Proceedings of Symposia in Pure Mathematics
Volume 58.2 (1995)

Formal Groups of Twisted Multiplicative Groups and L-series

NANCY CHILDRESS AND DAVID GRANT

ABSTRACT. Given a quadratic field with associated quadratic character χ, Honda attached a formal group H_χ to the L-series $L(s, \chi)$ and showed that it was strictly integrally isomorphic to the formal group at the origin of a quadratic twist of $\mathbf{G}_m$. This provided an elementary proof of quadratic reciprocity. Given any abelian Galois representation ρ, Honda also defined a formal group H_ρ attached to the "matrix L-series" of ρ. Let p be an odd prime. We show by an explicit and global method that for a particular $(p-2)$-dimensional representation Θ of the Galois group of the p^{th} cyclotomic field K, the formal group attached to the matrix L-series of Θ is strictly integrally isomorphic to the formal group at the origin of a twist over K of $\mathbf{G}_m^{p-2}$. As a consequence, we get a proof of a result on the road to Eisenstein reciprocity.

Introduction

In a seminal paper, Honda [Ho1] attached an integral formal group H_χ to the L-series of the nontrivial Dirichlet character χ associated to a quadratic field of discriminant D. He then proved that H_χ was strictly isomorphic over the ring of integers in $\mathbb{Q}(\sqrt{D})$ to the formal group $F_D(X, Y) = X + Y + \sqrt{D}XY$.

Considering other types of L-series, Honda also attached an integral formal group H_E to the L-series of an elliptic curve E defined over $\mathbb{Q}$ and showed that H_E was strictly isomorphic over $\mathbb{Z}$ to the formal group $\widehat{E}$ at the origin of a minimal model of E. This gave the first proof of the Atkin-Swinnerton-Dyer congruences. (See [Ho1, Ho2, Hi, C, Ha]; for generalizations to abelian varieties of higher dimension, see for example [D] and [DN].) Honda explained his motivation in [Ho3]. From the isomorphism of

---

1991 *Mathematics Subject Classification*. Primary 14L05, 11R42.

The second author was partially supported by National Science Foundation grant DMS-9102652.

This paper is in final form and no version of it will be submitted for publication elsewhere.

H_χ and F_D he was able to derive quadratic reciprocity. Thus the isomorphism of H_E and $\widehat{E}$ is an analogue of reciprocity for elliptic curves. Indeed, via the isomorphism between $\widehat{E}$ and H_E, he established that several elliptic curves were images of modular curves.

In [Ho2], Honda showed how to attach an integral n-dimensional formal group H_ρ to the "matrix L-series" of an n-dimensional abelian Galois representation ρ. Also attached to ρ is the torus T_ρ whose character group is a representation space for ρ. Since F_D is isomorphic to the formal group at the origin of a twist of $\mathbb{G}_m$ by χ, a number of authors have generalized Honda's theorem by showing that H_ρ is isomorphic to $\widehat{T}_\rho$, the formal group at the origin of T_ρ (see [I, Y, DN]).

What has not been done is to relate the generalizations of Honda's results on tori to higher reciprocity laws. Also, although Honda's local classification theorem of formal groups in terms of the characteristic polynomial of Frobenius was necessary for his work on elliptic curves, he used a global and elementary approach for tori, and this was missing in the subsequent work of [I] and [DN].

A step towards meeting these goals was recently taken by the first author and Stopple [CS]. Let ζ_p be a primitive p^{th} root of unity, $G = \text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, and let Θ be the representation of G whose representation space is the complement of the unit representation in the regular representation of G. They gave a global and explicit proof that H_Θ was strictly isomorphic over $\mathbb{Z}[\zeta_p]$ to a formal group F_Θ whose logarithm was analogous to that of F_D. What they did not do was to relate F_Θ to T_Θ.

In this note, we continue to explore the relationship between isomorphisms of formal groups and reciprocity. By writing an explicit model for T_Θ, we calculate its formal group at the origin $\widehat{T}_\Theta$, and then in Theorem 1 we give a global and elementary proof that $\widehat{T}_\Theta$ is strictly isomorphic over $\mathbb{Z}$ to H_Θ. Such a result would also follow from [I] or [DN], but the model of T_Θ we derive is sufficiently nice that we can exploit the isomorphism à la Honda, to give in Theorem 2 a proof of a result on the road to Eisenstein reciprocity.

1. Preliminaries

Let A be a commutative ring with identity 1. For a positive integer n, let $\vec{x}$ denote the n-tuple $\vec{x} = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$ and let $\vec{x}^m$ denote $\begin{bmatrix} x_1^m \\ \vdots \\ x_n^m \end{bmatrix}$. We set

$$\vec{\log}(\vec{1} - \vec{x}) = -\sum_{m=1}^{\infty} \frac{\vec{x}^m}{m} = \begin{bmatrix} \log(1-x_1) \\ \vdots \\ \log(1-x_n) \end{bmatrix}, \quad \vec{\exp}(\vec{x}) = \sum_{m=0}^{\infty} \frac{\vec{x}^m}{m!} = \begin{bmatrix} \exp(x_1) \\ \vdots \\ \exp(x_n) \end{bmatrix},$$

where $\vec{1}$ is the column vector whose entries are all 1.

For two formal power series $f, g \in A[[\vec{x}]]$ we write $f \equiv g \pmod{\deg d}$ if f and g coincide in terms of degree less than d. We typically denote a matrix whose entry in the i^{th}-row and j^{th}-column is m_{ij} by $[m_{ij}]_{ij}$.

