)$.

The Artin symbol provides a multiplicative homomorphism

8.3.6 $$\begin{aligned}\{\text{integral ideals of } K_0, \text{ prime to } N_0\bar{\mathfrak{p}}\} &\longrightarrow \operatorname{Gal}((N_0\bar{\mathfrak{p}}^\infty)/K_0)\,,\\ \mathfrak{A} &\longrightarrow \left(\frac{K(N_0\bar{\mathfrak{p}}^\infty)/K_0}{\mathfrak{A}}\right)\end{aligned}$$

whose image is a dense subgroup of Gal. If

$$F \in \bigcup_{n\geq 1} R^0\left(\mathcal{O}_{K_0}\left[\frac{1}{N_0}\right], \Gamma(N_0)^{\text{naive}} \cap \Gamma_{00}(p^n)_{\text{naive}}\right),$$

then the action of Galois on its value $F(\mathbf{C}/M, \check{\varphi}, \alpha)$ is specified by the formula

8.3.7 $$F(\mathbf{C}/M, \check{\varphi}, \alpha)^{\left(\frac{K(N_0\bar{\mathfrak{p}}^\infty)/K_0}{\mathfrak{A}}\right)} = F(\mathbf{C}/\mathfrak{A}^{-1}M, \mathfrak{A}^{-1}\check{\varphi}, \mathfrak{A}^{-1}\alpha)\,.$$

8.3.7.1. If the ideal $\mathfrak{A}$ is *principal*, say $\mathfrak{A} = (a)$ with $a \in \mathcal{O}_{K_0}$ prime to $N_0\bar{\mathfrak{p}}$, then $(\mathfrak{A}^{-1}M, \mathfrak{A}^{-1}\check{\varphi}, \mathfrak{A}^{-1}\alpha)$ maps isomorphically by "multiplication by a" to $(M, a\check{\varphi}, a\alpha)$. Notice that the "$a$" in $a\check{\varphi}$ is the *image* of a in $(\hat{\mathcal{O}}_{\bar{\mathfrak{p}}})^\times \simeq \mathbf{Z}_p^\times$, while the "$a$" in $a\alpha$ is the *image* of a in $(\mathcal{O}_{K_0}/N_0\mathcal{O}_{K_0})^\times$. Therefore

8.3.8 $$F(\mathbf{C}/M, \check{\varphi}, \alpha)^{\left(\frac{K(N_0\bar{\mathfrak{p}}^\infty)/K_0}{(a)}\right)} = F(\mathbf{C}/M, a\check{\varphi}, a\alpha)\,.$$

If we think of $\mathbf{Z}_p^\times \simeq (\hat{\mathcal{O}}_{\bar{\mathfrak{p}}})^\times$ sitting as the subgroup $(1, \cdots, 1, \bar{\mathfrak{p}}\text{-units at } \bar{\mathfrak{p}}, 1, \cdots, 1, \cdots)$ of the *ideles* of K_0, then norm residue symbol defines a homomorphism

8.3.9
$$\begin{aligned} \mathbf{Z}_p^\times \xrightarrow{\sim} (\mathcal{O}_{\bar{\mathfrak{p}}})^\times &\longrightarrow \mathrm{Gal}(K(N_0\bar{\mathfrak{p}}^\infty)/K_0) \\ a &\longmapsto [a] \end{aligned}$$

such that, for F as above,

8.3.10
$$F(\mathrm{C}/M, \check{\varphi}, \alpha)^{[a]} = F(\mathrm{C}/M, a^{-1}\check{\varphi}, \alpha) .$$

8.3.11. Now let us choose a place $\mathfrak{p}_\infty$ of $K(N_0\mathfrak{p}^\infty)$ lying over $\mathfrak{p}$, and denote by $\mathcal{O}_{\mathfrak{p}_\infty}$ its valuation ring. The decomposition group at $\mathfrak{p}$ is topologically generated by $\left(\dfrac{K(N_0\bar{\mathfrak{p}}^\infty)/K_0}{\mathfrak{p}}\right)$, the unique automorphism of $\mathcal{O}_{\mathfrak{p}_\infty}$ inducing absolute Frobenius on the residue field. Each triple $(M, \check{\varphi}, \alpha)$ provides the following:

8.3.12. An elliptic curve E_M *definable* over $K \cap \mathcal{O}_{\mathfrak{p}_\infty}$, with an action of $\mathcal{O}_{K_0}$ such that its representation on $H^0(\Omega^1)$ is the inclusion $\mathcal{O}_{K_0} \hookrightarrow K$. Over $\mathcal{O}_{\mathfrak{p}_\infty} \cap K(N_0)$, E_M acquires a $\Gamma(N_0)^{\mathrm{naive}}$-structure α. We fix a choice of *model* of E_M over $K \cap \mathcal{O}_{\mathfrak{p}_\infty}$.

8.3.13. Because $(p) = \mathfrak{p}\bar{\mathfrak{p}}$ in $\mathcal{O}_{K_0}$, with $\mathfrak{p}$ and $\bar{\mathfrak{p}}$ relatively prime, there is a canonical splitting over $\mathcal{O}_{\mathfrak{p}_\infty} \cap K$ of the p-divisible group of E_M into the product of its $\mathfrak{p}$ and $\bar{\mathfrak{p}}$-divisible groups.

$$\bigcup_n \mathrm{Ker}(p^n) = \bigcup_n \mathrm{Ker}(\mathfrak{p}^n) \times \bigcup_n \mathrm{Ker}(\bar{\mathfrak{p}}^n) .$$

8.3.14. We are given an isomorphism of p-divisible groups over $\mathcal{O}_{\mathfrak{p}_\infty}$,

$$\check{\varphi}\colon \mathbf{Q}_p/\mathbf{Z}_p \xrightarrow{\sim} \bigcup \mathrm{Ker}(\bar{\mathfrak{p}}^n) = \bigcup_n \bar{\mathfrak{p}}^{-n}M/M .$$

8.3.15. We have an isomorphism of p-divisible groups over $\mathcal{O}_{\mathfrak{p}_\infty}$,

$$\varphi\colon \bigcup_n \mathfrak{p}^{-n}M/M = \bigcup_n \mathrm{Ker}(\mathfrak{p}^n) \xrightarrow{\sim} \mu_{p^\infty} ,$$

obtained as the Cartier dual of 8.3.14 via the e_{p^n} pairings, so that $\varphi^{-1} \times \check{\varphi}\colon \mu_{p^\infty} \times \mathbf{Q}_p/\mathbf{Z}_p \simeq \bigcup_n \mathrm{Ker}(p^n)$ induces an *arithmetic* level p^n-structure for all $n \geqq 1$.

It will also be convenient to apply the functor $\mathrm{Hom}(\mathbf{Q}_p/\mathbf{Z}_p, \_\_)$ to these last two isomorphisms, obtaining isomorphisms, still noted $\check{\varphi}$ and φ,

8.3.14. bis
$$\check{\varphi}\colon \mathbf{Z}_p \xrightarrow{\sim} M_{\bar{\mathfrak{p}}} ;$$

8.3.15. bis
$$\varphi\colon M_{\mathfrak{p}} \xrightarrow{\sim} T_p(\mathrm{G}_m) = \lim \mu_{p^n} ,$$

where $M_{\bar{\mathfrak{p}}}$ and $M_{\mathfrak{p}}$ denote the $\bar{\mathfrak{p}}$-adic and $\mathfrak{p}$-adic completions of M. Let us now pass over to $\hat{\mathcal{O}}_{\mathfrak{p}_\infty}$, the p-adic completion of $\mathcal{O}_{\mathfrak{p}_\infty}$. Then the isomorphism

8.3.16
$$\varphi\colon \bigcup_n \mathrm{Ker}(\mathfrak{p}^n) \longrightarrow \mu_{p^\infty}$$

becomes *equivalent* to a trivialization

8.3.17
$$\varphi\colon \hat{E}_M \xrightarrow{\sim} \hat{G}_m \text{ over } \hat{\mathcal{O}}_{\mathfrak{p}_\infty} .$$

So we also have at our disposal a *magic differential* $\varphi^*(dT/(1+T))$ on E_M, defined over $\hat{\mathcal{O}}_{\mathfrak{p}\infty}$. It is surely *not* defined over $\mathcal{O}_{\mathfrak{p}\infty}$, so let us choose

8.3.16. A unit $c \in (\hat{\mathcal{O}}_{\mathfrak{p}\infty})^\times$ such that the differential $\omega \overset{\text{dfn}}{=} c\varphi^*(dT/(1+T))$ is defined over $\mathcal{O}_{\mathfrak{p}\infty} \cap K$ (this makes sense because E_M is itself defined over $\mathcal{O}_{\mathfrak{p}\infty} \cap K$, cf. 8.3.12).

Since the differential ω is defined over $\mathcal{O}_{\mathfrak{p}\infty} \subset K(N\bar{\mathfrak{p}}^\infty) \subset \mathbf{C}$, we can extend scalars and compare $\omega_{\mathbf{C}}$ to the standard differential dz on $\mathbf{C}/M$. We can write

8.3.17 $$\omega_{\mathbf{C}} = \Omega dz \quad \text{for some } \Omega \in \mathbf{C}^\times ,$$

and hence the period lattice of $(E_M, \omega_{\mathbf{C}})$ is ΩM.

To summarize briefly: the construction

8.3.18 $$(M, \check{\varphi}, \alpha) \longmapsto (E_M, \varphi, \beta_\alpha) \text{ over } \hat{\mathcal{O}}_{\mathfrak{p}\infty}$$

allows us to attach to any triple $(M, \check{\varphi}, \alpha)$ as in 8.3.2 a trivialized $\Gamma(N_0)^{\text{arith}}$ curve $(E_M, \varphi, \beta_\alpha)$ over $\hat{\mathcal{O}}_{\mathfrak{p}\infty}$. The ring $\hat{\mathcal{O}}_{\mathfrak{p}\infty}$ is Galois over $\mathbf{Z}_p = \hat{\mathcal{O}}_{\mathfrak{p}}$, with Galois group topologically generated by the Artin symbol $\left(\frac{K(N_0\bar{\mathfrak{p}}^\infty)/K_0}{\mathfrak{p}}\right)$. The trivialized $\Gamma(N_0)^{\text{arith}}$ curve *deduced* from $(E_M, \varphi, \beta_\alpha)$ by extension of scalars $\mathcal{O}_{\mathfrak{p}\infty} \xrightarrow{\sim} \mathcal{O}_{\mathfrak{p}\infty}$ by this Artin symbol is precisely the one attached to the triple $(\mathfrak{p}^{-1}M, \mathfrak{p}^{-1}\check{\varphi}, \mathfrak{p}^{-1}\alpha)$: symbolically

8.3.19 $$(E_M, \varphi, \beta_\alpha)^{\left(\frac{K(N_0\bar{\mathfrak{p}}^\infty)/K_0}{\mathfrak{p}}\right)} \simeq (E_{\mathfrak{p}^{-1}M}, \mathfrak{p}^{-1}\varphi, \beta_{\mathfrak{p}^{-1}\alpha}) .$$

Notice also that $(E_{\mathfrak{p}^{-1}M}, \mathfrak{p}^{-1}\varphi, \beta_{\mathfrak{p}^{-1}\alpha})$ is just the *Frobenius transform* of $(E_M, \varphi, \beta_\alpha)$,

8.3.20 $$(E_M, \varphi, \beta_\alpha)^{\left(\frac{K(N_0\bar{\mathfrak{p}}^\infty)/K_0}{\mathfrak{p}}\right)} \simeq (E'_M, \varphi', \beta'_\alpha) .$$

Given an element $F \in V(\mathbf{Z}_p, \Gamma(N_0)^{\text{arith}})$, we will abuse notations and write

8.3.21 $$F(M, \check{\varphi}, \beta_\alpha) \overset{\text{dfn}}{=} F(E_M, \varphi, \beta_\alpha) .$$

Compatibility 8.3.22. For any $F \in V(\mathbf{Z}_p, \Gamma(N_0)^{\text{arith}})$, the action of $\text{Gal}(\hat{\mathcal{O}}_{\mathfrak{p}\infty}/\mathbf{Z}_p)$ on its value $F(M, \check{\varphi}, \alpha)$ is given by the formula

8.3.23 $$\begin{aligned} F(M, \check{\varphi}, \alpha)^{\left(\frac{K(N_0\bar{\mathfrak{p}}^\infty)/K}{\mathfrak{p}}\right)} &= F(\mathfrak{p}^{-1}M, \mathfrak{p}^{-1}\check{\varphi}, \mathfrak{p}^{-1}\alpha) \\ &= (\text{Frob } F)(M, \check{\varphi}, \alpha) . \end{aligned}$$

Proof. The first equality results from 8.3.19 and the compatibility of F with extension of scalars, the second from 8.3.20 and the definition of Frob F.

8.3.24. Another remark, which we will need, is this. The trivialized $\Gamma(N_0)^{\text{arith}}$ curve attached to $(M, \check{\varphi}, \alpha)$ carries a canonical $\Gamma(p^\infty)^{\text{arith}}$-structure, as explained in 8.3.15. In 5.6.4, we constructed an isomorphism

$$V(\mathbf{Z}_p, \Gamma(p^r N_0)^{\text{arith}}) \xrightarrow{\sim} V(\mathbf{Z}_p, \Gamma(N_0)^{\text{arith}})$$

which was $G(N) \xrightarrow{\sim} G(N_0)$ equivariant and preserved q-expansions, by transposing a physical construction $(E, \varphi, \beta) \mapsto (E^{(r)}, \varphi^{(r)}, \beta^{(r)})$ which amounted to iterating the Frobenius construction r times, and observing that $E^{(r)} = E/\boldsymbol{\mu}_{p^r}$ picked up a canonical subgroup $\mathbf{Z}/p^r\mathbf{Z}$ (the kernel of the *dual* of the projection map $E \to E^{(r)}$). When (E, φ, β) comes from an $(M, \check{\varphi}, \alpha)$, this construction just amounts to applying $\mathfrak{p}$ r times, and remembering that the curve attached to $(\mathfrak{p}^{-r}M, \mathfrak{p}^{-r}\check{\varphi}, \mathfrak{p}^{-r}\alpha)$ carries a canonical $\Gamma(p^n)^{\text{arith}}$ structure for all n, in particular for $n = r$. Thus we have:

LEMMA 8.3.25. *Suppose we are given an element $F \in V(\mathbf{Z}_p, \Gamma(p^r N_0)^{\text{arith}})$, and a triple $(M, \check{\varphi}, \alpha)$. Let $F^{(r)} \in V(\mathbf{Z}_p, \Gamma(N_0)^{\text{arith}})$ be its image under the canonical isomorphism 5.6.4. Because the curve attached to any triple $(M, \check{\varphi}, \alpha)$ carries a $\Gamma(p^p)^{\text{arith}}$-structure for every r, both F and $F^{(r)}$ have values, in $\hat{\mathcal{O}}_{\mathfrak{p}_\infty}$, on $(M, \check{\varphi}, \alpha)$, and they are related by*

8.3.26
$$\begin{array}{c} F^{(r)}(M, \check{\varphi}, \alpha) = F(\mathfrak{p}^{-r}M, \mathfrak{p}^{-r}\check{\varphi}, \mathfrak{p}^{-r}\alpha) = (\mathrm{Frob})^r F(M, \check{\varphi}, \alpha) \\ \hspace{8cm} \| \\ \hspace{8cm} F(M, \check{\varphi}, \alpha)^{\left(\frac{K(N_0\bar{\mathfrak{p}}^\infty)/K}{\mathfrak{p}^r}\right)} \end{array}$$

(This lemma will be particularly useful when we try to calculate $\mathfrak{L}(\chi_{k,r}\varepsilon, f)$ where ε is a variable character of *finite order* of $\mathbf{Z}_p^\times \times \mathbf{Z}_p^\times$.)

Let us close with another compatibility (compare 8.3.10).

LEMMA 8.3.27. *For $F \in V(\mathbf{Z}_p, \Gamma(p^r N_0)^{\text{arith}})$, and $(a, b) \in G(N_0)$, we have*

$$([a, b]F)(M, \check{\varphi}, \alpha) = F(M, a^{-1}\check{\varphi}, \alpha \circ (b, b^{-1})) .$$

Proof. The only point is that on the curve $(E_M, \varphi, \beta_\alpha)$ attached to $(M, \check{\varphi}, \alpha)$, φ is the *dual* of $\check{\varphi}$, and $a^{-1}\check{\varphi}$ is indeed the dual of $a^{-1}\varphi$. Q.E.D.

8.4. *The L-function associated to $(M, \check{\varphi}, \alpha)$.*

8.4.0. We retain the setup of the previous Section 8.3, and fix a triple $(M, \check{\varphi}, \alpha)$. We will need to work over a much bigger ring than $\hat{\mathcal{O}}_{\mathfrak{p}_\infty}$, which, being absolutely unramified, contains almost no p-power roots of unity and consequently receives very few characters of finite order of $\mathbf{Z}_p^\times \times \mathbf{Z}_p^\times$. So let us choose an algebraic closure $K^{\text{alg cl}}$ of $K(N_0\bar{\mathfrak{p}}^\infty)$, a complex embedding $K^{\text{alg cl}} \hookrightarrow \mathbf{C}$ which induces on $K(N_0\bar{\mathfrak{p}}^\infty)$ the one provided by $(M, \check{\varphi}, \alpha)$ and a place $\mathfrak{p}_\infty^{\text{alg cl}}$ of $K^{\text{alg cl}}$ which lies over the place $\mathfrak{p}_\infty$ of $K(N_0\bar{\mathfrak{p}}^\infty)$. We will take for W the p-adic completion of the valuation ring of $\mathfrak{p}_\infty^{\text{alg cl}}$. It will also be convenient to choose an automorphism σ of $K^{\text{alg cl}}$ which lies in the decomposition group of $\mathfrak{p}_\infty^{\text{alg cl}}$, induces absolute Frobenius on the residue field at

$\mathfrak{p}_\infty^{\mathrm{alg\,cl}}$, and fixes all p-power roots of unity in $K^{\mathrm{alg\,cl}}$. Notice that σ automatically induces the Artin symbol $\left(\frac{K(N_0\bar{\mathfrak{p}}^\infty)/K_0}{\mathfrak{p}}\right)$ on $K(N_0\bar{\mathfrak{p}}^\infty)$.

