J. reine angew. Math. **586** (2006), 91—124

Journal für die reine und angewandte Mathematik

Geometric proofs of reciprocity laws

By *David Grant* at Boulder

The relationship between power reciprocity laws and geometry has a long history: Eisenstein used the arithmetic of torsion points on the elliptic curves $y^2 - y = x^3$ and $y^2 = x^3 - x$ to give proofs of cubic and biquadratic reciprocity. For a description of this and related history, see [C], [BEW], [Hilb], [IR], [Le], [W1], and [W2].

Some years ago, Kubota explored these relationships in [Kub1], and then in [Kub2] used power reciprocity laws to prove a geometric statement. Namely, let F be an abelian extension of the rationals containing a primitive ℓ^{th}-root of unity ζ, and let A be an absolutely simple abelian variety over F with complex multiplication $i : \mathcal{O}_F \to \mathrm{End}(A)$ defined over F by the ring of integers $\mathcal{O}_F$ of F. Then if t is a function in $F(A)$ such that $i(\zeta)^* t = \zeta t$, $\beta \equiv 1 \bmod \ell^2$ is in $\mathcal{O}_F$, and t is regular on the non-trivial β-torsion points $A[\beta]'$ of A, Kubota used power reciprocity laws to prove that

$$\prod_{u \in A[\beta]'} t(u) = \beta^{\sum_{\sigma \in \Phi} c_\sigma \sigma} \rho^\ell, \tag{1}$$

where Φ is the CM-type of (A, i), $c_\sigma \in \mathbb{Z}$ is such that $\zeta^{c_\sigma \sigma} = \zeta$, and $\rho \in F$.

The goal of this paper is to do the converse: to prove formulas like (1) directly for some choices of ℓ, A, t, and torsion points on A, and then to *derive* power reciprocity laws from it. This is a generalization of the approach taken by Eisenstein and which we took in [Gra] to derive quintic reciprocity from the arithmetic of the Jacobian of $y^2 = x^5 + 1/4$.

In sections 7 and 8, for regular primes ℓ, and for some choices of t and torsion points, we will prove a formula like (1) for the A which are the Jacobians of rational images of the ℓ^{th}-Fermat curve, which will allow us to derive the main law of ℓ^{th}-power Kummer reciprocity. Interestingly, if we look at the statement analogous to (1) for certain tori with "complex multiplication," we can similarly derive Eisenstein reciprocity. We do this first in sections 5 and 6 because it sets the stage for the proof of Kummer reciprocity. The statement of the reciprocity laws will be given in section 1.

In deference to the age of the theorems, we have tried to make the paper as elementary and self-contained as possible. The chief tools are the theory of abelian varieties in arbitrary characteristic and the theory of formal groups. Formal groups have many rela-

tions to reciprocity. See for example [I1] on local class field theory, [D] on global class field theory over function fields, [HT] on the local Langlands conjecture, and [Ho] on quadratic reciprocity. Section 2 contains what we will need of the theory of formal groups. The technical heart of the paper is a computation with p-typical formal groups with "complex multiplication" in section 3. From this we derive in section 4 a generalized Stickelberger relation (Theorem 3) which is the basis for the proofs of both reciprocity laws.

Perhaps some explanation is necessary to justify interest at the dawn of the 21st century in new proofs of theorems that were first proved in the 19th century, and which in the 20th century became corollaries of Artin reciprocity. On the one hand, work on the metaplectic group has shown the enduring import of power reciprocity laws in modern number theory, and on the other hand, product formulas in the shape of (1) have applications outside of reciprocity. In section 9 we discuss applications to Gauss sums and Manin-Mumford problems. There has also been recent remarkable work on proofs of power reciprocity laws achieved without the edifice of class field theory [Kub3], [Kub4], [KO], [Hill1], [Hill2]. Finally, Weil described the work of Kummer and Eisenstein on higher reciprocity laws as a place "where quite possibly there are valuable ideas which have not yet been fully exploited; the same can perhaps be said of the connections discovered by Eisenstein between elliptic functions and the cubic and biquadratic reciprocity laws" [W3]. We hope this paper adds to the understanding of those connections.

I would like to thank Nancy Childress for suggesting to me that formal groups could also be used to prove higher reciprocity laws [CG], Charles Matthews for introducing me to Kubota's work and this circle of ideas, John Boxall, Christopher Rowe, and Brett Tangedal for helpful discussions on this material, and the referee for useful comments on an earlier version of this paper. Some of the time the author was working on this paper he was supported by the NSF, and part of the time he was enjoying the hospitality of Columbia University.

§1. Statements of the reciprocity laws

Let ℓ be an odd prime and ζ a primitive ℓ^{th}-root of unity. Then $\mathbb{Z}[\zeta]$ is the ring of integers in $K = \mathbb{Q}(\zeta)$, and $\lambda = 1 - \zeta$ generates the lone prime in $\mathbb{Z}[\zeta]$ above ℓ. Recall that we call an element $\alpha \in \mathbb{Z}[\zeta]$ prime to λ *semi-primary* if it is congruent to a rational integer $\bmod \lambda^2$. Let $\mathfrak{p}$ be a prime ideal of $\mathbb{Z}[\zeta]$ prime to λ, and let $\alpha \in \mathbb{Z}[\zeta]$ be prime to $\mathfrak{p}$. We then define the ℓ^{th}-power residue symbol $\left(\frac{\alpha}{\mathfrak{p}}\right)$ of α on $\mathfrak{p}$ to be the ℓ^{th}-root of unity ζ^i such that

$$\alpha^{(N\mathfrak{p}-1)/\ell} \equiv \zeta^i \mod \mathfrak{p},$$

where N denotes the norm from K to $\mathbb{Q}$.

We extend the definition to non-prime ideals by the formula

$$\left(\frac{\alpha}{\mathfrak{ab}}\right) = \left(\frac{\alpha}{\mathfrak{a}}\right)\left(\frac{\alpha}{\mathfrak{b}}\right),$$

and to integral elements by the rule

$$\left(\frac{\alpha}{\beta}\right) = \left(\frac{\alpha}{(\beta)}\right).$$

Eisenstein proved the following in 1850 [E].

Theorem 1 (Eisenstein reciprocity). *Let $a \in \mathbb{Z}$ be prime to ℓ, and $\alpha \in \mathbb{Z}[\zeta]$ semi-primary and prime to a. Then*

$$\left(\frac{\alpha}{a}\right) = \left(\frac{a}{\alpha}\right).$$

Recall that we call a semi-primary element $\alpha \in \mathbb{Z}[\zeta]$ *primary* if α times its complex conjugate $\bar{\alpha}$ is congruent to a rational integer mod $\lambda^{\ell-1}$. Now take ℓ to be a regular prime, so that if h is the class number of K, then h is not divisible by ℓ. Kummer proved that if α is prime to λ, then α has a primary associate, and that any unit which is primary is the ℓ^{th}-power of a unit [Hilb], Thms. 156, 157. Let h^* be an integer such that $hh^* \equiv 1 \bmod \ell$. Now let $\mathfrak{p}$ and $\mathfrak{q}$ be any distinct prime ideals of $\mathbb{Z}[\zeta]$ prime to λ. We then define

$$\left(\frac{\mathfrak{p}}{\mathfrak{q}}\right) = \left(\frac{\alpha^{h^*}}{\mathfrak{q}}\right),$$

where α is any primary generator of the principal ideal $\mathfrak{p}^h$. It follows by the above that the definition is independent of the choices of α and h^*.

Kummer proved the following in 1858 [Kum].

Theorem 2 (Kummer reciprocity). *Let $\mathfrak{p}$ and $\mathfrak{q}$ be distinct prime ideals in $\mathbb{Z}[\zeta]$ prime to λ. Then*

$$\left(\frac{\mathfrak{p}}{\mathfrak{q}}\right) = \left(\frac{\mathfrak{q}}{\mathfrak{p}}\right).$$

If $\mathfrak{a}$ and $\mathfrak{b}$ are any relatively prime ideals in $\mathbb{Z}[\zeta]$ prime to λ, we can extend the definition of the ℓ^{th}-power residue symbol by bilinearity to $\left(\frac{\mathfrak{a}}{\mathfrak{b}}\right)$, and then Theorem 2 is equivalent to

$$\left(\frac{\mathfrak{a}}{\mathfrak{b}}\right) = \left(\frac{\mathfrak{b}}{\mathfrak{a}}\right).$$

Remark. In what follows, we will let $\Delta = \mathrm{Gal}(K/\mathbb{Q})$, and for $n \in (\mathbb{Z}/\ell\mathbb{Z})^\times$, let $\sigma_n \in \Delta$ denote the element such that $\sigma_n(\zeta) = \zeta^n$. The odd prime ℓ will be arbitrary, except in section 8, where it is assumed to be regular. For a prime p, we let $\mathbb{Z}_{(p)} = (\mathbb{Z} - p\mathbb{Z})^{-1}\mathbb{Z}$.

§2. Preliminaries on formal groups

We need a variety of results on formal groups, for which we refer to [Ha] as a general reference. We recall what we can for the ease of exposition.

Let A be a commutative ring with identity, and W, X, and Y be column vectors of g variables. We say a g-tuple of power series over A, $\mathscr{F} = {}^t(\mathscr{F}_1, \ldots, \mathscr{F}_g)$ in $2g$-variables defines a g-dimensional *formal group* (law) over A if

$$\mathscr{F}(X, Y) = X + Y + (d^o \geqq 2), \quad \mathscr{F}\big(\mathscr{F}(W, X), Y\big) = \mathscr{F}\big(W, \mathscr{F}(X, Y)\big),$$

where $(d^o \geqq m)$ denotes a g-tuple of power series, all of whose terms are of total degree at least m. If in addition $\mathscr{F}(X, Y) = \mathscr{F}(Y, X)$, then $\mathscr{F}$ is a *commutative* formal group. We will assume throughout that all our formal groups are commutative. We will also write $X +_{\mathscr{F}} Y$ for $\mathscr{F}(X, Y)$.

If $\mathscr{F}$, $\mathscr{G}$ are, respectively, g- and h-dimensional formal groups over A, a *homomorphism* $\phi : \mathscr{F} \to \mathscr{G}$ over A is an h-tuple of power series ϕ in g-variables over A, without constant terms, such that $\phi\big(\mathscr{F}(X, Y)\big) = \mathscr{G}\big(\phi(X), \phi(Y)\big)$. If $\rho : A \to B$ is a ring homomorphism, applying ρ to the coefficients of $\mathscr{F}$ and $\mathscr{G}$ give formal groups over B and applying ρ to ϕ gives a homomorphism over B we call, respectively, the *reduced* formal groups and homomorphism. We will assume throughout that our homomorphisms are always between formal groups of the same dimension.

Let $\psi = {}^t(\psi_1, \ldots, \psi_g)$ be a g-tuple of power series in g-variables $T = {}^t(t_1, \ldots, t_g)$ over A without constant terms, and suppose the linear term of $\psi_i(T)$ is $\sum_{k=1}^{g} a_{ik} t_k$. We call the matrix $[a_{ik}]_{1 \leqq i,k \leqq g}$ the *jacobian* $j(\psi)$ of ψ. By definition, a homomorphism ϕ of formal groups is an *isomorphism* if it has a two-sided inverse. The following is elementary.

Lemma 1. *A homomorphism ϕ between two formal groups of the same dimension over a ring A is an isomorphism if and only if $j(\phi)$ is an invertible matrix over A.*

If $j(\phi)$ is the identity, we say that ϕ is a *strict isomorphism*. Part (a) of the following is (A.4.7) in [Ha]. Its proof can be easily adapted to give part (b).

Lemma 2 (Formal implicit function theorem). *Let U be an m-tuple of variables and S be an n-tuple of variables. Let $F(U, S)$ be an n-tuple of power series over A in the variables U and S without constant terms. Suppose that when F is evaluated at $U = 0$ its jacobian with respect to S is invertible over A.*

(a) *Then there exists a unique n-tuple α of power series in m-variables over A such that $F\big(U, \alpha(U)\big) = 0$.*

(b) *If A is a complete discrete valuation ring with maximal ideal $\mathfrak{m}$, then the solutions to $F(U, S) = 0$ in $\mathfrak{m}^{m+n}$ are precisely the solutions $S = \alpha(U)$, $U \in \mathfrak{m}^m$.*

Let p be a prime number. We now need to recall some of the properties of p-typical formal groups. The theory is considerably simpler if A is a *characteristic* 0 *ring*, by which we mean that $A \to A \otimes \mathbb{Q}$ is an injection. From now on A will denote a characteristic 0 ring.

Let $\mathscr{F}$ be a g-dimensional formal group over A and t a variable. We consider the set of *curves*

$$C(\mathscr{F}) = \{\gamma(t) \mid \gamma \in A[[t]]^g, \gamma(0) = 0\}.$$

Then $C(\mathscr{F})$ is a group under the operation

$$(\gamma_1 +_{\mathscr{F}} \gamma_2)(t) = \mathscr{F}\big(\gamma_1(t), \gamma_2(t)\big).$$

If $\alpha \in \mathrm{End}(\mathscr{F})$, $\gamma(t) \in C(\mathscr{F})$, then $\hat{\alpha}(\gamma)(t) = \alpha\big(\gamma(t)\big)$ is a curve, so we get a map $v : \mathrm{End}(\mathscr{F}) \to \mathrm{End}\big(C(\mathscr{F})\big)$ by $v(\alpha) = \hat{\alpha}$. This turns $C(\mathscr{F})$ into an $\mathrm{End}(\mathscr{F})$-module.

On $C(\mathscr{F})$ we define operators:

Homothety: For any $a \in A$, $\leqq a \geqq \gamma(t) = \gamma(at)$.

Verschiebung: For any $n \geqq 1$, $V_n\gamma(t) = \gamma(t^n)$.

These operators commute with the group structure and module structure v on $C(\mathscr{F})$, so can be considered as endomorphisms of the $\mathrm{End}(\mathscr{F})$-module $C(\mathscr{F})$.

There is a unique strict isomorphism (called the *logarithm* of $\mathscr{F}$), $\log_{\mathscr{F}} : \mathscr{F} \to \hat{\mathbb{G}}_a^g$, defined over $A \otimes \mathbb{Q}$, from $\mathscr{F}$ to the g-dimensional formal additive group, which is defined by $\hat{\mathbb{G}}_a^g(X, Y) = X + Y$.

A curve γ is called *p-typical* if $\log_{\mathscr{F}} \gamma(t) = \sum_{i \geqq 0} a_i t^{p^i}$, for some column vectors $a_i \in (A \otimes \mathbb{Q})^g$. The formal group $\mathscr{F}$ is called *p-typical* if its logarithm is of the form

$$\log_{\mathscr{F}}(T) = \sum_{n \geqq 0} A_n{}^t(t_1^{p^n}, \ldots, t_g^{p^n}),$$

where $A_n \in M_g(A \otimes \mathbb{Q})$, the ring of $g \times g$ matrices with entries in $A \otimes \mathbb{Q}$. If $\mathscr{F}$ is p-typical, then the curve $\delta_i(t)$, which is defined to be 0 in all components except in the i^{th}, where it is t, is p-typical.

The following is established by taking logarithms of both sides.

Lemma 3. *Let $\mathscr{F}$ be a g-dimensional p-typical formal group over a characteristic* 0 *ring. Then*

$$\begin{pmatrix} t_1 \\ \vdots \\ t_g \end{pmatrix} = \begin{pmatrix} t_1 \\ \vdots \\ 0 \end{pmatrix} +_{\mathscr{F}} \cdots +_{\mathscr{F}} \begin{pmatrix} 0 \\ \vdots \\ t_g \end{pmatrix} = \delta_1(t_1) +_{\mathscr{F}} \cdots +_{\mathscr{F}} \delta_g(t_g).$$

Suppose from now on that A is a characteristic 0 ring and a $\mathbb{Z}_{(p)}$-algebra. Then any formal group $\mathscr{J}$ over A is strictly isomorphic to a p-typical formal group $\mathscr{F}$, which can be constructed as follows [Ha], (16.4.15). Given the logarithm of $\mathscr{J}$

$$\log_{\mathscr{J}}(T) = \sum_{\substack{N=(n_1,\ldots,n_g),\, n_i \geqq 0 \\ N \neq (0,\ldots,0)}} a_N t_1^{n_1} \cdots t_g^{n_g}, \quad a_N \in (A \otimes \mathbb{Q})^g,$$

we form the g-tuple

$$f(T) = \sum_{n \geqq 0} A_n {}^t(t_1^{p^n}, \ldots, t_g^{p^n}), \quad A_n \in M_g(A \otimes \mathbb{Q}),$$

by omitting those terms in $\log_{\mathscr{J}}$ that are not powers of some t_i with an exponent which is a power of p. Then

$$\mathscr{F}(X, Y) = f^{-1}\big(f(X) + f(Y)\big) \tag{2}$$

is a p-typical formal group over A which is strictly isomorphic over A to $\mathscr{J}$, the isomorphism $\phi : \mathscr{J} \to \mathscr{F}$ being given by $\log_{\mathscr{F}}^{-1} \circ \log_{\mathscr{J}}$. By construction $\log_{\mathscr{F}} = f$. We call $\mathscr{F}$ the *p-typification of $\mathscr{J}$*.

Recall from the last section that ℓ is an odd prime, ζ is a primitive ℓ^{th}-root of unity, $K = \mathbb{Q}(\zeta)$, and $\Delta = \mathrm{Gal}(K/\mathbb{Q})$. Suppose from now on that the prime $p \neq \ell$, and that $\mathbb{Z}[\zeta]$ is a subring of A. Let $\Phi = (\sigma_{n_1}, \ldots, \sigma_{n_g})$ be distinct elements of Δ. We say a g-dimensional formal group $\mathscr{F} = {}^t(\mathscr{F}_1, \ldots, \mathscr{F}_g)$ over A has CM-*type* Φ if for all $1 \leqq i \leqq g$, $\mathscr{F}_i(X, Y)$ is isobaric of weight $n_i \bmod \ell$, when x_j and y_j are given the weight $n_j \bmod \ell$, for all $1 \leqq j \leqq g$. This means the map defined by $\zeta(t_i) = \zeta^{n_i} t_i$ is an endomorphism of $\mathscr{F}$, so we get an embedding $\mathbb{Z}[\zeta] \subseteqq \mathrm{End}(\mathscr{F})$. For $\alpha \in \mathbb{Z}[\zeta]$, we let $[\alpha]$ denote the corresponding endomorphism of $\mathscr{F}$, and write $[\alpha]^* t_i$ for $[\alpha](T)_i$. Let x_i and y_i denote the i^{th} entries of X and Y. By definition, $\mathscr{F}_i(X, Y) = x_i + y_i + (d^o \geqq 2)$ for any $1 \leqq i \leqq g$, so for any rational integer a, $[a]^* t_i = a t_i + (d^o \geqq 2)$, and by the assumption on the CM-type,

$$[\alpha]^* t_i = \sigma_{n_i}(\alpha) t_i + (d^o \geqq 2), \tag{3}$$

for any $\alpha \in \mathbb{Z}[\zeta]$.

Let Z be the $g \times g$ diagonal matrix with diagonal entries $(\zeta^{n_1}, \ldots, \zeta^{n_g})$.