We refer the reader to **[Ha]** or **[CS]** for more on formal groups. If F is an n-dimensional formal group, we let id_n denote the identity homomorphism from F onto itself. We denote the logarithm of F by λ_F. The inverse of λ_F is the exponential, ε_F. For any n-tuple of power series $\alpha(\vec{x}) = {}^t(\alpha, \vec{x}), \ldots, \alpha_n(\vec{x}))$, we let $J(\alpha) = [\frac{\partial \alpha_i}{\partial x_j}(0)]_{ij}$ denote the Jacobian matrix of α. For any group variety V, we let $\widehat{V}$ denote its formal group at the origin.

LEMMA 1. *Let A be a $\mathbb{Q}$-algebra.*

(a) *The only homomorphisms over A from $\widehat{\mathbb{G}}_a^m$ to $\widehat{\mathbb{G}}_a^n$ are homomorphisms of the form $S_M(\vec{x}) = M\vec{x}$, for some $n \times m$ matrix M with entries in A.*

(b) *Let G and F be two formal groups defined over A, of dimensions m and n, with logarithms λ_G and λ_F, respectively. Suppose that α is an m-tuple of power series and that β is an m-tuple of power series such that $\beta \circ \alpha = \mathrm{id}_m$. Then the logarithm of G is $S_{J(\beta)} \circ \lambda_F \circ \alpha$.*

(c) *Let F, G, α, and β be as in* (b). *Then the exponential ε_G of G is given by $\beta \circ \varepsilon_F \circ S_{J(\alpha)}$, where ε_F denotes the exponential of F.*

PROOF. Part (a) is proved in **[Ha]**. Part (b) follows from the uniqueness of the logarithm, after noting that the Jacobian of $S_{J(\beta)} \circ \lambda_F \circ \alpha$ is $J(\beta) I_n J(\alpha) = I_m = J(\mathrm{id}_m)$. For part (c) note that $\lambda_F \circ \alpha \circ \varepsilon_G$ is a homomorphism from $\widehat{\mathbb{G}}_a^m$ to $\widehat{\mathbb{G}}_a^n$, so by part (a) is of the form S_M for some matrix M. Comparing Jacobians shows that $M = J(\alpha)$. Hence $\beta \circ \varepsilon_F \circ S_{J(\alpha)} = \beta \circ \varepsilon_F \circ \lambda_F \circ \alpha \circ \varepsilon_G = \varepsilon_G$. $\square$

Recall that a torus T over $\mathbb{Q}$ is a (necessarily affine) group variety which is isomorphic over some number field K to $\mathbb{G}_m^d$ for some d. If $\phi : T \to \mathbb{G}_m^d$ is one such isomorphism, then for every $\sigma \in G = \mathrm{Gal}(K/\mathbb{Q})$, $\phi^\sigma : T \to \mathbb{G}_m^d$ is another, and the map

$$\sigma \to \phi^\sigma \circ \phi^{-1}$$

gives a representation $\rho : G \to \mathrm{Aut}(\mathbb{G}_m^d)$. It is a theorem of Ono **[O]** that the $\mathbb{Q}$-isomorphism class of T is determined by the equivalence class of ρ, and that to every representation ρ there is a a torus T_ρ which gives rise to it. If $\Gamma_{\mathbb{Q}}(T_\rho)$ is the coordinate ring of T_ρ over $\mathbb{Q}$, then there is a K-isomorphism $\phi : T_\rho \to \mathbb{G}_m^d$ which gives rise to an isomorphism

$$\phi^* : \Gamma_K(\mathbb{G}_m^d) \to \Gamma_K(T_\rho).$$

Therefore via ϕ^*, $\Gamma_{\mathbb{Q}}(T_\rho)$ can be identified with the fixed ring under G of

$\Gamma_K(\mathbb{G}_m^d)$, where G acts naturally on K, and via ρ on $\Gamma_{\mathbb{Q}}(\mathbb{G}_m^d)$.

2. Theorems

Let p be an odd prime. For any $m > 0$, ζ_m will denote a primitive m^{th} root of unity. Let $K = \mathbb{Q}(\zeta_p)$, and $G = \mathrm{Gal}(K/\mathbb{Q})$. Let σ_m denote the element of G such that $\sigma_m(\zeta_p) = \zeta_p^m$.

In [Ho2], Honda attached to any representation

$$\rho : G \to \mathrm{Aut}(\mathbb{G}_m^d)$$

a formal group H_ρ associated with the matrix L-series

$$L(s, \rho) = \prod_{q \text{ prime}} (I - \rho(\sigma_q)q^{-s})^{-1} = \sum_{n \geq 1} \frac{\rho(\sigma_n)}{n^s}.$$

In particular, a formal group is determined by its logarithm, so we define H_ρ by specifying its logarithm as

$$\lambda_{H_\rho}(\vec{t}) = \sum_{n \geq 1} \frac{\rho(\sigma_n)}{n} \vec{t}^{\,n},$$

for any d-vector $\vec{t}$. Honda showed that H_ρ is d-dimensional and defined over $\mathbb{Z}$.

We now want to consider the representation of G studied in [CS]. We take $p-2$ copies of $\mathbb{G}_m$, the i^{th} copy defined by $X_i Y_i = 1$, for $i = 2, \dots, p-1$. Let V be the variety defined by $\prod_{i=1}^{p-1} \eta_i = 1$. Let g be a primitive root mod p. Then the map γ defined by

$$\gamma(\eta_i) = X_{g^{-i}}, \quad i = 1, \dots, p-2, \qquad \gamma(\eta_{p-1}) = Y_2 \cdots Y_{p-1},$$

is an isomorphism from V onto $\mathbb{G}_m^{p-2}$.