8.4.1. Evaluation at $(M, \check{\varphi}, \alpha)$ gives a homomorphism

8.4.2 $$V(W, \Gamma(N_0)^{\mathrm{arith}}) \longrightarrow W .$$

By composition, $\mu_{N_0}^{(a,b)}$ and μ_{N_0} give rise to W-valued measures $\mu_{N_0}^{(a,b)}(M, \check{\varphi}, \alpha)$ and $\mu_{N_0}(M, \check{\varphi}, \alpha)$, and our two variable L-function $\mathfrak{L}(\chi, f)$ gives rise to a W-valued L-function

8.4.3 $$\mathfrak{L}(\chi, f; M, \check{\varphi}, \alpha) \overset{\mathrm{dfn}}{=} \mathfrak{L}(\chi, f)(M, \check{\varphi}, \alpha)$$

which is just the Mellin transform of the measure $\mu_{N_0}(M, \check{\varphi}, \alpha)$.

We propose to give explicit "transcendental" formulas for all values

$$\mathfrak{L}(\varepsilon\chi_{k,l}, f; M, \check{\varphi}, \alpha)$$

where $k, l \geqq 0$, and ε is a *character of finite order* of $\mathbf{Z}_p^\times \times \mathbf{Z}_p^\times$.

Remark 8.4.4. By evaluating at *any* trivialized $\Gamma(N_0)^{\mathrm{arith}}$ curve over W, we could define an associated L-function. But it is only in the complex multiplication case that we have *any* idea of what this L-function is!

8.5. *Explicit formulas: the method.*

8.5.0. The method is based on a "changing level" trick. Suppose we have an integer $N_0 \geqq 1$ prime to p, a W-valued function f on $(\mathbf{Z}/N_0\mathbf{Z})^2$, a continuous W-valued function $\psi(x, y)$ on $\mathbf{Z}_p \times \mathbf{Z}_p$, and a locally constant W-valued function ε on $\mathbf{Z}_p \times \mathbf{Z}_p$. Then for $r \gg 0$, ε is constant on cosets mod p^r. For any such r, we can consider ε as a function on $\mathbf{Z}/p^r N_0\mathbf{Z} \times \mathbf{Z}/p^r N_0\mathbf{Z}$. This possibility allows us to consider various integrals:

8.5.1 $$\left\{\begin{aligned} &\int \psi(x, y)\varepsilon(x, y) f(u, v)\, d\mu_{N_0}^{(a,b)} \\ &\int \psi(x, y)\varepsilon(x, y) f(u, v)\, d\mu_{N_0} \end{aligned}\right\} \in V(W, \Gamma(N_0)^{\mathrm{arith}}) ,$$

8.5.2 $$\left\{\begin{aligned} &\int \psi(x, y) f(u, v)\varepsilon(u, v)\, d\mu_{p^r N_0}^{(a,b)} \\ &\int \psi(x, y) f(u, v)\varepsilon(u, v)\, d\mu_{p^r N_0} \end{aligned}\right\} \in V(W, \Gamma(p^r N_0)^{\mathrm{arith}} .$$

(The notation is slightly abusive: the (a, b) in $d\mu_{N_0}^{(a,b)}$ is the element (a, b) of $G(N_0) = \mathbf{Z}_p^\times \times (\mathbf{Z}/N_0\mathbf{Z})^\times$, while the (a, b) in $d\mu_{p^r N_0}^{(a,b)}$ is the corresponding element of

$$G(N) \subset \mathbf{Z}_p^\times \times (\mathbf{Z}/p^r N_0\mathbf{Z})^\times \simeq \mathbf{Z}_p^\times \times (\mathbf{Z}/p^r\mathbf{Z})^\times \times (\mathbf{Z}/N_0\mathbf{Z})^\times ,$$

whose expression in triple coordinates is $(a, a \bmod p^r, b)$.)

LEMMA 8.5.3. *Under the isomorphism* (5.6.4) *between* $V(W, \Gamma(p^r N_0)^{\mathrm{arith}})$ *and* $V(W, \Gamma(N_0)^{\mathrm{arith}})$, *the integrals* 8.5.2 *correspond respectively to the integrals* 8.5.1.

Proof. It suffices that they have equal q-expansions. For $\mu_{p^r N_0}$ and μ_{N_0}, this is obvious from 6.4.9. For $\mu^{(a,b)}_{p^r N_0}$ and $\mu^{(a,b)}_{N_0}$ this is obvious except for the constant terms, by 6.1.3. On the other hand, for fixed ε, f, it suffices to check for all ψ's of the form $x^k y^l$, with $k \geqq 0$, $l \geqq 0$. Then both integrals are of weight $k + l + 1$ under the action of the subgroup $(1 + p^r \mathbf{Z}_p) \times \{1\} \subset G(N)$, so their difference, a constant, is necessarily zero. (In view of the explicit formula 6.2.10 for the constant term, this proves a similar, but in that case obvious, invariance property for the Kubota-Leopoldt measures $\mu^{a,b}_{K.\text{-}L.}$ on $\mathbf{Z}_p \times \mathbf{Z}/N\mathbf{Z}$ as N varies.) Q.E.D.

COROLLARY 8.5.4. *With hypotheses as above, let ε be a locally constant W-valued functin on $\mathbf{Z}_p \times \mathbf{Z}_p$ which is supported in $\mathbf{Z}_p^\times \times \mathbf{Z}_p^\times$. Let $r > 0$ be such that ε is constant modulo p^r. For any integers $k \geqq 0$, $l \geqq 0$, and any W-valued function f on $\mathbf{Z}/N_0\mathbf{Z} \times \mathbf{Z}/N_0\mathbf{Z}$, the element*

8.5.5 $$2\Phi_{k,l,\varepsilon f} \in V(W, \Gamma(p^r N_0)^{\mathrm{arith}})$$

corresponds, via the isomorphism 5.6.4, *to the element*

8.5.6 $$\int x^k y^l \varepsilon(x, y) f(u, v) d\mu_{N_0} \in V(W, \Gamma(N_0)^{\mathrm{arith}}) .$$

In case ε is a character of $\mathbf{Z}_p^\times \times \mathbf{Z}_p^\times$ of finite order, extended by zero to all of $\mathbf{Z}_p \times \mathbf{Z}_p$, this last element is by definition

8.5.7 $$\mathfrak{L}(\varepsilon\chi_{k,l}, f) \in V(W, \Gamma(N_0)^{\mathrm{arith}}) .$$

Proof. The equality of 8.5.6 and 8.5.7, when ε is a character of finite order, is put just as a reminder. So let us prove that 8.5.5 and 8.5.6 correspond. Except possibly for their constant terms, they have the same q-expansion, the coefficient of q^n being

8.5.8 $$\sum_{n=dd'} \left(d^k (d')^l \varepsilon(d, d') f(d, d') - (-d)^k (-d')^l \varepsilon(-d, -d') f(-d, -d')\right) .$$

(Since ε is supported in $\mathbf{Z}_p^\times \times \mathbf{Z}_p^\times$, this vanishes identically unless $(p, n) = 1$.) Since both are of weight $k + l + 1$ under the subgroup $(1 + p^r\mathbf{Z}_p) \times \{1\} \subset G(N_0)$, their difference, a constant, is necessarily zero. Q.E.D.

8.6. *Explicit formulas: application of the method.* If we combine 8.5.4, in the case of a *character*, with 8.3.25, we get an explicit formula for $\mathfrak{L}(\varepsilon\chi_{k,l}, f; M, \check{\varphi}, \alpha)$.

THEOREM 8.6.0. *Let k, l be non-negative integers, and f a W-valued function on $(\mathbf{Z}/N_0\mathbf{Z})^2$. Let ε be a W-valued character of $\mathbf{Z}_p^\times \times \mathbf{Z}_p^\times$ which is of finite order. Let $r \geqq 1$ be an integer such that ε is constant on cosets modulo p^r. Denote by εf the function on $(\mathbf{Z}/p^rN_0\mathbf{Z})^2$ defined by $(u, v) \mapsto \varepsilon(u \bmod p^r, v \bmod p^r) f(u \bmod N_0, v \bmod N_0)$, where it is understood that $\varepsilon(u, v) = 0$ unless both u and v are prime to p. Then for any triple $(M, \check{\varphi}, \alpha)$ as in* 8.3, *we have the formula*

8.6.1 $$\mathfrak{L}(\varepsilon\chi_{k,l}, f; M, \check{\varphi}, \alpha) = 2\Phi_{k,l,\varepsilon f}(\mathfrak{p}^{-r}M, \mathfrak{p}^{-r}\check{\varphi}, \mathfrak{p}^{-r}\alpha) .$$

To use this effectively, we need the following σ-linear version of 8.3.26.

LEMMA 8.6.2. *Let $F \in V(W, \Gamma(p^rN_0)^{\text{arith}}) \xleftarrow{\sim} V(\mathbf{Z}_p, \Gamma(p^rN_0)^{\text{arith}}) \hat{\otimes} W$ and denote by F^σ the effect of applying $1 \hat{\otimes} \sigma$ to F. Then*

8.6.3 $$\sigma(F(M, \check{\varphi}, \alpha)) = F^\sigma(\mathfrak{p}^{-1}M, \mathfrak{p}^{-1}\check{\varphi}, \mathfrak{p}^{-1}\alpha) .$$

Proof. For $F \in V(\mathbf{Z}_p, \Gamma(p^rN_0)^{\text{arith}})$, we have $F^\sigma = F$, and the values lie in $\hat{\mathcal{O}}_{\mathfrak{p}\infty}$, on which σ is the Artin symbol of $\mathfrak{p}$, so we are only restating part of 8.3.26. The result follows for any F because both sides are σ-linear in F.

Q.E.D.

Notice that as σ fixes p-power roots of unity, as well as $p - 1^{\text{st}}$ roots of unity (these lie in $\mathbf{Z}_p$), it *fixes* our character ε. It may move the function f.

Thus 8.6.1 yields

8.6.4 $$\begin{aligned}\mathfrak{L}(\varepsilon\chi_{k,l}, f; M, \check{\varphi}, \alpha) &= 2\Phi_{k,l,\varepsilon f}(\mathfrak{p}^{-r}M, \mathfrak{p}^{-r}\check{\varphi}, \mathfrak{p}^{-r}\alpha) \\ &= 2\sigma^r(\Phi_{k,l,\varepsilon f^{\sigma^{-r}}}(M, \check{\varphi}, \alpha)) \qquad \text{by 8.6.3.}\end{aligned}$$

To continue the computation, we will view $\Phi_{k,l,\varepsilon f^{\sigma^{-r}}}$ as a "p-adic modular form of weight $k + l + 1$" in the manner of 5.10.3. Let us denote by $\beta_{\check{\varphi}}$ the canonical $\Gamma(p^r)^{\text{arith}}$ structure ($\varphi^{-1} \times \check{\varphi}$ restricted to $\mu_{p^r} \times \mathbf{Z}/p^r\mathbf{Z}$, cf. 8.3.15) carried by the curve E_M attached to $(M, \check{\varphi}, \alpha)$. We readily compute

8.6.5 $$\begin{aligned}\Phi_{k,l,\varepsilon f}\sigma^{-r}(M, \check{\varphi}, \alpha) &= \Phi_{k,l,\varepsilon f^{\sigma^{-r}}}(E_M, \varphi, \beta_{\check{\varphi}} \times \beta_\alpha) \\ &= \Phi_{k,l,\varepsilon f^{\sigma^{-r}}}(E_M, \varphi^*(dT/1 + T), \beta_{\check{\varphi}} \times \beta_\alpha) \\ &= \Phi_{k,l,\varepsilon f^{\sigma^{-r}}}(E_M, c^{-1}\omega, \beta_{\check{\varphi}} \times \beta_\alpha) \qquad \text{(by 8.3.16)} \\ &= c^{k+l+1}\Phi_{k,l,\varepsilon f^{\sigma^{-r}}}(E_M, \omega, \beta_{\check{\varphi}} \times \beta_\alpha) \\ &= c^{k+l+1}G_{k+l+1,-l,\varepsilon f^{\sigma^{-r}}}(E_M, \omega, \beta_{\check{\varphi}} \times \beta_\alpha) \quad \text{(cf. 5.11.10).}\end{aligned}$$

8.6.6. As already remarked, both the curve E_M and the differential ω are defined over $\mathcal{O}_{\mathfrak{p}\infty} \cap K(N_0\mathfrak{p}^r)$. To fix ideas, let us suppose that the function $f\colon (\mathbf{Z}/N\mathbf{Z})^2 \to W$ assumes *algebraic* values, and let L be the finite algebraic number field obtained by adjoining to $K(N_0\mathfrak{p}^r)$ the values of εf and the p^rN_0

roots of unity. Then $W \cap L$ is a valuation ring in L over which $(E_M, \omega, \beta_{\check{\varphi}}^{\vee}, \beta_\alpha)$ has *ordinary* reduction, and the field L comes equipped with a pre-chosen (8.0) complex embedding. So we may apply 8.0.9 and its Corollary 8.1.0 to $G_{k+l+1,-l,\varepsilon f^{\sigma^{-r}}}(E_M, \omega, \beta_{\check{\varphi}}^{\vee} \times \beta_\alpha)$; it lies in L, and in L it is equal to the *complex* number of the same name.

8.6.7. The period lattice of $(E_M, \omega)_{\mathbf{C}}$ is ΩM (cf. 8.3.17). The partial Fourier transform $P^{-1}(\varepsilon f^{\sigma^{-r}})$ is a function on $\mu_{N_0 p^r} \times \mathbf{Z}/N_0 p^r \mathbf{Z}$, which by means of $\beta_{\check{\varphi}}^{\vee} \times \beta_\alpha$ becomes a function on the group of points of order $p^r N_0$ on $(E_M)_{\mathbf{C}}$, i.e., it becomes a certain function g on $M/p^r N_0 M$, which we will determine explicitly below. The transcendental expression for $2G_{k+l+1,-l,\varepsilon f^{\sigma^{-r}}}(E_M, \omega, \beta_{\check{\varphi}}^{\vee} \times \beta_\alpha)$ is then (cf. 4.1.6)

8.6.8
$$\frac{(-1)^{k+l+1} k!\,(p^r N_0)^{k+1} \pi^l}{a(M)^l\, \Omega^{k+l+1}} \left(\sum_{\substack{m \in M \\ m \neq 0}} \frac{g(m)(\bar{m})^l}{m^{k+1} \mathbf{N}(m)^s} \right)_{\Big| s=0} ,$$

a complex number which lies in the number field L, and whose $\mathfrak{p}_\infty$-adic expression is

8.6.9
$$\frac{1}{c^{k+l+1}} \sigma^{-r}\big(\mathfrak{L}(\varepsilon \chi_{k,l}, f\colon M, \check{\varphi}, \alpha)\big) .$$

8.7. *Truly explicit formulas, when $\mathfrak{p}$ is principal and M is prime to p.* For the remainder of this section, we will make the following hypotheses 8.7.1–4.

8.7.1. The invertible $\mathcal{O}_{K_0}$ module $M \subset K_0$ is prime to p, in the sense that in $K_0 \otimes \mathbf{Z}_p$, we have $M \otimes \mathbf{Z}_p = \mathcal{O}_{K_0} \otimes \mathbf{Z}_p$.

Thus $M \otimes \mathbf{Z}_p$ is a ring, and the decomposition $M \otimes \mathbf{Z}_p \simeq M_{\mathfrak{p}} \times M_{\bar{\mathfrak{p}}}$ expresses $M \otimes \mathbf{Z}_p$ as a product of rings, each of which is canonically $\mathbf{Z}_p$.

8.7.2. The given isomorphism $\check{\varphi}\colon \mathbf{Z}_p \xrightarrow{\sim} M_{\bar{\mathfrak{p}}}$ (cf. 8.3.14 bis) is the unique ring isomorphism.

If we compose the unique ring isomorphism $\mathbf{Z}_p \xrightarrow{\sim} M_{\mathfrak{p}}$ with the given (8.3.15 bis) isomorphism $\varphi\colon M_{\mathfrak{p}} \xrightarrow{\sim} T_p(\mathbf{G}_m)$, we obtain an isomorphism $\mathbf{Z}_p \xrightarrow{\sim} T_p(\mathbf{G}_m)$, under which the element $1 \in \mathbf{Z}_p$ goes to an element $(, \cdots, \zeta_a, \cdots)$, with ζ_a a primitive p^ath root of unity. Given a character ε_1 on $(\mathbf{Z}/p^a\mathbf{Z})^\times$, we denote by $g(\zeta_a, \varepsilon_1)$ the Gauss sum

$$g(\zeta_a, \varepsilon_1) = \frac{1}{p^a} \sum_{\substack{n \bmod p^a \\ (n,p)=1}} \varepsilon_1(n) \zeta_a^{-n} .$$

We will systematically use the equality $M_{\mathfrak{p}} = \mathbf{Z}_p$ (in the $\mathfrak{p}$-adic completion of K_0) to view characters of $\mathbf{Z}_p^\times$ as characters of $M_{\mathfrak{p}}^\times$. We will then ues the composite ring isomorphism

$$\begin{aligned} M \otimes \mathbf{Z}_p \simeq M_{\mathfrak{p}} \times M_{\bar{\mathfrak{p}}} &\xrightarrow{\ \sim\ } M_{\mathfrak{p}} \times M_{\mathfrak{p}} \\ (m_1, m_2) &\longmapsto (m_1, \bar{m}_2) \end{aligned}$$

to transport characters of $\mathbf{Z}_p^\times \times \mathbf{Z}_p^\times$ (extended by zero $\mathbf{Z}_p \times \mathbf{Z}_p$) to $M \otimes \mathbf{Z}_p$. Thus given two characters χ_1 and χ_2 of $\mathbf{Z}_p^\times$, the product character $\chi_1(x)\chi_2(y)$ becomes the function on $M \otimes \mathbf{Z}_p$ whose restriction to M is

$$m \longmapsto \chi_1(m)\chi_2(\bar{m}) .$$

8.7.3 The ideal $\mathfrak{p}$ of $\mathcal{O}_{K_0}$ is principal .

Our previous choice of a model E_M for $\mathbf{C}/M$ over $K \cap \mathcal{O}_{\mathfrak{p}\infty}$ determines a canonical generator λ of $\mathfrak{p}$, as follows. Because $\mathfrak{p}$ is principal in K_0, it splits completely in the Hilbert class field K, and hence the residue field of $K \cap \mathcal{O}_{\mathfrak{p}\infty}$ is $\mathbf{F}_p$. So the special fibre $E_M \otimes \mathbf{F}_p$ is an ordinary elliptic curve over $\mathbf{F}_p$, with complex multiplication by $\mathcal{O}_{K_0}$. The numerator of its zeta function is $(1 - \lambda T)(1 - \bar{\lambda} T)$, with λ and $\bar{\lambda}$ in $\mathcal{O}_{K_0}$, and one of them, say λ, a generator of $\mathfrak{p}$. From the $\mathfrak{p}$-adic point of view, the unit root is then $\bar{\lambda}$, so that the unit c in $\hat{\mathcal{O}}_{\mathfrak{p}\infty}$ of 8.3.16 satisfies $c/c^\sigma = \bar{\lambda}$ (cf. 5.4.4). To avoid confusion, we will denote by $\langle \lambda \rangle \in \mathbf{Z}_p^\times$ the quantity "λ viewed $\bar{\mathfrak{p}}$-adically" equal to "$\bar{\lambda}$ viewed $\mathfrak{p}$-adically."