Lemma 4. *Let $\mathscr{J}$ be a g-dimensional formal group with* CM-*type* $\Phi = (\sigma_{n_1}, \ldots, \sigma_{n_g})$ *defined over a characteristic* 0 *ring A which contains $\mathbb{Z}[\zeta]$ as a subring. Further suppose that A is a $\mathbb{Z}_{(p)}$-algebra, and that* $\bigcap_{m \geqq 0} p^m A = 0$.

(a) *For all $1 \leqq i \leqq g$, $\big(\log_{\mathscr{J}}(T)\big)_i$ is isobaric of weight $n_i \bmod \ell$, when t_j is given the weight $n_j \bmod \ell$, for all $1 \leqq j \leqq g$.*

(b) *If $\mathscr{F}$ is the p-typification of $\mathscr{J}$, then for all $1 \leqq i \leqq g$, $\big(\log_{\mathscr{F}}(T)\big)_i$ is isobaric of weight $n_i \bmod \ell$, when t_j is given the weight $n_j \bmod \ell$, for all $1 \leqq j \leqq g$.*

(c) *For all $1 \leqq i \leqq g$, $\big(\log_{\mathscr{F}}^{-1}(T)\big)_i$ is isobaric of weight $n_i \bmod \ell$, when t_j is given the weight $n_j \bmod \ell$, for all $1 \leqq j \leqq g$.*

(d) *If $\phi = (\log_{\mathscr{F}}^{-1}) \circ \log_{\mathscr{J}}$ is the isomorphism from $\mathscr{J}$ to $\mathscr{F}$, then for all $1 \leqq i \leqq g$, $\phi_i(T)$ is isobaric of weight $n_i \bmod \ell$, when t_j is given the weight $n_j \bmod \ell$, for all $1 \leqq j \leqq g$.*

(e) *$\mathscr{F}$ is of* CM-*type* Φ.

Proof. (a) By the hypotheses on A, we have $\log_{\mathscr{J}}(T) = \lim_{m\to\infty} \frac{[p]^m(T)}{p^m}$ [Ha], (11.1.17). Hence $\big(\log_{\mathscr{J}}(T)\big)_i$ is also isobaric of weight $n_i \bmod \ell$, when t_j is given the weight $n_j \bmod \ell$.

(b) This follows immediately from (a) by the construction of $\log_{\mathscr{F}}$.

(c) Since $\log_{\mathscr{F}}(ZT) = Z\log_{\mathscr{F}}(T)$, we get that $ZT = \log_{\mathscr{F}}^{-1}\big(Z\log_{\mathscr{F}}(T)\big)$, so if $T' = \log_{\mathscr{F}}(T)$, then $Z\log_{\mathscr{F}}^{-1}(T') = \log_{\mathscr{F}}^{-1}(ZT')$.

(d) This follows immediately from parts (a) and (c).

(e) This follows immediately from parts (b) and (c) using (2).

If $\mathscr{F}$ is a p-typical formal group, the set of p-typical curves $C_p(\mathscr{F}) \subset C(\mathscr{F})$ forms a subgroup, and is fixed by all the homothety operators, as well as by $V = V_p$. Any $\gamma \in C_p(\mathscr{F})$ can be written uniquely in terms of the "V-basis" δ_i as

$$\gamma = \sum_{q\geqq 0}{}_{\mathscr{F}} \sum_{i=1}^{g}{}_{\mathscr{F}} V^q \leqq a_{q,i} \geqq \delta_i, \tag{4}$$

for some $a_{q,i} \in A$, where $\sum_{\mathscr{F}}$ denotes that the sum is taking place using the group law of $C(\mathscr{F})$.

Let $\mathscr{F}$ be a p-typical formal group over A of CM-type $\Phi = (\sigma_{n_1}, \ldots, \sigma_{n_g})$. Then taking logarithms, it is clear that $[\hat{\zeta}]$ preserves $C_p(\mathscr{F})$. Hence we can consider $\mathbb{Z}[\zeta]$ as endomorphisms of $C_p(\mathscr{F})$ which commute with all homotheties.

For any curve $\gamma = \begin{pmatrix} \gamma_1 \\ \vdots \\ \gamma_g \end{pmatrix} \in C(\mathscr{F})$, we have $[\hat{\zeta}]\gamma = Z\begin{pmatrix} \gamma_1 \\ \vdots \\ \gamma_g \end{pmatrix}$. For $i \in \mathbb{Z}/\ell\mathbb{Z}$, we want to study the $\mathbb{Z}[\zeta]$-submodules $C^i(\mathscr{F}) \subseteqq C_p(\mathscr{F})$, consisting of those γ such that $\leqq \zeta \geqq \gamma = [\hat{\zeta}]^i\gamma$. Note that $C^0(\mathscr{F}) = 0$, since if $\leqq \zeta \geqq \gamma = \gamma$, $\gamma \in C_p(\mathscr{F})$, then γ is isobaric of weight $0 \bmod \ell$, but since $\log_{\mathscr{F}} \gamma(t) = \sum_{n\geqq 0} a_n t^{p^n}$, $a_n \in (A \otimes \mathbb{Q})^g$, and p^n is never $0 \bmod \ell$, we get $\gamma = 0$.

Lemma 5. *Let A be a characteristic 0 ring which is a $\mathbb{Z}_{(p)}$-algebra containing $\mathbb{Z}[\zeta]$ as a subring, and $\mathscr{F}$ be a p-typical formal group over A of* CM*-type for some Φ.*

(a) *Taking the sum in $C_p(\mathscr{F})$, we get $C_p(\mathscr{F}) = \bigoplus_{i=1}^{\ell-1} C^i(\mathscr{F})$.*

(b) *The $C^i(\mathscr{F})$ are $\mathbb{Z}[\zeta]$-modules preserved by the homothety operators. We also have $V : C^i(\mathscr{F}) \to C^{pi}(\mathscr{F})$.*

Proof. (a) For $1 \leqq j \leqq \ell$, we define the operator

$$\varepsilon_j = \left[\frac{1}{\ell}\right] \sum_{i=0}^{\ell-1}{}_{\mathscr{F}} [\hat{\zeta}]^{-ij} \leqq \zeta^i \geqq.$$

A calculation shows that the ε_j, $1 \leqq j \leqq \ell$, are commuting idempotents whose sum (using the group law in $\mathrm{End}(C_p(\mathscr{F}))$) is the identity. Finally, a calculation shows that $C^i(\mathscr{F}) = \varepsilon_i C_p(\mathscr{F})$, and we have shown $C^0(\mathscr{F}) = 0$.

(b) The first statement is clear since the idempotents commute with $\mathbb{Z}[\zeta]$ and homotheties. Take $\gamma \in C^i(\mathscr{F})$. The second statement follows from

$$\leqq \zeta \geqq V\gamma = V \leqq \zeta^p \geqq \gamma = V[\widehat{\zeta^{pi}}]\gamma = [\widehat{\zeta^{pi}}]V\gamma.$$

Now let k be a field of characteristic $p > 0$. Let $\mathscr{F}, \mathscr{G}$, be g-dimensional formal groups over k, and let $\alpha : \mathscr{F} \to \mathscr{G}$ be a homomorphism over k. Using the theory of p-typical formal groups, it is shown in [Ha], (28.2.6), that there are isomorphisms of formal groups $\phi : \mathscr{F} \to \mathscr{F}'$, $\psi : \mathscr{G} \to \mathscr{G}'$, such that the homomorphism $\beta = \psi \circ \alpha \circ \phi^{-1}$ is of the form

$$\beta({}^t(t_1, \ldots, t_g)) = {}^t(t_1^{p^{h_1}}, \ldots, t_r^{p^{h_r}}, 0, \ldots, 0).$$

If $r = g$, we call α an *isogeny*. Hence α is an isogeny if and only if $k[[t_1, \ldots, t_g]]$ is a finitely-generated module over the subring $k[[\alpha_1(t_1, \ldots, t_g), \ldots, \alpha_g(t_1, \ldots, t_g)]]$, and if so, $k[[t_1, \ldots, t_g]]$ is in fact free over $k[[\alpha_1(t_1, \ldots, t_g), \ldots, \alpha_g(t_1, \ldots, t_g)]]$ of rank p^h, $h = \sum_{i=1}^{g} h_i$. We call $h = \mathrm{ht}(\alpha)$ the *height* of the isogeny α. Using this, the following is easy to establish.

Lemma 6. *Let $\alpha : \mathscr{F} \to \mathscr{G}$ and $\beta : \mathscr{G} \to \mathscr{H}$ be homomorphisms of formal groups over k.*

(a) *If α and β are isogenies, then so is their composite, and*

$$\mathrm{ht}(\beta \circ \alpha) = \mathrm{ht}(\alpha) + \mathrm{ht}(\beta).$$

(b) *If $\beta \circ \alpha$ is an isogeny, then so are α and β.*

If now A is any ring, and $\mathfrak{m}$ is a maximal ideal of A with residue field k of characteristic $p > 0$, and α is a homomorphism over A from a formal group $\mathscr{F}$ over A to a formal group $\mathscr{G}$ over A, we define $\mathrm{ht}_{\mathfrak{m}}(\alpha)$, the *height of α at $\mathfrak{m}$*, to be the height of the reduced homomorphism $\tilde{\alpha}$ over k from the reduced formal group $\tilde{\mathscr{F}}$ over k to the reduced formal group $\tilde{\mathscr{G}}$ over k.

§3. A calculation with formal groups

Throughout the rest of the paper, we fix the following notation. Let p be a prime different from ℓ, and $\mathfrak{p}$ be a prime of K above p. Let D be the decomposition group of $\mathfrak{p}$ in Δ, and $f = \#(D)$. Let R be the completion of $\mathbb{Z}[\zeta]$ at $\mathfrak{p}$, $K_{\mathfrak{p}}$ be its fraction field, and let $\mathfrak{P}$ denote the maximal ideal of R. Let L denote an algebraic closure of $K_{\mathfrak{p}}$, $\mathcal{O}$ its ring of integers, and $\mathfrak{m}$ the maximal ideal of $\mathcal{O}$.

Let $\mathscr{F}$ be a formal group of dimension g defined over R with CM type $\Phi = (\sigma_{n_1}, \ldots, \sigma_{n_g})$. For $x, y \in \mathfrak{m}^g$, defining the sum of x and y as $\mathscr{F}(x, y) \in \mathfrak{m}^g$ gives a group structure on $\mathfrak{m}^g$ we denote by $\mathscr{F}(\mathfrak{m})$, which is also a $\mathbb{Z}[\zeta]$-module. For any $\alpha \in \mathbb{Z}[\zeta]$

we denote the corresponding endomorphism of $\mathscr{F}$ as $[\alpha]$, which we think of as g-tuple of power series in the variables $T = {}^t(t_1, \ldots, t_g)$, and whose i^{th}-component we write as $[\alpha]^* t_i$. We let $\mathscr{F}[\alpha]$ denote the α-torsion in $\mathscr{F}(\mathfrak{m})$, which is the set of simultaneous solutions to the power series equations $[\alpha]^* t_i = 0$ for $1 \leqq i \leqq g$. For an ideal $\mathfrak{a} \subseteqq \mathbb{Z}[\zeta]$, we let $\mathscr{F}[\mathfrak{a}] = \bigcap_{\alpha \in \mathfrak{a}} \mathscr{F}[\alpha]$. We let $\mathscr{F}[\mathfrak{a}]'$ denote the non-zero elements of $\mathscr{F}[\mathfrak{a}]$. We can also view T as a set of coordinate functions on $\mathscr{F}[\mathfrak{a}]$, so for $u = {}^t(u_1, \ldots, u_g) \in \mathscr{F}[\mathfrak{a}]$, we will also write $t_i(u)$ for u_i.

Let s be the number of cosets of D in Δ which have non-trivial intersection with Φ, let W_r, $1 \leqq r \leqq s$, denote these intersections, and $d_r = \#(W_r)$. We arbitrarily choose an element $\sigma_{m_r} \in W_r$ for each $1 \leqq r \leqq s$. We call such an ordering of $W_1, \ldots, W_s$ and selection of $\sigma_{m_r} \in W_r$ a *choice of type coset representatives*, and denote a given choice by $c = c(p, \Phi)$. Since σ_p generates D, given such a choice c we have $W_r = \{\sigma_{m_r}\sigma_p^{e_{r,1}}, \ldots, \sigma_{m_r}\sigma_p^{e_{r,d_r}}\}$, for some integers

$$0 = e_{r,1} < \cdots < e_{r,d_r} < f. \tag{5}$$

So for each $1 \leqq i \leqq g$, there are unique $1 \leqq r \leqq s$ and $1 \leqq j \leqq d_r$ such that $\sigma_{n_i} = \sigma_{m_r}\sigma_p^{e_{r,j}}$. Mapping i into these r and j, and considering $j \bmod d_r$, defines a bijection from $\{1, \ldots, g\}$ to the disjoint union $\mathbb{Z}/d_1\mathbb{Z} \amalg \cdots \amalg \mathbb{Z}/d_s\mathbb{Z}$. We denote the inverse of this bijection as χ, so for any $1 \leqq r \leqq s$ and $j \in \mathbb{Z}/d_r\mathbb{Z}$ we have

$$\sigma_{n_{\chi(r,j)}} = \sigma_{m_r}\sigma_p^{e_{r,j}}. \tag{6}$$

We call χ the *exponential indexing* of $\{1, \ldots, g\}$ corresponding to c.

If there is an element $\alpha_\mathfrak{p} \in \mathbb{Z}[\zeta]$ such that $[\alpha_\mathfrak{p}]$ reduces to the Frobenius morphism on $\mathscr{F} \bmod \mathfrak{P}$, and such that the ideal it generates has a factorization

$$(\alpha_\mathfrak{p}) = \prod_{1 \leqq r \leqq s} \sigma_{m_r}^{-1}(\mathfrak{p})^{b_r}, \quad b_r \geqq 0, \quad \sum_{r=1}^{s} b_r = g, \tag{7}$$

then we say $\alpha_\mathfrak{p}$ satisfies a *weak congruence relation*. If $b_r = d_r$ for each $1 \leqq r \leqq s$, then

$$(\alpha_\mathfrak{p}) = \prod_{\sigma \in \Phi} \sigma^{-1}(\mathfrak{p}), \tag{8}$$

and we say $\alpha_\mathfrak{p}$ satisfies the *strong congruence relation*.

For any integer a and positive integer n, let $\langle a \rangle_n$ and $\langle a \rangle^n$ denote respectively the least non-negative and the least positive residue of $a \bmod n$, and let $\langle a \rangle$ denote $\langle a \rangle_\ell$.

Proposition 1. *Suppose that $\mathscr{F}$ is a g-dimensional p-typical formal group over R with* CM *type $\Phi = (\sigma_{n_1}, \ldots, \sigma_{n_g})$. Let $c(p, \Phi)$ be a choice of type coset representatives and $\chi(r, j)$, $1 \leqq r \leqq s$, $j \in \mathbb{Z}/d_r\mathbb{Z}$, be the corresponding exponential indexing of $\{1, \ldots, g\}$.*

Suppose there is an $\alpha_\mathfrak{p} \in \mathbb{Z}[\zeta]$ such that $[\alpha_\mathfrak{p}]$ reduces to the Frobenius on $\mathscr{F} \bmod \mathfrak{P}$, and which satisfies a weak congruence relation (7).

(a) *Then we have the strong congruence relation* (8).

(b) *Suppose further that* $\mathscr{F}[\sigma_{m_r}^{-1}(\mathfrak{p}^{d_r})]$ *is a rank-one* $\mathbb{Z}[\zeta]/\mathfrak{p}^{d_r}$*-module for every* $1 \leqq r \leqq s$. *Then for any* $1 \leqq r \leqq s$, $j \in \mathbb{Z}/d_r\mathbb{Z}$,

$$\operatorname{ord}_{\mathfrak{p}} \prod_{u \in \mathscr{F}[\sigma_{m_r}^{-1}(\mathfrak{p})]'} t_{\chi(r,j)}(u) = \sum_{z \in \mathbb{Z}/d_r\mathbb{Z}} p^{\langle e_{r,j} - e_{r,z} \rangle_f},$$

where $T = {}^t(t_1, \ldots, t_g)$ *are the coordinate functions on* $\mathscr{F}[\sigma_{m_r}^{-1}(\mathfrak{p})]$.

Proof. For any r, $1 \leqq r \leqq s$, by the Chinese remainder theorem, there is a $\pi_r \in \mathbb{Z}[\zeta]$ such that $\operatorname{ord}_{\sigma_{m_r}^{-1}(\mathfrak{p})} \pi_r = 1$, and $\operatorname{ord}_{\sigma(\mathfrak{p})} \pi_r = 0$, for all $\sigma^{-1} \notin \sigma_{m_r} D$. Hence

$$\prod_{r=1}^{s} \pi_r^{b_r} = \alpha_{\mathfrak{p}} \beta, \tag{9}$$

for some $\beta \in \mathbb{Z}[\zeta]$ prime to p.

For any $1 \leqq r \leqq s$, $j \in \mathbb{Z}/d_r\mathbb{Z}$, writing $[\widehat{\pi}_r]\delta_{\chi(r,j)}$ in terms of the V-basis $\delta_1, \ldots, \delta_g$ as in (4), we have

$$[\widehat{\pi}_r]\delta_{\chi(r,j)} = \sum_{k=1}^{s}{}_{\mathscr{F}} \sum_{z \in \mathbb{Z}/d_k\mathbb{Z}}{}_{\mathscr{F}} \sum_{q \geqq 0}{}_{\mathscr{F}} V^q \leqq a_{q,k,z} \geqq \delta_{\chi(k,z)}, \tag{10}$$

for some $a_{q,k,z} \in R$.