There is an automorphism μ of order $p-1$ on V defined by

$$\eta_i \xrightarrow{\mu} \eta_{i+1}, \qquad i = 1, \dots, p-2, \qquad \eta_{p-1} \xrightarrow{\mu} \eta_1.$$

Hence via γ, we get a corresponding element ν in $\mathrm{Aut}(\mathbb{G}_m^{p-2})$ of order $p-1$. For any integer b, we get a matrix representative $[\nu_{ij}^{(b)}]_{ij}$ for ν^b (with $i, j \neq 1 \in (\mathbb{Z}/p\mathbb{Z})^\times$) by setting $(d_2, \dots, d_{p-1}) = (c_2, \dots, c_{p-1})[\nu_{ij}^{(b)}]_{ij}$ when $\nu^b(X_2^{c_2} \cdots X_{p-1}^{c_{p-1}}) = (X_2^{d_2} \cdots X_{p-1}^{d_{p-1}})$. A calculation shows

$$\nu_{ij}^{(b)} = \begin{cases} -1 & \text{if } i = g^b, \\ 1 & \text{if } j = g^{-b} i, \\ 0 & \text{otherwise.} \end{cases}$$

Now σ_g is a generator of G, so we get a representation

$$\Theta : G \to \mathrm{Aut}(\mathbb{G}_m^{p-2})$$

by defining $\Theta(\sigma_g^b) = \nu^b$; i.e., if $a = g^b$, then

$$\Theta(\sigma_a)_{ij} = \begin{cases} -1 & \text{if } i = a, \\ 1 & \text{if } j = a^{-1}i, \\ 0 & \text{otherwise.} \end{cases}$$

We will write $\Theta(a)$ for $\Theta(\sigma_a)$, and H for H_Θ, the formal group whose logarithm is

$$\lambda_H(\vec{t}) = \sum_{n \geq 1} \frac{\Theta(n)}{n} \vec{t}^{\,n}.$$

We want an explicit model for $T = T_\Theta$. We define x_i, $1 \leq i \leq p-1$, by

$$\eta_i = 1 + \sum_{j=1}^{p-1} \sigma_g^{i-1}(\zeta_p^j) x_j, \quad i = 1, \dots, p-1.$$

We act on $\Gamma_K(V) = K[\eta_i] \Big/ \left(\prod_{i=1}^{p-1} \eta_i - 1\right)$ by letting G act naturally on K and via Θ on $\Gamma_{\mathbf{Q}}(V)$. Since $\left[\sigma_g^{i-1}(\zeta_p^j)\right]_{ij}$ is invertible, we see that $\sigma_g(x_i) = x_i$ for all i, $1 \leq i \leq p-1$, so the coordinate ring of T is generated by the x_i, $1 \leq i \leq p-1$.

Hence we get a model for T by taking the equation

$$1 = \prod_{i=1}^{p-1} \left(1 + \sum_{j=1}^{p-1} \sigma_g^{i-1}(\zeta_p^j) x_j\right) \in \mathbf{Z}[x_1, \dots, x_{p-1}].$$

A calculation shows that this model is of the form

$$0 = -x_1 - x_2 - \cdots - x_{p-1} + \cdots + x_1^{p-1} + \cdots + x_{p-1}^{p-1}.$$

So by the implicit function theorem, on T there is an integral power series κ without linear or constant terms, such that

$$x_1 = -x_2 - \cdots - x_{p-1} + \kappa(x_2, \dots, x_{p-1}). \tag{1}$$

Although what we seek is the formal group $\widehat{T}$ at the origin of T, it will be easier to resort to Lemma 1 and first compute the formal group $\widehat{F}$ at the origin of the $(p-1)$-dimensional torus F defined by

$$1 = x_0 \prod_{i=1}^{p-1} \left(1 + \sum_{j=1}^{p-1} \sigma_g^{i-1}(\zeta_p^j) x_j\right) \in \mathbf{Z}[x_0, \dots, x_{p-1}].$$

Indeed, $x_1, \dots, x_{p-1}$ form a set of parameters at the origin of F. So a formal group law for $\widehat{F}$ is the set of power series $F_i(\vec{x}, \vec{y})$, $1 \leq i \leq p-1$, satisfying

$$1 + \sum_{j=1}^{p-1} F_j(\vec{x}, \vec{y}) \zeta_p^j = \left(1 + \sum_{j=1}^{p-1} \zeta_p^j x_j\right) \left(1 + \sum_{j=1}^{p-1} \zeta_p^j y_j\right). \tag{2}$$

Since the F_j have rational coefficients, we can expand (2) and equate coefficients of powers of ζ_p^i, $1 \le i \le p-1$. If we identify subscripts of x and y mod p, we get

$$F_i(\vec{x}, \vec{y}) = x_i + y_i - x_i y_{-i} + \sum_{\substack{j=1 \\ j \ne i}}^{p-1} x_j(y_{i-j} - y_{-j}).$$

To compute the logarithm λ_F of $\widehat{F}$, we follow a procedure described by Honda in [Ho2]. Namely, for $i, j = 1, \ldots, p-1$, we set

$$DF := \left[\frac{\partial F_i}{\partial x_j}\right]_{ij} = \begin{cases} 1 - y_{-i}, & j = i, \\ y_{i-j} - y_{-j}, & j \ne i, \end{cases}$$

so that

$$DF\Big|_{(\vec{0}, \vec{z})} = \begin{cases} 1 - z_{-i}, & j = i, \\ z_{i-j} - z_{-j}, & j \ne i. \end{cases}$$

Then λ_F is the set of power series f_j, $1 \le j \le p-1$, without constant term, such that

$$\left[\frac{\partial f_j}{\partial z_i}\right]_{ji} = \left[DF\Big|_{(\vec{0}, \vec{z})}\right]^{-1}.$$

It is not difficult to invert $DF\Big|_{(\vec{0}, \vec{z})}$.