Given a function f on $\mathbf{Z}/N_0\mathbf{Z} \times \mathbf{Z}/N_0\mathbf{Z}$, we denote by $g(m)$ the function on M/N_0M which, when transported to $\boldsymbol{\mu}_{N_0} \times \mathbf{Z}/N_0\mathbf{Z}$ by the composite isomorphism Ⓑ,

$$\begin{tikzcd}
\boldsymbol{\mu}_{N_0} \times \mathbf{Z}/N_0\mathbf{Z} \arrow[r, "\sim", "\textcircled{B}"'] \arrow[d, "(\det(\alpha))^n \mapsto n \ \wr \quad \wr\ \mathrm{id.}"'] & M/N_0M \\
\mathbf{Z}/N_0\mathbf{Z} \times \mathbf{Z}/N_0\mathbf{Z} \arrow[r, "\sim", "\alpha"'] & \frac{1}{N_0}M/M \arrow[u, "\wr\ \times N_0"']
\end{tikzcd} ,$$

becomes the inverse partial Fourier transform $P^{-1}f$ of f:

$$P^{-1}f = g \circ \textcircled{B} .$$

8.7.4. The function g on M/N_0M transforms under $(\mathcal{O}_{K_0}/N_0\mathcal{O}_{K_0})^\times$ by a W-valued character ρ:

$$g(am) = \rho(a) g(m) \qquad \text{for } a \in (\mathcal{O}_{K_0}/N_0\mathcal{O}_{K_0})^\times .$$

8.7.5. *Formulas* (*under the hypotheses* 8.7.1–2–3–4). Let k, l be non-negative integers, ε_1 and ε_2 W-valued characters of finite order of $\mathbf{Z}_p^\times$, and $\varepsilon = \varepsilon_1(x)\varepsilon_2(y)$ their product. Then we have the following transcendental formulas for the algebraic number

$$\frac{1}{c^{k+l+1}}\mathfrak{L}(\varepsilon\chi_{k,l}, f)(M, \check{\varphi}, \alpha) .$$

8.7.6. *Case* I: ε_1, ε_2 *both trivial*:

$$(N_0)^{k+1}\frac{(-1)^{k+l+1}k!\pi^l}{a(M)^l\Omega^{k+l+1}}\left(1-\frac{\lambda^k}{\bar{\lambda}^{l+1}\rho(\lambda)}\right)\left(1-\frac{\lambda^l\rho(\bar{\lambda})}{\bar{\lambda}^{k+1}}\right)\left(\sum_{\substack{m\in M\\ m\neq 0}}\frac{g(m)\bar{m}^l}{m^{k+1}\mathbf{N}(m)^s}\right)_{|s=0} .$$

8.7.7. *Case* II: ε_1 *non-trivial, exact conductor* p^a; ε_2 *trivial*:

$$\varepsilon_1(N_0)(N_0)^{k+1}\frac{g(\zeta_a, \varepsilon_1)(\lambda^a)^{k+l+1}}{p^{al}\varepsilon_1(\langle\lambda^a\rangle)\rho(\lambda^a)}\cdot\frac{(-1)^{k+l+1}k!\pi^l}{a(M)^l\Omega^{k+l+1}}\left(1-\frac{\rho(\bar{\lambda})\lambda^l}{\varepsilon_1(\langle\lambda\rangle)\bar{\lambda}^{k+1}}\right)$$
$$\times\left(\sum_{\substack{m\in M\\ m\notin\lambda M}}\frac{g(m)\bar{m}^l}{\varepsilon_1(m)m^{k+1}\mathbf{N}(m)^s}\right)_{|s=0} .$$

8.7.8. *Case* III: ε_1 *trivial*, ε_2 *non-trivial*:

$$(N_0)^{k+1}\frac{(-1)^{k+l+1}k!\pi^l}{a(M)^l\Omega^{k+l+1}}\left(1-\frac{\lambda^k}{\bar{\lambda}^{l+1}\varepsilon_2(\langle\lambda\rangle)\rho(\lambda)}\right)\left(\sum_{\substack{m\in M\\ m\neq 0}}\frac{g(m)\varepsilon_2(\bar{m})\bar{m}^l}{m^{k+1}\mathbf{N}(m)^s}\right)_{|s=0} .$$

8.7.9. *Case* IV: ε_1, ε_2 *both non-trivial*, ε_1 *of exact conductor* p^a:

$$\varepsilon_1(N_0)(N_0)^{k+1}\frac{g(\zeta_a, \varepsilon_1)(\lambda^a)^{k+l+1}}{p^{al}\rho(\lambda^a)\varepsilon_1(\langle\lambda^a\rangle)\varepsilon_2(\langle\lambda^a\rangle)}\frac{(-1)^{k+l+1}k!\pi^l}{a(M)^l\Omega^{k+l+1}}$$
$$\times\left(\sum_{\substack{m\in M\\ m\notin\lambda M}}\frac{g(m)\varepsilon_2(\bar{m})\bar{m}^l}{\varepsilon_1(m)m^{k+1}\mathbf{N}(m)^s}\right)_{|s=0} .$$

Remark 8.7.10. These formulas can also be obtained by using 6.4.15 to reduce the calculation of a Φ^* to that of several Φ's. An advantage of this method is that the Euler factors which appear when either ε_1 or ε_2 is trivial seem somewhat less artificial. Compare [15], 3.7.3 and 3.8, where this approach is carried out for the one-variable Eisenstein measure.

8.8. *Verification of the formulas of* 8.7. Let us *use* λ to recalculate $\mathfrak{L}(\varepsilon\chi_{k,l}, f; M, \check{\varphi}, \alpha)$, beginning again at 8.6.1. We have

$$\begin{aligned}
\text{8.8.1}\quad \mathfrak{L}(\varepsilon\chi_{k,l}, f; M, \check{\varphi}, \alpha) &= 2\Phi_{k,l,\varepsilon f}(\mathfrak{p}^{-r}M, \mathfrak{p}^{-r}\check{\varphi}, \mathfrak{p}^{-r}\alpha)\\
&= 2\Phi_{k,l,\varepsilon f}(M, \langle\lambda\rangle^r\check{\varphi}, \lambda^r\alpha) \qquad \text{(by 8.3.7.1)}\\
&= 2\Phi_{k,l,\varepsilon f}(E_M, \langle\lambda^r\rangle\varphi, \beta_{\langle\lambda^r\rangle\check{\varphi}}\times\beta_{\lambda^r\alpha})\\
&= 2\langle\lambda^r\rangle^{-k-l-1}\Phi_{k,l,\varepsilon f}(E_M, \varphi^*(dT/(1+T)), \beta_{\langle\lambda^r\rangle\check{\varphi}}\times\beta_{\lambda^r\alpha})\\
&= 2\left(\frac{c}{\langle\lambda^r\rangle}\right)^{k+l+1}G_{k+l+1,-l,\varepsilon f}(E_M, \omega, \beta_{\langle\lambda^r\rangle\check{\varphi}}\times\beta_{\lambda^r\alpha})
\end{aligned}$$

(compare 8.6.5).

To proceed further, we must analyse the relation between $\beta_{\langle\lambda^r\rangle\check{\varphi}}\times\beta_{\lambda^r\alpha}$ and $\beta_{\check{\varphi}}\times\beta_\alpha$. By definition, the latter sits in a commutative diagram

8.8.2
$$\begin{tikzcd}
 & \mathfrak{p}^{-r}M/M \times \bar{\mathfrak{p}}^{-r}M/M \arrow[rr, "p^r", "\sim"'] & & \bar{\mathfrak{p}}^{r}M/p^rM \times \mathfrak{p}^{r}M/p^rM \arrow[d, "\text{addition}", "\sim"'] & \\
\mu_{p^r} \times \mathbf{Z}/p^r\mathbf{Z} \arrow[ur, "\varphi^{-1}\ ,\ \check{\varphi}\circ\frac{1}{p^r}"] \arrow[rrr, "\textcircled{A}"] \arrow[d, "\mathrm{incl}\ ,\ N_0"'] \arrow[d, phantom, shift left=4, "\textcircled{D}"] & & & M/p^rM \arrow[dl, "N_0"'] & \\
\mu_{p^rN_0} \times \mathbf{Z}/p^rN_0\mathbf{Z} \arrow[r, "\check{\beta_\varphi}\times\beta_\alpha", "\sim"'] \arrow[rr, bend left, "\textcircled{C}"] & \frac{1}{p^rN_0}M/M \arrow[r, "p^rN_0", "\sim"'] & M/p^rN_0M \arrow[rr, "\sim"] & & M/p^rM \times M/N_0M \arrow[ul, "pr_1"'] \arrow[dl, "pr_2"] \\
\mu_{N_0} \times \mathbf{Z}/N_0\mathbf{Z} \arrow[u, "\mathrm{incl}\ ,\ p^r"] \arrow[u, phantom, shift right=4, "\textcircled{E}"] \arrow[rrr, "\textcircled{B}"] \arrow[dr, "\det(\alpha)^n\mapsto n\ ,\ \mathrm{id}"'] & & & M/N_0M \arrow[ul, "p^r"'] & \\
 & \mathbf{Z}/N_0\mathbf{Z} \times \mathbf{Z}/N_0\mathbf{Z} \arrow[r, "\alpha", "\sim"'] & \frac{1}{N_0}M/M \arrow[ur, "N_0", "\sim"'] & &
\end{tikzcd}$$

The product structure $\beta_{\langle\lambda^r\rangle\check{\varphi}} \times \beta_{\lambda^r\alpha}$ sits in an analogous diagram, with isomorphisms

8.8.3
$$\begin{aligned}
\text{Ⓒ}_{\lambda^r}&: \mu_{p^rN_0} \times \mathbf{Z}/p^rN_0\mathbf{Z} \xrightarrow{\sim} M/p^rN_0M\,,\\
\text{Ⓐ}_{\lambda^r}&: \mu_{p^r} \times \mathbf{Z}/p^r\mathbf{Z} \xrightarrow{\sim} M/p^rM\,,\\
\text{Ⓑ}_{\lambda^r}&: \mu_{N_0} \times \mathbf{Z}/N_0\mathbf{Z} \xrightarrow{\sim} M/N_0M\,,
\end{aligned}$$

deduced from $\beta_{\langle\lambda^r\rangle\check{\varphi}} \times \beta_{\lambda^r\alpha}$, $\beta_{\langle\lambda^r\rangle\check{\varphi}}$, and $\beta_{\lambda^r\alpha}$ respectively, as in 8.8.2. They are related to their brethren Ⓐ, Ⓑ, Ⓒ of 8.8.2 by the formulas

8.8.4
$$\begin{aligned}
\text{Ⓐ}_{\lambda^r}(\zeta_1, b_1) &= \text{Ⓐ}(\zeta_1^{\langle 1/\lambda^r\rangle}, \langle\lambda^r\rangle b_1)\,,\\
\text{Ⓑ}_{\lambda^r}(\zeta_2^{p^r}, b_2) &= \lambda^r\,\text{Ⓑ}(\zeta_2, b_2) \quad (\text{because } \det(\alpha)^{p^r} = \det(\lambda^r\alpha)),\\
\text{Ⓒ}_{\lambda^r}\big(\text{Ⓓ}(\zeta_1, b_1) + \text{Ⓔ}(\zeta_2, b_2)\big) &= N_0\text{Ⓐ}_{\lambda^r}(\zeta_1, b_1) + p^r\,\text{Ⓑ}_{\lambda^r}(\zeta_2, b_2)\,.
\end{aligned}$$

We now introduce the functions

8.8.5
$$\begin{cases} h,\ h^{(r)} & \text{on } M/p^rN_0M\\ e & \text{on } M/p^rM\\ g & \text{on } M/N_0M \end{cases}$$

defined by

8.8.6
$$\begin{cases} h\circ\text{Ⓒ} = P^{-1}(\varepsilon f) = h^{(r)}\circ\text{Ⓒ}_{\lambda^r}\\ e\circ\text{Ⓐ} = P^{-1}(\varepsilon)\\ g\circ\text{Ⓑ} = P^{-1}(f)\,. \end{cases}$$

Just as in 8.6.8–9, the transcendental expression of the $\mathfrak{L}$-value involves the function $h^{(r)}$: the algebraic number

$$\left(\frac{\langle\lambda^r\rangle}{c}\right)^{k+l+1} \mathfrak{L}(\varepsilon\chi_{k,l}, f\colon M, \check{\varphi}, \alpha)$$

is given transcendentally as

8.8.7 $$\frac{(-1)^{k+l+1}k!\,(p^r N_0)^{k+1}\pi^l}{a(M)^l\,\Omega^{k+l+1}}\left(\sum_{\substack{m\in M\\ m\neq 0}}\frac{h^{(r)}(m)(\bar{m})^l}{m^{k+1}\mathrm{N}(m)^s}\right)_{|s=0}.$$

PROPOSITION 8.8.8. *The function $h^{(p)}$ is given in terms of ε_1, ε_2 and g by*

$$h^{(r)}(m) = \frac{\varepsilon_1(N_0)}{\varepsilon_1(\langle\lambda^r\rangle)\varepsilon_2(\langle\lambda^r\rangle)\rho(\lambda^r)}\cdot e_1(m)\varepsilon_2(\bar{m})\,g(m)$$

where $e_1(m)$ is the following function:

8.8.9. *If ε_1 is trivial, then e_1 has exact support $\mathfrak{p}^{r-1}M = \lambda^{r-1}M$, and*

$$e_1(\lambda^{r-1}m) = \begin{cases} 1 - \dfrac{1}{p} & \text{if } m \in \mathfrak{p}M \\[2ex] \dfrac{-1}{p} & \text{if not}\ . \end{cases}$$

8.8.10. *If ε_1 is non-trivial, of exact conductor p^a, then e_1 has exact support $\mathfrak{p}^{r-a}M - \mathfrak{p}^{r+1-a}M$, and for $m \in M - \mathfrak{p}M$, we have*

$$e_1(\lambda^{r-a}m) = \frac{\varepsilon_1(\langle\lambda^{r-a}\rangle)\,g(\zeta_a, \varepsilon_1)}{\varepsilon_1(m)}\ .$$

The formulas given in 8.7 now follow by direct substitution of 8.8.8 into 8.8.7. The calculation is left to the reader.

To prove 8.8.8, we begin by expressing $h^{(r)}$ in terms of e and g.

LEMMA 8.8.11. *We have the formula*

$$h^{(r)}(m) = \frac{\varepsilon_1(N_0)}{\varepsilon_1(\langle\lambda^r\rangle)\varepsilon_2(\langle\lambda^r\rangle)\rho(\lambda^r)}e(m)\,g(m)\ .$$

Before giving the proof of 8.8.11, we need two sublemmas.

SUBLEMMA 8.8.12. *If $\varepsilon = \varepsilon_1(x)\varepsilon_2(y)$ is a character of $(\mathbf{Z}/p^p\mathbf{Z})^\times \times (\mathbf{Z}/p^r\mathbf{Z})^\times$, extended by zero, the function $p^{-1}(\varepsilon)$ on $\boldsymbol{\mu}_p r \times \mathbf{Z}/p^r\mathbf{Z}$ satisfies*

$$P^{-1}(\varepsilon)(\zeta^a, bn) = \frac{\varepsilon_2(b)}{\varepsilon_1(a)}P^{-1}(\varepsilon)(\zeta, n)$$

for any a, b in $(\mathbf{Z}/p^r\mathbf{Z})^\times$.

Proof. This follows immediately from the definition (3.6.1) of $P^{-1}(\varepsilon)$.