Using the decomposition of Lemma 5, we can equate the $C^b(\mathscr{F})$-components of the curves in both sides of (10) for $1 \leqq b \leqq \ell - 1$. Also by Lemma 5 we have induced maps on curves, $[\widehat{\pi}_r] : C^b(\mathscr{F}) \to C^b(\mathscr{F})$, and $V : C^b(\mathscr{F}) \to C^{pb}(\mathscr{F})$. Hence since $\delta_{\chi(r,j)} \in C^{n_{\chi(r,j)}^{-1}}(\mathscr{F})$, so is $[\widehat{\pi}_r]\delta_{\chi(r,j)}$. Now $V^q \leqq a_{q,k,z} \geqq \delta_{\chi(k,z)} \in C^{n_{\chi(r,j)}^{-1}}(\mathscr{F})$ implies that $p^q n_{\chi(k,z)}^{-1} \equiv n_{\chi(r,j)}^{-1} \bmod \ell$. So since σ_p generates D, for $a_{q,k,z}$ to be non-zero, by (6) we need that $n_{\chi(k,z)} = p^q(p^{e_{r,j}} m_r) \bmod \ell$, which implies that $\sigma_{n_{\chi(k,z)}} \in W_r$, and hence $k = r$. But this implies that $p^{e_{r,z}} \equiv p^{q+e_{r,j}} \bmod \ell$, which holds if and only if $e_{r,z} \equiv q + e_{r,j} \bmod f$. So we have that

$$[\widehat{\pi}_r]\delta_{\chi(r,j)} = \sum_{z \in \mathbb{Z}/d_r\mathbb{Z}}{}_{\mathscr{F}} \sum_{\substack{q \equiv e_{r,z} - e_{r,j} \bmod f \\ q \geqq 0}}{}_{\mathscr{F}} V^q \leqq a_{q,r,z} \geqq \delta_{\chi(r,z)} \tag{11}$$

$$= \leqq a_{0,r,j} \geqq \delta_{\chi(r,j)} +_{\mathscr{F}} \sum_{\substack{z \in \mathbb{Z}/d_r\mathbb{Z} \\ m \geqq 0}}{}_{\mathscr{F}} V^{\langle e_{r,z} - e_{r,j} \rangle^f + mf} \leqq a_{\langle e_{r,z} - e_{r,j} \rangle^f + mf, r, z} \geqq \delta_{\chi(r,z)}.$$

Writing (11) as a power series in the variable t we have

$$\left([\widehat{\pi}_r]\delta_{\chi(r,j)}(t)\right)_{\chi(r,j)} = a_{0,r,j}t + (d^o \geqq 2), \tag{12}$$

but from (3) (taking $t_{\chi(r,j)} = t$, $t_v = 0$ for $v \neq \chi(r,j)$), we have

$$\left([\widehat{\pi}_r]\delta_{\chi(r,j)}(t)\right)_{\chi(r,j)} = \sigma_{n_{\chi(r,j)}}(\pi_r)t + (d^o \geqq 2). \tag{13}$$

Suppose now that $b_r > 0$. Comparing (12) and (13) gives $a_{0,r,j} = \sigma_{n_{\chi(r,j)}}(\pi_r) \equiv 0 \bmod \mathfrak{P}$. Note therefore that we can rewrite (11) as

$$[\widehat{\pi_r}]\delta_{\chi(r,j)}(t) = \leqq \sigma_{n_{\chi(r,j)}}(\pi_r) \geqq \delta_{\chi(r,j)}(t) +_{\mathscr{F}} V^{\langle e_{r,j+1}-e_{r,j}\rangle^f}\gamma_{\chi(r,j)}(t), \tag{14}$$

where

$$\gamma_{\chi(r,j)}(t) = \sum_{\substack{z\in\mathbb{Z}/d_r\mathbb{Z}\\ m\geqq 0}}{}_{\mathscr{F}} V^{\langle e_{r,z}-e_{r,j+1}\rangle_f+mf} \leqq a_{\langle e_{r,z}-e_{r,j}\rangle^f+mf,r,z} \geqq \delta_{\chi(r,z)}(t), \tag{15}$$

$$= \leqq a_{\langle e_{r,j+1}-e_{r,j}\rangle^f,r,j+1} \geqq \delta_{\chi(r,j+1)}(t) + (d^o \geqq 2),$$

since by (5), $\langle e_{r,z} - e_{r,j}\rangle^f$ is minimized when $z \equiv j+1 \bmod d_r$.

From Lemma 3, we have for variables $T = {}^t(t_1, \ldots, t_g)$ that

$$[\pi_r](T) = [\pi_r]\big(\delta_1(t_1) +_{\mathscr{F}} \cdots +_{\mathscr{F}} \delta_g(t_g)\big) = [\widehat{\pi_r}]\delta_1(t_1) +_{\mathscr{F}} \cdots +_{\mathscr{F}} [\widehat{\pi_r}]\delta_g(t_g). \tag{16}$$

Hence from (14) and (16), we have

$$\mathrm{ht}_{\mathfrak{P}}([\pi_r]) \geqq \sum_{j\in\mathbb{Z}/d_r\mathbb{Z}} \langle e_{r,j+1} - e_{r,j}\rangle^f = f. \tag{17}$$

Now $[\alpha_{\mathfrak{p}}]$ reduces mod $\mathfrak{P}$ to the Frobenius morphism on $\mathscr{F}$ mod $\mathfrak{P}$, hence $[\alpha_{\mathfrak{p}}]$ has height fg at $\mathfrak{P}$. By Lemma 1 and (9), $[\beta]$ is an automorphism of $\mathscr{F}$, so Lemma 6 shows that $\prod_{r=1}^{s}[\pi_r^{b_r}]$ has height fg at $\mathfrak{P}$. Hence by Lemma 6 all the inequalities in (17) are equalities, and

$$\mathrm{ht}_{\mathfrak{P}}([\pi_r]) = f. \tag{18}$$

If follows from (15) and (18) that for $j \in \mathbb{Z}/d_r\mathbb{Z}$,

$$a_{\langle e_{r,j+1}-e_{r,j}\rangle^f,r,j+1} \not\equiv 0 \mod \mathfrak{P}. \tag{19}$$

Also by (3), if $1 \leqq k \leqq s$, $k \neq r$, then $[\widehat{\pi_k}]\delta_{\chi(r,z)}(t)$, $z \in \mathbb{Z}/d_r\mathbb{Z}$, is a g-tuple of power series in t of the form $\leqq \sigma_{n_{\chi(r,z)}}(\pi_k) \geqq \delta_{\chi(r,z)}(t) + (d^o \geqq 2)$, where

$$\sigma_{n_{\chi(r,z)}}(\pi_k) \not\equiv 0 \mod \mathfrak{P}. \tag{20}$$

Hence, since $[\alpha_{\mathfrak{p}}]$ reduces mod $\mathfrak{P}$ to the Frobenius morphism on $C_p(\mathscr{F})$, by (9), (15), (19) and (20), we have

$$[\widehat{\pi_r^{b_r}}]\delta_{\chi(r,j)}(t) \equiv \kappa_1 V^E \delta_{\chi(r,j+b_r)}(t) + (d^o \geqq p^E + 1) \mod \mathfrak{P}, \tag{21}$$

$$\prod_{k=1}^{s}[\widehat{\pi_k^{b_k}}]\delta_{\chi(r,j)}(t) \equiv \kappa_2\kappa_1 V^E \delta_{\chi(r,j+b_r)}(t) + (d^o \geqq p^E + 1) \mod \mathfrak{P},$$

$$= [\hat{\beta}][\widehat{\alpha_{\mathfrak{p}}}]\delta_{\chi(r,j)}(t) = [\hat{\beta}]V^f\delta_{\chi(r,j)}(t) \mod \mathfrak{P},$$

where κ_1 and κ_2 are non-zero mod $\mathfrak{P}$, and $E = \sum_{w=1}^{b_r} \langle e_{r,j+w} - e_{r,j} \rangle^f$. From (21) we have $E = f = \sum_{w=1}^{d_r} \langle e_{r,j+w} - e_{r,j} \rangle^f$. Hence whenever $b_r > 0$, we have $b_r = d_r$. Since $\sum_{r=1}^{s} b_r = \sum_{r=1}^{s} d_r = g$, we get $b_r = d_r$ for all $1 \leqq r \leqq s$, which gives part (a).

To show part (b), we first note that by assumption $\mathscr{F}[\alpha_\mathfrak{p}] \cong \prod_{r=1}^{s} \mathscr{F}[\sigma_{m_r}^{-1}(\mathfrak{p}^{d_r})]$, so $\#(\mathscr{F}[\alpha_\mathfrak{p}]) = p^{fg}$. We claim that $\mathscr{F}[\sigma_{m_r}^{-1}(\mathfrak{p}^{d_r})] = \mathscr{F}[\pi_r^{d_r}]$. Indeed, for all $1 \leqq r \leqq s$, $\mathscr{F}[\sigma_{m_r}^{-1}(\mathfrak{p}^{d_r})] \subseteqq \mathscr{F}[\pi_r^{d_r}]$, and since by (9) and Lemma 1, $[\beta]$ is invertible over R, all these inclusions must be equalities. It follows that we can identify $\mathscr{F}[\sigma_{m_r}^{-1}(\mathfrak{p})]$ and $\mathscr{F}[\pi_r]$.

We now fix an r, $1 \leqq r \leqq s$. To compute the value of the functions $t_{\chi(r,j)}$ for $j \in \mathbb{Z}/d_r\mathbb{Z}$ on points of $\mathscr{F}[\pi_r]$, by (16) we need to solve in $\mathscr{F}(\mathfrak{m})$ the simultaneous equations

$$0 = [\pi_r]T = \sum_{1 \leqq k \leqq s}^{\mathscr{F}} \sum_{h \in \mathbb{Z}/d_k\mathbb{Z}}^{\mathscr{F}} [\widehat{\pi}_r]\delta_{\chi(k,h)}(t_{\chi(k,h)}). \tag{22}$$

$$= \sum_{j \in \mathbb{Z}/d_r\mathbb{Z}}^{\mathscr{F}} [\widehat{\pi}_r]\delta_{\chi(r,j)}(t_{\chi(r,j)}) +_{\mathscr{F}} \sum_{\substack{k=1 \\ k \neq r}}^{s\ \mathscr{F}} \sum_{h \in \mathbb{Z}/d_k\mathbb{Z}}^{\mathscr{F}} [\widehat{\pi}_r]\delta_{\chi(k,h)}(t_{\chi(k,h)}).$$

For this it will be convenient to treat $[\widehat{\pi}_r]\delta_{\chi(r,j)}(t_{\chi(r,j)})$ as a specialization of a g-tuple of power series in the two independent variables $x_{\chi(r,j)}$ and $y_{\chi(r,j)}$. So we define

$$[\widehat{\pi}_r]\delta_{\chi(r,j)}(x_{\chi(r,j)}, y_{\chi(r,j)}) = \delta_{\chi(r,j)}(x_{\chi(r,j)}) +_{\mathscr{F}} \gamma_{\chi(r,j)}(y_{\chi(r,j)}), \tag{23}$$

so that by (14), $[\widehat{\pi}_r]\delta_{\chi(r,j)}(x_{\chi(r,j)}, y_{\chi(r,j)}) = [\hat{\pi}_r]\delta_{\chi(r,j)}(t_{\chi(r,j)})$ when we substitute

$$x_{\chi(r,j)} = \sigma_{n_{\chi(r,j)}}(\pi_r)t_{\chi(r,j)} \quad \text{and} \quad y_{\chi(r,j)} = t_{\chi(r,j)}^{p^{\langle e_{r,j+1} - e_{r,j} \rangle^f}}.$$

Note by (15) and (23) that the linear term of $[\hat{\pi}](\delta_{\chi(r,j)})(x_{\chi(r,j)}, y_{\chi(r,j)})$ is

$$\delta_{\chi(r,j)}\big(x_\chi(r,j)\big) + a_{\langle e_{r,j+1} - e_{r,j} \rangle^f, r, j+1}\delta_{\chi(r,j+1)}(y_{\chi(r,j)}). \tag{24}$$

Now solving (22) is equivalent to solving $g + 2d_r$ power series equations, the first g given by

$$0 = \sum_{j \in \mathbb{Z}/d_r\mathbb{Z}}^{\mathscr{F}} [\widehat{\pi}_r]\delta_{\chi(r,j)}(x_{\chi(r,j)}, y_{\chi(r,j)}) +_{\mathscr{F}} \sum_{\substack{k=1 \\ k \neq r}}^{s\ \mathscr{F}} \sum_{h \in \mathbb{Z}/d_k\mathbb{Z}}^{\mathscr{F}} [\widehat{\pi}_r]\delta_{\chi(k,h)}(t_{\chi(k,h)}), \tag{25}$$

and the other $2d_r$ series being

$$\begin{aligned} x_{\chi(r,j)} &= \sigma_{n_{\chi(r,j)}}(\pi_r)t_{\chi(r,j)}, \\ y_{\chi(r,j)} &= t_{\chi(r,j)}^{p^{\langle e_{r,j+1} - e_{r,j} \rangle^f}}, \quad j \in \mathbb{Z}/d_r\mathbb{Z}. \end{aligned} \tag{26}$$

By (24), the linear terms of the series in (25) are:

$$x_{\chi(r,j)} + a_{\langle e_{r,j} - e_{r,j-1} \rangle^f, r, j} y_{\chi(r,j-1)}, \quad j \in \mathbb{Z}/d_r\mathbb{Z},$$

and

$$\sigma_{n_{\chi(k,h)}}(\pi_r)t_{\chi(k,h)}, \quad 1 \leqq k \leqq s,\ k \neq r,\ h \in \mathbb{Z}/d_k\mathbb{Z},$$

where $\sigma_{n_{\chi(k,h)}}(\pi_r)$, $1 \leqq k \leqq s$, $k \neq r$, $h \in \mathbb{Z}/d_k\mathbb{Z}$, and $a_{\langle e_{r,j}-e_{r,j-1}\rangle^f,r,j}$, $j \in \mathbb{Z}/d_r\mathbb{Z}$, are units in R. Hence, for $1 \leqq k \leqq s$, $k \neq r$, $h \in \mathbb{Z}/d_k\mathbb{Z}$, and $j \in \mathbb{Z}/d_r\mathbb{Z}$, by the formal implicit function theorem (Lemma 2) we can identically solve the system (25) by setting

$$\begin{aligned} t_{\chi(k,h)} &= \phi_{\chi(k,h)}(x_{\chi(r,1)}, \ldots, x_{\chi(r,d_r)}), \\ y_{\chi(r,j)} &= \psi_{\chi(r,j)}(x_{\chi(r,1)}, \ldots, x_{\chi(r,d_r)}), \end{aligned} \tag{27}$$

for some power series $\phi_{\chi(k,h)}$, $\psi_{\chi(r,j)}$ with coefficients in R, which have no constant terms, and where the linear term of $\psi_{\chi(r,j)}$ is $-x_{\chi(r,j+1)}/a_{\langle e_{r,j+1}-e_{r,j}\rangle^f,r,j+1}$. The solutions of (22) therefore are same as those of the system gotten by plugging (27) into (26). This gives d_r equations for $j \in \mathbb{Z}/d_r\mathbb{Z}$,

$$a_{\langle e_{r,j+1}-e_{r,j}\rangle^f,r,j+1}t_{\chi(r,j)}^{p^{\langle e_{r,j+1}-e_{r,j}\rangle^f}} = -\sigma_{n_{\chi(r,j+1)}}(\pi_r)t_{\chi(r,j+1)} + (d^o \geqq 2), \tag{28}$$

where the right hand side is a power series in $\sigma_{n_{\chi(r,z)}}(\pi_r)t_{\chi(r,z)}$, $z \in \mathbb{Z}/d_r\mathbb{Z}$. Now let $\pi = \sigma_{m_r}(\pi_r)$, and $|\cdot|$ be an absolute value on L. Note that all the terms of degree at least two in the right hand side of (28) evaluated at any $u \in \mathscr{F}[\sigma_{m_r}^{-1}(\mathfrak{p})]'$ have absolute value less than $|\pi|^2$.

Lemma 7. *For any $u \in \mathscr{F}[\sigma_{m_r}^{-1}(\mathfrak{p})]'$, and all $1 \leqq j \leqq d_r$, $|t_{\chi(r,j)}(u)| \geqq |\pi|$.*

Proof. Fix any $u \in \mathscr{F}[\sigma_{m_r}^{-1}(\mathfrak{p})]'$. Pick a $j = j_0$ such that $|t_{\chi(r,j_0)}(u)|$ is maximal. Comparing terms of (28) of greatest absolute value, we have

$$|t_{\chi(r,j_0-1)}(u)^{p^{\langle e_{r,j_0}-e_{r,j_0-1}\rangle^f}}| = |\pi|\,|t_{\chi(r,j_0)}(u)| \geqq |\pi|\,|t_{\chi(r,j_0-1)}(u)|,$$

by maximality, so since $p^{\langle e_{r,j_0}-e_{r,j_0-1}\rangle^f} \geqq 2$,

$$|t_{\chi(r,j_0-1)}(u)| \geqq |\pi|^{1/(p^{\langle e_{r,j_0}-e_{r,j_0-1}\rangle^f}-1)} \geqq |\pi|.$$

Hence also from (28), comparing terms of greatest absolute value, we have

$$|t_{\chi(r,j_0-2)}(u)^{p^{\langle e_{r,j_0-1}-e_{r,j_0-2}\rangle^f}}| = |\pi|\,|t_{\chi(r,j_0-1)}(u)| \geqq |\pi|^2,$$

and so $|t_{\chi(r,j_0-2)}(u)| \geqq |\pi|$. Hence continuing successively in this manner, we get for all $j \in \mathbb{Z}/d_r\mathbb{Z}$ that $|t_{\chi(r,j)}(u)| \geqq |\pi|$, as desired.

As a consequence of Lemma 7, $t_{\chi(r,j)}(u) \neq 0$ for all $j \in \mathbb{Z}/d_r\mathbb{Z}$ and all $u \in \mathscr{F}[\sigma_{m_r}^{-1}(\mathfrak{p})]'$. So for all $1 \leqq j \leqq d_r$, comparing terms in (28) of greatest absolute value, from Lemma 7 we have

$$|\pi|\,|t_{\chi(r,j)}(u)| = |t_{\chi(r,j-1)}(u)^{p^{\langle e_{r,j}-e_{r,j-1}\rangle^f}}|. \tag{29}$$

Hence applying (29) repeatedly, we have

$$\begin{aligned}
|t_{\chi(r,j)}(u)| &= |t_{\chi(r,j-1)}(u)^{p^{\langle e_{r,j}-e_{r,j-1}\rangle^f}}|/|\pi| \\
&= \left(|t_{\chi(r,j-2)}(u)|^{p^{\langle e_{r,j-1}-e_{r,j-2}\rangle^f}}/|\pi|\right)^{p^{\langle e_{r,j}-e_{r,j-1}\rangle^f}}/|\pi| \\
&= |t_{\chi(r,j-2)}(u)|^{p^{\langle e_{r,j}-e_{r,j-2}\rangle^f}}/|\pi|^{p^{\langle e_{r,j}-e_{r,j-1}\rangle^f}+1} = \cdots \\
&= |t_{\chi(r,j)}(u)|^{p^{\langle e_{r,j}-e_{r,j}\rangle^f}}/|\pi|^{1+p^{\sum_{\substack{z\in\mathbb{Z}/d_r\mathbb{Z}\\ z\neq j}}\langle e_{r,j}-e_{r,z}\rangle^f}} \\
&= |t_{\chi(r,j)}(u)|^{p^f}/|\pi|^{p^{\sum_{z\in\mathbb{Z}/d_r\mathbb{Z}}\langle e_{r,j}-e_{r,z}\rangle_f}}.
\end{aligned}$$

Therefore

$$|t_{\chi(r,j)}(u)|^{p^f-1} = \left|\prod_{v\in\mathscr{F}[\sigma_{m_r}^{-1}(\mathfrak{p})]'} t_{\chi(r,j)}(v)\right| = |\pi|^{\sum_{z\in\mathbb{Z}/d_r\mathbb{Z}} p^{\langle e_{r,j}-e_{r,z}\rangle_f}}.$$

Remark. (1) If each W_r contains only one element (for example, if $f=1$), then the same result holds without assuming $\mathscr{F}$ is p-typical. See the argument in [Gra2].

(2) Since $\phi_{\chi(k,h)}$ has no linear term, $\operatorname{ord}_{\mathfrak{p}}(t_{\chi(k,h)})$ $1\leqq k\leqq s$, $k\neq r$, $h\in\mathbb{Z}/d_k\mathbb{Z}$, is at least twice the minimum of $\operatorname{ord}_{\mathfrak{p}}\left(t_{\chi(r,j)}\right)$, $j\in\mathbb{Z}/d_r\mathbb{Z}$.