LEMMA 2. *Let* $\psi_j(k) = \zeta_p^{jk}$. *Then for* $1 \le i, j \le p-1$,

$$\left[DF\Big|_{(\vec{0}, \vec{z})}\right]^{-1} = \left[\frac{1}{p}\sum_{\ell=1}^{p-1} \frac{(\psi_\ell(j) - 1)(\psi_\ell(-i))}{\left(1 + \sum_{k=1}^{p-1} z_k \psi_\ell(-k)\right)}\right]_{ji}.$$

PROOF. This follows from orthogonality of the characters ψ_j on $\mathbb{Z}/p\mathbb{Z}$. $\square$

By Lemma 2, we have that

$$f_j(\vec{z}) = \frac{1}{p}\sum_{\ell=1}^{p-1}(\psi_\ell(j) - 1)\log\left(1 + \sum_{k=1}^{p-1} z_k \psi_\ell(-k)\right), \tag{3}$$

for $1 \le j \le p-1$, give the logarithm λ_F.

The exponential map ε_F is the inverse of the logarithm (3). To compute it we set

$$w_j = \frac{1}{p}\sum_{\ell=1}^{p-1}(\psi_\ell(j) - 1)\log\left(1 + \sum_{k=1}^{p-1} z_k \psi_\ell(-k)\right), \tag{4}$$

for $j = 1, \ldots, p-1$, and solve for z_k. In terms of matrices, (4) becomes

$$\vec{w} = \left[\frac{\psi_\ell(j) - 1}{p}\right]_{j\ell} \vec{\log}(\vec{1} + [\psi_\ell(-k)]_{\ell k}\vec{z}).$$

So by orthogonality, for $1 \le j, k, l \le p-1$,

$$\left(\left[\psi_\ell(-k)\right]_{\ell k}\right)^{-1} = \left[\frac{\psi_\ell(j)-1}{p}\right]_{j\ell},$$

and hence

$$\left[\psi_\ell(-k)\right]_{\ell k}\vec{w} = \vec{\log}\left(\vec{1} + \left[\psi_\ell(-k)\right]_{\ell k}\vec{z}\right)$$

or

$$\vec{\exp}\left(\left[\psi_\ell(-k)\right]_{\ell k}\vec{w}\right) = \vec{1} + \left[\psi_\ell(-k)\right]_{\ell k}\vec{z}.$$

Since by orthogonality $[(\psi_\ell(j)-1)/p]_{j\ell}\vec{1} = -\vec{1}$, we see that

$$\vec{1} + \left[\frac{\psi_\ell(j)-1}{p}\right]_{j\ell}\vec{\exp}\left(\left[\psi_\ell(-k)\right]_{\ell k}\vec{w}\right) = \vec{z} \tag{5}$$

gives the exponential.

Now let T be obtained from F by setting $x_0 = 1$. Then a model for $\widehat{T}$ is obtained from $\widehat{F}$ by setting $x_0 = 1$. We can now find $\widehat{T}$ explicitly, as well as its logarithm λ_T, and exponential ε_T.

Lemma 3. (a) *The formal group $\widehat{T}$ is defined over $\mathbb{Z}$.*
(b) *For $2 \le j, k \le p-1$,*

$$f_j(\vec{z}) = \frac{1}{p}\sum_{\ell=1}^{p-1}(\psi_\ell(j)-1)\log\Big(l + \left[\psi_\ell(-k) - \psi_\ell(-1)\right]_{\ell k}\vec{z} + \psi_\ell(-1)_{\ell 1}\kappa(\vec{z})\Big)$$

give $\lambda_T(\vec{z})$, where $\vec{z}$ is the transpose of $(z_2, \dots, z_{p-1})$.
(c) *For $2 \le j \le p-1$,*

$$z_j = 1 + \frac{1}{p}\sum_{\ell=1}^{p-1}(\psi_\ell(j)-1)\exp\left(\sum_{k=2}^{p-1}(\psi_\ell(-k) - \psi_\ell(-1))w_k\right)$$

give ε_T.

Proof. (a) Setting $x_0 = 1$ gives an embedding of T into F, and choosing $x_2, \dots, x_{p-1}$ as a system of parameters at the origin of T gives a corresponding map on formal groups $\alpha : \widehat{T} \longrightarrow \widehat{F}$, given by

$$\alpha\left(\begin{bmatrix} x_2 \\ \vdots \\ x_{p-1}\end{bmatrix}\right) = \begin{bmatrix} -x_2 - \cdots - x_{p-1} + \kappa(x_2, \dots, x_{p-1}) \\ x_2 \\ \vdots \\ x_{p-1}\end{bmatrix}, \tag{6}$$

where $\widehat{T}$ is defined by the set of power series

$$T_i(\vec{x}, \vec{y}) = F_i(\alpha(\vec{x}), \alpha(\vec{y})),$$

for $i = 2, \dots, p-1$. Since the F_i have integral coefficients, and κ does too, the T_i do as well.

(b) If we define β by

$$\beta\left(\begin{bmatrix} x_1 \\ \vdots \\ x_{p-1} \end{bmatrix}\right) = \begin{bmatrix} x_2 \\ \vdots \\ x_{p-1} \end{bmatrix},$$

then $\beta \circ \alpha = \mathrm{id}_{p-2}$. So by Lemma 1, $\lambda_T = S_{J(\beta)} \circ \lambda_F \circ \alpha$. Since

$$J(\beta) = \begin{bmatrix} 0 & \\ \vdots & I_{p-2} \\ 0 & \end{bmatrix},$$

(b) follows immediately from (3) and (6).