SUBLEMMA 8.8.13. *Given*

$$(\zeta_1, b_1) \in \boldsymbol{\mu}_{p^r} \times \mathbf{Z}/p^r\mathbf{Z} \text{ and } (\zeta_2, b_2) \in \boldsymbol{\mu}_{N_0} \times \mathbf{Z}/N_0\mathbf{Z}\ ,$$

we have

$$P^{-1}(\varepsilon f)\big(Ⓓ(\zeta_1, b_1) + Ⓔ(\zeta_2, b_2)\big) = P^{-1}(\varepsilon)(\zeta_1, N_0 b_1) \cdot P^{-1}(f)(\zeta_2, p^r b_2) .$$

Proof. Simply compute:

$$\begin{aligned}
&P^{-1}(\varepsilon f)\big(Ⓓ(\zeta_1, b_1) + Ⓔ(\zeta_2, b_2)\big) \\
&\quad = P^{-1}(\varepsilon f)(\zeta_1\zeta_2, N_0 b_1 + p^r b_2) \\
&\quad \overset{\text{dfn}}{=} \frac{1}{p^r N_0}\sum\nolimits_{a \bmod p^r N_0} (\varepsilon f)(a, N_0 b_1 + p^r b_2)(\zeta_1\zeta_2)^{-a} \\
&\quad = \frac{1}{p^r N_0}\sum\nolimits_{\substack{a_1 \bmod p^r \\ a_2 \bmod N_0}} (\varepsilon f)(N_0 a_1 + p^r a_2, N_0 b_1 + p^r b_2)(\zeta_1\zeta_2)^{-N_0 a_1 - p^r a_2} \\
&\quad = \frac{1}{p^r N_0}\sum\nolimits_{\substack{a_1 \bmod p^r \\ a_2 \bmod N_0}} \varepsilon(N_0 a_1, N_0 b_1)\zeta_1^{-N_0 a_1} f(p^r a_2, p^r b_2)\zeta_2^{-p^r a_2} \\
&\quad = P^{-1}(\varepsilon)(\zeta_1, N_0 b_1) P^{-1}(f)(\zeta_2, p^r b_2) . \qquad \text{Q.E.D.}
\end{aligned}$$

We can now prove 8.8.11. Write $m = N_0 m_1 + p^r m_2$, so that the assertion becomes

8.8.14
$$h^{(r)}(N_0 m_1 + p^r m_2) = \frac{\varepsilon_1(N_0)}{\varepsilon_1(\langle\lambda^r\rangle)\varepsilon_2(\langle\lambda^r\rangle)} e(N_0 m_1)\, g(\lambda^{-r} p^r m_2) .$$

We may write

8.8.15
$$\begin{cases} m_1 \equiv Ⓐ_{\lambda^r}(\zeta_1, b_1) \bmod p^r \\ m_2 \equiv Ⓑ_{\lambda^r}(\zeta_2, b_2) \bmod N_0 . \end{cases}$$

Then

$$\begin{aligned}
&h^{(r)}(N_0 m_1 + p^r m_2) \\
&\quad = h^{(r)}\big(N_0 Ⓐ_{\lambda^r}(\zeta_1, b_1) + p^r Ⓑ_{\lambda^r}(\zeta_2, b_2)\big) \\
&\quad = h^{(r)}\big(Ⓒ_{\lambda^{(r)}}\big(Ⓓ(\zeta_1, b_1) + Ⓔ(\zeta_2, b_2)\big)\big) && \text{(by 8.8.4)} \\
&\quad = P^{-1}(\varepsilon f)\big(Ⓓ(\zeta_1, b_1) + Ⓔ(\zeta_2, b_2)\big) && \text{(by 8.8.6)} \\
&\quad = P^{-1}(\varepsilon)(\zeta_1, N_0 b_1) P^{-1}(f)(\zeta_2, p^r b_2) && \text{(by 8.8.13)} \\
&\quad = \frac{\varepsilon_1(N_0)}{\varepsilon_1(\langle\lambda^r\rangle)\varepsilon_2(\langle\lambda^r\rangle)} P^{-1}(\varepsilon)\big(\zeta_1^{N_0/\langle\lambda^r\rangle}, N_0\langle\lambda^r\rangle b_1\big) P^{-1}(f)(\zeta_2, p^r b_2) && \text{(by 8.8.12)} \\
&\quad = \frac{\varepsilon_1(N_0)}{\varepsilon_1(\langle\lambda^r\rangle)\varepsilon_2(\langle\lambda^r\rangle)} e\big(Ⓐ\big(\zeta_1^{N_0/\langle\lambda^r\rangle}, N_0\langle\lambda^r\rangle b_1\big)\big) g\big(Ⓑ(\zeta_2, p^r b_2)\big) && \text{(by 8.8.6)} \\
&\quad = \frac{\varepsilon_1(N_0)}{\varepsilon_1(\langle\lambda^r\rangle)\varepsilon_2(\langle\lambda^r\rangle)} e\big(N_0 Ⓐ_{\lambda^r}(\zeta_1, b_1)\big) g\big(\lambda^{-r} p^r Ⓑ_{\lambda^r}(\zeta_2, b_2)\big) && \text{(by 8.8.4)} \\
&\quad = \frac{\varepsilon_1(N_0)}{\varepsilon_1(\langle\lambda^r\rangle)\varepsilon_2(\langle\lambda^r\rangle)} e(N_0 m_1) g(\lambda^{-r} p^r m_2) && \text{(by 8.8.15).}
\end{aligned}$$

Q.E.D.

LEMMA 8.8.16. *The function* $e(m)$ *is a product function* $e_1(m)e_2(m)$, *where*

8.8.17. *$e_2(m)$ is the $\bar{\mathfrak{p}}$-adically continuous, locally constant function on M obtained by transporting ε_2 via the given isomorphism $\check{\varphi}\colon \mathbf{Z}_p \xrightarrow{\sim} M_{\bar{\mathfrak{p}}}$. So with the conventions of* 8.7, *we have $e_2(m) = \varepsilon_2(\bar{m})$.*

8.8.18 *$e_1(m)$ is the function described in* 8.8.9–10.

Proof. Because ε is a product function $\varepsilon_1(x)\varepsilon_2(y)$, $P^{-1}(\varepsilon)$ is itself a product function on $\mu_{p^r} \times \mathbf{Z}/p^r\mathbf{Z}$:

$$P^{-1}(\varepsilon)(\zeta, b) = \hat{\varepsilon}_1(\zeta)\varepsilon_2(b)$$

where

$$\hat{\varepsilon}_1(\zeta) = \frac{1}{p^r}\sum\nolimits_{a \bmod p^r} \varepsilon_1(a)\zeta^{-a} .$$

The isomorphism Ⓐ sits in the commutative diagram

8.8.19
$$\begin{tikzcd}
\mu_{p^r} \times \mathbf{Z}/p^r\mathbf{Z} \arrow[r, "\varphi^{-1}\times\check{\varphi}\circ\frac{1}{p^r}", "\sim"'] \arrow[d, "Ⓐ"] \arrow[drr] & \mathfrak{p}^{-r}M/M \times \bar{\mathfrak{p}}^{-r}M/M \arrow[r, "p^r", "\sim"'] & \bar{\mathfrak{p}}^rM/p^rM \times \mathfrak{p}^rM/p^rM \arrow[d, "\text{mod } \mathfrak{p}^r \ \mid\ \text{mod } \bar{\mathfrak{p}}^r"] \\
M/p^rM \arrow[rr, "(\text{mod } \mathfrak{p}^r,\ \text{mod } \bar{\mathfrak{p}}^r)"] & & M/\mathfrak{p}^rM \times M/\bar{\mathfrak{p}}^rM .
\end{tikzcd}$$

Thus $e(m) = e_1(m)e_2(m)$, where

8.8.20
$$\begin{cases} e_1(m) = \hat{\varepsilon}_1(\zeta) & \text{if } p^r\varphi^{-1}(\zeta) \equiv m \bmod \mathfrak{p}^r \\ e_2(m) = \varepsilon_2(b) & \text{if } p^r\check{\varphi}\left(\dfrac{b}{p^r}\right) \equiv m \bmod \bar{\mathfrak{p}}^r . \end{cases}$$

The truth of 8.8.17 now follows from this last formula, and the definition (8.3.14 bis) of $\check{\varphi}$. To prove 8.8.18, we consider the commutative diagram

8.8.21
$$\begin{tikzcd}
\mathbf{Z}/p^r\mathbf{Z} \arrow[r, "n\mapsto\xi_r^n", "\sim"'] \arrow[rr, bend left=50, "\text{the ring isom.}"] & \mu_{p^r} \arrow[r, "p^r\varphi^{-1}", "\sim"'] & M/\mathfrak{p}^rM \\
\mathbf{Z}/p^a\mathbf{Z} \arrow[u, "p^{r-a}"] \arrow[r, "\sim", "n\mapsto\xi_a^n"'] \arrow[rr, bend right=50, "\text{the ring isom.}"'] & \mu_{p^a} \arrow[u, phantom, "\bigcup"] \arrow[r, "\sim", "p^a\varphi^{-1}"'] & M/\mathfrak{p}^aM \arrow[u, "p^{r-a} = \langle\lambda^{r-a}\rangle\lambda^{r-a}"']
\end{tikzcd} .$$

By transport of structure, the function $e_1(m)$ corresponds to the function $\hat{\varepsilon}_1$ on μ_{p^r} defined above. The assertions 8.8.9–10 become the following standard facts about Gauss sums (cf. [32], p. 91), whose proof is left to the reader.

LEMMA 8.8.22. *Let ε_1 be a character of $(\mathbf{Z}/p^r\mathbf{Z})^\times$. Then:*

8.8.23. *For $b \in (\mathbf{Z}/p^r\mathbf{Z})^\times$ and $\zeta \in \boldsymbol{\mu}_{p^r}$, we have*

$$\hat{\varepsilon}_1(\zeta^b) = \frac{1}{\varepsilon_1(b)}\hat{\varepsilon}_1(\zeta) .$$

8.8.24. *If ε_1 is trivial, then*

$$\hat{\varepsilon}_1(\zeta) = \begin{cases} 1 - \dfrac{1}{p} & \textit{if } \zeta = 1 \\ \dfrac{-1}{p} & \textit{if } \zeta^p = 1, \textit{ but } \zeta \neq 1 \\ 0 & \textit{if } \zeta^p \neq 1 . \end{cases}$$

8.8.25. *If ε_1 is non-trivial, of exact conductor p^a, then $\hat{\varepsilon}_1(\zeta) = 0$ unless ζ has exact order p^a, and the restriction of $\hat{\varepsilon}_1$ to $\boldsymbol{\mu}_{p^a}$ is independent of the auxiliary $r \geqq a$ used to define it.*

Chapter IX. Yet another measure, and passage to the limit

9.0. *A critique of μ_N.* The measure μ_N, while magnificently suited to q-expansion computations, is somewhat clumsy when it comes to "transcendental" calculations, as we saw in the last chapter, where both the level "N" and a persistent partial Fourier transform (g) occurred in the formulas for $\mathfrak{L}(\chi_{k,l}, f; M, \check{\varphi}, \alpha)$. In this chapter, we will outline an artifice for correcting these defects, and at the same time "beautifying" the formulas of Section 8.7 for $\mathfrak{L}(\varepsilon\chi_{k,l}, f; M, \check{\varphi}, \alpha)$. The idea is simply to replace the "f" in the nomenclature by the "g" to which it gives rise, and to divide by $\varepsilon_1(N_0)N_0^{k+1}$ to get an expression which is "independent of N_0." It is obvious from the explicit formulas of the last section that this "works" for $(M, \check{\varphi}, \alpha)$'s but we will see that it is a special case of a *modular* construction.

9.1. *Construction of ν_N.* For the rest of this chapter, N denotes an integer *prime* to p. We will construct a $V(\mathbf{Z}_p, \Gamma(N)^{\text{navie}})$-valued measure ν_N on $(\mathbf{Z}_p^\times)^2 \times (\mathbf{Z}/N\mathbf{Z})^2$ out of μ_N, by the following artifice.

Given a trivialized $\Gamma(N)^{\text{naive}}$ curve (E, φ, α) over a p-adic ring B, and a B-valued function f on $(\mathbf{Z}/N\mathbf{Z})^2$, we can define two new B-valued functions, $P_\alpha f$ and $\hat{f}_\alpha$, on $(\mathbf{Z}/N\mathbf{Z})^2$, the partial and the symplectic Fourier transforms, by (compare 3.2.1, 3.0.1) the formulas

9.1.1 $$(P_\alpha f)(n, m) = \textstyle\sum_{a \bmod N} f(a, m) \det(\alpha)^{an} ,$$

9.1.2 $$\hat{f}_\alpha(c, d) = \frac{1}{N}\textstyle\sum_{a,b \bmod N} f(a, b) \det(\alpha)^{ad-bc} .$$

Definition 9.1.3. The $V(\mathbf{Z}_p, \Gamma(N)^{\text{naive}})$-valued measure ν_N on $(\mathbf{Z}_p^\times)^2 \times (\mathbf{Z}/N\mathbf{Z})^2$ is defined by

9.1.4
$$\left(\int \psi(x, y)f(u, v)d\nu_N\right)(E, \varphi, \alpha) \stackrel{\text{dfn}}{=} \left(\int \frac{1}{N}\psi(x/N, y)(P_\alpha f)(u, v)d\mu_N\right)(E, \varphi, \beta_\alpha) .$$

The following proposition results from the definition, and the analogous properties of μ_N (cf. 6.4.17 and 6.4.5).

PROPOSITION 9.1.5. *The behaviour of ν_N under the derivation θ of $V(\mathbf{Z}_p, \Gamma(N)^{\text{naive}})$ is given by*

9.1.6
$$\theta\left(\int \psi(x, y)f(u, v)d\nu_N\right) = \int xy\psi(x, y)f(u, v)d\nu_N .$$

For a given test object (E, φ, α), we have the functional equation

9.1.7
$$\left(\int \psi(x, y)f(u, v)d\nu_N\right)(E, \varphi, \alpha) = \left(\int \psi(y/N, Nx)\hat{f}_\alpha(u, v)\,d\nu_N\right)(E, \varphi, \alpha) .$$

It remains to discuss *transformation.* The group which replaces $G(N)$ is the group

9.1.8
$$H(N) \stackrel{\text{dfn}}{=} \mathbf{Z}_p^\times \times \operatorname{Aut}\left((\mathbf{Z}/N\mathbf{Z})^2\right) ,$$

an element (a, g) of which operates on $V(\mathbf{Z}_p, \Gamma(N)^{\text{naive}})$ by the rule

9.1.9
$$([a, g]F)(E, \varphi, \alpha) \stackrel{\text{dfn}}{=} F(E, a^{-1}\varphi, \alpha \circ g) .$$

9.1.10. Given an element $b \in (\mathbf{Z}/N\mathbf{Z})^\times$, we denote by $\langle b\rangle \in \operatorname{Aut}\left((\mathbf{Z}/N\mathbf{Z})^2\right)$ the automorphism (b, b^{-1}), i.e., $(x, y) \mapsto (bx, b^{-1}y)$. Then $G(N) \hookrightarrow H(N)$ by $(a, b) \to (a, \langle b\rangle)$, and clearly $\beta_{\alpha\circ\langle b\rangle} = \beta_\alpha \circ (b, b^{-1})$.

PROPOSITION 9.1.11. *Under the action of $H(N)$, we have the transformation formula*

9.1.12
$$[a, g]\int \psi(x, y)f(u, v)\,d\nu_N = \int a\psi(ax, ay)(f \circ g^{-1})(u, v)d\nu_N .$$

Proof. For $g = \langle b\rangle$, this follows from 6.4.10 and the definition of ν_N. It remains to check elements of the form $(1, g)$, with arbitrary $g \in \operatorname{Aut}\left((\mathbf{Z}/N\mathbf{Z})^2\right)$. This is proved by a "reduction to the transcendental case" argument similar to that given in 5.11.16. To carry it out in detail involves introducing a measure $\nu_N^{(a,1)}$ on $(\mathbf{Z}_p)^2 \times (\mathbf{Z}/N\mathbf{Z})^2$ analogous to $\mu_N^{(a,1)}$ (to which ν_N is related by the analogue of 6.4.11), and using the "reduction to moments," 9.1.6, and 9.1.7, to reduce to checking it for the *true* modular form

$$\int_{(\mathbf{Z}_p)^2\times(\mathbf{Z}/N\mathbf{Z})^2} x^k f(u, v)d\nu_N^{(a,1)} \in R^{k+1}\left(\mathbf{Z}_p, \Gamma(N)^{\text{naive}}\right) .$$

We omit the details.

Remark 9.1.12. An alternate proof could be based on the Zariski denseness of those trivialized $\Gamma(N)^{\text{naive}}$ curves arising from triples $(M, \check{\varphi}, \alpha)$

over *variable* quadratic imaginary fields in which p splits. The point is that in the *formulas* of 8.7 for

$$\begin{aligned}\mathfrak{L}(\varepsilon\chi_{k,l},\, f)(M,\, \check{\varphi},\, \alpha) &= \int \varepsilon(x,\, y)x^k y^l f(u,\, v)d\mu_N(M,\, \check{\varphi},\, \alpha) \\ &= \varepsilon_1(N)N^{k+1}\int \varepsilon(x,\, y)x^k y^l (P_\alpha^{-1}f)(u,\, v)d\nu_N(M,\, \check{\varphi},\, \alpha)\end{aligned}$$

with $k,\, l \geqq 0$, it is only the function $(P_\alpha^{-1}f)\circ\alpha^{-1}$ which enters, so that the truth of the proposition results from the identity

$$(P_\alpha^{-1}f)\circ(\alpha\circ g)^{-1} = \big((P_\alpha^{-1}f)\circ g^{-1}\big)\circ\alpha^{-1} \quad \text{for } g \in \operatorname{Aut}\big((\mathbf{Z}/N\mathbf{Z})^2\big)\,.$$

9.2. *Independence of N.* Here are two equivalent descriptions of how a naive level NM structure α_{NM} induces a naive level N structure α_N.

9.2.1 *First*: View α_{NM} as $\left(\frac{1}{NM}\mathbf{Z}/\mathbf{Z}\right)^2 \xrightarrow{\sim} {}_{NM}E$

$$\begin{array}{ccc} \cup & & \cup \end{array}$$

and restrict $\left(\frac{1}{N}\mathbf{Z}/\mathbf{Z}\right)^2 \xrightarrow[\sim]{\alpha_N} {}_N E\,.$

9.2.2 *Second*: View α_{NM} as $(\mathbf{Z}/NM\mathbf{Z})^2 \xrightarrow{\sim} {}_{NM}E$ and reduce mod N

$$\begin{array}{ccc} (\mathbf{Z}/NM\mathbf{Z})^2 & \xrightarrow{\sim} & {}_{NM}E \\ \Big\downarrow{\scriptstyle \text{red. mod } N} & & \Big\downarrow{\scriptstyle \text{mult. by } M} \\ (\mathbf{Z}/N\mathbf{Z})^2 & \xrightarrow[\sim]{\alpha_N} & E_N\,. \end{array}$$

For our purposes, it will be more convenient to work systematically with the second.

9.2.3. The construction $\alpha_{NM} \mapsto \alpha_N$ determines an inclusion of rings $V(\mathbf{Z}_p,\, \Gamma(N)^{\text{naive}}) \subset V(\mathbf{Z}_p,\, \Gamma(NM^{\text{naive}}),\, F \to \tilde{F}$, defined modularly by

9.2.4 $$\tilde{F}(E,\, \varphi,\, \alpha_{NM}) = F(E,\, \varphi,\, \alpha_N)\,.$$

We will drop the $\sim$ notation, and view $V(\mathbf{Z}_p,\, \Gamma(N)^{\text{naive}})$ as canonically sitting inside $V(\mathbf{Z},\, \Gamma(NM)^{\text{naive}})$ as the *invariants* under the subgroup

$$\Gamma(N)/\Gamma(NM) \subset \operatorname{Aut}\big((\mathbf{Z}/NM\mathbf{Z})^2\big)\,.$$

Similarly, the map "reduction mod N"

9.2.5 $$(\mathbf{Z}/NM\mathbf{Z})^2 \twoheadrightarrow (\mathbf{Z}/N\mathbf{Z})^2$$

gives an inclusion: "functions on $(\mathbf{Z}/N\mathbf{Z})^2$" $\subset$ "functions on $(\mathbf{Z}/NM\mathbf{Z})^2$"; for a function f on $(\mathbf{Z}/N\mathbf{Z})^2$, we still denote by f the function on $(\mathbf{Z}/NM\mathbf{Z})^2$ given by $(u,\, v) \mapsto f(u \bmod N,\, v \bmod N)$.