§4. Stickelberger relations on certain group varieties

We will say that a commutative group variety G defined over K has CM *by* $\mathbb{Z}[\zeta]$ *over* K if there is an embedding $\varepsilon:\mathbb{Z}[\zeta]\to\operatorname{End}(G)$, whose image consists of endomorphisms $[\alpha]=\varepsilon(\alpha)$ defined over K. For any $\alpha\in\mathbb{Z}[\zeta]$, let $G[\alpha]$ denote the kernel of $[\alpha]$ in an algebraic closure of K, and for any ideal $\mathfrak{a}\subseteqq\mathbb{Z}[\zeta]$, let $G[\mathfrak{a}]=\bigcap_{\alpha\in\mathfrak{a}} G[\alpha]$. Let $G[\mathfrak{a}]'$ be the non-trivial elements of $G[\mathfrak{a}]$. We say the CM of G is *simple at* $\mathfrak{a}$ if for all $n\geqq 1$, $G[\mathfrak{a}^n]$ is a rank-one $\mathbb{Z}[\zeta]/\mathfrak{a}^n$-module.

Let $\mathfrak{p}$ be as in the last section. Note that if G has CM by $\mathbb{Z}[\zeta]$ over K which is simple at $\mathfrak{p}$, then any $\tau\in\operatorname{Gal}\left(K(G[\mathfrak{p}])/K\right)$ acts on $G[\mathfrak{p}]$ via an $[\alpha]$, $\alpha\in\mathbb{Z}[\zeta]/\mathfrak{p}$. We write $\tau=\tau_\alpha$.

Let μ_ℓ denote the group of ℓ^{th}-roots of unity. The following is a generalized Gauss's Lemma, along the lines of [Kub1], which we include for the convenience of the reader.

Lemma 8 (Gauss's Lemma). *Suppose that G is a commutative group variety with* CM *by $\mathbb{Z}[\zeta]$ over K which is simple at $\mathfrak{p}$. Let S be a set of representatives of the orbits of $G[\mathfrak{p}]'$ under the action of μ_ℓ, and $\theta\in K(G)$ a function regular at all points of $G[\mathfrak{p}]'$, such that $[\zeta]^*\theta=\zeta^n\theta$. Then*

$$\tau_\alpha\left(\prod_{u\in S}\theta(u)\right)=\left(\frac{\alpha}{\mathfrak{p}}\right)^n\prod_{u\in S}\theta(u).$$

Proof. The result is trivial if the product vanishes, so suppose that $\prod_{u\in S}\theta(u)\neq 0$. Let v be a basis for $G[\mathfrak{p}]$ as a $\mathbb{Z}[\zeta]/\mathfrak{p}$-vector space. Then we can write $S=Bv$, where B is a set of representatives of the orbits of $(\mathbb{Z}[\zeta]/\mathfrak{p})^{\times}$ under μ_ℓ. Therefore we get that

$$\begin{aligned}\tau_\alpha\Big(\prod_{k\in B}\theta([k]v)\Big)\Big/\Big(\prod_{k\in B}\theta([k]v)\Big)&=\Big(\prod_{k\in B}\theta([\alpha k]v)\Big)\Big/\Big(\prod_{k\in B}\theta([k]v)\Big)\\&=\frac{\prod_{m=1}^{\ell}\prod_{k\in B\cap\alpha^{-1}\zeta^m B}\theta([\alpha k]v)}{\prod_{k\in B}\theta([k]v)}=\frac{\prod_{m=1}^{\ell}\prod_{z\in\zeta^{-m}\alpha B\cap B}\zeta^{nm}\theta([z]v)}{\prod_{k\in B}\theta([k]v)}\\&=\prod_{m=1}^{\ell}\zeta^{nm\#(\{\zeta^{-m}\alpha B\cap B\})},\end{aligned}$$

letting $z=\zeta^{-m}\alpha k$. But the same argument with the function θ' defined on $\mathbb{Z}[\zeta]/\mathfrak{p}$ by $\theta'(k)=k^n$, gives $\bmod\mathfrak{p}$ that

$$\begin{aligned}\prod_{m=1}^{\ell}\zeta^{nm\#(\{\zeta^{-m}\alpha B\cap B\})}&\equiv\frac{\prod_{k\in B}\theta'(\alpha k)}{\prod_{k\in B}\theta'(k)}\\&\equiv\frac{\prod_{k\in B}(\alpha k)^n}{\prod_{k\in B}k^n}\equiv\alpha^{n(N\mathfrak{p}-1)/\ell}\equiv\left(\frac{\alpha}{\mathfrak{p}}\right)^n\mod\mathfrak{p}.\end{aligned}$$

For every $\sigma\in\Delta$, we let R_σ denote the completion of $\mathbb{Z}[\zeta]$ at $\sigma(\mathfrak{p})$, $K_{\sigma(\mathfrak{p})}$ denote its fraction field, and $\mathfrak{P}_\sigma$ denote its maximal ideal. We let L_σ denote an algebraic closure of $K_{\sigma(\mathfrak{p})}$, $\mathcal{O}_\sigma$ be its ring of integers, and $\mathfrak{m}_\sigma$ be the maximal ideal of $\mathcal{O}_\sigma$.

We say a commutative group variety G of dimension g with CM by $\mathbb{Z}[\zeta]$ over K has a *congruence formal group $\mathcal{G}$ at $\mathfrak{p}$ of type $\Phi=(\sigma_{n_1},\dots,\sigma_{n_g})$* if:

(i) There are local parameters $T={}^t(t_1,\dots,t_g)$ at the origin of G, defined over K, such that $[\zeta]^*t_i=\zeta^{n_i}t_i$, and such that for independent generic points x, y on G, setting $\mathcal{G}_i\big(T(x),T(y)\big)$ to be the expansion of $t_i(x+_G y)$ in the completed local ring of the origin, and then setting $\mathcal{G}=(\mathcal{G}_i)_{1\leqq i\leqq\ell}$, defines a formal group over $\mathbb{Z}_{(p)}[\zeta]$ (so is of CM type Φ). We call such a T a *set of parameters for $\mathcal{G}$*.

(ii) G extends to a group scheme $\mathbb{G}$ over $\mathbb{Z}_{(p)}[\zeta]$, and for every $\sigma\in\Phi$, $u\to T(u)$ is an isomorphism from the kernel of reduction of $\mathbb{G}(\mathcal{O}_\sigma)\bmod\mathfrak{m}_\sigma$ to $\mathcal{G}(\mathfrak{m}_\sigma)$. Hence we can also think of T as a set of coordinate functions on $\mathcal{G}(\mathfrak{m}_\sigma)$.

(iii) For every $\sigma\in\Phi$ there is an $\alpha_{\sigma(\mathfrak{p})}\in\mathbb{Z}[\zeta]$ such that $[\alpha_{\sigma(\mathfrak{p})}]$ reduces to the Frobenius on $\mathcal{G}\bmod\mathfrak{P}_\sigma$, and satisfies a weak congruence relation (7) for some (hence any) choice of type coset representatives $c(P,\Phi)$.

Note that if the weak congruence relation (7) holds at some $\sigma(\mathfrak{p})$ for $\sigma\in\Phi$, and if a corresponding $b_r>0$, then (iii) implies that $G\big[\sigma_{m_r}^{-1}\big(\sigma(\mathfrak{p})\big)^{b_r}\big]$ is in the kernel of reduction

mod $\mathfrak{m}_\sigma$, so (ii) implies that we can identify $\mathscr{G}\big[\sigma_{m_r}^{-1}\big(\sigma(\mathfrak{p})\big)^{b_r}\big] = G\big[\sigma_{m_r}^{-1}\big(\sigma(\mathfrak{p})\big)^{b_r}\big]$. Hence if G is a commutative group variety with CM by $\mathbb{Z}[\zeta]$ over K with a congruence formal group at $\mathfrak{p}$ of type Φ, and the CM is simple at $\sigma_{m_r}^{-1}\big(\sigma(\mathfrak{p})\big)$, we get that $\mathscr{G}\big[\sigma_{m_r}^{-1}\big(\sigma(\mathfrak{p})\big)^{b_r}\big]$ is a rank-one $\mathbb{Z}[\zeta]/\mathfrak{p}^{b_r}$-module.

Theorem 3. *Let $\Phi = (\sigma_{n_1}, \ldots, \sigma_{n_g})$, with $n_1 = 1$. Let G be a commutative group variety of dimension g with* CM *by $\mathbb{Z}[\zeta]$ defined over K, which for every $\sigma, \tau \in \Phi$ is simple at $\tau^{-1}\big(\sigma(\mathfrak{p})\big)$, and has a congruence formal group $\mathscr{G}$ at $\mathfrak{p}$ of type Φ.*

Then there is a $w \in K(G)$ satisfying $[\zeta]^* w = \zeta w$, such that

$$\left(\prod_{u \in G[\mathfrak{p}]'} w(u)\right) = \prod_{i=1}^{g} \sigma_{n_i}(\mathfrak{p})^{\langle n_i^{-1} \rangle} \cdot \mathfrak{a}\mathfrak{b}^{\ell},$$

where $\mathfrak{a}$ is a fractional ideal of K prime to $\prod_{\sigma \in \Phi} \sigma(\mathfrak{p})$ which is ℓ^{th}-power free, and $\mathfrak{b}$ is some non-zero fractional ideal.

Proof. Let $c(p, \Phi)$ be a choice of type coset representatives for p and Φ, and let $\chi(r, j)$, $1 \leqq r \leqq s$, $j \in \mathbb{Z}/d_r\mathbb{Z}$ be the corresponding exponential indexing of $\{1, \ldots, g\}$. Let $T = {}^t(t_1, \ldots, t_g)$ be a set of parameters for $\mathscr{G}$.

Let $\mathscr{F}$ be the p-typification of $\mathscr{G}$, and $\phi : \mathscr{G} \to \mathscr{F}$ the accompanying strict isomorphism of formal groups, both defined over $\mathbb{Z}_{(p)}[\zeta]$. By Lemma 4, $\mathscr{F}$ also has CM type Φ, and for every $\sigma \in \Phi$, ϕ induces an isomorphism of $\mathscr{G}(\mathfrak{m}_\sigma)$ and $\mathscr{F}(\mathfrak{m}_\sigma)$ as $\mathbb{Z}[\zeta]$-modules. In particular, if $V = {}^t(v_1, \ldots, v_g) = \phi(T)$, then V is a set of coordinate functions on $\mathscr{F}(\mathfrak{m}_\sigma)$, and $[\alpha_{\sigma(\mathfrak{p})}]$ reduces to the Frobenius endomorphism on $\mathscr{F} \bmod \mathfrak{P}_\sigma$. We can consider $\mathscr{F}$ defined over R_σ, and we can apply Proposition 1 (a) with $\mathfrak{p}$ replaced by $\sigma(\mathfrak{p})$ to show that the strong congruence relation (8) holds. Hence by the discussion above, for any $\sigma \in \Phi$ and $1 \leqq r \leqq s$, $\mathscr{F}\big[\sigma_{m_r}^{-1}\big(\sigma(\mathfrak{p})\big)^{d_r}\big]$ is a rank-one $\mathbb{Z}[\zeta]/\mathfrak{p}^{d_r}$-module. Now we can apply Proposition 1 (b) with $\mathfrak{p}$ replaced by $\sigma(\mathfrak{p})$.

Hence for any $1 \leqq r \leqq s$ and $j \in \mathbb{Z}/d_r\mathbb{Z}$, identifying $G[\mathfrak{p}]$ with $\mathscr{G}[\mathfrak{p}]$ and $\mathscr{F}[\mathfrak{p}]$, we get

$$\operatorname{ord}_{\sigma_{m_r}(\mathfrak{p})} \prod_{u \in G[\mathfrak{p}]'} v_{\chi(r,j)}(u) = \sum_{z \in \mathbb{Z}/d_r\mathbb{Z}} p^{\langle e_{r,j} - e_{r,z} \rangle_f}. \tag{30}$$

By Lemma 4, the i^{th} component of ϕ is a power series ϕ_i with coefficients in $\mathbb{Z}_{(p)}[\zeta][[x_1, \ldots, x_g]]$ which is isobaric of weight $n_i \bmod \ell$ when x_k is given the weight $n_k \bmod \ell$. Now let $\psi_i \in \mathbb{Z}_{(p)}[\zeta][x_1, \ldots, x_g]$ be the truncation of ϕ_i after a sufficiently high power of $x_1, \ldots, x_g$ such that if $w_i = \psi_i(T)$, then $\operatorname{ord}_{\wp_\sigma} w_i(u) = \operatorname{ord}_{\wp_\sigma} v_i(u)$ for every $u \in G[\mathfrak{p}]'$, for every $1 \leqq i \leqq g$, and for every $\sigma \in \Phi$, where $\wp_\sigma$ is the maximal ideal in $K_{\sigma(\mathfrak{p})}(G[\mathfrak{p}])$. Then $w_i \in K(G)$ and $[\zeta]^* w_i = \zeta^{n_i} w_i$. Hence for every $1 \leqq r \leqq s$ and $j \in \mathbb{Z}/d_r\mathbb{Z}$,

$$\operatorname{ord}_{\sigma_{m_r}(\mathfrak{p})} \prod_{u \in G[\mathfrak{p}]'} w_{\chi(r,j)}(u) = \operatorname{ord}_{\sigma_{m_r}(\mathfrak{p})} \prod_{u \in G[\mathfrak{p}]'} v_{\chi(r,j)}(u). \tag{31}$$

In particular, since for every $1 \leqq i \leqq g$, $i = \chi(r, j)$ for some r and some $j \in \mathbb{Z}/d_r\mathbb{Z}$, we have by (30) and (31) that for all $1 \leqq i \leqq g$,

$$\prod_{u \in G[\mathfrak{p}]'} w_i(u) \neq 0.$$

Take $1 \leqq r \leqq s$. Since $p^f \equiv 1 \bmod \ell$ and $e_{r,1} = 0$, letting $j = 1$, the exponent on the right hand side of (30) is

$$(32) \qquad p^{f-e_{r,d_r}} + \cdots + p^{f-e_{r,2}} + 1 \equiv p^{-e_{r,d_r}} + \cdots + p^{-e_{r,1}} \equiv m_r \sum_{\sigma_{n_k} \in W_r} n_k^{-1} \mod \ell.$$

So by (32) and (31) we have, since $\chi(r, 1) = m_r$,

$$(33) \qquad \operatorname{ord}_{\sigma_{m_r}(\mathfrak{p})} \prod_{u \in G[\mathfrak{p}]'} w_{m_r}(u) \equiv m_r \sum_{\sigma_{n_k} \in W_r} n_k^{-1} \mod \ell.$$

Since we required $n_1 = 1$, if $w = w_1$, then $[\zeta]^* w = \zeta w$. Let S be a set of representatives for the orbits of the action of μ_ℓ on $G[\mathfrak{p}]'$. Then by Gauss's Lemma (Lemma 8), it follows that

$$\xi = \prod_{u \in S} w(u)^{m_r} / w_{m_r}(u) \in K,$$

and $\xi^\ell = \prod_{u \in G[\mathfrak{p}]'} w(u)^{m_r} \Big/ \prod_{u \in G[\mathfrak{p}]'} w_{m_r}(u)$, so from (33) we get that

$$(34) \qquad \operatorname{ord}_{\sigma_{m_r}(\mathfrak{p})} \prod_{u \in G[\mathfrak{p}]'} w(u) \equiv \sum_{\sigma_{n_k} \in W_r} n_k^{-1} \mod \ell.$$

Finally, considering (34) for all $1 \leqq r \leqq s$, we have,

$$\left(\prod_{u \in G[\mathfrak{p}]'} w(u) \right) = \prod_{i=1}^{g} \sigma_{n_i}(\mathfrak{p})^{\langle n_i^{-1} \rangle} \cdot \mathfrak{a}\mathfrak{b}^\ell,$$

where $\mathfrak{a}$ is a fractional ideal of K prime to $\prod_{\sigma \in \Phi} \sigma(\mathfrak{p})$ which is ℓ^{th}-power free, and $\mathfrak{b}$ is some non-zero fractional ideal.

Remark. By Remark (1) of section 3, if each W_r contains only one element (for example, if $f = 1$), then we can apply the result of Proposition 1 without assuming $\mathscr{F}$ is p-typical, so we can take the g-tuple of power series ϕ to be the identity in the proof of Theorem 3.

§5. Geometry of J_0

Our proof of Theorem 1 will use the arithmetic of tori with complex multiplication, employed in a different fashion in [CG]. Let G be the group scheme defined over $\mathbb{Z}$ by $x_1 x_2 \ldots x_\ell = 1$. The group morphism $+_G$ for G is given by

$$(x_1, x_2, \ldots, x_\ell) +_G (y_1, y_2, \ldots, y_\ell) = (x_1 y_1, x_2 y_2, \ldots, x_\ell y_\ell),$$

and the inverse morphism is given by $x_i \to \prod_{j \neq i} x_j$. Note that G is isomorphic to the $(\ell-1)$-fold product of the multiplicative group $\mathbb{G}_m$. There is an automorphism z of order ℓ on G defined by $z(x_i) = x_{i+1}$ for $1 \leqq i \leqq \ell - 1$, and $z(x_\ell) = x_1$. Since z commutes with the group morphism and $1 + z + \cdots + z^{\ell-1} = 0$, we get an embedding $\varepsilon : \mathbb{Z}[\zeta] \to \mathrm{End}(G)$, sending $\zeta \to z$. We denote $\varepsilon(\alpha)$ by $[\alpha]$. The origin on G is the $\mathbb{Z}$-point $(1, 1, \ldots, 1)$, and if we set $x_i' = x_i - 1$, then x_i', $1 \leqq i \leqq \ell - 1$, form a set of parameters at the origin of G, and

$$x_\ell' = \sum_{j_i \geqq 0,\, (j_1,\ldots,j_{\ell-1}) \neq (0,\ldots,0)} \prod_{i=1}^{\ell-1} (-x_i')^{j_i} \in \mathbb{Z}[[x_1', \ldots, x_{\ell-1}']]. \tag{35}$$

Using these parameters, we can define a formal group at the origin of G by setting

$$\begin{pmatrix} \vdots \\ \mathscr{G}_i(x_1', \ldots, x_{\ell-1}', y_1', \ldots, y_{\ell-1}') \\ \vdots \end{pmatrix} = \begin{pmatrix} \vdots \\ x_i' \\ \vdots \end{pmatrix} +_G \begin{pmatrix} \vdots \\ y_i' \\ \vdots \end{pmatrix} = \begin{pmatrix} \vdots \\ x_i' + y_i' + x_i' y_i' \\ \vdots \end{pmatrix},$$

which are power series over $\mathbb{Z}$, for $1 \leqq i \leqq \ell - 1$. Then $\mathscr{G} = \{\mathscr{G}_i\}_{1 \leqq i \leqq \ell-1}$ is a formal group over $\mathbb{Z}$, which is just the product of $\ell - 1$ formal multiplicative groups. Since for any i, $[\zeta]^* x_i'$ is a power series in $\mathbb{Z}[[x_1', \ldots, x_{\ell-1}']]$, for any $\alpha \in \mathbb{Z}[\zeta]$, we get an endomorphism $[\alpha] = {}^t(\rho_1, \ldots, \rho_{\ell-1})$ of $\mathscr{G}$ by setting $\rho_i(x_1', \ldots, x_{\ell-1}') = [\alpha]^* x_i'$, $\rho_i \in \mathbb{Z}[[x_1', \ldots, x_{\ell-1}']]$.