(c) By (5), ε_F is given by

$$z_j = 1 + \frac{1}{p}\sum_{\ell=1}^{p-1}(\psi_\ell(j) - 1)\exp\left(\sum_{k=1}^{p-1}\psi_\ell(-k)w_k\right), \tag{7}$$

for $1 \le j \le p-1$. By Lemma 1, $\varepsilon_T = \beta \circ \varepsilon_F \circ S_{J(\alpha)}$. The effect of $S_{J(\alpha)}$ is to set $w_1 = -w_2 - \cdots - w_{p-1}$, so plugging this value into (7) and restricting to $2 \le j \le p-1$ gives the result. □

To analyze H further, we need to diagonalize Θ.

Let $\{\chi_j \mid j = 2, \dots, p-1\}$ be the $p-2$ nontrivial characters of $G \cong (\mathbb{Z}/p\mathbb{Z})^\times$. Then by orthogonality,

$$\left(\left[\chi_j(i^{-1})\right]_{ij}\right)^{-1} = \left[\frac{\chi_j(k) - 1}{p-1}\right]_{jk},$$

and so with $2 \le i, j, k \le p-1$,

$$\Theta(a) = \left[\chi_j(i^{-1})\right]_{ij} \operatorname{diag}(\chi_j(a)) \left[\frac{\chi_j(k) - 1}{p-1}\right]_{jk}. \tag{8}$$

For a Dirichlet character χ modulo p, we let $\tau_\chi = \sum_{a=1}^{p-1}\chi(a)\zeta_p^a$ be the Gauss sum. We also define $\bar{\chi}(a) = \chi(a^{-1})$, $\bar{\Theta}(a) = \Theta(a^{-1})$, and a $(p-2) \times (p-2)$ matrix Gauss sum

$$\tau(\bar{\Theta}) = \sum_{a=1}^{p-1}\bar{\Theta}(a)\zeta_p^a = \left[\chi_j(i^{-1})\right]_{ij} \operatorname{diag}(\tau_{\bar{\chi}_j}) \left[\frac{\chi_j(k) - 1}{p-1}\right]_{jk}. \tag{9}$$

Theorem 1. *$\widehat{T}$ and H are strictly isomorphic over $\mathbb{Z}$.*

Proof. It suffices to show that the composition of ε_T with λ_H is an integral power series. The composite is strict because both ε_T and λ_μ are strict.

As in [CS], if $\vec{t}$ is the transpose of $(t_2, \ldots, t_{p-1})$, then we have

$$\lambda_H(\vec{t}) = \sum_{n=1}^{\infty} \frac{\Theta(n)}{n} \vec{t}^{\,n} = -\tau(\bar{\Theta})^{-1} \sum_{a=1}^{p-1} \bar{\Theta}(a) \,\vec{\log}(\vec{1} - \zeta_p^a \vec{t}).$$

Composing for $2 \le j, k \le p-1$, we get:

$$\varepsilon_T \circ \lambda_H(\vec{t})_j = 1 + \frac{1}{p} \sum_{\ell=1}^{p-1} (\psi_\ell(j) - 1) \exp\Bigg(-\Big[\psi_\ell(-k) - \psi_\ell(-1)\Big]_{1k} \tau(\bar{\Theta})^{-1} \times \sum_{a=1}^{p-1} \bar{\Theta}(a) \vec{\log}(\vec{1} - \zeta_p^a \vec{t}) \Bigg).$$

To simplify this we need a lemma.

Lemma 4. *Let δ_{ij} be the Kronecker delta. Then for $2 \le i, k \le p-1$, $1 \le \ell \le p-1$,*

$$\Big[\psi_\ell(-k) - \psi_\ell(-1)\Big]_{1k} \tau(\bar{\Theta})^{-1} = \Big[\delta_{\ell(-i^{-1})}\Big]_{1i}$$

if $\ell \ne p-1$, and

$$\Big[\psi_{-1}(-k) - \psi_{-1}(-1)\Big]_{1k} \tau(\bar{\Theta})^{-1} = -{}^t\vec{1},$$

where ^{t} denotes the transpose.

Proof. By (9), for $2 \le i, j, k \le p-1$,

$$\tau(\bar{\Theta})^{-1} = \Big[\chi_j(k^{-1})\Big]_{kj} \operatorname{diag}\left(\frac{1}{\tau_{\bar{\chi}_j}}\right) \left[\frac{\chi_j(i) - 1}{p-1}\right]_{ji},$$

so

$$\begin{aligned}
&\Big[\psi_\ell(-k) - \psi_\ell(-1)\Big]_{1k} \tau(\bar{\Theta})^{-1} \\
&\quad = \Big[\psi_\ell(-k) - \psi_\ell(-1)\Big]_{1k} \Big[\chi_j(k^{-1})\Big]_{kj} \operatorname{diag}\left(\frac{1}{\tau_{\bar{\chi}_j}}\right) \left[\frac{\chi_j(i) - 1}{p-1}\right]_{ji} \\
&\quad = \Big[\chi_j(-\ell)\tau_{\bar{\chi}_j}\Big]_{1j} \operatorname{diag}\left(\frac{1}{\tau_{\bar{\chi}_j}}\right) \left[\frac{\chi_j(i) - 1}{p-1}\right]_{ji} \qquad (10)\\
&\quad = \Big[\chi_j(-\ell)\Big]_{1j} \left[\frac{\chi_j(i) - 1}{p-1}\right]_{ji}.
\end{aligned}$$

If $\ell \ne p-1$, then (10) gives $\delta_{\ell(-i)^{-1}}$ by orthogonality. If $\ell = p-1$, then $\Big[\chi_j(-\ell)\Big]_{1j} = {}^t\vec{1}$, and

$${}^t\vec{1} \left[\frac{\chi_j(i) - 1}{p-1}\right]_{ji} = -{}^t\vec{1}. \qquad \square$$

