The Scheme-Theoretic Theta Convolution

by Shinichi Mochizuki

September 1999

Contents:

§0. Introduction

§1. The Scheme-Theoretic Fourier Transform

§2. Discrete Gaussians and Gauss Sums

§3. Review of Degree Computations in [HAT]

§4. The Fourier Transform of an Algebraic Theta Function:
The Case of an Étale Lagrangian Subgroup

§5. The Fourier Transform of an Algebraic Theta Function:
The Case of a Lagrangian Subgroup with Nontrivial Multiplicative Part

§6. Generic Properties of the Norm

§7. Some Elementary Computational Lemmas

§8. The Various Contributions at Infinity

§9. The Main Theorem

§10. The Theta Convolution

§0. Introduction

In this paper, we continue our development of the theory of the Hodge-Arakelov Comparison Isomorphism of [HAT]. Our main result concerns the *invertibility of the coefficients of the Fourier transform of an algebraic theta function.* Using this result, we obtain a modified version of the Hodge-Arakelov Comparison Isomorphism of [HAT], which we refer to as the *Theta-Convoluted Comparison Isomorphism.* The significance of this modified version is that the principle obstruction to the application of the theory of [HAT] to diophantine geometry — namely, the *Gaussian poles* — partially vanishes in the theta-convoluted context. Thus, the results of this paper bring the theory of [HAT] *one step closer to possible application to diophantine geometry.*

Perhaps the simplest way to explain the *main idea* of the present paper is the following: The theory of [HAT] may be thought of as a sort of discrete, scheme-theoretic version of the theory of the *classical Gaussian* e^{-x^2} *(on the real line) and its derivatives* (cf. [HAT], Introduction, §2). The reason for the appearance of the "Gaussian poles" — which, as remarked above, constitute the principle obstruction to the application of the theory of [HAT] to diophantine geometry — is that, if, for instance, $P(-)$ is a polynomial with constant coefficients, then, at its most *fundamental combinatorial level*, the "comparison isomorphism" of [HAT] may be thought of as the mapping

$$P(-) \mapsto P(\frac{\partial}{\partial x})\ e^{-x^2} = P(-2x) \cdot e^{-x^2}$$

from a certain *space of polynomials* — which constitutes the *de Rham side* of the comparison isomorphism — to a certain space of *set-theoretic functions* — which constitutes the *étale side* of the comparison isomorphism. Roughly speaking, in order to make this morphism into an isomorphism, it is necessary to *eliminate the extra factor of* e^{-x^2} *on the right*. Once this extra factor is eliminated, the mapping $P(-) \mapsto P(-2x)$ is "manifestly" an isomorphism.

The approach of [HAT] to making this mapping into an isomorphism is to introduce *poles into the de Rham side* of the morphism (i.e., the "Gaussian poles"), which amounts (relative to the above discussion) to artificially tensoring the left-hand side of the morphism with the "symbol" e^{x^2}, which then is to map to the "function" e^{x^2}. Once this operation is performed, the right-hand side becomes $P(-2x)e^{-x^2} \cdot e^{x^2} = P(-2x)$, so we get an isomorphism $P(-) \mapsto P(-2x)$ as desired.

The problem with this approach of [HAT] is that for diophantine applications, one wishes to *leave the de Rham side of the comparison isomorphism untouched*. On the other hand, although one wishes to modify the étale side, one wants to modify it in such a way that the resulting modified étale side *still admits a natural Galois action*, which is necessary in order to construct the *arithmetic Kodaira-Spencer morphism* (cf. [HAT], Chapter IX, §3, as well as Remark 2 following Theorem 10.1 in the present paper).

In the present paper, the approach that we take may be explained in terms of the above discussion as follows: Instead of modifying the de Rham side of the comparison morphism, we modify the étale side by *"tensoring it with the inverse of the line bundle defined by the image on the étale side of the element '1' (on the de Rham side)."* Of course this image is simply e^{-x^2}, so dividing by this image amounts to multiplying by e^{x^2} on the étale side, thus giving us the desired isomorphism $P(-) \mapsto P(-2x)$.