PROPOSITION 9.2.6. *Let f be a function on $(\mathbf{Z}/N\mathbf{Z})^2$. For any M prime to p, we have an equality*

9.2.7
$$\underbrace{\int \psi(x, y) f(u, v)\, d\nu_N}_{\substack{\cap \\ V(\mathbf{Z}_p,\, \Gamma(N)^{\text{naive}})}} = \underbrace{\int \psi(x, y) f(u, v)\, d\nu_{NM}}_{\substack{\cap \\ V(\mathbf{Z}_p,\, \Gamma(NM)^{\text{naive}})}} , \qquad V(\mathbf{Z}_p, \Gamma(N)^{\text{naive}}) \subset V(\mathbf{Z}_p, \Gamma(NM)^{\text{naive}}) .$$

Proof. We will use a q-expansion argument. Recall that

$$V(\mathbf{Z}_p, \Gamma(N)^{\text{naive}}) \simeq V(\mathbf{Z}_p, \Gamma(N)^{\text{arith}}) \otimes_{\mathbf{Z}} \mathbf{Z}\left[\frac{1}{N}, \zeta_N\right],$$

where $\mathbf{Z}[1/N, \zeta_N]$ means the ring $\mathbf{Z}[1/N, X]/(\phi_N(X))$, ϕ_N the N^{th} cyclotomic polynomial. By the q-expansion principle for $V(\mathbf{Z}_p, \Gamma(N)^{\text{arith}})$, it follows that an element of $V(\mathbf{Z}_p, \Gamma(N)^{\text{naive}})$ is determined by its *value* in $\widehat{\mathbf{Z}_p((q))} \otimes_{\mathbf{Z}} \mathbf{Z}[1/N, \zeta_N]$ on the test object $(\text{Tate}(q^N), \varphi_{\text{can}}, \alpha_N\colon (n, m) \to \zeta_N^n q^m)$ over $\widehat{\mathbf{Z}_p((q))} \otimes_{\mathbf{Z}} \mathbf{Z}[1/N, \zeta_N]$.

On the other hand, the *natural* inclusion $V(\mathbf{Z}_p, \Gamma(N)^{\text{naive}}) \to V(\mathbf{Z}_p, \Gamma(NM)^{\text{naive}})$ is not compatible with this notion of q-expansion, but replaces q by q^M (once ζ_N and ζ_{NM} are "normalized" so that $(\zeta_{NM})^M = \zeta_N$). If we view $\int \psi(x, y) f(u, v) d\nu_N \in V(\mathbf{Z}_p, \Gamma(N)^{\text{naive}})$ as *lying* in $V(\mathbf{Z}_p, \Gamma(NM)^{\text{naive}})$ by the natural inclusion, its q-expansion is

9.2.8
$$\sum_{\substack{n \geq 1 \\ (p, n) = 1}} q^{Mn} \sum_{n = dd'} \Big(\frac{1}{N} \psi(d/N, d')(P_{\alpha_N} f)(d, d') - \frac{1}{N} \psi(-d/N, -d')(P_{\alpha_N} f)(-d, -d') \Big) ,$$

whereas $\int \psi(x, y) f(u, v) d\nu_{NM} \in V(\mathbf{Z}_p, \Gamma(\mathbf{Z}_p, \Gamma(NM)^{\text{naive}}))$ has q-expansion

9.2.9
$$\sum_{\substack{n \geq 1 \\ (p, n) = 1}} q^n \sum_{n = dd'} \Big(\frac{1}{NM} \psi(d/NM, d')(P_{\alpha_{NM}} f)(d, d') - \frac{1}{NM} \psi(-d/NM, -d')(P_{\alpha_{NM}} f)(-d, -d') \Big) .$$

In fact, the *individual terms* match up, as follows:

9.2.10
$$(P_{\alpha_{NM}} f)(d, d') = \begin{cases} 0 & \text{unless } d \equiv 0 \bmod M \\ M P_{\alpha_N}\Big(\dfrac{d}{M}, d'\Big) & \text{if } d \equiv 0 \bmod M \end{cases}$$

when f is periodic mod N (it is the "periodicity $\leftrightarrow$ support" duality of Fourier transform). To check 9.2.10, we may assume f is a *product* function $f(n, m) = A(n)B(m)$. Then

$$(P_{\alpha_{NM}} f)(d, d') = A_{NM}(d) B(d'), \quad (P_{\alpha_N} f)(d, d') = A_N(d) B(d') ,$$

where

9.2.11
$$\begin{cases} A_{NM}(d) = \sum_{a \bmod NM} A(a) \zeta_{NM}^{ad} \\ A_N(d) = \sum_{a \bmod N} A(a) \zeta_N^{ad} . \end{cases}$$

Because A is periodic mod N, we can write

$$A_{NM}(d) = \left(\sum_{a=0}^{N-1} A(a)\zeta_{NM}^{ad}\right)\sum_{b=0}^{M-1} \zeta_{NM}^{bNd}$$
$$= \left(\sum_{a=0}^{N-1} A(a)\zeta_{NM}^{ad}\right)\sum_{b=0}^{M-1} \zeta_{M}^{bd}$$

$$A_{NM}(d) = \begin{cases} 0 \text{ if } \zeta_M^d \neq 1, \text{ i.e., if } d \not\equiv 0(M) \\ M\sum_{a=0}^{N-1} A(a)\zeta_N^{a(d/M)} = MA_N\left(\frac{d}{M}\right) \text{ if } d \equiv 0(M). \end{cases} \qquad \text{Q.E.D.}$$

Remark 9.2.12 (compare 9.1.12). This "independence of N" is obvious from the transcendental formulas 8.7.6–9 for values on $(M, \check{\varphi}, \alpha)$'s.

9.3. *Passage to the limit: definition of the measure ν and the modified $\mathfrak{L}$ function $\mathfrak{L}_\nu$.* Given an elliptic curve E over a ring B, we define a $\Gamma(\text{not } p)^{\text{naive}}$ structure on E to be a compatible system of isomorphisms

9.3.0 $$\alpha_N\colon (\mathbf{Z}/N\mathbf{Z})^2 \xrightarrow{\sim} {}_NE$$

for all N prime to p (compatibility in the sense of 9.2.2), which we abbreviate as a single isomorphism

9.3.1 $$\begin{array}{ccc} \alpha\colon \left(\prod_{l\neq p} \mathbf{Z}_l\right)^2 & \xrightarrow{\sim} & \prod_{l\neq p} T_l(E) \\ \Big\| \text{dfn} & & \Big\| \text{dfn} \\ (\hat{\mathbf{Z}}_{\text{not } p})^2 & \xrightarrow{\sim} & T_{\text{not } p}(E)\,. \end{array}$$

9.3.2. The corresponding moduli problem "trivialized $\Gamma(\text{not } p)^{\text{naive}}$ curves" is *represented* by a ring $V(\mathbf{Z}_p, \Gamma(\text{not } p)^{\text{naive}})$, which is none other than the p-adic completion of the ring

9.3.3 $$\bigcup_{\substack{N \\ (p,N)=1}} V(\mathbf{Z}_p, \Gamma(N)^{\text{naive}})\,.$$

The group $\mathbf{Z}_p^\times \times \operatorname{Aut}((\hat{\mathbf{Z}}_{\text{not } p})^2)$ operates on $V(\mathbf{Z}_p, \Gamma(\text{not } p)^{\text{naive}})$ by the rule

9.3.4 $$[a, g]F(E, \varphi, \alpha) \overset{\text{dfn}}{=} F(E, a^{-1}\varphi, \alpha\circ g)\,.$$

For any integer N prime to p, the ring $V(\mathbf{Z}_p, \Gamma(N)^{\text{naive}})$ sits inside $V(\mathbf{Z}_p, \Gamma(\text{not } p)^{\text{naive}})$ as the group of *invariants* of the subgroup

$$\{1\} \times \left(\text{Kernel: } \operatorname{Aut}((\hat{\mathbf{Z}}_{\text{not } p})^2) \twoheadrightarrow \operatorname{Aut}((\mathbf{Z}/N\mathbf{Z})^2)\right)\,.$$

9.3.5. The measures ν_N for variable N prime to p form an inverse system of measures on the spaces $(\mathbf{Z}_p^\times)^2 \times (\mathbf{Z}/N\mathbf{Z})^2$, each of which we can view as taking values in the single ring $V(\mathbf{Z}_p, \Gamma(\text{not } p)^{\text{naive}})$. By passage to the limit, they define a single measure ν on the space

$$(\mathbf{Z}_p^\times)^2 \times (\hat{\mathbf{Z}}_{\text{not } p})^2 = \varprojlim_{(p,N)=1} (\mathbf{Z}_p^\times)^2 \times (\mathbf{Z}/N\mathbf{Z})^2$$

with values in $V(\mathbf{Z}_p, \Gamma(\text{not } p)^{\text{naive}})$.

PROPOSITION 9.3.6. *The* $V(\mathbf{Z}_p, \Gamma(\text{not } p)^{\text{naive}})$*-valued measure* ν *on* $(\mathbf{Z}_p^\times)^2 \times (\hat{\mathbf{Z}}_{\text{not } p})^2$ *enjoys the following properties*:

9.3.7 (*Transformation*). *For any* $(a, g) \in \mathbf{Z}_p^\times \times \operatorname{Aut}((\hat{\mathbf{Z}}_{\text{not } p})^2)$,

$$[a, g]\int \psi(x, y)f(u, v)d\nu = \int a\psi(ax, ay)(f \circ g^{-1})(u, v)d\nu \;.$$

9.3.8 (*Differentiation*). *The derivation* θ *of* $V(\mathbf{Z}_p, \Gamma(\text{not } p)^{\text{naive}})$ *acts on* ν *by*

$$\theta\int \psi(x, y)f(u, v)d\nu = \int xy\psi(x, y)f(u, v)d\nu \;.$$

Proof. This follows immediately from its finite-level analogues 9.1.5 and 9.1.12. Q.E.D.

Remark 9.3.7. Notice that we "*lose*" the functional equation 9.1.7, which at finite level N depended upon N (cf. 9.1.7).

Definition 9.3.8 (compare 7.1). For $\chi \in \operatorname{Hom}_{\text{contin}}((\mathbf{Z}_p^\times)^2, W)$, and any continuous W-valued function f on $(\hat{\mathbf{Z}}_{\text{not } p})$, we define

9.3.9 $$\int \chi(x, y)f(u, v)d\nu \overset{\text{dfn}}{=} \mathfrak{L}_\nu(\chi, f) \in V(\mathbf{Z}_p, \Gamma(\text{not } p)^{\text{naive}}) \;.$$

9.4. *Evaluation of* $\mathfrak{L}_\nu(\chi, f)(M, \check{\varphi}, \alpha)$ *with* $\mathfrak{p}$ *principal and* M *prime to* p. We return to the setting of Section 8.7, but now consider triples $(M, \check{\varphi}, \alpha)$ with α an isomorphism

9.4.1 $$\alpha\colon (\hat{\mathbf{Z}}_{\text{not } p})^2 \xrightarrow{\sim} \hat{M}_{\text{not } p} = M \otimes_{\mathbf{Z}} \hat{\mathbf{Z}}_{\text{not } p} \;.$$

Combining this isomorphism with the ring isomorphism

9.4.2 $$\begin{array}{c} \mathbf{Z}_p \times \mathbf{Z}_p = M_{\mathfrak{p}} \times M_{\mathfrak{p}} \xrightarrow{\sim} M_{\mathfrak{p}} \times M_{\bar{\mathfrak{p}}} \simeq M \otimes \mathbf{Z}_p \\ (m_1, m_2) \longmapsto (m_1, \bar{m}_2) \end{array}$$

gives a single isomorphism

9.4.3 $$(\hat{\mathbf{Z}})^2 \xrightarrow{\sim} M \otimes \hat{\mathbf{Z}} \;.$$

This allows us to view ν as being a $V(\mathbf{Z}_p, \Gamma(\text{not } p)^{\text{naive}})$-valued measure on $M \otimes \hat{\mathbf{Z}}$, which is *supported* in the open set $(M \otimes \mathbf{Z}_p)^\times \times (M \otimes \hat{\mathbf{Z}}_{\text{not } p})$. By *evaluation* at $(M, \check{\varphi}, \alpha)$, we get a W-valued measure on $M \otimes \hat{\mathbf{Z}}$. This measure depends only on M (because $\check{\varphi}$ is determined by M (cf. 8.7.2), and α "occurs twice" in its definition). We denote it $\nu(M)$, and denote its Mellin transform $\mathfrak{L}_\nu(\chi, g)(M)$:

9.4.4 $$\mathfrak{L}_\nu(\chi, g)(M) = \int_{M \otimes \hat{\mathbf{Z}}} \chi(m)g(m)d\nu(M)$$

for $\begin{cases} \chi \in \mathrm{Hom}_{\mathrm{contin}}((M \otimes \mathbf{Z}_p)^\times, W^\times) \\ g \in \mathrm{Contin}\,(M \otimes \hat{\mathbf{Z}}_{\mathrm{not}\ p}, W) . \end{cases}$

9.4.5. *Formulas.* We suppose that the hypotheses 8.7.1–2–3 hold, and that the function g on $M \otimes \hat{\mathbf{Z}}_{\mathrm{not}\ p}$ is locally constant, has algebraic values, and transforms under the group $(\mathcal{O}_{K_0} \otimes \hat{\mathbf{Z}}_{\mathrm{not}\ p})^\times$ by a W-valued character ρ.

Let k, l be non-negative integers, and ε_1 and ε_2 W-valued characters of finite order of $\mathbf{Z}_p^\times$. When ε_1 is *non-trivial*, its exact conductor is denoted p^a. Then we have the following explicit formulas for the algebraic number

$$\frac{1}{c^{k+l+1}} \mathfrak{L}_\nu(\varepsilon_1 \varepsilon_2 \chi_{k,l}, g)(M) \overset{\mathrm{dfn}}{=} \frac{1}{c^{k+l+1}} \int_{M \otimes \hat{\mathbf{Z}}} \varepsilon_1(m)\varepsilon_2(\bar{m}) m^k \bar{m}^l g(m) d\nu(M) :$$

9.4.6. *Case* I: ε_1, ε_2 *both trivial:*

$$\frac{(-1)^{k+l+1} k!\pi^l}{a(M)^l \Omega^{k+l+1}} \left(1 - \frac{\lambda^k}{\bar{\lambda}^{l+1}\rho(\lambda)}\right)\left(1 - \frac{\lambda^l \rho(\bar{\lambda})}{\bar{\lambda}^{k+1}}\right)\left(\sum_{\substack{m \in M \\ m \neq 0}} \frac{g(m)\bar{m}^l}{m^{k+1} \mathbf{N}(m)^s}\right)_{|s=0} .$$

9.4.7. *Case* II: ε_1 *non-trivial, exact conductor* p^a; ε_2 *trivial*

$$\frac{g(\zeta_a, \varepsilon_1)(\lambda^a)^{k+l+1}}{p^{al}\varepsilon_1(\langle \lambda^a \rangle)\rho(\lambda^a)} \cdot \frac{(-1)^{k+l+1} k!\pi^l}{a(M)^l \Omega^{k+l+1}} \left(1 - \frac{\rho(\bar{\lambda})\lambda^l}{\varepsilon_1(\langle\lambda\rangle)\bar{\lambda}^{k+1}}\right)$$
$$\times \left(\sum_{\substack{m \in M \\ m \notin \lambda M}} \frac{g(m)\bar{m}^l}{\varepsilon_1(m) m^{k+1} \mathbf{N}(m)^s}\right)_{|s=0} .$$

9.4.8. *Case* III: ε_1 *trivial,* ε_2 *non-trivial:*

$$\frac{(-1)^{k+l+1} k!\pi^l}{a(M)^l \Omega^{k+l+1}} \left(1 - \frac{\lambda^k}{\bar{\lambda}^{l+1}\varepsilon_2(\langle\lambda\rangle)\rho(\lambda)}\right)\left(\sum_{\substack{m \in M \\ m \neq 0}} \frac{g(m)\varepsilon_2(\bar{m})\bar{m}^l}{m^{k+1} \mathbf{N}(m)^s}\right)_{|s=0} .$$

9.4.9. *Case* IV: ε_1, ε_2 *both non-trivial,* ε_1 *of exact conductor* p^a:

$$\frac{g(\zeta_a, \varepsilon_1)(\lambda^a)^{k+l+1}}{p^{al}\rho(\lambda^a)\varepsilon_1(\langle \lambda^a \rangle)\varepsilon_2(\langle \lambda^a \rangle)} \frac{(-1)^{k+l+1} k!\pi^l}{a(M)^l \Omega^{k+l+1}} \left(\sum_{\substack{m \in M \\ m \notin \lambda M}} \frac{g(m)\varepsilon_2(\bar{m})\bar{m}^l}{\varepsilon_1(m) m^{k+1} \mathbf{N}(m)^s}\right)_{|s=0} .$$

9.4.10. *Relation to "grossencharacters of type A_0."* Let K_0 be a quadratic imaginary field, given with a complex embedding $K_0 \hookrightarrow \mathbf{C}$. Given an ideal $\mathfrak{C} \subset \mathcal{O}_{K_0}$ and two integers (a, b), we have the notion of a grossencharacter χ of (not necessarily exact) conductor $\mathfrak{C}$, and type (a, b): this means that χ is a $\mathbf{C}$-valued multiplicative function on the group of functional ideals of K_0 which are prime to $\mathfrak{C}$, such that if $\alpha \in K_0$ is $\equiv 1 \bmod \mathfrak{C}$, then

$$\chi((\alpha)) = \alpha^a \bar{\alpha}^b .$$

We can define a function ψ_χ on the group $\{m \in K_0^\times \mid m \text{ is prime to } \mathfrak{C}\}$ by setting

$$\psi_\chi(m) = \chi((m))/m^a \bar{m}^b .$$

This is a multiplicative function, trivial on m's $\equiv 1 \bmod \mathfrak{C}$, hence ψ_χ is just a character of the finite group $(\mathcal{O}_{K_0}/\mathfrak{C})^\times$, which we extend by zero to all of $\mathcal{O}_{K_0}/\mathfrak{C}$.

The fact that $m^a\bar{m}^b\psi_\chi(m)$ is a multiplicative function of the *ideal* (m) shows that for any unit $e \in \mathcal{O}_{K_0}$, we have

$$e^a\bar{e}^b\psi_\chi(e) = 1\ .$$

Conversely, given a character ψ of $(\mathcal{O}_{K_0}/\mathfrak{C})^\times$ such that the above equality holds for all units e, then ψ is of the form ψ_χ for some χ of conductor $\mathfrak{C}$ and type (a, b) and this χ is unique up to multiplication by a character of the absolute ideal class group of K_0.