Using Lemma 4, for $2 \le i, j, k \le p-1$, we get

$$\begin{aligned}
\varepsilon_T \circ \lambda_H(\vec{t})_j &= 1 + \frac{1}{p}\sum_{\ell=1}^{p-2}(\psi_\ell(j)-1)\exp\left(-\left[\delta_{\ell(-i^{-1})}\right]_{1i}\sum_{a=1}^{p-1}\bar{\Theta}(a)\vec{\log}(\vec{1}-\zeta_p^a\vec{t})\right) \\
&\quad + \frac{1}{p}(\psi_{-1}(j)-1)\exp\left({}^t\vec{1}\sum_{a=1}^{p-1}\bar{\Theta}(a)\vec{\log}(\vec{1}-\zeta_p^a\vec{t})\right) \\
&= 1 + \frac{1}{p}\sum_{\ell=1}^{p-2}(\psi_\ell(j)-1)\exp\left(-\sum_{a=1}^{p-1}(\Theta(a)\vec{\log}(\vec{1}-\zeta_p^a\vec{t}))_{-\ell^{-1}}\right) \\
&\quad + \frac{1}{p}(\psi_{-1}(j)-1)\exp\left(\sum_{a=1}^{p-1}\left[\delta_{a,1}-\delta_{k,a}\right]_{1k}\vec{\log}(\vec{1}-\zeta_p^a\vec{t})\right) \\
&= 1 + \frac{1}{p}\sum_{\ell=1}^{p-2}(\psi_\ell(j)-1)\prod_{a=1}^{p-1}\prod_{k=2}^{p-1}(1-\zeta_p^a t_k)^{-\Theta(a^{-1})_{-\ell^{-1}k}} \\
&\quad + \frac{1}{p}(\psi_{-1}(j)-1)\prod_{k=2}^{p-1}(1-\zeta_p t_k)\prod_{a=2}^{p-1}(1-\zeta_p^a t_a)^{-1} \\
&= 1 + \frac{1}{p}\sum_{\ell=1}^{p-2}(\psi_\ell(j)-1)\frac{\prod_{k=2}^{p-1}(1-\zeta_p^{-\ell}t_k)}{\prod_{a=2}^{p-1}(1-\zeta_p^{-a\ell}t_a)} \\
&\quad + \frac{1}{p}(\psi_{-1}(j)-1)\frac{\prod_{k=2}^{p-1}(1-\zeta_p t_k)}{\prod_{a=2}^{p-1}(1-\zeta_p^a t_a)}.
\end{aligned}$$

So

$$\varepsilon_T \circ \lambda_H(\vec{t})_j = 1 + \frac{1}{p}\sum_{\ell=1}^{p-1}(\psi_\ell(j)-1)\frac{\prod_{a=2}^{p-1}(1-\zeta_p^{-\ell}t_a)}{\prod_{a=2}^{p-1}(1-\zeta_p^{-a\ell}t_a)}. \tag{11}$$

Since (11) is fixed by G,

$$\varepsilon_T \circ \lambda_H(\vec{t})_j \in \mathbb{Q}[[t_2, \dots, t_{p-1}]] \bigcap \frac{1}{p}(1-\zeta_p)\mathbb{Z}[\zeta_p][[t_2, \dots, t_{p-1}]],$$

and hence lies in $\mathbb{Z}[[t_2, \dots, t_{p-1}]]$.

REMARK. Composing ε_T with $\tau(\bar{\Theta})^{-1}\vec{\log}(\vec{1}+\tau(\bar{\Theta})\vec{t})$, it is not hard to recover the main theorem of [CS]. (In [CS], the contragredient of Θ was used, but the results there apply mutatis mutandis).

COROLLARY 1. (a) *Let φ be the integral power series such that $\lambda_H = \lambda_T \circ \varphi$.*

Let M be the $(p-2)\times(p-2)$ matrix $[\chi_j(k)^{-1}]_{kj}$, and define

$$T'(\vec{x}, \vec{y}) = M^{-1}(T(M\vec{x}, M\vec{y})),$$
$$H'(\vec{x}, \vec{y}) = M^{-1}(H(M\vec{x}, M\vec{y})).$$

Then T' and H' are integral over the ring R obtained by inverting all the primes in $\mathbb{Z}[\zeta_{p-1}]$ that divide $(p-1)\mathbb{Z}[\zeta_{p-1}]$. If we define ξ such that the following diagram commutes

$$\begin{tikzcd} \widehat{T'} \arrow[r, "S_M"] & \widehat{T} \\ H' \arrow[u, "\xi"] \arrow[r, "S_M"] & H \arrow[u, "\varphi"'] \end{tikzcd}$$

(here $S_M(\vec{x}) = M\vec{x}$), then ξ is a strict isomorphism from H' to $\widehat{T'}$ defined over R.

(b) *For $2 \le i, j \le p-1$, $1 \le \ell \le p-1$,*

$$\lambda_{T'}(\vec{z}) = \frac{1}{p}\,\frac{1}{p-1}\Big[\bar{\chi}_i(\ell)\tau_{\chi_i} + p\Big]_{i\ell}\,\vec{\log}\Big(\vec{1} + \Big[\chi_j(-\ell)\tau_{\bar{\chi}_j}\Big]_{\ell j}\vec{z} + \Big[\psi_\ell(-1)\Big]_{\ell 1}\kappa(M\vec{z})\Big).$$

(c) *For $2 \le j, k \le p-1$,*

$$\lambda_{H'}(\vec{t}) = \sum_{n\ge 1}\frac{1}{n}\operatorname{diag}(\chi_j(n))\left[\frac{\chi_j(k)-1}{p-1}\right]_{jk}\left(\left[\chi_j(k)^{-1}\right]_{kj}\vec{t}\right)^n.$$

Proof. (a) This follows from Theorem 1 once we note that

$$M^{-1} = \left[\frac{\chi_i(j)-1}{p-1}\right]_{ij}$$

has entries in R.