Now considering $\mathscr{G}$ as a formal group over the p-adic integers $\mathbb{Z}_p$, if M is an algebraic closure of $\mathbb{Q}_p$, $\mathcal{O}_M$ is its ring of integers, and $\mathfrak{m}_M$ the maximal ideal of $\mathcal{O}_M$, we get an isomorphism from the kernel of reduction of $G(\mathcal{O}_M) \bmod \mathfrak{m}_M$ to $\mathscr{G}(\mathfrak{m}_M)$ via $u \to \big(x_1'(u), \ldots, x_{\ell-1}'(u)\big)$, the inverse being given by

$$(v_1, \ldots, v_{\ell-1}) \to \left(1 + v_1, \ldots, 1 + v_{\ell-1}, 1 + \sum_{j_i \geqq 0,\, (j_1,\ldots,j_{\ell-1}) \neq (0,\ldots,0)} \prod_{i=1}^{\ell-1} (-v_i)^{j_i}\right).$$

Define t_i, $1 \leqq i \leqq \ell$, by

$$t_i = \sum_{j=1}^{\ell} \zeta^{-ij} x_j'. \tag{36}$$

Since $[\zeta^{-ij}]_{1 \leqq i,j \leqq \ell}^{-1} = \dfrac{1}{\ell} [\zeta^{jk}]_{1 \leqq j,k \leqq \ell}$, we get that

$$1 = \prod_{j=1}^{\ell} \left(1 + (1/\ell) \sum_{k=1}^{\ell} \zeta^{jk} t_k\right)$$

defines a group scheme J_0 over $\mathbb{Z}\left[\dfrac{1}{\ell}\right]$ which is isomorphic to G over $\mathbb{Z}\left[\dfrac{1}{\ell}\right][\zeta]$.

Let $g = \ell - 1$, and $\Phi_0 = (\sigma_{n_1}, \ldots, \sigma_{n_g}) = (\sigma_1, \ldots, \sigma_g)$.

Proposition 2. (a) *J_0 is a commutative group variety of dimension g with* CM *by $\mathbb{Z}[\zeta]$ defined over K which is simple at $\tau^{-1}(\sigma(\mathfrak{p}))$ for every $\sigma, \tau \in \Phi_0$.*

(b) *J_0 has a congruence formal group at $\mathfrak{p}$ of type Φ_0.*

Proof. (a) Note that by (36),

$$[\zeta]^* t_i = \zeta^i t_i, \tag{37}$$

so J_0 has CM by $\mathbb{Z}[\zeta]$ defined over K. For every $n \geqq 1$, the points of $G[p^n]$ are of the form $(\zeta_{p^n}^{c_1}, \ldots, \zeta_{p^n}^{c_\ell})$, $\sum_{i=1}^{\ell} c_i \equiv 0 \bmod p^n$, so $J_0[p^n] \cong \mathbb{Z}[\zeta]/p^n\mathbb{Z}[\zeta]$, and the Chinese Remainder Theorem shows that $J_0\left[\tau^{-1}(\sigma(\mathfrak{p}))^n\right]$ is a rank-one $\mathbb{Z}[\zeta]/\mathfrak{p}^n$-module for every $\sigma, \tau \in \Phi_0$.

(b) Using (35) and (36) for $1 \leqq i \leqq \ell - 1$, we can write $t_i = \phi_i(x'_1, \ldots, x'_{\ell-1})$, with $\phi_i \in \mathbb{Z}[\zeta][[x'_1, \ldots, x'_{\ell-1}]]$. Since the linear term of ϕ_i is $\sum_{j=1}^{\ell-1}(\zeta^{-ij} - 1)x'_j$, and $[\zeta^{-ij} - 1]^{-1}_{1 \leqq i,j \leqq \ell-1} = \frac{1}{\ell}[\zeta^{jk}]_{1 \leqq j,k \leqq \ell-1}$, we have that $\phi = \{\phi_i\}_{1 \leqq i \leqq \ell-1}$ is an invertible set of power series over $\mathbb{Z}\left[\frac{1}{\ell}\right][\zeta]$. Let ψ be the inverse. If for g-tuples of variables W and Z we set

$$\mathscr{F}_j(W, Z) = \phi_j\big(\mathscr{G}\big(\psi(W), \psi(Z)\big)\big),$$

then $\mathscr{F} = \{\mathscr{F}_j\}_{1 \leqq j \leqq \ell-1}$ is a formal group over $\mathbb{Z}\left[\frac{1}{\ell}\right]$ isomorphic to $\mathscr{G}$ over $\mathbb{Z}\left[\frac{1}{\ell}\right][\zeta]$, which by (37) has CM-type Φ_0. For any $\sigma \in \Phi_0$, considering $\mathscr{F}$ as a formal group over R_σ, via ϕ we get an isomorphism from the kernel of reduction of $J_0(\mathcal{O}_\sigma) \bmod \mathfrak{m}_\sigma$ to $\mathscr{F}(\mathfrak{m}_\sigma)$.

Finally, since $[p^f]$ reduces to the Frobenius on $G \bmod \sigma(\mathfrak{p})$, for every $\sigma \in \Phi_0$, it does the same on J_0 and $\mathscr{F} \bmod \sigma(\mathfrak{p})$, and since $n_i = i$, we have the (strong) congruence relation $(p^f) = \prod_{\tau \in \Phi_0} \tau^{-1}(\sigma(\mathfrak{p}))$.

§6. Proof of Eisenstein reciprocity

Now take $\alpha \in \mathbb{Z}[\zeta]$ to be any semi-primary element. If $\mathfrak{p} \nmid (\lambda)$, by Proposition 2 and Theorem 3, there is a function $w_0 \in K(J_0)$, such that $[\zeta]^* w_0 = \zeta w_0$, and such that if we set $\Psi(\mathfrak{p}) = \prod_{u \in J_0[\mathfrak{p}]'} w_0(u)$, then

$$\big(\Psi(\mathfrak{p})\big) = \prod_{i=1}^{\ell-1} \sigma_i(\mathfrak{p})^{\langle i^{-1} \rangle} \mathfrak{a}\mathfrak{b}^\ell,$$

where $\mathfrak{a}$ is a fractional prime to p and is ℓ^{th}-power free, and $\mathfrak{b}$ is a non-zero fractional ideal. Note that w_0 is not unique, but we will assume that we have fixed a choice of w_0 for every choice of $\mathfrak{p}$. Let ζ_p be a primitive p^{th}-root of unity. We saw in the proof of Proposition 2 that $J_0[\mathfrak{p}] \subseteqq K(\zeta_p)$. Let S be a set of representatives of the orbits of $J_0[\mathfrak{p}]'$ under the action of μ_ℓ, and $\nu(\mathfrak{p}) = \prod_{u \in S} w_0(u)$.

Since $v(\mathfrak{p})^\ell = \Psi(\mathfrak{p})$, and $v(\mathfrak{p}) \in K(\zeta_p)$, which is ramified over K only at primes above p, we see that $\mathfrak{a}$ is the unit ideal.

We extend the definition of Ψ to products of primes prime to λ by

$$\Psi(\mathfrak{cd}) = \Psi(\mathfrak{c})\Psi(\mathfrak{d}),$$

and set $\Psi(\alpha) = \Psi((\alpha))$. We define $b \in K$ by the rule

$$\Psi(\alpha) = \Upsilon(\alpha)b, \tag{38}$$

where $\Upsilon(\alpha) = \alpha^{\sum_{i=1}^{\ell-1} i\sigma_{i^{-1}}} = \alpha^{\sum_{i=1}^{\ell-1} \langle i^{-1}\rangle \sigma_i}$. Then we have that $\operatorname{ord}_{\mathfrak{q}} b \equiv 0 \bmod \ell$ for all primes $\mathfrak{q}$ of $\mathbb{Z}[\zeta]$. This shows that $K(b^{1/\ell})/K$ is unramified outside λ. In fact we have:

Lemma 9. *$K(b^{1/\ell})/K$ is an unramified extension.*

Proof of lemma. We only have to show that the extension is unramified over λ. We know that for every $\mathfrak{p}$ dividing α, $K\big(v(\mathfrak{p})\big)/K$ is unramified over λ, so by (38) it suffices to show that the same is true of $K\big(\Upsilon(\alpha)^{1/\ell}\big)/K$. For this it suffices to show ([CF], Ex. 2.12) that

$$\Upsilon(\beta) \equiv 1 \mod \lambda^\ell,$$

for $\beta = \alpha^{\ell-1}$. Note that since α is semi-primary, $\beta \equiv 1 \bmod \lambda^2$. Since for all j prime to ℓ, we have

$$(\sigma_j - j)\sum_{i=1}^{\ell-1} i\sigma_{i^{-1}} \in \ell\mathbb{Z}[\Delta], \tag{39}$$

we have that $\Upsilon(\beta)^{\sigma_j}/\Upsilon(\beta)^j \in (K^\times)^\ell$. Further, $\Upsilon(\beta)^{\sigma_j}/\Upsilon(\beta)^j$ is congruent to $1 \bmod \lambda$, so it is congruent to $1 \bmod \lambda^\ell$, and $\Upsilon(\beta)^{\sigma_j} \equiv \Upsilon(\beta)^j \bmod \lambda^\ell$. Now write $\Upsilon(\beta) = 1 + \lambda^d\varepsilon$, with $\varepsilon \in \mathbb{Z}[\zeta]$ prime to λ. We know that $d > 1$. Suppose that $d < \ell$. Then we have $(1 + \lambda^d\varepsilon)^{\sigma_j} \equiv (1 + \lambda^d\varepsilon)^j \bmod \lambda^{d+1}$, so $1 + (1 - \zeta^j)^d\varepsilon^{\sigma_j} \equiv 1 + j\lambda^d\varepsilon \bmod \lambda^{d+1}$. Hence

$$\big((1 - \zeta^j)/(1 - \zeta)\big)^d\varepsilon^{\sigma_j} \equiv j\varepsilon \bmod \lambda, \quad \text{or} \quad (1 + \zeta + \cdots + \zeta^{j-1})^d\varepsilon \equiv j\varepsilon \bmod \lambda.$$

Therefore, $j^d \equiv j \bmod \ell$, for all $(j, \ell) = 1$. This gives $d \equiv 1 \bmod \ell - 1$, so since $d > 1$, we have $d \geqq \ell$, as desired.

Lemma 10. *$K(b^{1/\ell})$ is abelian over $\mathbb{Q}$.*

Proof of lemma. We know for any prime $\mathfrak{p} \nmid \lambda$ with $p^f = N\mathfrak{p}$, that $K\big(\Psi(\mathfrak{p})^{1/\ell}\big) = K\big(v(\mathfrak{p})\big) \subseteqq \mathbb{Q}(\zeta, \zeta_p)$, which is abelian over $\mathbb{Q}$, so $K\big(\Psi(\alpha)^{1/\ell}\big)$ is abelian over $\mathbb{Q}$. Hence by (38) it suffices to show that $K\big(\Upsilon(\alpha)^{1/\ell}\big)$ is abelian over $\mathbb{Q}$, which is well known ([Hilb], Theorem 147), and follows readily from (39).

Completion of proof of Theorem 1. We first claim that $b \in (K^\times)^\ell$. If not, let M be the fixed field in $K(b^{1/\ell})$ of the inertia group over $\mathbb{Q}$ of any (hence by Lemma 10, all) primes

above ℓ. Then by Lemma 9, $[M:\mathbb{Q}]=\ell$ and $M/\mathbb{Q}$ is a totally unramified extension. By the theorem of Hermite-Minkowski, this is a contradiction, so $b=\gamma^{\ell}$, for some $\gamma\in K$. Now let $\mathfrak{q}$ be any prime in K, with $N\mathfrak{q}$ prime to $\lambda\alpha$, and say $\mathfrak{q}$ lies over the rational prime q. Let τ be the Frobenius attached to $\mathfrak{q}$ in $\mathrm{Gal}\big(K(J_0[\alpha])/K\big)$. Then for any prime $\mathfrak{p}$ dividing α, τ restricts to the Frobenius attached to $\mathfrak{q}$ in $\mathrm{Gal}\big(K(J_0[\mathfrak{p}])/K\big)$, which is the restriction of the map $\tau_{N\mathfrak{q}}:\zeta_p\to\zeta_p^{N\mathfrak{q}}$ in $\mathrm{Gal}\big(K(\zeta_p)/K\big)$. Since $\tau_{N\mathfrak{q}}$ acts as multiplication by $N\mathfrak{q}$ on $J_0[\mathfrak{p}]$, we know by Gauss's Lemma (Lemma 8) that for any $\mathfrak{p}$ dividing α,

$$\tau\big(\Psi(\mathfrak{p})^{1/\ell}\big)/\Psi(\mathfrak{p})^{1/\ell}=\left(\frac{N\mathfrak{q}}{\mathfrak{p}}\right).$$

Hence

$$\tau\big(\Psi(\alpha)^{1/\ell}\big)/\Psi(\alpha)^{1/\ell}=\left(\frac{N\mathfrak{q}}{\alpha}\right).$$

But

$$\tau\big(\Psi(\alpha)^{1/\ell}\big)/\Psi(\alpha)^{1/\ell}\equiv\Psi(\alpha)^{(N\mathfrak{q}-1)/\ell}\equiv\left(\frac{\Psi(\alpha)}{\mathfrak{q}}\right)\equiv\left(\frac{\Upsilon(\alpha)\gamma^{\ell}}{\mathfrak{q}}\right)\equiv\left(\frac{\Upsilon(\alpha)}{\mathfrak{q}}\right)\mod\mathfrak{q}.$$

Therefore

$$\left(\frac{N\mathfrak{q}}{\alpha}\right)=\left(\frac{\Upsilon(\alpha)}{\mathfrak{q}}\right)=\left(\frac{\alpha^{\sum_{i=1}^{\ell-1}i\sigma_{i-1}}}{\mathfrak{q}}\right)$$

$$=\prod_{i=1}^{\ell-1}\left(\frac{\alpha^{\sigma_{i-1}}}{\mathfrak{q}}\right)^{i}=\prod_{i=1}^{\ell-1}\left(\frac{\alpha^{\sigma_{i-1}}}{\mathfrak{q}}\right)^{\sigma_i}=\prod_{i=1}^{\ell-1}\left(\frac{\alpha}{\sigma_i(\mathfrak{q})}\right)=\left(\frac{\alpha}{N\mathfrak{q}}\right).$$

Hence $\left(\frac{q}{\alpha}\right)=\left(\frac{\alpha}{q}\right)$, and Theorem 1 follows by bilinearity.

§7. Geometry of J_a

Let C_a be the projective non-singular curve defined over $\mathbb{Q}$ by the affine model $y(1-y)^a=x^{\ell}$, $1\leqq a\leqq\ell-2$, which is a quotient of the ℓ^{th} Fermat curve. Then C_a is a curve of genus $g=(\ell-1)/2$. Let ∞ denote the lone point at infinity on the affine model. Let J_a be the Jacobian of C_a (for basic properties of abelian and Jacobian varieties, we refer the reader to [Mi]). The automorphism ξ over K of C_a given by $(x,y)\to(\zeta x,y)$, extends to divisor classes, which gives an embedding $\varepsilon:\mathbb{Z}[\zeta]\to\mathrm{End}(J_a)$. The images of ε are endomorphisms which are all defined over K, and we denote $\varepsilon(\alpha)$ by $[\alpha]$. We let $J_a[p^{\infty}]=\bigcup_{n\geqq 0}J_a[p^n]$ and $J_{a,\mathrm{tors}}=\bigcup_{n\geqq 0}J_a[n]$. For $\beta\in\mathrm{End}(J_a)$, we let $v(\beta)$ denote the degree of β.

Note that C_a and hence J_a have good reduction at p. Until further notice, let a tilde on top of a symbol denote its reduction mod p. Let

$$\eta = \{1 \leqq n \leqq \ell - 1 \mid \langle n \rangle + \langle na \rangle \leqq \ell - 1\}.$$

Then $\#(\eta) = g$, and we pick an ordering $\eta = \{n_1, \ldots, n_g\}$ such that $n_1 = 1$. For every $n_i \in \eta$, let c_i be such that $n_i a - \langle n_i a \rangle = c_i \ell$. Then

$$\omega_i = x^{n_i}\, dy / y(1-y)^{c_i+1},$$

$1 \leqq i \leqq g$, is a basis of $H^0(C_a, \Omega)$. Note that $\xi^* \omega_i = \zeta^{n_i} \omega_i$. The ω_i are defined over $\mathbb{Q}$, and the $\tilde{\omega}_i$ form a basis of the holomorphic differentials on $\tilde{C}_a$.

Let $\kappa : C_a \to J_a$ denote the albanese embedding of C_a into J_a using ∞ as base point, which commutes with reduction mod p. Via the isomorphism $\kappa^* : H^0(J_a, \Omega) \to H^0(C_a, \Omega)$, we see that the $\Omega_i = (\kappa^*)^{-1}(\omega_i)$ are defined over $\mathbb{Q}$, that the $\tilde{\Omega}_i$ form a basis of the holomorphic differentials on $\tilde{J}_a$, and $[\zeta]^* \Omega_i = \zeta^{n_i} \Omega_i$.

Let $\mathfrak{n}$ be the maximal ideal of the local ring at the origin of J_a, and let ψ be the isomorphism $\mathfrak{n}/\mathfrak{n}^2 \xrightarrow{\sim} H^0(J_a, \Omega)$, which takes a $t \in \mathfrak{n}$ and maps it to the holomorphic differential represented by dt at the origin. Then ψ commutes with $[\zeta]^*$ and reduction mod p. Since J_a is defined over $\mathbb{Q}$ and has good reduction at $\mathfrak{p}$, $\mathfrak{n}$ contains a set of parameters at the origin of J_a defined over $\mathbb{Q}$ which reduce to parameters at the origin of $\tilde{J}_a$. Hence we can find a set of parameters $s_1, \ldots, s_g$ at the origin of J_a defined over $\mathbb{Q}$ that reduce mod $\mathfrak{n}^2$ to the $\psi^{-1}(\Omega_i)$, and such that $\tilde{s}_1, \ldots, \tilde{s}_g$ form a system of parameters at the origin of $\tilde{J}_a$. Therefore $[\zeta]^* s_i = \zeta^{n_i} s_i + (d^o \geqq 2)$ in the completed local ring at the origin. For $1 \leqq i \leqq g$, we now set $t_i = \dfrac{1}{\ell} \displaystyle\sum_{j=0}^{\ell-1} \zeta^{-n_i j} [\zeta^j]^* s_i$. Since for all $\sigma \in \Delta$, $[\zeta]^\sigma = [\zeta^\sigma]$, we have $t_i \in \mathbb{Q}(J_a)$. In addition, $[\zeta]^* t_i = \zeta^{n_i} t_i$, and $t_i = s_i + (d^o \geqq 2)$, so $T = {}^t(t_1, \ldots, t_g)$ is a system of parameters at the origin of J_a, and $(\tilde{t}_1, \ldots, \tilde{t}_g)$ is a system of parameters at the origin of $\tilde{J}_a$.