The Hecke L-series $L(s, \chi)$ attached to χ is defined to be the Dirichlet series

9.4.30
$$L(s, \chi) = \sum_{\substack{\mathfrak{A} \subset \mathcal{O}_{K_0} \\ \mathfrak{A} \text{ prime to } \mathfrak{C}}} \frac{\chi(\mathfrak{A})}{\mathrm{N}\mathfrak{A}^s} = \prod_{\mathfrak{p} \text{ prime to } \mathfrak{C}} \frac{1}{\left(1 - \dfrac{\chi(\mathfrak{p})}{\mathrm{N}\mathfrak{p}^s}\right)}\ .$$

Let $\mathfrak{A}_1, \cdots, \mathfrak{A}_h$ be a set of prime to $\mathfrak{C}$ representative ideals $\mathfrak{A}_i \subset \mathcal{O}_{K_0}$ for the *absolute* ideal class group of K_0. Then the $\mathfrak{A}_i^{-1}$ are also a set of representatives, and any integral ideal $\mathfrak{A} \subset \mathcal{O}_{K_0}$ can be written $\mathfrak{A} = (m_i)\mathfrak{A}_i^{-1}$ for some unique i and some element $m_i \in \mathfrak{A}_i$, determined uniquely up to a unit of $\mathcal{O}_{K_0}$. Then we can rewrite $L(s, \chi)$ as

9.4.31
$$L(s, \chi) = \frac{1}{\#\text{ units in } K_0} \sum_{i=1}^h \frac{\chi(\mathfrak{A}_i)^{-1}}{(\mathrm{N}\mathfrak{A}_i)^{-s}} \sum_{\substack{m \in \mathfrak{A}_i \\ m \neq 0}} \frac{m^a\bar{m}^b\psi_\chi(m)}{\mathrm{N}(m)^s}\ .$$

9.4.32. The value at $s = 0$ of each inner sum comes under our p-adic theory, provided that p splits in K_0. To fix ideas, suppose that the primes $\mathfrak{p}, \bar{\mathfrak{p}}$ lying over p are principal ideals. (This is not essential, but slightly simplifies the formulas.) We may always choose the representative ideals $\mathfrak{A}_i$ to be prime to p. To fix ideas, let us also suppose that p divides the (not necessarily exact) conductor $\mathfrak{C}$; at worst this amounts to discarding the $\mathfrak{p}$ and $\bar{\mathfrak{p}}$ Euler factors from $L(s, \chi)$. We can decompose the character $\psi_\chi(m)$ of $\mathcal{O}_{K_0}/(\mathfrak{C}\mathcal{O}_{K_0})^\times$ into a product of its $\mathfrak{p}$, $\bar{\mathfrak{p}}$, and prime-to-p component characters

9.4.33
$$\psi_\chi(m) = \varepsilon_1(m)\varepsilon_2(\bar{m})g_\chi(m)\ .$$

Then the inner sum becomes

$$\sum_{\substack{m \in \mathfrak{A}_i \\ m \neq 0}} \frac{m^a\bar{m}^b\varepsilon_1(m)\varepsilon_2(\bar{m})g_\chi(m)}{\mathrm{N}(m)^s}\ .$$

In the quadrant $b \geq 0$, $a \leq -1$, the value at $s = 0$ of this sum is p-adically interpolated by the p-adic L-function

$$\mathfrak{L}_\nu(\varepsilon_1^{-1}\varepsilon_2\chi_{-1-a,\, b},\ g_\chi)(\mathfrak{A}_i)$$

in the sense that the formulas 9.4.6–9 hold.

9.5. *Relation to the measure of Mazur-Swinnerton-Dyer and Manin* ([20], [21], [25]). The above named authors consider an elliptic curve E over $\mathbf{Q}$ which is "uniformized by $\Gamma_0(N)$" for a suitable integer N, outside of which N the curve has good reduction. For each prime p not dividing N at which the curve has *ordinary* reduction and each integer f_0 prime to Np, they construct a p-adic measure on the multiplicative group $\mathbf{Z}_p^\times \times (\mathbf{Z}/f_0\mathbf{Z})^\times$.

9.5.1. To relate their theory to ours, we must at present limit the discussion to elliptic curves E over $\mathbf{Q}$ with complex multiplication, and it seems plausible that this is the only case where there is a simple relation. To further simplify, we will suppose that $\mathrm{End}(E_{\mathbf{C}})$ is the *full* ring of integers $\mathcal{O}_{K_0}$ in the quadratic imaginary multiplication field K_0. The fact that E is defined over $\mathbf{Q}$ implies that K_0 has class number one (since its Hilbert class field is $K_0(j(E))$). Such a curve is well-known to be uniformized by $\Gamma_0(N)$ for some N (cf. [33]), so that the Manin-Mazur-Swinnerton-Dyer theory applies. We will briefly explain their construction in this particular case.

For each prime number l which is *unramified* in K_0, and at which E has good reduction, we consider the *numerator* of the zeta function of $E \otimes \mathbf{F}_l$, as a polynomial in the quantity l^{-s}.

9.5.2
$$P_l(l^{-s}) = 1 - a(l)l^{-s} + l^{1-2s}$$
where $\quad a(l) = 1 + l - \#E(\mathbf{F}_l) = \text{trace of Frobenius on } E \otimes \mathbf{F}_l\,.$

The Dirichlet series

9.5.3
$$L(E/\mathbf{Q}, s) = \prod_{\substack{l \text{ unram. in } K_0 \\ E \text{ good red. at } l}} \frac{1}{P_l(l^{-s})} \overset{\text{dfn}}{=} \sum a(n)n^{-s}$$

is called the L-series of $E/\mathbf{Q}$. It is defined for *any* curve over $\mathbf{Q}$. Because we are in the situation of complex multiplication, the L-series $L(E/\mathbf{Q}, s)$ can be rewritten as an "L-series with grossencharacter" of the field K_0 as follows.

9.5.4. For each prime ideal q of $\mathcal{O}_{K_0}$ which lies over some prime l of the above type, we can define a canonical generator $\chi(q) \in \mathcal{O}_{K_0}$ by the following device:

9.5.5. If $q = (l)$ is a rational prime which stays prime in K_0, then its residue field is $\mathbf{F}_{l^2}$, and the Frobenius endomorphism of $E \otimes \mathbf{F}_{l^2}$ is the scalar $-l$ (i.e., $a(l) = 0$ if l stays prime in K_0). We take $\chi(q) = -l$ if $q = (l)$.

9.5.6. If q has residue field $\mathbf{F}_l$, then the polynomial $X^2 - a(l)X + l$ factors in $\mathcal{O}_{K_0}$, and exactly one of its roots generates q; the other root generates $\bar{q}$. We define $\chi(q) \in \mathcal{O}_{K_0}$ to be that zero of $X^2 - a(l)X + l$ which generates q. Thus $\chi(\bar{q}) = \overline{\chi(q)}$, and $X^2 - a(l)X + l = (X - \chi(q))(X - \chi(\bar{q}))$.

(Thus $\chi(\mathfrak{p}) = \lambda$ in the notation of 8.8.)

Thus in either case we have

9.5.7 $$P_l(l^{-s}) = \prod_{q|l}(1 - \chi(q)\mathrm{N}(q)^{-s}) .$$

so that we can rewrite

9.5.8 $$L(E/\mathbf{Q}, s) = \prod_q \left(\frac{1}{1 - \chi(q)\mathrm{N}q^{-s}}\right) .$$

It is a fundamental theorem of Deuring that the assignment

9.5.9 $$q \longmapsto \chi(q)$$

is a K_0-valued *grossencharacter* of K_0. Concretely, this means that there exists an integer N, divisible precisely by those primes which either ramify in K_0 or at which E has bad reduction, such that when we extend χ by multiplicativity to *all* fractional ideals of K_0 prime to N, then

9.5.10 $$\chi((\alpha)) = \alpha \quad \text{if } \alpha \in K_0, \text{ and } \alpha \equiv 1 \bmod N .$$

Equivalently, this means that there is a K_0-valued Dirichlet character of $\mathcal{O}_{K_0}$ mod N,

9.5.11 $$\psi_\chi\colon (\mathcal{O}_{K_0}/N\mathcal{O}_{K_0})^\times \longrightarrow (\mathcal{O}_{K_0})^\times ,$$

such that

9.5.12 $$\chi((\beta)) = \beta\psi_\chi(\beta) \quad \text{if } \beta \in \mathcal{O}_{K_0} \text{ is prime to } N .$$

Caution. This N is not the N figuring in $\Gamma_0(N)$, but it has the same prime factors. According to [33], if we denote by $\mathfrak{A}$ the ideal of $\mathcal{O}_{K_0}$ which is the *exact* conductor of χ, and by $-D$ the discriminant of K_0, then our curve is uniformized by $\Gamma_0(D\mathrm{N}(\mathfrak{A}))$.

Thus we can rewrite the L-series $L(E/\mathbf{Q}, s)$ in the form

9.5.13 $$L(E/\mathbf{Q}, s) = \frac{1}{\#\text{ units in } \mathcal{O}_{K_0}} \sum_{\substack{m \in \mathcal{O}_{K_0} \\ m \text{ prime to } N}} m\psi_\chi(m)\mathrm{N}(m)^{-s} = \sum a(n)n^{-s}$$

(replacing m by $\bar{m}$, and using $\psi_\chi(\bar{m}) = \overline{\psi_\chi(m)}$)

$$= \frac{1}{\#\text{ units in } \mathcal{O}_{K_0}} \sum_{\substack{m \in \mathcal{O}_{K_0} \\ m \text{ prime to } N}} \bar{m}\bar{\psi}_\chi(m)\mathrm{N}(m)^{-s} .$$

Now let $\rho\colon (\mathbf{Z}/f\mathbf{Z})^\times \rightarrow \mathbf{C}^\times$ be an ordinary Dirichlet character, of exact conductor f prime to N. Then one defines the ρ-twist of $L(E/\mathbf{Q}, s)$, noted $L(E/\mathbf{Q}, \rho, s)$, to be the Dirichlet series

9.5.14 $$\begin{aligned} L(E/\mathbf{Q}, \rho, s) &\overset{\text{dfn}}{=} \sum \rho(n)a(n)n^{-s} \\ &= \frac{1}{\#\text{ units in } \mathcal{O}_{K_0}} \sum_{\substack{m \in \mathcal{O}_{K_0} \\ m \text{ prime to } N}} m\psi_\chi(m)\rho(\mathrm{N}m)\mathrm{N}m^{-s} \\ &= \prod_q \left(\frac{1}{1 - \chi(q)\rho(\mathrm{N}q)\mathrm{N}q^{-s}}\right) . \end{aligned}$$

Let us denote by ω a chosen Neron differential on $E/\mathbf{Q}$ (unique up to ± 1), and by $\Omega \in \mathbf{C}$ the constant (unique up to a unit of $\mathcal{O}_{K_0}$) such that $\Omega\mathcal{O}_{K_0}$ is the period lattice of $(E, \omega)_{\mathbf{C}}$. By Damerell's theorem, the ratio

9.5.15
$$\frac{L(E/\mathbf{Q}, \rho, s)_{|s=1}}{\Omega}$$

is algebraic.

In terms of this, we can describe the Mazur-Swinnerton-Dyer and Manin measure MMSW as follows. Fix an integer f_0 prime to Np, and let $\rho_0\colon (\mathbf{Z}/f_0\mathbf{Z})^\times \to W^\times$ be a character of *exact* conductor f_0. Let $\varepsilon\colon \mathbf{Z}_p^\times \to W^\times$ be a character of finite order, of exact conductor p^a. Then the measure MMSW_{f_0} on $\mathbf{Z}_p^\times \times (\mathbf{Z}/f_0\mathbf{Z})^\times$ satisfies (cf. [23] and [25])

9.5.16
$$\int_{\mathbf{Z}_p^\times \times (\mathbf{Z}/f_0\mathbf{Z})^\times} \varepsilon(x)\rho_0(u)d\mathrm{MMSW}_{f_0} = \frac{\left(\sum_{b \bmod f_0p^a}(\varepsilon\rho_0)^{-1}(b)e^{2\pi i b/p^a f_0}\right)}{\bar{\lambda}^a}\,\frac{L(E/\mathbf{Q}, \varepsilon\rho_0, s)_{|s=1}}{\Omega}\,.$$

If we write out the series for $L(E/\mathbf{Q}, \varepsilon\rho_0, s)$, but sum over $\bar{m}$, we get

9.5.17
$$L(E/\mathbf{Q}, \varepsilon\rho_0, s) = \sum_{\substack{m \in \mathcal{O}_{K_0} \\ m \text{ prime to } Np}} \bar{m}\bar{\psi}_\chi(m)\varepsilon(m)\varepsilon(\bar{m})\rho_0(\mathrm{N}(m))\mathrm{N}(m)^{-s}$$

whence

9.5.18
$$L(E/\mathbf{Q}, \varepsilon\rho_0, s)_{|s=0} = \left(\sum_{\substack{m \in \mathcal{O}_{K_0} \\ m \text{ prime to } Np}} \frac{\varepsilon(\bar{m})\bar{\psi}_\chi(m)\,\rho_0(\mathrm{N}(m))}{\varepsilon^{-1}(m)m\mathrm{N}(m)^s}\right)_{|s=0}.$$

Comparing this with 9.4.9, we see that the above value is one of our $\mathfrak{L}$-values, with $k = l = 0$, and $\varepsilon_1 = \varepsilon^{-1}$, $\varepsilon_2 = \varepsilon$. Explicitly we have

9.5.19
$$\frac{1}{c}\int_{M\otimes\hat{\mathbf{Z}}} \varepsilon^{-1}(m)\varepsilon(\bar{m})\bar{\psi}_\chi(m)\rho_0(\mathrm{N}(m))d\nu(M) = \frac{p^a g(\zeta_a, \varepsilon^{-1})}{\bar{\lambda}^a\rho_0(p^a)}\cdot\left(\frac{-1}{\Omega}L(E/\mathbf{Q}, \varepsilon\rho_0, s)\right)_{|s=1}.$$

(In transcribing 9.4.9, the apparent denominator is

$$\bar{\lambda}^a\rho_0(\mathrm{N}(\lambda^a))\bar{\psi}_\chi(\lambda^a)\varepsilon_1(\langle\lambda^a\rangle)\varepsilon_2(\langle\lambda^a\rangle)\,.$$

But $\varepsilon_1 = \varepsilon_2^{-1}$, so the ε's go out, and $\psi_\chi(\lambda) = \chi(\mathfrak{p})/\lambda = 1$, so the $\bar{\psi}_\chi$ goes out.)

We can transform the Gauss sum occurring in 9.5.16 by writing $b = -f_0b_1 - p^ab_2$. The result is easily seen to be

9.5.20
$$\sum_{b \bmod f_0p^a}(\varepsilon\rho_0)^{-1}(b)e^{2\pi i b/f_0p^a} = \frac{1}{\varepsilon(-f_0)\rho_0(-p^a)}\left(\sum_{b_1 \bmod p^a}\varepsilon^{-1}(b_1)e^{-2\pi i b_1/p^a}\right) \times \left(\sum_{b_2 \bmod f_0}\rho_0^{-1}(b_2)e^{-2\pi i b_2/f_0}\right).$$

To compare the first factor in this decomposition to $p^a g(\zeta_a, \varepsilon^{-1})$, we introduce the p-adic unit $A \in \mathbf{Z}_p^\times$ which relates the two bases $(\cdots, e^{2\pi i/p^a}, \cdots)$ and $(\cdots, \zeta_a, \cdots)$ to $T_p(\mathbf{G}_m)$ (cf. 8.7.2), i.e.,

9.5.21 $$\zeta_a = e^{2\pi i(A \bmod p^a)/p^a} \qquad \text{for } a = 1, 2, \cdots.$$

An easy computation gives

9.5.22 $$\textstyle\sum_{b \text{ mob } p^a} \varepsilon^{-1}(b) e^{-2\pi i b/p^a} = \varepsilon^{-1}(A) p^a g(\zeta_a, \varepsilon^{-1}) .$$

Putting it all together, we find

9.5.23 $$\left(\frac{-1}{f_0}\textstyle\sum_{b \bmod f_0} \rho_0(b) e^{2\pi i b/f_0}\right)\displaystyle\int_{\mathbf{Z}_p^\times \times (\mathbf{Z}/f_0\mathbf{Z})^\times} \varepsilon(-Af_0x)\rho_0(-u)d\,\mathrm{MMSW}_{f_0}$$
$$= \frac{1}{c}\int_{M \otimes \hat{\mathbf{Z}}} \varepsilon^{-1}(m)\varepsilon(\bar{m})\bar{\psi}_\chi(m)\rho_0(\mathrm{N}(m))d\nu(M) .$$

9.5.24. Let us denote by $m \to \bar{m}/m$ the continuous mapping $(M \otimes \mathbf{Z}_p)^\times \to \mathbf{Z}_p^\times \simeq M_\mathfrak{p}^\times$ which sends $m \in M$ to $\bar{m}/m$. In terms of the isomorphism $(M \otimes \mathbf{Z}_p)^\times \simeq M_\mathfrak{p}^\times \times M_{\bar{\mathfrak{p}}}^\times \simeq \mathbf{Z}_p^\times \times \mathbf{Z}_p^\times$, it is $(x, y) \to y/x$.

COMPARISON THEOREM 9.5.25. *Let f be a continuous W-valued function on $\mathbf{Z}_p^\times$, and let $\rho_0\colon (\mathbf{Z}/f_0\mathbf{Z})^\times \to W^\times$ be a primitive character modulo f_0, with f_0 prime to pN. Then we have the integration formula*

9.5.26 $$\left(\frac{-1}{f_0}\textstyle\sum_{b \bmod f_0} \rho_0(b) e^{2\pi i b/f_0}\right)\displaystyle\int_{\mathbf{Z}_p^\times \times (\mathbf{Z}/f_0\mathbf{Z})^\times} f(-Af_0x)\rho_0(-u)d\,\mathrm{MMSW}_{f_0}$$
$$\frac{1}{c}\int_{M \otimes \hat{\mathbf{Z}}} f(\bar{m}/m)\bar{\psi}_\chi(m)\rho_0(\mathrm{N}(m))d\nu(M) .$$

Proof. For $f = \varepsilon$ a character of finite order, this is just 9.5.23. Any locally constant W-valued function in $\mathbf{Z}_p^x$ is a $W \otimes \mathbf{Q}_p$-linear combination of ε's of finite order, so the theorem holds for f locally constant, and locally constant functions are uniformly dense in $\mathrm{Contin}(\mathbf{Z}_p^\times, W)$. Q.E.D.