(b) We apply Lemma 1 to Lemma 3, for $2 \le i, j, k \le p-1$, $1 \le \ell \le p-1$, to get

$$\begin{aligned}
\lambda_{T'}(\vec{z}) &= S_{M^{-1}} \circ \lambda_T \circ S_M(\vec{z}) \\
&= \left[\frac{\chi_i(j)-1}{p-1}\right]_{ij} \left[\frac{\psi_\ell(j)-1}{p}\right]_{j\ell} \vec{\log}\Big(\vec{1} + \Big[\psi_\ell(-k) - \psi_\ell(-1)\Big]_{\ell k} \\
&\qquad \cdot \left(\Big[\chi_j(k)^{-1}\Big]_{kj}\right)\vec{z} + \Big[\psi_\ell(-1)\Big]_{\ell 1} \kappa(M\vec{z})\Big) \\
&= \frac{1}{p(p-1)} \left[\sum_{j=2}^{p-1} (\chi_i(j)\psi_\ell(j) - \psi_\ell(j) - \chi_i(j) + 1)\right]_{i\ell} \\
&\qquad \cdot \vec{\log}\left(\vec{1} + \left[\sum_{k=2}^{p-1} \psi_\ell(-k)\chi_j(k)^{-1} - \psi_\ell(-1)\chi_j(k)^{-1}\right]_{\ell j} \vec{z} \right. \\
&\qquad \left. + \Big[\psi_\ell(-1)\Big]_{\ell 1} \kappa(M\vec{z})\right) \\
&= \frac{1}{p(p-1)} \Big[\bar{\chi}_i(\ell)\tau_{\chi_i} + p\Big]_{i\ell} \vec{\log}\Big(\vec{1} + \Big[\chi_j(-\ell)\tau_{\bar{\chi}_j}\Big]_{\ell j} \vec{z} \\
&\qquad + \Big[\psi_\ell(-1)\Big]_{\ell 1} \kappa(M\vec{z})\Big)
\end{aligned}$$

as desired.

(c) This follows by applying Lemma 1 and (8) to λ_H. $\square$

We are now in a position to prove a partial result in the direction of Eisenstein reciprocity. (The missing ingredients for Eisenstein reciprocity are the Stickelberger relation for Gauss sums and a version of Theorem 2 below which holds for all $p \neq q$ relatively prime to m.) The classical proof of Theorem 2 is not difficult — it only involves manipulation of Gauss sums (see e.g. **[IR]**). We give the (somewhat more involved) demonstration below to show how Theorem 1 can be considered as a "formal analogue" of reciprocity, just as Honda did for quadratic reciprocity in **[Ho3]**.

Theorem 2. *Let $m \geq 2$, and let p, q be distinct rational primes with $p \equiv 1 \pmod m$, $(q, p-1) = 1$. Let $\mathfrak{p}, \mathfrak{q}$ be primes in $\mathbb{Z}[\zeta_m]$ dividing p and q, respectively. For $\alpha \notin \mathfrak{p}$, let $(\frac{\alpha}{\mathfrak{p}})_m$ denote the m^{th} root of unity such that $\alpha^{\frac{\mathbf{N}\mathfrak{p}-1}{m}} \equiv (\frac{\alpha}{\mathfrak{p}})_m \pmod{\mathfrak{p}}$, where $\mathbf{N}$ denotes the absolute norm. Let*

$$\Phi(\mathfrak{p}) = \left(\sum_{a=1}^{p-1} \left(\frac{a}{\mathfrak{p}}\right)_m^{-1} \zeta_p^a\right)^m.$$

Then

$$\left(\frac{\mathbf{N}\mathfrak{q}}{\mathfrak{p}}\right)_m = \left(\frac{\Phi(\mathfrak{p})}{\mathfrak{q}}\right)_m.$$

Proof. From the corollary, writing $\vec{z} = \xi(\vec{t})$, we have for $2 \leq i, j, k \leq$

$p-1$, $1 \leq \ell \leq p-1$,

$$\sum_{n\geq 1} \frac{1}{n} \operatorname{diag}(\chi_j(n)) \left[\frac{\chi_j(k)-1}{p-1}\right]_{kj} \left(\left[\chi_j(k)^{-1}\right]_{kj} \vec{t}\right)^n$$

$$= \frac{1}{p}\,\frac{1}{p-1}\left[\bar{\chi}_i(\ell)\tau_{\chi_i} + p\right]_{i\ell} \overrightarrow{\log}\left(\vec{1} + \left[\chi_j(-\ell)\tau_{\bar{\chi}_j}\right]_{\ell j} \xi(\vec{t}) + \left[\psi_\ell(-1)\right]_{\ell 1} \kappa(M\xi(\vec{t})\right).$$