For independent generic points u and v on J_a, we define a formal group $\mathscr{J}^a = \{\mathscr{J}_i^a\}_{1 \leqq i \leqq g}$ over $\mathbb{Q}$ by setting $\mathscr{J}_i^a\big(T(u), T(v)\big)$ to be the expansion of $t_i(u +_{J_a} v)$ in the completed local ring at the origin of J_a. Again by good reduction, $\tilde{\mathscr{J}}_i^a\big(\tilde{T}(\tilde{u}), \tilde{T}(\tilde{v})\big)$ gives the expansion of $\tilde{t}_i(\tilde{u} +_{\tilde{J}_a} \tilde{v})$ in the completed local ring of the origin of $\tilde{J}_a$, for independent generic points $\tilde{u}$, $\tilde{v}$ on $\tilde{J}_a$. So $\mathscr{J}_i^a$ is a power series with coefficients in $\mathbb{Z}_{(p)}$. In addition, if $g \in \mathbb{Q}(J_a) \cap \mathfrak{n}$ reduces to a function mod p, then the power series expansion of g at the origin in T has coefficients in $\mathbb{Z}_{(p)}$. Hence for every $\sigma \in \Delta$ we have an isomorphism $u \to T(u)$ from the kernel of reduction mod $\mathfrak{m}_\sigma$ of $J_a(\mathscr{O}_\sigma)$ to $\mathscr{J}^a(\mathfrak{m}_\sigma)$. (Here $J_a(\mathscr{O}_\sigma)$ denotes the $\mathscr{O}_\sigma$-points of the Néron model of J_a over $\mathscr{O}_\sigma$.) Since for all $1 \leqq i \leqq g$, $[\zeta]^* t_i = \zeta^{n_i} t_i$, for any $\alpha \in \mathbb{Z}[\zeta]$, we get an endomorphism $[\alpha] = {}^t(\rho_1, \ldots, \rho_g)$ of $\mathscr{J}^a$ over $\mathbb{Z}_{(p)}[\zeta]$ by setting $\rho_i(t_1, \ldots, t_g) = [\alpha]^* t_i$. We have shown the following:

Lemma 11. *$\mathscr{J}^a$ is a formal group of dimension g defined over $\mathbb{Z}_{(p)}$ with* CM*-type $\Phi_a = (\sigma_{n_1}, \ldots, \sigma_{n_g})$, and for all $\sigma \in \Phi_a$, $\mathscr{J}^a(\mathfrak{m}_\sigma)$ is isomorphic to the kernel of reduction of $J_a(\mathscr{O}_\sigma)$ mod $\mathfrak{m}_\sigma$. Here $n_1 = 1$.*

There is very little of the general theory of complex multiplication of abelian varieties that we need to apply to J_a. In keeping with the philosophy of the paper, we will develop what we need directly, following [La] as a general reference. We just recall the following, which follows from the fact that $[K : \mathbb{Q}] = 2 \dim(J_a)$ and that $\mathbb{Z}[\zeta]$ is the maximal order in K [La], pp. 9, 112. Now let a tilde above a symbol denote its reduction mod $\mathfrak{p}$.

Lemma 12. (a) *For any non-zero ideal* $\mathfrak{a} \subset \mathbb{Z}[\zeta]$, $J_a[\mathfrak{a}]$ *is a free* $\mathbb{Z}[\zeta]/\mathfrak{a}$*-module of rank* 1.

(b) *The embedding* ε *is an isomorphism and we can identify* K *with* $\mathrm{End}(J_a) \otimes \mathbb{Q}$. *Reducing endomorphisms* mod $\mathfrak{p}$, K *is its own commutant in* $\mathrm{End}(\tilde{J}_a) \otimes \mathbb{Q}$.

There is an analytic isomorphism ϕ from $J_a(\mathbb{C})$ to a complex torus $\mathbb{C}^g/\Lambda$, where Λ is a lattice in $\mathbb{C}^g$, which induces a degree-preserving isomorphism $\phi_* : \mathrm{End}(J_a) \to \mathrm{End}(\mathbb{C}^g/\Lambda)$ from the (algebraic) endomorphisms of J_a to the (analytic) endomorphisms of $\mathbb{C}^g/\Lambda$. Any $\gamma \in \mathrm{End}(\mathbb{C}^g/\Lambda)$ lifts to an analytic endomorphism of its covering space $\mathbb{C}^g$, which must be a linear map γ'. Note that $\gamma'\Lambda \subseteqq \Lambda$, so picking a base for Λ, γ can be represented as a matrix $M_\gamma \in M_{2g}(\mathbb{Z})$. Hence we get the faithful *rational representation* $\rho_{\mathbb{Q}} : \mathrm{End}(J_a) \to M_{2g}(\mathbb{Z})$ by setting $\rho_{\mathbb{Q}}(\beta) = M_{\phi_*(\beta)}$.

Lemma 13. *For* $\alpha \in \mathbb{Z}[\zeta]$, $v([\alpha]) = \det \rho_{\mathbb{Q}}([\alpha]) = N(\alpha)$.

Proof. By the irreducibility of the ℓ^{th}-cyclotomic polynomial over $\mathbb{Q}$, we get that $\rho_{\mathbb{Q}}([\zeta])$ must have all possible conjugates of ζ as eigenvalues, so for $\alpha \in \mathbb{Z}[\zeta]$, $\rho_{\mathbb{Q}}([\alpha])$ has $\sigma_i(\alpha)$, $1 \leqq i \leqq 2g$, as eigenvalues, and the result follows.

For any prime q, since $(\mathbb{C}^g/\Lambda)[q^n] \cong \Lambda/q^n\Lambda$, the *q-adic representation* ρ_q of $\mathrm{End}(J_a)$ on the Tate module $T_q\big(J_a(\mathbb{C})\big) = \lim_{\infty \leftarrow n} A(\mathbb{C})[q^n]$ is equivalent to the rational representation, so $\rho_q([\alpha])$ can be represented by a matrix in $\mathrm{GL}_{2g}(\mathbb{Z}_q)$ whose determinant is $N(\alpha) = v([\alpha])$ for $\alpha \in \mathbb{Z}[\zeta]$. Now let q be a prime different from p. Since J_a has good reduction mod $\mathfrak{p}$, representing endomorphisms on $T_q(J_a)$ inject when reduced mod $\mathfrak{p}$.

Lemma 14. (a) $\mathrm{Gal}\big(K(J_{a,\mathrm{tors}})/K\big)$ *is abelian.*

(b) *Let* $\mathrm{Fr}_{\mathfrak{p}}$ *denote the Frobenius morphism on* $\tilde{J}_a$. *Then there exists an* $\alpha_{\mathfrak{p}} \in \mathbb{Z}[\alpha]$ *such that* $[\widetilde{\alpha_{\mathfrak{p}}}] = \mathrm{Fr}_{\mathfrak{p}}$.

Proof. (a) It suffices to show for every non-zero ideal $\mathfrak{a} \subset \mathbb{Z}[\zeta]$ that $G_{\mathfrak{a}} = \mathrm{Gal}\big(K(J_a[\mathfrak{a}])/K\big)$ is abelian. The action of $G_{\mathfrak{a}}$ on $J_a[\mathfrak{a}]$ gives an injection $G_{\mathfrak{a}} \to \mathrm{Aut}(J_a[\mathfrak{a}])$, and since all elements of $\varepsilon(\mathbb{Z}[\zeta])$ are defined over K, the image is contained in the group of automorphisms of $J_a[\mathfrak{a}]$ as an $\mathbb{Z}[\zeta]/\mathfrak{a}$-module. By Lemma 12 (a), $G_{\mathfrak{a}}$ injects into the abelian group $\mathrm{Aut}(\mathbb{Z}[\zeta]/\mathfrak{a})$.

(b) Since $\mathrm{Fr}_{\mathfrak{p}}$ commutes with the reduction mod $\mathfrak{p}$ of $\mathrm{End}(J_a) \otimes \mathbb{Q}$, by Lemma 12 (b), there exists an $\alpha_{\mathfrak{p}} \in K$ that reduces to $\mathrm{Fr}_{\mathfrak{p}}$. Since the characteristic polynomial of $\mathrm{Fr}_{\mathfrak{p}}$ acting on $T_q(\tilde{J}_a)$ has integer coefficients, and it coincides with the characteristic polynomials of $\rho_q([\alpha_{\mathfrak{p}}])$ and $\rho_{\mathbb{Q}}([\alpha_{\mathfrak{p}}])$—which has $\alpha_{\mathfrak{p}}$ as a root—in fact $\alpha_{\mathfrak{p}} \in \mathbb{Z}[\zeta]$.

We now gather what we need about $\alpha_{\mathfrak{p}}$.

Lemma 15. (a) (Weak congruence relation) *We have an ideal factorization* $(\alpha_{\mathfrak{p}}) = \prod_{\sigma \in \Phi_a} \sigma^{-1}(\mathfrak{p})^{b_\sigma}$, *where* $\sum_{\sigma \in \Phi_a} b_\sigma = g$.

(b) (Strong congruence relation) $(\alpha_{\mathfrak{p}}) = \prod_{\sigma \in \Phi_a} \sigma^{-1}(\mathfrak{p})$.

(c) $\alpha_{\mathfrak{p}}\bar{\alpha}_{\mathfrak{p}} = p^f$.

(d) $\alpha_{\mathfrak{p}}$ *is primary*.

(e) *The extension* $K(J_a[\mathfrak{p}^\infty])/K$ *is unramified outside* $\lambda \prod_{\sigma\in\Phi_a} \sigma(\mathfrak{p})$.

(f) *Let* $\mathfrak{q}$ *be a prime of* K *prime to* $\lambda \prod_{\sigma\in\Phi_a} \sigma(\mathfrak{p})$, *and let* $\tau_{\mathfrak{q}}$ *be the Frobenius automorphism attached to* $\mathfrak{q}$ *in* $\mathrm{Gal}\big(K(J_a[\mathfrak{p}^\infty])/K\big)$. *Then* $\tau_{\mathfrak{q}}(x) = [\alpha_{\mathfrak{q}}](x)$ *for all* $x \in J[\mathfrak{p}^\infty]$.

Proof. (a) By Lemma 13, since degrees of endomorphisms are preserved under reduction at a prime of good reduction, $N(\alpha_{\mathfrak{p}}) = v([\alpha_{\mathfrak{p}}]) = v([\widetilde{\alpha_{\mathfrak{p}}}]) = N(\mathfrak{p})^g = p^{fg}$. Let $c(p,\Phi_a)$ be a choice of type coset representatives for p and Φ_a. Let $C_{s+1},\dots,C_t$ denote the cosets of D in Δ that have trivial intersection with Φ_a, and pick $\sigma_{m_r} \in C_r$ for $s+1 \leqq r \leqq t$. Hence we have $(\alpha_{\mathfrak{p}}) = \prod_{r=1}^{t} \sigma_{m_r}^{-1}(\mathfrak{p})^{b_r}$ for some b_r with $\sum_{r=1}^{t} b_r = g$. We now claim that if $r > s$, then $b_r = 0$. Indeed, let $\pi \in \mathbb{Z}[\zeta]$ be such that $\mathrm{ord}_{\sigma_{m_r}^{-1}(\mathfrak{p})}\,\pi = 1$ but $\mathrm{ord}_{\sigma^{-1}(\mathfrak{p})}\,\pi = 0$ for all $\sigma \notin C_r$. Then $J_a[\sigma_{m_r}^{-1}(\mathfrak{p})] \subseteqq J_a[\pi]$, but by Lemma 1, $[\pi]$ is an automorphism of $\mathscr{J}_a$ over R, so $\mathscr{J}_a[\sigma_{m_r}^{-1}(\mathfrak{p})]$ is trivial. But all of $J[\alpha_{\mathfrak{p}}]$ must be in the kernel of reduction mod $\mathfrak{m}$, which establishes our claim.

(b) By Lemma 11 and part (a), considering $\mathscr{J}_a$ defined over R, we can apply Proposition 1 (a) to the p-typification of $\mathscr{J}^a$, and our weak congruence relation is the strong one.

(c) Since Φ_a is a set of representatives for the orbits of Δ under the action of complex conjugation, part (b) implies $(\alpha_{\mathfrak{p}}\bar{\alpha}_{\mathfrak{p}}) = (p^f)$, so there is a totally positive unit $u \in K$ such that $\alpha_{\mathfrak{p}}\bar{\alpha}_{\mathfrak{p}} = up^f$.

Extending κ to w-fold symmetric products $C^{(w)}$ of C, we get that $\Theta = \kappa(C^{(g-1)})$ is an ample divisor of J_a that defines a principal polarization.

Recall that for any ample divisor X on J_a, there is an isogeny ϕ_X from J_a to its dual $\hat{J}_a$, taking a point $V \in J_a$ to the linear equivalence class of $X_V - X$, where X_V is the image of X under the translation-by-V map. Note that an ample X is algebraically equivalent to a divisor Y, which we write as $X \equiv Y$, if and only if $\phi_X = \phi_Y$. If $\alpha \in \mathrm{End}(J_a)$, then pulling back under α gives a transpose isogeny $\alpha^t : \hat{J} \to \hat{J}$. Since Θ gives a principal polarization, ϕ_Θ is an isomorphism, and for $\alpha \in \mathrm{End}(J_a)$, we set $\alpha' = \phi_\Theta^{-1} \circ \alpha^t \circ \phi_\Theta$, the map $\alpha \to \alpha'$ being the *Rosatti involution* determined by Θ.

Since Θ is fixed under $[\zeta]$, it follows that the Rosatti involution determined by Θ is complex conjugation on $\mathbb{Z}[\zeta]$, and hence a calculation ([La], p. 71) shows that if $\phi \in \mathbb{Z}[\zeta]$ is such that $[\phi]^*\Theta \equiv \Theta$, then $\phi\bar{\phi} = 1$. It is standard that $\mathrm{Fr}_{\mathfrak{p}}^*\tilde{\Theta} = p^f\tilde{\Theta}$ as divisors mod $\mathfrak{p}$, so $\phi_{[\widetilde{\alpha_{\mathfrak{p}}}]^*\Theta}$ and $\phi_{p^f\tilde{\Theta}}$ have the same q-adic representations mod $\mathfrak{p}$ for any $q \neq p$ as isogenies from $\tilde{J}_a$ to $\hat{\tilde{J}}_a \cong \tilde{\hat{J}}_a$, and hence $\phi_{[\alpha_{\mathfrak{p}}]^*\Theta}$ and $\phi_{p^f\Theta}$ have the same q-adic representations as isogenies from J_a to $\hat{J}_a$, and therefore are equal. Hence $[\alpha]_{\mathfrak{p}}^*\Theta \equiv p^f\Theta$. Since Θ is defined over $\mathbb{Q}$, we also have $[\bar{\alpha}_{\mathfrak{p}}]^*\Theta \equiv p^f\Theta$. Hence $[\alpha_{\mathfrak{p}}\bar{\alpha}_{\mathfrak{p}}]^*\Theta \equiv p^{2f}\Theta$, and since always $[p^f]^*\Theta \equiv p^{2f}\Theta$, we get that $[u]^*\Theta \equiv \Theta$. Therefore $u\bar{u} = 1$, and u is a totally positive unit of absolute value 1 in some complex embedding, so $u = 1$.

(d) By part (c), all we have to show is that $\alpha_{\mathfrak{p}}$ is congruent to a rational integer mod λ^2. It follows from a theorem of Greenberg [Gre] (which now has an explicit construction by Tzermias [T1]) that $J_a[\lambda^3]$ is rational over K, so $[\tilde{\alpha}_{\mathfrak{p}}]$ fixes $\tilde{J}_a[\lambda^3]$, and we even get that $\alpha_{\mathfrak{p}} \equiv 1 \bmod \lambda^3$.

(e) If $\mathfrak{q}$ is a prime of K prime to $\lambda \prod_{\sigma \in \Phi_a} \sigma(\mathfrak{p})$, then the same argument in part (a) shows that $J_a[\mathfrak{p}^\infty]$ injects mod $\mathfrak{q}$.

(f) For any $n \geqq 1$, take $x \in J_a[\mathfrak{p}^n]$. Since $[\alpha_{\mathfrak{q}}]$ reduces to the Frobenius endomorphism on $J_a \bmod \mathfrak{q}$, $\tau_{\mathfrak{q}}(x)$ and $[\alpha_{\mathfrak{q}}](x)$ agree mod $\mathfrak{q}$. Since by (e), $J_a[\mathfrak{p}^n]$ injects mod $\mathfrak{q}$, we have $\tau_{\mathfrak{q}}(x) = [\alpha_{\mathfrak{q}}](x)$.

Proposition 3. (a) *J_a is a commutative group variety of dimension g with* CM *by $\mathbb{Z}[\zeta]$ defined over K which is simple at $\tau^{-1}\big(\sigma(\mathfrak{p})\big)$ for every $\sigma, \tau \in \Phi_a$.*

(b) *J_a has a congruence formal group at $\mathfrak{p}$ of type Φ_a, and $n_1 = 1$ in Φ_a.*

Proof. First we apply Lemma 11 and Lemma 15 for $\sigma(\mathfrak{p})$ for all $\sigma \in \Phi_a$. Note that by Lemma 12 (a), for every $n \geqq 1$ and $\sigma, \tau \in \Phi_a$, we get that $J_a\big[\tau^{-1}\big(\sigma(\mathfrak{p}^n)\big)\big]$ is a rank-one $\mathbb{Z}[\zeta]/\mathfrak{p}^n$ module.

§8. Proof of Kummer reciprocity

In this section let ℓ be an odd regular prime. For $\mathfrak{a}$, $\mathfrak{b}$ relatively prime ideals in $\mathbb{Z}[\zeta]$ prime to λ, we set $\{\mathfrak{a}, \mathfrak{b}\} = \left(\frac{\mathfrak{a}}{\mathfrak{b}}\right)\left(\frac{\mathfrak{b}}{\mathfrak{a}}\right)^{-1}$. Theorem 2 says that for every distinct pair of prime ideals $\mathfrak{p}$, $\mathfrak{q}$ prime to λ, we have $\{\mathfrak{p}, \mathfrak{q}\} = 1$. We prove this via Propositions 4 and 5.

For any $1 \leqq a \leqq \ell - 2$, let J_a and Φ_a be as in the last section. If $\Upsilon(\mathfrak{p}) = \prod_{i=1}^{g} \mathfrak{p}^{\langle n_i^{-1} \rangle \sigma_{n_i}}$, then by Proposition 3 and Theorem 3 there is a function $w_a \in K(J_a)$ such that $[\zeta]^* w_a = \zeta w_a$, and such that if $\Psi(\mathfrak{p}) = \prod_{u \in J_a[\mathfrak{p}]'} w_a(u)$, then

$$\big(\Psi(\mathfrak{p})\big) = \Upsilon(\mathfrak{p})\mathfrak{a}\mathfrak{b}^{\ell}, \tag{40}$$

where $\mathfrak{a}$ is a fractional ideal prime to $\prod_{\sigma \in \Phi_a} \sigma(\mathfrak{p})$ and is ℓ^{th}-power free, and $\mathfrak{b}$ is some non-zero fractional ideal.

Let S be a set of representatives for the orbits of $J_a[\mathfrak{p}]'$ under the action of μ_ℓ, and $v(\mathfrak{p}) = \prod_{u \in S} w_a(u)$. Then $v(\mathfrak{p})^{\ell} = \Psi(\mathfrak{p})$.

Lemma 16. *There is some $e \in \mathbb{Z}$ such that if*

$$\delta = \big(a^a/(1+a)^{1+a}\big)^e \Psi(\mathfrak{p}),$$

then $K(\delta^{1/\ell})/K$ is unramified over λ.