9.5.27. *Remark.* The p-adic unit $A \in \mathbf{Z}_p^\times$ is given explicitly in terms of the unit root $\langle\lambda\rangle$ and the *area* $a(\mathcal{O}_{K_0})$ by the formula $\langle\lambda\rangle^2 A = \mathrm{Im}(\lambda^2)/a(\mathcal{O}_{K_0})$, as follows immediately from computing $e_{p^n}(\bar{\lambda}/p^n, \lambda/p^n)$ using 2.0.2.

Chapter X. The p-adic analogue of Kronecker's second limit formula

10.0. *The Siegel functions $H_{\zeta,s}$ and H_ζ as "true" modular functions.* Fix an integer $N \geqq 2$. Given a ring B, an N^{th} root of unity $\zeta \in \mu N(B)$, and an integer $s \geqq 0$, we form the infinite product

10.0.1 $$H_{\zeta,s}(q) \overset{\text{dfn}}{=} q^{N^2 - 6sN + 6s^2}\zeta^{6s}\left[(1 - q^s\zeta)\textstyle\prod_{n \geq 1}(1 - q^{Nn+s}\zeta)(1 - q^{Nn-s}\zeta^{-1})\right]^{12N} .$$

This product depends only on s modulo N. For $s = 0$ and $\zeta = 1$, the product is zero. In terms of these products, we define

10.0.2
$$H_\zeta(q) = \prod_{s=0}^{N-1} H_{\zeta,s}(q) ;$$

an easy calculation then gives the formula

10.0.3
$$H_\zeta(q) = q^N[(1-\zeta)\prod_{n\geq 1}(1-q^n\zeta)(1-q^n\zeta^{-1})]^{12N} .$$

LEMMA 10.0.4. *The products $H_{\zeta,s}(q)$ (resp. $H_\zeta(q)$) are the q-expansions of elements of $R^0(B, \Gamma(N)^{\text{arith}})$ (resp. $\Gamma_{00}(N)^{\text{arith}}$). If $s \neq 0 \bmod N$, then $H_{\zeta,s}$ is a unit in $R^0(B, \Gamma(N)^{\text{arith}})$. If $1-\zeta$ is a unit in B, then $H_{\zeta,0}$ (resp. H_ζ) is a unit in $R^0(B, \Gamma(N)^{\text{arith}})$ (resp. $\Gamma_{00}(N)^{\text{arith}}$).*

Proof. This is proved when $B = \mathbf{C}$ in Lang ([18], p. 262). It follows over any sub-ring of $\mathbf{C}$ by the q-expansion principle, then over any B by "reduction to the universal case."

COROLLARY 10.0.5. *If B is an integral domain, and $\zeta, \zeta' \in \mu_N(B)$ are both $\neq 1$, and if $1-\zeta/1-\zeta'$ lies in B and is a unit in B, then $H_{\zeta,0}/H_{\zeta',0}$ (resp. $H_\zeta/H_{\zeta'}$) is a unit in $R^0(B, \Gamma(N)^{\text{arith}})$ (resp. $\Gamma_{00}(N)^{\text{arith}}$).*

Proof. This follows from 10.0.4 and the q-expansion principle 2.2.8, applied to $B \subset B[1/(1-\zeta)]$.

LEMMA 10.0.6 (*Transformation*). *Under the action* (5.4.8) *of the group $(\mathbf{Z}/N\mathbf{Z})^\times$ on $R^0(B, \Gamma(N)^{\text{arith}})$ and on $R^0(B, \Gamma_{00}(N)^{\text{arith}})$, the elements $H_{\zeta,s}$, H_ζ transform by*

10.0.7
$$\begin{cases} [b]H_{\zeta,s} = H_{\zeta^b, s/b} \\ [b]H_\zeta \;\; = H_{\zeta^b} . \end{cases}$$

Proof. If we use 10.0.2, the second formula is a consequence of the first. By the standard reductions, it suffices to prove the first over $\mathbf{C}$. But given a $\Gamma(N)^{\text{arith}}$-curve (E, β) over $\mathbf{C}$, the transcendental description of $H_{\zeta,s}(E, \beta)$ shows that it depends only on the division point $\beta(\zeta, s)$. This makes the assertion obvious from the definition of $[b]$. Q.E.D.

10.1. *Logarithms of ratios of Siegel functions as p-adic modular functions.* Fix a complete p-adic mixed characteristic valuation ring W as in 7.1, and denote by $\mathfrak{p}$ its maximal ideal. For any W-flat p-adic W-algebra B, the logarithm

10.1.1
$$\log(1+x) = \sum_{n\geq 1} \frac{(-1)^{n+1}x^n}{n}$$

defines a group homomorphism from the multiplicative group $1 + \mathfrak{p}B$ to the additive group $B \otimes \mathbf{Q}$. It extends uniquely to the multiplicative group $\{\varphi \in B | \exists n \geq 1 \text{ with } \varphi^n \in 1 + \mathfrak{p}B\}$, by defining

10.1.2 $$\log(\varphi) = \frac{1}{n}\log(\varphi^n) \in B \otimes \mathbf{Q} \quad \text{if } \varphi^n \in 1 + \mathfrak{p}B\,.$$

Given any homomorphism $\sigma: B \to B'$ of such rings, we have

10.1.3 $$\log(\sigma(\varphi)) = \sigma(\log \varphi) \quad \text{for any } \varphi \text{ as in 10.1.2.}$$

Now we will consider $R^0(W, \Gamma(N)^{\text{arith}})$ as a subring of $GV^0(W, \Gamma(N)^{\text{arith}})$ (cf. 5.9, 5.10) and similarly for their $\Gamma_{00}(N)^{\text{arith}}$ analogues. Recall that by the q-expansion principle (5.2.1), any element of $GV^0(W, \Gamma(N)^{\text{arith}})$ whose q-expansion lies in $1 + \mathfrak{p}W((q))$ itself lies in $1 + \mathfrak{p}GV^0(W, \Gamma(N)^{\text{arith}})$, and similarly for $\Gamma_{00}(N)^{\text{arith}}$. Looking at q-expansions, we get the next lemma.

LEMMA 10.1.4. *If* $\zeta, \zeta' \in \boldsymbol{\mu}_N(W)$, $\zeta \equiv \zeta' \bmod \mathfrak{p}$ *and* $s \not\equiv 0 \bmod N$, *then* $H_{\zeta,s}/H_{\zeta',s}$ *lies in* $1 + \mathfrak{p}\, GV^0(W, \Gamma(N)^{\text{arith}})$.

10.1.5. *If* $\zeta, \zeta' \in \boldsymbol{\mu}_N(W)$, $\zeta \neq 1$, $\zeta' \neq 1$, $\zeta \equiv \zeta' \bmod \mathfrak{p}$, *and if* $(1-\zeta)/(1-\zeta')$ *lies in* $W^\times$, *then a power of* $H_{\zeta,0}/H_{\zeta',0}$ *lies in* $1 + \mathfrak{p}\, GV^0(W, \Gamma(N)^{\text{arith}})$, *and a power of* $H_\zeta/H_{\zeta'}$ *lies in* $1 + \mathfrak{p}\, GV^0(W, \Gamma_{00}(N)^{\text{arith}})$.

10.1.6. *If* $s \not\equiv 0 \bmod N$, *then for any* $\zeta \in \boldsymbol{\mu}_N(W)$, $(H_{\zeta,s})^p/\mathrm{Frob}(H_{\zeta^p,s})$ *lies in* $1 + \mathfrak{p}\, GV^0(W, \Gamma(N)^{\text{arith}})$.

10.1.7. *If* $\zeta \in \boldsymbol{\mu}_N(W)$, $\zeta^p \neq 1$, *then* $(H_{\zeta,0})^p/\mathrm{Frob}(H^p_{\zeta,0})$ *lies in* $1 + \mathfrak{p}GV^0(W, \Gamma(N)^{\text{arith}})$, *and* $(H_\zeta)^p/\mathrm{Frob}(H_{\zeta^p})$ *lies in* $1 + \mathfrak{p}GV^0(W, \Gamma_{00}(N)^{\text{arith}})$.

The power is needed in 10.1.5 when ζ and ζ' are non-trivial p-power roots of unity of exactly the same order. Then $(1-\zeta)/(1-\zeta')$ is a unit in W, but modulo $\mathfrak{p}W$ it may be any element of $\mathbf{F}_p$. So in fact the $p - 1^{\text{st}}$ power will do.

10.2. *Application to the "one-variable" L-function* $\mathbf{L}$ (cf. 7.2), *and Leopoldt's formula* (cf. [12]). Let $\rho: (\mathbf{Z}/N\mathbf{Z})^\times \to W^\times$ be a character of exact conductor N. Then $\mathbf{L}(\rho)$ lies in $GV^0(W, \Gamma_{00}(N)^{\text{arith}}) \otimes \mathbf{Q}$, and it has nebentypus ρ (5.3.4). If ρ is an *odd* character $(\rho(-x) = -\rho(x))$, then $\mathbf{L}(\rho) = 0$, simply because $(-1, -1) \in G(N)$ acts *trivially* on GV^0. We henceforth assume that ρ is *even*. By 7.2.3, the *q-expansion of* $\mathbf{L}(\rho)$ is given in terms of an auxiliary element $(a, b) \in G(N)$ by the formula

10.2.1 $$\mathbf{L}(\rho) = \left(\frac{1}{1-\rho(b)}\right)\int_{\mathbf{Z}_p^\times \times \mathbf{Z}/N\mathbf{Z}} \frac{1}{x}\rho(u)\,d\mu^{(a,b)}_{K.\text{-}L.} + 2\sum\nolimits_{n \geq 1} q^n \sum\nolimits_{\substack{d \mid n \\ (p,d)=1}} \frac{\rho(d)}{d}\,.$$

Recall that for $k \geqq 0$, we have the formula (6.2.8)

10.2.2 $$\left(\frac{1}{1-a^{k+1}\rho(b)}\right)\int_{\mathbf{Z}_p^\times \times \mathbf{Z}/N\mathbf{Z}} x^k\rho(u)\,d\mu^{(a,b)}_{K.\text{-}L.} = (1-\rho(p)p^k)L(-k, \rho)$$

where $L(-k, \rho)$ is the value at $-k$ of the classical Dirichlet L-function.

We will give a "modular" formula for $\mathbf{L}(\rho)$ in terms of logarithms of ratios of Siegel functions. Comparing constant terms in the q-expansions will give Leopoldt's formula for "p-adic $L(1, \rho)$."

Recall that for a function f on $\mathbf{Z}/N\mathbf{Z}$, its Fourier transform $\hat{f}$ is the function on μ_N defined by

10.2.3
$$\hat{f}(\zeta) = \frac{1}{N}\sum_{a \bmod N} f(a)\zeta^{-a} .$$

The original f may be recovered from $\hat{f}$ by the formula

10.2.4
$$f(b) = \sum_{\zeta \in \mu_N} \hat{f}(\zeta)\zeta^{b} .$$

When f is a character $\rho\colon (\mathbf{Z}/N\mathbf{Z})^\times \to W$ of exact conductor N, then $\hat{\rho}$ is supported in $\mu_N^\times$, the set of primitive Nth roots of unity. If we choose a primitive $\zeta = \zeta_N$, then

10.2.5
$$\hat{\rho}(\zeta^a) = \begin{cases} \rho^{-1}(a)\hat{\rho}(\zeta) & \text{for } a \in (\mathbf{Z}/N\mathbf{Z})^\times \\ 0 & \text{if } (a, N) > 1 . \end{cases}$$

THEOREM 10.2.6. *Suppose that $N \geqq 2$ is prime to p, and $\rho\colon (\mathbf{Z}/N\mathbf{Z})^\times \to W$ is an even character of exact conductor N. Suppose that W contains the* Nth *roots of unity. Then* $\mathrm{L}(\rho)$ *is given by the formula*

10.2.7
$$\mathrm{L}(\rho) = \frac{-1}{12Np}\sum_{\zeta \in \mu_N(W)} \hat{\rho}(\zeta)\log\left((H_\zeta)^p/\mathrm{Frob}\,(H_{\zeta^p})\right) .$$

If we choose a primitive Nth *root of unity ζ, we can rewrite this*

10.2.8
$$\mathrm{L}(\rho) = \left(\frac{-1}{12pN}\sum_{a \bmod N} \rho(a)\zeta^{-a}\right) \times \sum_{\substack{a \bmod N \\ (a,N)=1}} \rho^{-1}(a)\log\left((H_{\zeta^a})^p/\mathrm{Frob}\,(H_{\zeta^{ap}})\right) .$$

Proof. The two assertions are obviously equivalent, in view of 10.2.5. Notice that *both* sides of the asserted equality are of weight zero and nebentypus ρ, thanks to 10.0.7. Since a non-zero *constant* cannot be of nebentypus ρ, (ρ being non-trivial), it suffices to show that the difference of their q-expansions is a constant. This results immediately from the explicit formulas 10.2.1 (for $\mathrm{L}(\rho)$), 10.0.3 (for H_ζ) and 5.5.7 (for Frob). The actual calculation is left to the reader. Q.E.D.

Comparing constant terms gives Leopoldt's formula (cf. [12]):

COROLLARY 10.2.9 (*Leopoldt*). *With hypotheses as in* 10.2.6, *we have the formula*

10.2.10
$$\frac{1}{1-\rho(b)}\int_{\mathbf{Z}_p^\times \times \mathbf{Z}/N\mathbf{Z}} \frac{1}{x}\,\rho(u)\,d\mu^{(a,b)}_{K.-L.} = -\frac{1}{p}\sum_{\substack{\zeta \in \mu_N(W) \\ \zeta \text{ primitive}}} \hat{\rho}(\zeta)\log\left(\frac{(1-\zeta)^p}{1-\zeta^p}\right)$$
$$= -\left(1 - \frac{\rho(p)}{p}\right)\sum_{\substack{\zeta \in \mu_N(W) \\ \zeta \text{ primitive}}} \hat{\rho}(\zeta)\log(1-\zeta) .$$

(*To get the second expression, notice that for* $\zeta \in \mu_N(W)$ *not of p-power order,* $1-\zeta$ *lies in* $W^\times$ *and a power of it lies in* $1+\mathfrak{p}W$. *Thus* $\log(1-\zeta)$ *is defined, and* $\log\left((1-\zeta)^p/1-\zeta^p\right) = p\log(1-\zeta) - \log(1-\zeta^p)$.)

10.2.11. We now turn to the case where p divides N. We write $N = N_0 p^r$, and we *choose* a primitive p^rth root of unity ζ_1. For each *primitive* Nth root of unity ζ, we denote by ζ' the primitive Nth root of unity which satisfies $(\zeta')^{p^r} = \zeta^{p^r}$, $(\zeta')^{N_0} = (\zeta_1)^{N_0}$. Then $1-\zeta/1-\zeta'$ is a unit in W, and $\zeta \equiv \zeta' \bmod \mathfrak{p}$.

THEOREM 10.2.12. *Suppose that p divides N, and that* $\rho\colon (\mathbf{Z}/N\mathbf{Z})^\times \to W$ *is an even character of exact conductor N. When W contains the* Nth *roots of unity,* $\mathrm{L}(\rho)$ *is given by the formula*

10.2.13
$$\mathrm{L}(\rho) = \frac{-1}{12N}\sum_{\substack{\zeta\in\mu_N(W)\\ \zeta \text{ primitive}}} \hat{\rho}(\zeta)\log(H_\zeta/H_{\zeta'})\ .$$

If we choose a primitive Nth *root of unity* $\zeta^{N_0} = \zeta_1^{N_0}$, *then we can rewrite this as*

10.2.14
$$\mathrm{L}(\rho) = \frac{-1}{12N^2}\Big(\sum_{a \bmod N}\rho(a)\zeta^{-a}\Big)\sum_{a\in(\mathbf{Z}/N\mathbf{Z})^\times}\rho^{-1}(a)\log(H_{\zeta^a}/H_{\zeta^{a'}})\ ,$$

where $a' \equiv a \bmod N_0$, $a' \equiv 1 \bmod p^r$.

Proof. The proof is identical to that of 10.2.6: the hypothesis that ρ has exact conductor N assures that for each fixed $a' \in (\mathbf{Z}/N\mathbf{Z})^\times$, $a' \equiv 1\ (p^r)$, the sum $\sum \rho^{-1}(a)$ (extended to all $a \in (\mathbf{Z}/N\mathbf{Z})^\times$ with $a \equiv a' \bmod N_0$) *vanishes*, so that the right-hand side is independent of the initial choice of ζ_1 used to define $\zeta \mapsto \zeta'$. This means that *formally* (but in no other sense), we have

10.2.15 (formal)
$$\mathrm{L}(\rho) = \frac{-1}{12N}\sum_{\substack{\zeta\in\mu_N(W)\\ \zeta \text{ primitive}}} \hat{\rho}(\zeta)\log H_\zeta\ . \qquad \text{Q.E.D.}$$

10.2.16. To exploit the above formal formula, we resort to Iwasawa's "$\log_p$" artifice. Given a complete valued overfield K of $\mathbf{Q}_p$ with value group contained in $\mathbf{Q}$ and residue field *algebraic* over $\mathbf{F}_p$, there is a unique group homomorphism

10.2.17
$$\log_p\colon K^\times \longrightarrow K^+$$

satisfying

$$\begin{cases}\log_p(p) = 0\\ \log_p(1+x) = \log(1+x) \quad \text{if } \operatorname{ord}(x) > 0\ .\end{cases}$$

With this function, we can nicely write the constant terms.

COROLLARY 10.2.18 (Leopoldt). *With hypotheses as in* 10.2.12, *we have the formula*

10.2.19 $$\frac{1}{1-\rho(b)}\int_{\mathbf{Z}_p^\times \times \mathbf{Z}/N\mathbf{Z}} \frac{1}{x}\rho(u)d\mu_{K.-L.}^{(a,b)} = -\sum_{\substack{\zeta\in\mu_N(W)\\ \zeta \text{ primitive}}} \hat{\rho}(\zeta)\log_p(1-\zeta) .$$

Notice that this formula is formally identical to 10.2.10, because by convention $\rho(p) = 0$ when p divides N.