Suppose that $\mathrm{Nq} = q^f$, so that $q^f \equiv 1 \pmod{m}$. Let R be as in Corollary 1. Then multiplying both sides by q^f, and taking the result first mod $\deg(q^f+1)$, and then mod $qR\mathbb{Z}[\zeta_{p(p-1)}]$, we have (using the power series expansion of $\overrightarrow{\log}$ and that ξ is a strict isomorphism)

$$\operatorname{diag}(\chi_j(q^f)) \left[\frac{\chi_j(k)-1}{p-1}\right]_{jk} \left(\left[\chi_j(k)^{-1}\right]_{kj} \vec{t}\right)^{q^f}$$

$$\equiv \frac{1}{p}\,\frac{1}{p-1}\left[\bar{\chi}_i(\ell)\tau_{\chi_i} + p\right]_{i\ell} \left(\left[\chi_j(-\ell)\tau_{\bar{\chi}_j}\right]_{\ell j} \vec{t}\right)^{q^f},$$

since κ is without constant or linear term, and q is odd. So

$$\operatorname{diag}(\chi_j(q^f)) \left[\frac{\chi_j(k)-1}{p-1}\right]_{jk} \left[\chi_j^{q^f}(k)^{-1}\right]_{kj} \vec{t}^{\,q^f}$$

$$\equiv \frac{1}{p}\,\frac{1}{p-1}\left[\bar{\chi}_i(\ell)\tau_{\chi_i} + p\right]_{i\ell} \left[\chi_j^{q^f}(-\ell)\tau_{\bar{\chi}_j}^{q^f}\right]_{\ell j} \vec{t}^{\,q^f} \tag{12}$$

$$\pmod{qR\mathbb{Z}[\zeta_{p(p-1)}],\ \deg q^f+1}.$$

Now

$$\left[\bar{\chi}_i(\ell)\tau_{\chi_i} + p\right]_{i\ell} \left[\chi_j^{q^f}(-\ell)\tau_{\bar{\chi}_j}^{q^f}\right]_{\ell j} = \left[\sum_{\ell=1}^{p-1} \bar{\chi}_i(\ell)\chi_j^{q^f}(-\ell)\tau_{\chi_i}\tau_{\bar{\chi}_j}^{q^f} + p\chi_j^{q^f}(-\ell)\tau_{\bar{\chi}_j}^{q^f}\right]_{ij}$$

$$= \left[\chi_j^{q^f}(-1)(p-1)\delta_{\chi_i,\chi_j^{q^f}}\tau_{\chi_i}\tau_{\bar{\chi}_j}^{q^f}\right]_{ij}.$$

So if χ_j is a character of order m, then $\chi_j^{q^f} = \chi_j$, and comparing the coefficient of $t_j^{q^f}$ in the j^{th} entry of (12) gives us

$$\chi_j(q^f) \equiv \frac{1}{p}\,\chi_j(-1)\tau_{\chi_j}\tau_{\bar{\chi}_j}^{q^f} \qquad \pmod{q\mathbb{Z}[\zeta_{p(p-1)}]}.$$

Since $\tau_{\chi_j}\tau_{\bar{\chi}_j} = p\chi_j(-1)$, we have

$$\chi_j(q^f) \equiv \tau_{\bar{\chi}_j}^{q^f-1} \qquad \pmod{q\mathbb{Z}[\zeta_{p(p-1)}]}.$$

In particular, if

$$\chi(n) = \left(\frac{n}{\mathfrak{p}}\right)_m,$$

then χ is a Dirichlet character modulo p of order m, and $\Phi(\mathfrak{p}) = (\tau_\chi)^m \in \mathbb{Z}[\zeta_{p-1}]$, so

$$\chi(q^f) \equiv \Phi(\mathfrak{p})^{\frac{q^f-1}{m}} \qquad (\mathrm{mod}\ q\mathbb{Z}[\zeta_{p(p-1)}])$$

so

$$\chi(q^f) \equiv \Phi(\mathfrak{p})^{\frac{q^f-1}{m}} \qquad (\mathrm{mod}\ q\mathbb{Z}[\zeta_{p-1}]),$$

or

$$\chi(\mathrm{N}\mathfrak{q}) = \left(\frac{\Phi(\mathfrak{p})}{\mathfrak{q}}\right)_m,$$

as desired. □

References

[C] P. Cartier, *Groupes formels, fonctions automorphes et fonctions zêta de courbes elliptiques*, Proc. Internat. Congr. Math. (Nice, 1970), Vol. 2, Gauthier-Villars, Paris, 1971, pp. 290–299.

[CS] N. Childress and J. Stopple, *Formal groups and Dirichlet L-functions*. I and II, J. Number Theory **41** (1992), 283–302.

[D] E. Ditters, *On the classification of commutative formal group laws over p-Hilbert domains and a finiteness theorem for higher Hasse-Witt matrices*, Math. Z. **202** (1989), 83–109.

[DN] C. Deninger and E. Nart, *Formal groups and L-series*, Comment. Math. Helv. **65** (1990), 318–333.

[Ha] M. Hazewinkel, *Formal groups and applications*, Academic Press, New York, 1978.

[Hi] W. Hill, *Formal groups and zeta functions of elliptic curves*, Invent. Math. **12** (1971), 321–336.

[Ho1] T. Honda, *Formal groups and zeta-functions*, Osaka J. Math. **5** (1968), 199–213.

[Ho2] ——, *On the theory of commutative formal groups*, J. Math. Soc. Japan **22** (1970), 213–246.

[Ho3] ——, *Invariant differentials and L-functions: reciprocity laws for quadratic fields and elliptic curves over* $\mathbf{Q}$, Rend. Sem. Mat. Univ. Padova **49** (1973), 323–335.

[I] T. Ibukiyama, *Formal groups and L-functions*, J. Fac. Sci. Univ. Tokyo Sect. 1A Math. **21** (1974), 249–262.

[IR] K. Ireland and M. Rosen, *A classical introduction to modern number theory*, 2nd ed., Springer-Verlag, New York, 1990.

[O] T. Ono, *Arithmetic of algebraic tori*, Ann. of Math. (2) **74** (1961), 101–139.

[Y] N. Yui, *A note on formal groups and zeta functions*, J. Reine Angew. Math. **303/304** (1978), 159–169.

Department of Mathematics, Arizona State University, Tempe, Arizona 85287-1804

E-mail address: `nc@artin.la.asu.edu`

Department of Mathematics, University of Colorado at Boulder, Boulder, Colorado 80309-0395

E-mail address: `grant@boulder.colorado.edu`