Proof. Let α be any ℓ^{th}-root of $a^a/(a+1)^{a+1}$, $F = K(\lambda^{1/2}, \alpha)$. It is shown in [CM] that C_a—and hence J_a—has good reduction over F. Let $M = K(\alpha)$, which is easily seen to be of degree ℓ over K. Since $F\big(v(\mathfrak{p})\big)/F$ is an extension which is unramified at primes over ℓ in F, the same is true for the extension $M\big(v(\mathfrak{p})\big)/M$. Suppose no such e exists. Then taking $e = 0$, we have that $K\big(v(\mathfrak{p})\big)/K$ is an extension of degree ℓ totally ramified over λ. If $K\big(v(\mathfrak{p})\big) = K(\alpha)$, then there is some e such that $\delta \in (K^\times)^\ell$, so we must have that $\big[K\big(\alpha, v(\mathfrak{p})\big) : K\big] = \ell^2$. Since $K\big(\alpha, v(\mathfrak{p})\big)/K(\alpha)$ is unramified at primes over ℓ, the inertia field I in $K\big(\alpha, v(\mathfrak{p})\big)/K$ of primes over λ is a degree ℓ extension over K which is unramified at λ. If $I = K(\delta^{1/\ell})$ for some choice of e, this gives a contradiction. So $I = K(\alpha)$, which means that $K\big(\alpha, v(\mathfrak{p})\big)/K$ is unramified over λ, also a contradiction. This establishes the lemma.

Proposition 4. *Let* $\gamma_a = \sum_{\sigma \in \Phi_a} \sigma^{-1}$, *and let* $\mathfrak{p}$ *and* $\mathfrak{q}$ *be primes of* $\mathbb{Z}[\zeta]$ *with* $\mathfrak{p} \neq (\lambda)$, *and* $\mathfrak{q}$ *prime to* $\lambda \prod_{\sigma \in \Phi_a} \sigma(\mathfrak{p})$. *Then*

$$\left(\frac{\mathfrak{q}^{\gamma_a}}{\mathfrak{p}}\right) = \left(\frac{\mathfrak{p}}{\mathfrak{q}^{\gamma_a}}\right).$$

Proof. We first note that $\mathfrak{a}$ in (40) is the unit ideal. Indeed, since $v(\mathfrak{p}) \in K(J_a[\mathfrak{p}])$, which by Lemma 15 is unramified outside primes dividing $\lambda \prod_{\sigma \in \Phi_a} \sigma(\mathfrak{p})$, we get immediately that $\mathfrak{a}$ is a power of λ. Since ℓ is prime to a and $a+1$, Lemma 16 shows that $\mathfrak{a}$ must be prime to λ.

Now let h be the class number of K, and $\mathfrak{p}^h = (\wp)$, where $\wp$ is primary. For $\alpha \in \mathbb{Z}[\zeta]$, let $\Upsilon(\alpha) = \prod_{i=1}^{g} \alpha^{\langle n_i^{-1} \rangle \sigma_{n_i}}$. Then by (40) we have

$$\Psi(\mathfrak{p})^h = \prod_{u \in J_a[\mathfrak{p}]'} w_a(u)^h = \varepsilon \Upsilon(\wp) b^\ell, \tag{41}$$

where b is a generator of $\mathfrak{b}^h$ and ε is a unit.

We now claim that ε is primary. Indeed by Lemma 16, choosing e so that $K(\delta^{1/\ell})/K$ is unramified over λ, δ is primary, and the ℓ^{th} power of an element of $\mathbb{Z}[\zeta]$ prime to λ is primary, as is any rational integer prime to ℓ, so $\varepsilon\Upsilon(\wp)$ is primary, too. Finally, since $\wp$ is primary, ε is primary. This shows that ε is an ℓ^{th} power, so multiplying b by a unit if necessary in (41), we can assume $\varepsilon = 1$.

For $\mathfrak{q} \in \mathbb{Z}[\zeta]$ prime to $\lambda \prod_{\sigma \in \Phi_a} \sigma(\mathfrak{p})$, we know by Lemma 15 that the Frobenius $\tau_\mathfrak{q}$ attached to $\mathfrak{q}$ in $\mathrm{Gal}\big(K(J_a[\mathfrak{p}])/K\big)$ acts on $J_a[\mathfrak{p}]$ via $[\alpha_\mathfrak{q}]$. Let h^* be any integer such that $hh^* \equiv 1 \bmod \ell$. Then by (41), Gauss's Lemma (Lemma 8), and the definition of the power residue symbol,

$$\left(\frac{\Upsilon(\mathfrak{p})}{\mathfrak{q}}\right) = \left(\frac{\Upsilon(\wp)}{\mathfrak{q}}\right)^{h^*} = \left(\frac{\Psi(\mathfrak{p})^h/b^\ell}{\mathfrak{q}}\right)^{h^*} = \left(\frac{\Psi(\mathfrak{p})}{\mathfrak{q}}\right) = v(\mathfrak{p})^{(\tau_\mathfrak{q} - 1)} = \left(\frac{\alpha_\mathfrak{q}}{\mathfrak{p}}\right). \tag{42}$$

Now Lemma 15 gives

$$(\alpha_{\mathfrak{q}}) = \prod_{\sigma \in \Phi_a} \sigma^{-1}(\mathfrak{q}) = \mathfrak{q}^{\gamma_a}, \tag{43}$$

and shows that $\alpha_{\mathfrak{q}}$ is primary.

Now from (42) and (43) we have

$$\left(\frac{\mathfrak{q}^{\gamma_a}}{\mathfrak{p}}\right) = \left(\frac{\Upsilon(\mathfrak{p})}{\mathfrak{q}}\right) = \prod_{i=1}^{g}\left(\frac{\sigma_{n_i}(\mathfrak{p})}{\mathfrak{q}}\right)^{n_i^{-1}} = \prod_{i=1}^{g}\left(\frac{\sigma_{n_i}(\mathfrak{p})}{\mathfrak{q}}\right)^{\sigma_{n_i^{-1}}} = \prod_{i=1}^{g}\left(\frac{\mathfrak{p}}{\sigma_{n_i^{-1}}(\mathfrak{q})}\right) = \left(\frac{\mathfrak{p}}{\mathfrak{q}^{\gamma_a}}\right),$$

which proves the proposition.

Proposition 5. *For all* $1 \leqq a \leqq \ell - 2$, *suppose* $\{\mathfrak{q}^{\gamma_a}, \mathfrak{p}\} = 1$ *for all primes* $\mathfrak{p}, \mathfrak{q} \subset \mathbb{Z}[\zeta]$, $\mathfrak{q} \neq (\lambda)$, $\mathfrak{p}$ *prime to* $\lambda\mathfrak{q}^{\gamma_a}$. *Then* $\{\mathfrak{p}, \mathfrak{q}\} = 1$ *for all distinct primes* $\mathfrak{p}, \mathfrak{q} \subset \mathbb{Z}[\zeta]$ *prime to* λ.

Proof. Case 1: $\mathfrak{q}$ *is not a conjugate of* $\mathfrak{p}$. Let X consist of the $x \in \mathbb{Z}/\ell\mathbb{Z}[\Delta]$ such that $\{\mathfrak{q}^x, \mathfrak{p}\} = 1$, for all prime ideals $\mathfrak{p}$, $\mathfrak{q}$ which are prime to λ and are not conjugates of each other. Our goal is to show that X is all of $\mathbb{Z}/\ell\mathbb{Z}[\Delta]$.

Lemma 17. *X is a $\mathbb{Z}/\ell\mathbb{Z}[\Delta]$-module.*

Proof of lemma. The bilinearity of the power residue symbol shows that X is a subgroup of $\mathbb{Z}/\ell\mathbb{Z}[\Delta]$. To see that X is a submodule of $\mathbb{Z}/\ell\mathbb{Z}[\Delta]$, it suffices to show $\sigma X \subseteqq X$ for every $\sigma \in \Delta$. But for $x \in \mathbb{Z}/\ell\mathbb{Z}[\Delta]$, $\{\mathfrak{q}^x, \mathfrak{p}\} = 1$, implies $\{\mathfrak{q}^{\sigma x}, \mathfrak{p}^{\sigma}\} = 1$, and $\mathfrak{q}$ is not a conjugate of $\mathfrak{p}^{\sigma}$.

Since ℓ is odd, we can decompose $\mathbb{Z}/\ell\mathbb{Z}[\Delta]$ into the direct sum of $\mathbb{Z}/\ell\mathbb{Z}$-vector spaces $\mathbb{Z}/\ell\mathbb{Z}[\Delta]^+$ and $\mathbb{Z}/\ell\mathbb{Z}[\Delta]^-$, which are respectively, the eigenspaces under multiplication by σ_{-1} with eigenvalues 1 and -1. There is an involution $\rho : \mathbb{Z}/\ell\mathbb{Z}[\Delta] \to \mathbb{Z}/\ell\mathbb{Z}[\Delta]$ defined by

$$\rho\left(\sum_{i \in (\mathbb{Z}/\ell\mathbb{Z})^{\times}} a_i\sigma_i\right) = \sum_{i \in (\mathbb{Z}/\ell\mathbb{Z})^{\times}} i a_i \sigma_{i^{-1}},$$

for $a_i \in \mathbb{Z}/\ell\mathbb{Z}$, $\sigma_i \in \Delta$. The involution is a $\mathbb{Z}/\ell\mathbb{Z}$-linear transformation, and since for any $\alpha \in \mathbb{Z}/\ell\mathbb{Z}[\Delta]$, $\rho(\sigma_{-1}\alpha) = -\sigma_{-1}\rho(\alpha)$, ρ exchanges $\mathbb{Z}/\ell\mathbb{Z}[\Delta]^+$ and $\mathbb{Z}/\ell\mathbb{Z}[\Delta]^-$.

By Lemma 17, X also decomposes into the direct sum of X^+ and X^-, its eigenspaces under the action of σ_{-1} with eigenvalues $+1$ and -1, respectively.

Lemma 18. *X is stable under ρ, so ρ interchanges X^+ and X^-.*

Proof of lemma. Suppose $x = \sum a_i\sigma_i \in X$. Then if $\mathfrak{p}$ and $\mathfrak{q}$ are primes prime to λ, and are not conjugates of each other,

$$\left(\frac{\mathfrak{q}^{\rho(\sum a_i\sigma_i)}}{\mathfrak{p}}\right) = \left(\frac{\mathfrak{q}^{\sum i a_i \sigma_{i^{-1}}}}{\mathfrak{p}}\right) = \prod\left(\frac{\mathfrak{q}^{\sigma_{i^{-1}}}}{\mathfrak{p}}\right)^{i a_i} = \prod\left(\frac{\mathfrak{q}^{\sigma_{i^{-1}}}}{\mathfrak{p}}\right)^{\sigma_i a_i} = \left(\frac{\mathfrak{q}}{\mathfrak{p}^x}\right)$$

$$= \left(\frac{\mathfrak{p}^x}{\mathfrak{q}}\right) = \prod\left(\frac{\mathfrak{p}^{\sigma_i}}{\mathfrak{q}}\right)^{a_i} = \prod\left(\frac{\mathfrak{p}^{\sigma_i}}{\mathfrak{q}}\right)^{i a_i \sigma_{i^{-1}}} = \left(\frac{\mathfrak{p}}{\mathfrak{q}^{\rho(\sum a_i\sigma_i)}}\right),$$

as desired, where all sums and products are over $i \in (\mathbb{Z}/\ell\mathbb{Z})^{\times}$.

We conclude from Lemma 18 that to show that $X = \mathbb{Z}/\ell\mathbb{Z}[\Delta]$, it suffices to show that $X^- = \mathbb{Z}/\ell\mathbb{Z}[\Delta]^-$. Note that the idempotents

$$\varepsilon_\chi = -\sum_{\sigma\in\Delta} \chi(\sigma)\sigma^{-1},$$

where χ is an odd $(\mathbb{Z}/\ell\mathbb{Z})^\times$-valued character of Δ, span $\mathbb{Z}/\ell\mathbb{Z}[\Delta]^-$ as a $\mathbb{Z}/\ell\mathbb{Z}$-vector space. So to show $X = \mathbb{Z}/\ell\mathbb{Z}[\Delta]$, we are reduced to showing that for every odd character χ, there is an $x \in X$ such that $\varepsilon_\chi x \neq 0$. We know from Proposition 4 that for $1 \leqq a \leqq \ell - 2$, $\gamma_a = \sum_{\sigma\in\Phi_a} \sigma^{-1} \in X$. Let $s(\chi, a) = \sum_{\sigma\in\Phi_a} \chi(\sigma)$. Then we compute $\varepsilon_\chi\gamma_a = s(\chi^{-1}, a)\varepsilon_\chi$. So Case 1 follows from the following Lemma 19.

We call an $1 \leqq a \leqq \ell - 2$ *admissible* if a is not a primitive third root of unity $\bmod \ell$.

Lemma 19. *For every odd character $\chi : \Delta \to (\mathbb{Z}/\ell\mathbb{Z})^\times$, there is an admissible a such that $s(\chi, a) \neq 0$.*

Proof of lemma. Let $\omega : \Delta \to (\mathbb{Z}_\ell)^\times$ be the Teichmüller character, so that for all $\sigma_j \in \Delta$, $\omega(\sigma_j) \equiv j \bmod \ell$. Then it suffices to show that for every odd i, $1 \leqq i \leqq \ell - 2$, that

$$s(\omega^i, a) = \sum_{\sigma\in\Phi_a} \omega^i(\sigma)$$

is in $(\mathbb{Z}_\ell)^\times$ for some admissible a.

Following the calculation in [Kub5], we get as in [R], that for i odd, $1 \leqq i \leqq \ell - 2$, that after identifying Δ with $(\mathbb{Z}/\ell\mathbb{Z})^\times$ by sending $\sigma_j \to j$, we have

$$s(\omega^i, a) = B_{1,\omega^i}\big(\omega^{-i}(a+1) - \omega^{-i}(a) - 1\big), \tag{44}$$

where $B_{1,\omega^i} = \Big(\sum_{1\leqq j\leqq \ell-1} j\omega^i(j)\Big)/\ell$ is a generalized Bernoulli number. Let $1 \leqq i \leqq \ell - 4$ be odd. Then since ℓ is regular, B_{1,ω^i} is a unit in $(\mathbb{Z}_\ell)^\times$. So (44) vanishes $\bmod \ell$ only if

$$\omega^{-i}(a+1) \equiv \omega^{-i}(a) + 1 \mod \ell.$$

But we claim that if $\omega^{-i}(a+1) \equiv \omega^{-i}(a) + 1$ for all admissible a, then ω^{-i} reduces to the identity character $\bmod \ell$. Indeed, let b be the smallest positive integer less than $\ell - 1$ such that $\omega^{-i}(b+1) \not\equiv b + 1 \bmod \ell$. Then for all $c \leqq b$, $\omega^{-i}(c) \equiv c \bmod \ell$. By hypothesis, b cannot be admissible, but also b cannot be of order 3 in $(\mathbb{Z}/\ell\mathbb{Z})^\times$, since then

$$\omega^{-i}(b+1) = \omega^{-i}(-b^2) = -\omega^{-i}(b)^2 \equiv -b^2 \equiv b + 1 \equiv \omega^{-i}(b) + 1 \mod \ell.$$

This establishes the lemma for $\chi \not\equiv \omega^{\ell-2} \bmod \ell$. So we now only need to show that $s(\omega^{\ell-2}, a)$ is in $(\mathbb{Z}_\ell)^\times$ for some admissible a. In that case $\ell B_{1,\omega^{\ell-2}} \in (\mathbb{Z}_\ell)^\times$, and $\omega^{-(\ell-2)} = \omega$ reduces to the identity character $\bmod \ell$. So by (44), we need to show that there is an admissible a such that the equality

$$\omega(a+1) \equiv \omega(a) + 1 \mod \ell^2$$

fails. Suppose not, and let $1 \leqq b \leqq \ell - 2$ be minimal such that $\omega(b+1) \not\equiv b+1 \bmod \ell^2$. By hypothesis, b is not admissible, but if b is of order 3 in $(\mathbb{Z}/\ell\mathbb{Z})^\times$, then $\omega(b)$ is of order three in $(\mathbb{Z}_\ell)^\times$, so $\omega(b+1) = \omega(-b^2) = -\omega(b)^2 = \omega(b) + 1$. Hence there is no such b, and $\omega(\ell - 1) \equiv \ell - 1 \bmod \ell^2$. But $\omega(\ell - 1) = \omega(-1) = -1$, a contradiction, which proves Lemma 19 and completes Case 1 of Proposition 5.

Case 2: $\mathfrak{q}$ *is a non-trivial conjugate of* $\mathfrak{p}$. If there is a non-trivial element σ in the decomposition group of $\mathfrak{p}$, then $\left(\frac{\mathfrak{q}}{\mathfrak{p}}\right)$ is invariant under σ, so is trivial. Therefore we can assume without loss of generality that $\mathfrak{p}$ is a first degree prime. Hence by assumption, for any $1 \leqq a \leqq \ell - 2$, and any $\sigma_i \in \Phi_a$, since $\sigma_{-i} \notin \Phi_a$, we have

$$\{\mathfrak{p}^{\sigma_{-i}\gamma_a}, \mathfrak{p}\} = 1. \tag{45}$$

Since the coefficient of σ_{-1} in $\sigma_{-i}\gamma_a$ is 1, if we prove this case for all non-trivial conjugates $\mathfrak{q}$ of $\mathfrak{p}$ other than $\sigma_{-1}(\mathfrak{p})$, then by (45) and bilinearity this case will hold for $\mathfrak{q} = \sigma_{-1}(\mathfrak{p})$ as well. So we can assume without loss of generality that $\mathfrak{q}$ is not the complex conjugate of $\mathfrak{p}$. Now taking $i = j$ and $i = 1$ in (45), we get

$$\{\mathfrak{p}^{(\sigma_{-j} - \sigma_{-1})\gamma_a}, \mathfrak{p}\} = 1, \tag{46}$$

for any $1 \leqq a \leqq \ell - 2$, and any $\sigma_j \in \Phi_a$. Note that

$$(\sigma_{-j} - \sigma_{-1})\gamma_a \in T = \bigoplus_{\sigma_i \in \Delta,\, i \neq 1, -1} (\mathbb{Z}/\ell\mathbb{Z})\sigma_i.$$

Now T is a $\mathbb{Z}/\ell\mathbb{Z}$-subspace of $\mathbb{Z}/\ell\mathbb{Z}[\Delta]$, stable under multiplication by σ_{-1}, so decomposes into the direct sum of T^+ and T^-, the eigenspaces under multiplication by σ_{-1} with eigenvalues $+1$ and -1, respectively. Note that ρ preserves T and interchanges T^+ and T^-. Let $U \subseteq T$ be the subspace of $u \in T$ such that $\{\mathfrak{p}^u, \mathfrak{p}\} = 1$. Our goal is to show that $U = T$. Let V be the subspace of T generated by all $(\sigma_{-j} - \sigma_{-1})\gamma_a$, for all $1 \leqq a \leqq \ell - 2$ and all $\sigma_j \in \Phi_a$. By (46), $V \subset U$, and by the argument of Lemma 18, $\rho(V) \subset U$. Furthermore, $(1 + \sigma_{-1})(\sigma_{-j} - \sigma_{-1})\gamma_a = (\sigma_{-j} - \sigma_{-1})(-\varepsilon_{\chi_0}) = 0$, where χ_0 is the trivial character. Hence $(\sigma_{-j} - \sigma_{-1})\gamma_a \in T^-$ for all $1 \leqq a \leqq \ell - 2$ and $\sigma_j \in \Phi_a$, and so $V \subset T^-$. If we can show $V = T^-$, then $\rho(V) = T^+$, and $V \oplus \rho(V) = U = T$, and the proposition will be complete.