10.3. *Applications to the two variable L-functions $\mathfrak{L}$ and $\mathfrak{L}_\nu$.* Fix an integer $N \geqq 2$. In view of the explicit formulas of Chapters 8 and 9 in the complex multiplication case, the p-adic analogue of an abelian L-series of a quadratic imaginary field at $s = 1$ is an integral

10.3.1 $$\mathfrak{L}\left(\frac{1}{y}, f\right) = \int \frac{1}{y} f(u, v)d\mu_N ,$$

while the analogue of "$s = 0$" is an integral

10.3.2 $$\mathfrak{L}\left(\frac{1}{x}, f\right) = \int \frac{1}{x} f(u, v)d\mu_N .$$

In the p-adic setting these integrals are related by the functional equation (7.3.2):

10.3.3 $$\int \frac{1}{x} f(u, v)\, d\mu_N = \int \frac{1}{y} f^t(u, v)d\mu_N\colon f^t(u, v) = f(v, u),$$

which should be interpreted as the p-adic analogue of the classical $s \to 1 - s$ functional equation.

In the following, we will consider only the *second* integral

10.3.4 $$\mathfrak{L}\left(\frac{1}{x}, f\right) = \int \frac{1}{x} f(u, v)d\mu_N .$$

Its q-expansion is given explicitly by (cf. 7.3.5)

10.3.5 $$\mathfrak{L}\left(\frac{1}{x}, f\right)\sum_{(p,n)=1} q^n \sum_{n=dd'} \frac{f(d, d') + f(-d, -d')}{d} ,$$

so we will henceforth suppose f *even*. To *further* simplify, we will suppose that

10.3.6 $$\begin{cases} p \mid N \\ f(pu, v) = f(u, pv) = 0 \quad \text{for all } u, v \in \mathbf{Z}/N\mathbf{Z} . \end{cases}$$

We write $N = N_0 p^r$ with $(p, N_0) = 1$.

The inverse partial Fourier transform $P^{-1}f$ on $\mu_N \times \mathbf{Z}/N\mathbf{Z}$ will then satisfy

10.3.7 $$\begin{cases} P^{-1}f(\zeta, 0) = 0 & \text{because } f(n, 0) = 0 \text{ for all } n \\ \sum_{\zeta\in\mu_{p^r}} P^{-1}f(\zeta\zeta_0, s) = 0 & \text{because } f(p^r, s) = 0 . \end{cases}$$

10.3.8. Let W be a complete mixed characteristic p-adic valuation ring containing the N^{th} roots of unity. For any $\zeta \in \mu_N(W)$, let $\mathrm{Teich}(\zeta) \in \mu_N(W)$ be the unique root of unity of order prime to p with $\zeta \equiv \mathrm{Teich}(\zeta) \bmod \mathfrak{p}$ (so $\zeta = \zeta_1 \cdot \mathrm{Teich}(\zeta)$, for some p-power root of unity ζ_1).

THEOREM 10.3.8. *With hypotheses as above* (10.3.6), *we have an identity in* $GV^0(W, \Gamma(N)^{\text{arith}}) \otimes \mathbf{Q}$:

10.3.9 $$\mathcal{L}\left(\frac{1}{x}, f\right) = \frac{-1}{12N} \sum_{\substack{(\zeta, s) \in \mu_N(W) \times \mathbf{Z}/N\mathbf{Z} \\ s \neq 0}} (P^{-1}f)(\zeta, s) \log\left(H_{\zeta,s}/H_{\mathrm{Teich}(\zeta),s}\right) .$$

Proof. Both sides have the same q-expansion! Q.E.D.

In view of 10.3.7, we can *formally* rewrite this as

10.3.10 (formal) $$\mathcal{L}\left(\frac{1}{x}, f\right) = \frac{-1}{12N} \sum_{(\zeta, s) \in \mu_N(W) \times \mathbf{Z}/N\mathbf{Z}} P^{-1}f(\zeta, s) \log\left(H_{\zeta,s}\right) .$$

Suppose now that we have $N = N_0 p^r$, and are given

10.3.10 $$\begin{cases} \varepsilon\colon \mathbf{Z}_p^\times \times \mathbf{Z}_p^\times \longrightarrow W^\times, & \text{a } \textit{character} \bmod p^r \\ f_0\colon (\mathbf{Z}/N_0\mathbf{Z})^2 \longrightarrow W & \text{an arbitrary function .} \end{cases}$$

Then we can look at the integral

10.3.11 $$\int \frac{\varepsilon(x, y)}{x} f_0(u, v) d\mu_{N_0} .$$

We know that if we are given a trivialized $\Gamma(N_0)^{\text{arith}}$-curve (E, φ, β), then by "dividing r times by the canonical subgroup" we get a trivialized $\Gamma(N)^{\text{arith}}$-curve $(E^{(r)}, \varphi^{(r)}, \beta^{(r)})$, and (cf. 8.5.3, 8.6.1)

10.3.12 $$\int \frac{\varepsilon(x, y)}{x} f_0(u, v)\, d\mu_{N_0}(E, \varphi, \beta) = \int \frac{1}{x}(\varepsilon(u, v) f_0(u, v)) d\mu_N(E^{(r)}, \varphi^{(r)}, \beta^{(r)}).$$

The right-hand integral may then be "evaluated" by 10.3.9.

Finally, when we are given an integer N_0 prime to p, a W-valued function g on $(\mathbf{Z}/N_0\mathbf{Z})^2$, and a possibly trivial character $\varepsilon(x, y) = \varepsilon_1(x)\varepsilon_2(y)$ of $(\mathbf{Z}/p^r\mathbf{Z})^\times \times (\mathbf{Z}/p^r\mathbf{Z})^\times$, for some $r \geqq 1$, we can form

10.3.13 $$\mathcal{L}_\nu\left(\frac{\varepsilon_1 \varepsilon_2}{x}, g\right) = \frac{\varepsilon_1(x)\varepsilon_2(y)}{x} g(u, v) d\nu_N ,$$

whose *value* on a trivialized $\Gamma(N_0)^{\text{arith}}$-curve (E, φ, α) is given by (9.1.4)

10.3.14 $$\begin{aligned} &\int \frac{\varepsilon_1(x)\varepsilon_2(y)}{x} g(u, v) d\nu_{N_0}(E, \varphi, \alpha) \\ &= \frac{1}{\varepsilon_1(N_0)} \int \frac{\varepsilon_1(x)\varepsilon_2(y)}{x} (P_\alpha g)(u, v) d\mu_{N_0}(E, \varphi, \beta_\alpha) \\ &= \frac{1}{\varepsilon_1(N_0)} \int \frac{1}{x} \varepsilon_1(u)\varepsilon_2(v)(P_\alpha g)(u, v) d\mu_N(E^{(r)}, \varphi^{(r)}, \beta_\alpha^{(r)}) \qquad \text{(by 10.3.12)} \end{aligned}$$

We can evaluate this last integral using 10.3.9.

10.4. *Special values in the case of complex multiplication.* We have already noted that for fixed N the value $H_{\zeta,s}(E, \beta)$ depends *only* on the division point $P = \beta(\zeta, s)$, so we write it

10.4.1 $$H^{12N}(P: E) = H_{\zeta,s}(E, \beta) \quad \text{if } \beta(\zeta, s) = P \in {}_NE .$$

The formal exponent $12N$ serves to remind us that if $N = N_1N_2$, and if P has order N_1, then

10.4.2 $$(H^{12N_1}(P, E))^{N_2} = H^{12N}(P, E)$$

(a property which follows from the transcendental *definition* of $H_{\zeta,s}$, and which could have been stated in 10.0). Thus given an elliptic curve E over a reasonable p-adic field K as in (10.2.16), and a point $P \in E(K)$ of *finite order* N, $P \neq 0$, the value $H^{12N}(P; E)$ lies in $K^\times$, and the quantity

10.4.3 $$\frac{1}{12N}\log_p(H^{12N}(P, E)) \in K$$

is *independent* of the auxiliary choice of N. Thus we may define

10.4.4 $$\log_p H(P, E) \overset{\text{dfn}}{=} \frac{1}{12N}\log_p (H^{12N}(P, E)) \in K .$$

We will also make use of the following compatibility with isogeny (easily checked transcendentally using the product formula 10.0.1).

Let $G \subset E(K)$ be a finite subgroup, and let $P \in E(K)$ be a point of finite order *not* lying in G. Let $\pi: E \to E/G$ denote the projection. Then

10.4.5 $$\sum_{g \in G} \log_p H(P + g, E) = \log_p H(\pi(P), E/G) .$$

We now apply this in the complex multiplication case. For simplicity, we adopt the notations and hypotheses of 9.4.5. If P is a point of finite order N on the curve $E_M = \mathbf{C}/M$ corresponding to m/N, we write $\log_p H(m/N, M)$ instead of $\log_p H(P, E_M)$.

Let N_0 be a prime-to-p not necessarily exact conductor for the function g. As already noted above (10.3.14), we have

10.4.6 $$\mathfrak{L}_\nu\left(\frac{\varepsilon_1\varepsilon_2}{x}, g\right)(M) = \frac{1}{\varepsilon_1(N_0)}\int\frac{1}{x}\varepsilon_1(u)\varepsilon_2(v)(P_\alpha g)(u, v)d\mu_{p^rN_0}(M, \lambda^r\check{\varphi}, \lambda^r\alpha) .$$

Using 10.3.9, together with 8.8.11, we find that this is equal to

10.4.7 $$-\sum_{\substack{m \in M/p^rN_0M \\ m\neq 0}}\frac{e_1(m)\varepsilon_2(\bar{m})g(m)}{\varepsilon_1(\langle\lambda^r\rangle)\varepsilon_2(\langle\lambda^r\rangle)\rho(\lambda^r)}\log_p H\left(\frac{m}{p^rN_0}, M\right) .$$

Substituting the value of $e_1(m)$ given by 8.8.9–10, and using (10.4.5), we obtain explicit formulas. The actual computation is left to the reader.

Formulas 10.4.8. With hypotheses as in 9.4.5, let N_0 be a prime-to-p conductor for g. Then we have the following formulas for

$$\mathfrak{L}_\nu\Big(\frac{\varepsilon_1\varepsilon_2}{x}, g\Big)(M).$$

10.4.9. *Case* I. ε_1 *non-trivial, exact conductor* p^a, ε_2 *non-trivial of exact conductor* p^b:

$$\frac{-g(\zeta_a, \varepsilon_1)}{\rho(\lambda^a)\varepsilon_1(\langle\lambda^a\rangle)\varepsilon_2(\langle\lambda^a\rangle)}\sum_{\substack{m \in M/\lambda^a\bar{\lambda}^b N_0 M\\ m \notin \lambda M\\ m \notin \bar{\lambda} M}} \frac{\varepsilon_2(\bar{m})g(m)}{\varepsilon_1(m)}\log_p H\Big(\frac{m}{\lambda^a\bar{\lambda}^b N_0}, M\Big).$$

10.4.10. *Case* II. ε_1 *non-trivial, exact conductor* p^a, ε_2 *trivial:*

$$\frac{-g(\zeta_a, \varepsilon_1)}{\rho(\lambda^a)\varepsilon_1(\langle\lambda^a\rangle)}\Big(1 - \frac{\rho(\bar{\lambda})}{\varepsilon_1(\bar{\lambda})}\Big)\sum_{\substack{m \in M/\lambda^a N_0 M\\ m \notin \lambda M}} \frac{g(m)}{\varepsilon_1(m)}\log_p H\Big(\frac{m}{\lambda^a N_0}, M\Big).$$

10.4.11. *Case* III. ε_1 *trivial*, ε_2 *non-trivial, exact conductor* p^a:

$$-\Big(1 - \frac{1}{p\rho(\lambda)\varepsilon_2(\langle\lambda\rangle)}\Big)\sum_{\substack{m \in M/\bar{\lambda}^a N_0 M\\ m \neq 0}} \varepsilon_2(\bar{m})g(m)_p \log H\Big(\frac{m}{\bar{\lambda}^a N_0}, M\Big).$$

10.4.12. *Case* IV. ε_1, ε_2 *both trivial:*

$$-(1 - \rho(\bar{\lambda}))\Big(1 - \frac{1}{p\rho(\lambda)}\Big)\sum_{\substack{m \in M/N_0 M\\ m \neq 0}} g(m)\log_p H\Big(\frac{m}{N_0}, M\Big)$$

$$+ g(0)\Big[\frac{1}{p\rho(\lambda)}\sum_{\substack{m \bmod p\\ m\neq 0}}\log_p H\Big(\frac{m}{p}, M\Big)$$

$$- \frac{\rho(\bar{\lambda})}{p\rho(\lambda)}\sum_{\substack{m \bmod \lambda\\ m\neq 0}}\log_p H\Big(\frac{m}{\lambda}, M\Big) - \sum_{\substack{m \bmod \bar{\lambda}\\ m\neq 0}}\log_p H\Big(\frac{m}{\bar{\lambda}}, M\Big)\Big].$$

PRINCETON UNIVERSITY

REFERENCES

[1] J. COATES and W. SINNOTT, On p-adic L-functions over real quadratic fields, Inv. Math. **25** (1974), 252-279.

[2] R.M. DAMERELL, L-functions of elliptic curves with complex multiplication I, Acta Arith. **17** (1970), 287-301.

[3] P. DELIGNE and M. RAPOPORT, Les schémas de modules de courbes elliptiques, Proc. 1972 Antwerp Summer School, Springer Lecture Notes in Math. **349** (1973) 143-316.

[4] P. DELIGNE and K. RIBET, p-adic L-functions for totally real fields, in preparation.

[5] B. DWORK, A deformation theory for the zeta function of a hypersurface, Proc. Intl. Cong. Math. (1962), Stockholm, 247-259.

[6] R. FRICKE, Die Elliptischen Funktionen und ihre Anwendungen, Vol. I, II, Leipzig, Berlin, Teubner, 1916 and 1923.

[7] G.H. HALPHEN, *Traité des Fonctions Elliptiques et de Leur Applications*, Première Partie, Paris, Gauthier-Villars, 1886.

[8] G.H. HARDY, *Ramanujan. Twelve Lectures on Subjects Suggested by His Life and Work*, New York, Chelsea, 1940.

[9] E. HECKE, Darstellung von Klasszahlen als Perioden von Integralen 3. Gattung aus dem Gebiet der Elliptischen Modulfunktionen, Abh. Math. Sem. Hamb. Bd. **4** (1925), 211-223 (No. 21 in *Math. Werke*, Gottingen, Vandenhoeck & Rupert, 1970.

[10] E. HECKE, Theorie der Eisensteinschen Reihen Höherer Stufe und Ihre Anwendung auf

Funktionentheorie und Arithmetik, Abh. Math. Sem. Hamb. Bd. **5** (1927), 199-224 (No. 24 in *Math. Werke*).

[11] A. HURWITZ, Uber die Entwicklungskoeffizienten der Lemniscatischen Funktionen, Math. Ann. **51** (1899), 196-226.

[12] K. IWASAWA, *Lectures on p-adic L-Functions*, Annals of Math. Studies 74, Princeton Univ. Press, 1972.

[13] N. KATZ, p-adic properties of modular schemes and modular forms, Proc. 1972 Antwerp Summer School, Springer Lecture Notes in Math. **350** (1973), 70-189.

[14] ———, Higher congruences between modular forms, Ann. of Math. **101** (1975), 332-367.

[15] ———, The Eisenstein measure and p-adic interpolation, to appear in Amer. J. Math.

[16] ———, p-adic L-functions via moduli of elliptic curves, to appear in *Proc.* 1974 *AMS Summer Inst. in Alg. Geom.*

[17] T. KUBOTA and H.W. LEOPOLDT, Eine p-adische Theorie der Zetawerte I, J. Reine Ang. Math. **214/215** (1964), 328-339.

[18] S. LANG, *Elliptic Functions*, Reading, Addison-Wesley, 1973.

[19] K. MAHLER, An interpolation series for a continuous function of a p-adic variable, J. Reine Ang. Math. **199** (1958), 23-34.

[20] J.I. MANIN, Parabolic points and zeta functions of modular curves, Izv. Akad. Nauk. **36** (1972), 1966.

[21] ———, Periods of parabolic forms and p-adic Hecke series, Math. Sbornik V. **93** (134), No. 3 (11), 1973.

[22] J. MANIN and S. VISHIK, p-adic Hecke series for quadratic imaginary fields, Math. Sbornik, V. **95** (137), No. 3 (11), 1974.

[23] B. MAZUR, Courbes elliptiques et symboles modulaires, Exposé 414, Séminaire Bourbaki 1971/72, Springer Lecture Notes in Math. **317** (1973), 277-294.

[24] ———, Analyse p-adique. Secret Bourbaki rédaction, 1973.

[25] B. MAZUR and H.P.F. SWINNERTON-DYER, Arithmetic of Weil curves, Inv. Math. **25** (1974), 1-61.

[26] H. RADEMACHER, *Topics in Analytic Number Theory*, Springer-Verlag, 1973.

[27] S. RAMANUJAN, On certain arithmetical functions, Trans. Camb. Phil. Soc. **22**, No. 9 (1916), 159-184 (No. 18 in *Collected Papers*, New York, Chelsea, reprinted 1962).

[28] ———, On certain trigonometrical sums and their applications in the theory of numbers, Trans. Camb. Phil. Soc. **22**, No. 13 (1918), 259-276 (No. 21 in *Collected Papers*).

[29] K. RIBET, p-adic interpolation via Hilbert modular forms, to appear in *Proc.* 1974 *AMS Summer Inst. on Alg. Geom.*

[30] J.-P. SERRE, Congruences et formes modulaires, Exposé 416, Séminaire N. Bourbaki 1971/72, Springer Lecture Notes in Math. **317** (1973), 319-338.

[31] ———, Formes modulaires et fonctions zeta p-adiques, Proc. 1972 Antwerp Summer School, Springer Lecture Notes in Math. **350** (1973), 191-268.

[32] G. SHIMURA, *Introduction to the arithmetic theory of automorphic functions*, Pub. Math. Soc. Japan, No. 11, Tokyo, Iwanami Shoten and Princeton Univ. Press, 1971.

[33] ———, On elliptic curves with complex multiplication as factors of the Jacobians of modular function fields, Nagoya Math. J. **43** (1971), 199-208.

[34] C.L. SIEGEL, *Lectures on advanced analytic number theory*, Tata Institute, Bombay, 1961.

[35] A. WEIL, On a certain type of characters of the idèle-class group of an algebraic number field, *Proc. Int'l. Symp. Tokyo-Nikko*, (1955), 1-7.

[36] ———, Uber die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen, Math. Ann. **168** (1967), 149-156.

[37] ———, Elliptic functions according to Eisenstein, Lectures at Institute for Advanced Theory, 1974.

(Received October 15, 1975)