Lemma 20. $V = T^-$.

Proof of lemma. Note that T^- is an $(\ell - 3)/2$-dimensional $\mathbb{Z}/\ell\mathbb{Z}$-vector space, so is spanned by $\{\varepsilon_\chi - \varepsilon_{\chi_{\text{inv}}} \mid \chi \neq \chi_{\text{inv}}, \chi \text{ odd}\}$, where χ_{inv} is the character $\chi_{\text{inv}}(\sigma_i) = i^{-1}$. From (46), we have for every $1 \leqq a \leqq \ell - 2$ and any odd χ that

$$\psi_{a,\chi} = \sum_{\sigma_i \in \Phi_a} \chi(\sigma_{-i}^{-1})(\sigma_{-i} - \sigma_{-1})\gamma_a = \left(\sum_{\sigma_i \in \Phi_a} \chi(\sigma_{-i}^{-1})\sigma_{-i}\gamma_a\right) + s(\chi^{-1}, a)\sigma_{-1}\gamma_a \tag{47}$$

is in V. Since $V \subseteq T^-$, $(1 - \sigma_{-1})\psi_{a,\chi} = 2\psi_{a,\chi}$. Hence multiplying (47) by $(1 - \sigma_{-1})$ yields

$$\begin{aligned} 2\psi_{a,\chi} &= \left(\sum_{\sigma_i \in \Phi_a} \chi(\sigma_{-i}^{-1})(\sigma_{-i} - \sigma_i)\gamma_a\right) + s(\chi^{-1}, a)(\sigma_{-1} - 1)\gamma_a \\ &= -\varepsilon_\chi\gamma_a + s(\chi^{-1}, a)(\sigma_{-1} - 1)\gamma_a, \end{aligned}$$

since χ is odd. So

$$2\psi_{a,\chi} = -s(\chi^{-1},a)\varepsilon_\chi + s(\chi^{-1},a)(\sigma_{-1}-1)\gamma_a \tag{48}$$
$$= s(\chi^{-1},a)\big(-\varepsilon_\chi + (\sigma_{-1}-1)\gamma_a\big).$$

Now by Lemma 19, we can pick an admissible a such that $s(\chi^{-1},a) \neq 0$, so by (48), for this a we get

$$-\varepsilon_\chi + (\sigma_{-1}-1)\gamma_a \in V. \tag{49}$$

But we claim also for this a that $s(\chi_{\text{inv}}^{-1},a) \neq 0$, because

$$s(\chi_{\text{inv}}^{-1},a) \equiv s(\omega,a) \mod \ell,$$

and by (44),

$$s(\omega,a) = B_{1,\omega}\big(\omega^{-1}(a+1) - \omega^{-1}(a) - 1\big).$$

Furthermore, $B_{1,\omega} \in (\mathbb{Z}_\ell)^\times$, and if $\dfrac{1}{a+1} = \dfrac{1}{a} + 1 \bmod \ell$, then a is of order 3 in $(\mathbb{Z}/\ell\mathbb{Z})^\times$, and is not admissible. Hence by (49), subtracting the case where $\chi = \chi_{\text{inv}}$ gives

$$-\varepsilon_\chi + \varepsilon_{\chi_{\text{inv}}} \in V,$$

as desired. This completes the proof of Lemma 20, hence Case 2 of Proposition 5, and the proof of Kummer reciprocity.

§9. Applications

Relations to Gauss sums. In this section, ℓ is once again an arbitrary odd prime. As in section 6, by Proposition 2 and Theorem 3, for every prime $\mathfrak{p} \in \mathbb{Z}[\zeta]$ prime to λ, there exists a function $w_0 \in K(J_0)$, such that $[\zeta]^* w_0 = \zeta w_0$, and such that

$$\left(\prod_{u \in J_0[\mathfrak{p}]'} w_0(u)\right) = \prod_{i=1}^{\ell-1} \sigma_i(\mathfrak{p})^{\langle i^{-1}\rangle} \cdot \mathfrak{a}\mathfrak{b}^\ell, \tag{50}$$

where $\mathfrak{a}$ is a fractional ideal of K prime to $N\mathfrak{p}$ which is ℓ^{th}-power free, and $\mathfrak{b}$ is a non-zero fractional ideal. In particular, for all $u \in J_0[\mathfrak{p}]'$, $w_0(u) \neq 0$.

Now let $\chi(\alpha) = \left(\dfrac{\alpha}{\mathfrak{p}}\right)^{-1}$ for $\alpha \in (\mathbb{Z}[\zeta]/\mathfrak{p})^*$, so χ is a character of order ℓ on $(\mathbb{Z}[\zeta]/\mathfrak{p})^*$. We let g_{χ^j} be the Gauss sum $\displaystyle\sum_{\alpha \in (\mathbb{Z}[\zeta]/\mathfrak{p})^*} \chi^j(\alpha)\zeta_p^{\text{tr}(\alpha)}$, where ζ_p is a primitive p^{th} root of unity, tr denotes the trace from $\mathbb{Z}[\zeta]/\mathfrak{p}$ to $\mathbb{Z}/p\mathbb{Z}$, and $1 \leqq j \leqq \ell - 1$. Then if $\tau_a \in \text{Gal}\big(K(\zeta_p)/K\big)$ is such that $\tau_a(\zeta_p) = \zeta_p^a$, we have immediately that $\tau_a(g_{\chi^j}) = \left(\dfrac{a^j}{\mathfrak{p}}\right) g_{\chi^j}$.

By Gauss's Lemma (Lemma 8), if S is a set of representatives for the action of μ_ℓ on $J_0[\mathfrak{p}]'$, then $v(\mathfrak{p}) = \prod_{u \in S} w_0(u) \in K(\zeta_p)$ has the property that $\tau_a\big(v(\mathfrak{p})\big) = \left(\frac{a}{\mathfrak{p}}\right) v(\mathfrak{p})$, so $v(\mathfrak{p})^j / g_{\chi^j} \in K^\times$, and

$$g_{\chi^j}^\ell = \prod_{u \in J_0[\mathfrak{p}]'} w_0(u)^j / \beta^\ell, \tag{51}$$

for some $\beta \in K^\times$. By (50) and (51), using that g_{χ^j} is an algebraic integer of absolute value $\sqrt{N\mathfrak{p}}$, we get immediately that

$$(g_{\chi^j}^\ell) = \prod_{i=1}^{\ell-1} \sigma_i(\mathfrak{p})^{\langle ji^{-1} \rangle}, \tag{52}$$

which is the Stickelberger relation for the factorization of Gauss sums. Kubota [Kub2] considered (1) an analogue of Stickelberger's relation for abelian functions, and since both (52) and examples of (1) follow from Theorem 3, we also think of Theorem 3 as a generalized Stickelberger relation, which is why we so named section 4. Shimura and Taniyama noted [ST] that the congruence relation of the theory of complex multiplication of abelian varieties applied to J_1 gave a part of Stickelberger's theorem on annihilating ideal classes. The argument above shows that Stickelberger's theorem is also directly related to the arithmetic of the torus J_0.

From (52), for any $1 \leqq a \leqq \ell - 2$, one immediately gets that the factorization of the Jacobi sum $J(\bar{\chi}, \bar{\chi}^a) = -g_{\bar{\chi}} g_{\bar{\chi}^a} / g_{\bar{\chi}a+1}$ is $\prod_{\sigma \in \Phi_a} \sigma^{-1}(\mathfrak{p})$. Lemma 15 shows that $\alpha_\mathfrak{p}$ has the same ideal factorization as $J(\bar{\chi}, \bar{\chi}^a)$, and that they have the same absolute value in every complex embedding. Hence they differ by a root of unity, and since both are congruent to $1 \bmod \lambda^2$ (see [I2] and Lemma 15), they are equal. This recovers the result of Weil [W4] that the $\alpha_\mathfrak{p}$ are just the Jacobi sums $J(\bar{\chi}, \bar{\chi}^a)$ (see [Gre]).

If $\mathfrak{p}$ is a first degree prime, then the remark in section 4 says we can take $w_0 = t_1$ as defined in section 5. Then if $\mathfrak{p} = (p, \zeta - a)$ for some $a \in \mathbb{Z}$, we have $u \in J_0[\mathfrak{p}]$ if and only if

$$t_1(u) = \sum_{j=1}^{\ell} \zeta^{-j} \zeta_p^{ia^j}, \tag{53}$$

for some $i \in \mathbb{Z}/p\mathbb{Z}$. The product of the sums in (53) were studied by Cauchy, who established (51) in this case (see [Lo] and [Br] for recent results). Hence (51) can be considered as a generalization of the relationship between these classical products and Gauss sums. In the cubic and biquadratic case, Loxton studied the arguments of the product of the sums in (53) [Lo]. In addition, in the case $\ell = 3$, if π is a first degree prime in $\mathbb{Z}[\zeta]$, taking $w_0 = t_1$, Philipbar [P] calculated some values of $\beta_\pi = v((\pi))/g_\chi \in \mathbb{Z}[\zeta]$, and for the first 1250 values of $p = N\pi$, found that

$$\log(|\beta_\pi|)$$

is very nearly a linear function in p. It would be nice to have a better understanding of this phenomenon.

Finally we note that Matthews produced formulas for cubic and biquadratic Gauss sums in terms of torsion points on the elliptic curves $y^2 - y = x^3$ and $y^2 = x^3 - x$ [Ma1], [Ma2].

Related Manin-Mumford problems. As in the proof of Proposition 4, Proposition 3 and Theorem 3 give a function $w_a \in K(J_a)$ which is regular and non-zero at all $u \in J_a[\mathfrak{p}]'$. We see therefore, that if E is the divisor of zeros of w_a, then E is a divisor upon which $J_a[\mathfrak{p}]'$ does not lie.

The best explicit result in this direction is due to Anderson [A], who using p-adic soliton theory, showed that if $\mathfrak{p} \subset \mathbb{Z}[\zeta]$ is a first degree prime prime to λ, then

$$J_a[\lambda\mathfrak{p}] \cap \Theta = J_a[\lambda] \cap \Theta.$$

When $a = 1$, C_a is hyperelliptic, and one can be more explicit about the functions in J_a that can be used as the parameters of a formal group at the origin. Let $J = J_1$, $\Phi = \Phi_1$. Using the techniques of this paper, we can show:

Theorem A. *Let $\mathfrak{p} \neq (\lambda)$ be a first or second degree prime of $\mathbb{Z}[\zeta]$. Then for any $n \geqq 1$, $J[\lambda\mathfrak{p}^n] \cap \Theta = J[\lambda] \cap \Theta$.*

We can sometimes say something more for primes $\mathfrak{p}$ of higher degree. Let $c(p, \Phi)$ be a choice of type coset representatives for p and Φ, and $\chi(r, j)$, $1 \leqq r \leqq s$, $j \in \mathbb{Z}/d_r\mathbb{Z}$, the corresponding exponential indexing of $\{1, \ldots, g\}$. In line with Proposition 1, we call $\sum_{z \in \mathbb{Z}/d_r\mathbb{Z}} p^{\langle e_{r,j} - e_{r,z} \rangle_f}$ the *exponent* attached to $\chi(r, j)$. If r is such that there is a unique $j' \in \mathbb{Z}/d_r\mathbb{Z}$ such that $\chi(r, j')$ has minimal exponent, we say that $\chi(r, j')$ is *admissible* for p. Let $[\cdot]$ denote the greatest integer function. If $0 \leqq k \leqq g - 1$ is such that $[(g + k + 1)/2] = \chi(r, j')$ for some $\chi(r, j')$ admissible for p, then we call k *good* for p. Let A_p denote the set of all k which are good for p, which depends only on the residue class of $p \bmod \ell$.

Let P be the divisor class of $(0, 0) - \infty$ in J. Since $[\zeta]P = P$, $P \in J[\lambda]$. For any $Q \in J$, let Θ_Q denote the image of Θ under translation by the addition of Q.

Theorem B. *$J[\mathfrak{p}]' \cap \Theta_{[b]P}$ is empty for all $b \in \pm(A_p \cup \{g\})$.*

The proofs of these theorems are in [Gra2]. For some more general results, see [Si]. See [T2] for a summary of what is known about $\kappa(C_a) \cap J_{a,\mathrm{tors}}$.

References

[A] *G. Anderson*, Torsion points on Jacobians of quotients of Fermat curves and p-adic soliton theory, Invent. Math. **118** (1994), no. 3, 475–492.

[Ba] *A. Bayad*, Loi de réciprocité quadratique dans les corps quadratiques imaginaires, Ann. Inst. Fourier **48** (1995), 1223–1237.

[BEW] *B. Berndt*, *R. Evans*, and *K. Williams*, Gauss and Jacobi Sums, Canadian Math. Soc. Ser. Monogr. Adv. Texts **21**, Wiley, New York 1998.

[Br] *J. Brinkhuis*, On a comparison of Gauss sums with products of Lagrange resolvents, Comp. Math. **93** (1994), 155–170.

[C] *J. W. S. Cassels*, On Kummer Sums, Proc. London Math. Soc. (3) **21** (1970), 19–27.
[CF] *J. W. S. Cassels* and *A. Fröhlich*, eds., Algebraic Number Theory, Academic Press, London 1967.
[CG] *N. Childress* and *D. Grant*, Formal groups of twisted multiplicative groups and *L*-series, Proc. Symp. Pure Math. **58.2** (1995), 89–102.
[CM] *R. Coleman* and *W. McCallum*, Stable reduction of Fermat curves and Jacobi sum Hecke characters, J. reine angew. Math. **385** (1988), 41–101.
[D] *V. G. Drinfeld*, Elliptic Modules, Mat. Sb. **94** (1974), 561–592.
[E] *G. Eisenstein*, Beweis der allgemeinsten Reziprozitätsgesetze zwichen reellen und komplexen Zahlen, Ber. K. Akad. Wiss. Berlin (1850), 189–198.
[Gra1] *D. Grant*, A proof of quintic reciprocity using the arithmetic of $y^2 = x^5 + 1/4$, Acta Arith. **LXXV.4** (1996), 321–337.
[Gra2] *D. Grant*, Torsion on theta divisors of hyperelliptic Fermat jacobians, Compos. Math. **140** (2004), 1432–1438.
[Gre] *R. Greenberg*, On the Jacobian variety of some algebraic curves, Compos. Math. **42** (1981), no. 3, 345–359.
[HT] *M. Harris* and *R. Taylor*, On the geometry and cohomology of some simple Shimura varieties, Ann. Math. Stud. **151**, Princeton 2001.
[Ha] *M. Hazewinkel*, Formal Groups and Applications, Academic Press, New York 1978.
[Hilb] *D. Hilbert*, The Theory of Algebraic Number Fields, Springer-Verlag, Berlin 1998. Translation by I. Adamson of "Die Theorie der algebraischen Zahlkörper".
[Hill1] *R. Hill*, Space forms and higher metaplectic groups, Math. Ann. **310** (1998), 735–775.
[Hill2] *R. Hill*, A geometric proof of a reciprocity law, Nagoya Math. J. **137** (1995), 77–144.
[Ho] *T. Honda*, Invariant differentials and *L*-functions: reciprocity laws for quadratic fields and elliptic curves over $\mathbb{Q}$, Rend. Sem. Mat. Univ. Padova **49** (1973), 323–335.
[IR] *K. Ireland* and *M. Rosen*, A classical introduction to modern number theory, GTM **84**, Springer-Verlag 1982.
[I1] *K. Iwasawa*, Local Class Field Theory, Oxford-New York 1986.
[I2] *K. Iwasawa*, A note on Jacobi sums, Sympos. Math. **15** (1975), 447–459.
[Kub1] *T. Kubota*, Reciprocities in Gauss' and Eisenstein's number fields, J. reine angew. Math. **208** (1961), 39–59.
[Kub2] *T. Kubota*, An application of the power residue theory to some abelian functions, Nagoya Math. J. **27** (1966), 51–54.
[Kub3] *T. Kubota*, Geometry of numbers and class field theory, Japan. J. Math. (N.S.) **13** (1987), no. 2, 235–275.
[Kub4] *T. Kubota*, The foundation of class field theory based on the principles of space diagrams, Sugaku **44** (1992), no. 1, 1–12.
[Kub5] *T. Kubota*, On the field extension by complex multiplication, Trans. AMS **118** (1965), no. 6, 113–122.
[KO] *T. Kubota* and *S. Oka*, On the deduction of the class field theory from the general reciprocity of power residues, Nagoya Math. J. **160** (2000), 135–142.
[Kum] *E. Kummer*, Über die allgemeinen Reziprozitätsgesetze der Potenzreste, Ber. K. Akad. Wiss. Berlin (1858), 158–171.
[La] *S. Lang*, Complex Multiplication, Springer-Verlag, Berlin 1983.
[Le] *F. Lemmermeyer*, Reciprocity Laws From Euler to Eisenstein, Springer-Verlag, Berlin 2000.
[Lo] *J. H. Loxton*, Products related to Gauss sums, J. reine angew. Math. **268/269** (1974), 53–67.
[Ma1] *C. R. Matthews*, Gauss sums and elliptic functions: I. The Kummer sum, Invent. math. **52** (1979), 163–185.
[Ma2] *C. R. Matthews*, Gauss sums and elliptic functions: II. The quartic sum, Invent. Math. **54** (1979), no. 1, 23–52.
[Mi] *J. Milne*, Abelian Varieties, and Jacobian Varieties, in: G. Cornell, J. Silverman, eds., Arithmetic Geometry, Springer-Verlag, New York (1986), 103–150, 167–212.
[P] *D. Philipbar*, On Products and Gauss Sums, Master's Thesis, University of Colorado at Boulder, 1996.
[R] *K. Ribet*, Division fields of abelian varieties with complex multiplication, Soc. Math. France (2) **2** (1980), 75–94.
[ST] *G. Shimura* and *Y. Taniyama*, Complex Multiplication of Abelian Varieties and its Applications to Number Theory, The Mathematical Society of Japan, 1961.
[Si] *B. Simon*, Torsion points on a theta divisor in the Jacobian of a Fermat quotient, Ph.D. Thesis, University of Colorado at Boulder, 2003.
[T1] *P. Tzermias*, Explicit rational functions on Fermat curves and a theorem of Greenberg, Compos. Math. **122** (2000), no. 3, 337–345.

[T2] *P. Tzermias*, The Manin-Mumford conjecture: a brief survey, Bull. London Math. Soc. **32** (2000), no. 6, 641–652.
[W1] *A. Weil*, Introduction to E.E. Kummer, Collected Papers, Vol. 1, Springer-Verlag, New York (1975), 1–11.
[W2] *A. Weil*, Review of "Mathematische Werke, by Gotthold Eisenstein", Bull. Am. Math. Soc. **82** (1976), 658–663.
[W3] *A. Weil*, Two lectures on number theory, past and present, Ensiegn. Math. **XX** (1974), 87–110.
[W4] *A. Weil*, Jacobi Sums as Grössencharaktere, Trans. Amer. Math. Soc. **73** (1952), 487–495.

Department of Mathematics, University of Colorado at Boulder, Boulder, CO 80309-0395, USA
e-mail: grant@boulder.colorado.edu

Eingegangen 11. September 2002, in revidierter Fassung 22. März 2004