Of course, in the theory of [HAT] and the present paper, we are not working literally with the Gaussian or even classical theta functions, but rather their *discrete algebraic analogues*. Thus, it is not surprising that many of the technical computations of this paper involve certain *discrete analogues of the classical Gaussian on the real line* (cf. §2). Since the correspondence between theta functions and Gaussian is, in essence, that the Gaussian represents the Fourier transform of a theta function, multiplying by a Gaussian corresponds, at the level of theta functions, to the operation of *convolution*. Thus, the operation which we wish to perform (cf. the preceding paragraph) on the étale side of the comparison isomorphism is to apply the *inverse of convolution with the theta function*. In the present paper, we refer to the operation of convolution with the theta function as the *"theta convolution."* Thus, the key technical result that is necessary in order to realize the philosophical idea explained above is a result concerning the *invertibility of the theta convolution*. Put another way, since our theta functions (in the theory of [HAT] and the present paper) are the *algebraic theta functions of Mumford* (cf. [Mumf1,2,3]), we thus see that the result that we need is a result concerning the *invertibility of the coefficients of the Fourier transform of certain algebraic theta functions*.

This result is the *first main result of this paper* (Theorem 9.1). We refer to §9 for explicit technical details concerning its statement. In a word, this result states that the coefficients of the Fourier transform of certain algebraic theta functions are *invertible in characteristic* 0 *away from the divisor at infinity* (i.e., the locus where the elliptic curve in question degenerates). Moreover, in mixed characteristic and near the divisor at infinity, we analyze explicitly the extent to which these coefficients fail to be invertible. In fact, the proof of this result proceeds precisely by comparing the degree of the line bundle (on the moduli stack of elliptic curves) of which the *norm* of the Fourier transform (i.e., the product of its coefficients) is a section to the degree of the zero locus of this norm in a neighborhood of the divisor at infinity. A rather complicated calculation reveals that these two degrees coincide. This *coincidence of degrees* implies that the norm is therefore invertible (in characteristic 0) away from the divisor at infinity. Finally, we apply our first main result to prove our *second main result*, i.e., the *theta-convoluted comparison isomorphism* (Theorem 10.1).

Before proceeding, we would like to explain several ways to think about the contents of this paper. First of all, the fact that the coefficients of the Fourier transform of certain algebraic theta functions are invertible away from the divisor at infinity appears (to the knowledge of the author) to be *new* (i.e., it does not seem to appear in the classical theory of theta functions). Thus, one way to interpret Theorem 9.1 is as a result which implies the existence of certain *interesting, new modular units*. It would be interesting to see if this point of view can be pursued further (cf. the Remark following Theorem 9.1).

Another way to think about the contents of this paper is the following. The classical representation of the Fourier expansion of a theta function — i.e., the representation which states that the Fourier coefficients are essentially a "Gaussian" — arises from the Fourier expansion of the restriction of a theta function to a certain *particular cycle* (or copy of the circle $\mathbf{S^1}$) on the elliptic curve E in question. More explicitly, if one thinks of this elliptic curve E as being

$$E = \mathbf{C}^\times / q^{\mathbf{Z}}$$

then this special cycle is the image of the natural copy of $\mathbf{S^1} \subseteq \mathbf{C}^\times$. In the present context, we are considering discrete analogues of this classical complex theory, so instead of working with this $\mathbf{S^1}$, we work with its *d-torsion points* (for some fixed positive integer d), i.e., $\boldsymbol{\mu}_d \subseteq \mathbf{S^1} \subseteq \mathbf{C}^\times$.

On the other hand, in order to obtain a theory valid over the entire moduli stack of elliptic curves, we must consider Fourier expansions of theta functions restricted not just to this special cyclic subgroup of order d, i.e., $\boldsymbol{\mu}_d \subseteq E$, (with respect to which the Fourier expansion is particularly simply and easy to understand), but rather with respect to an *arbitrary* cyclic subgroup of order d. Viewed from the classical complex theory, considering Fourier expansions arising from more general restriction subgroups amounts to considering the *functional equation of the theta function.* In the classical complex theory, Gauss sums arise naturally in the functional equation of the theta function. Thus, *it is not surprising that Gauss sums (and, in particular, their invertibility) also play an important role in the theory of the present paper.*

In fact, returning to the theory of the Gaussian on the real line, one may recall that one "important number" that arises in this theory is the *integral of the Gaussian* (over the real line). This integral is (roughly speaking) $\sqrt{\pi}$. On the other hand, in the theory of this paper, Gaussians correspond to "discrete Gaussians" (cf. §2), so integrals of Gaussians correspond to "Gauss sums." That is to say, *Gauss sums may be thought of as a sort of discrete analogue of* $\sqrt{\pi}$. Thus, the appearance of Gauss sums in the theory of this paper is also natural from the point of view of the above discussion of the "main idea" involving Gaussians.

Indeed, this discussion of discrete analogues of Gaussians and $\sqrt{\pi}$ leads one to suspect that there is also a natural *p-adic analogue* of the theory of this paper involving the *p-adic ring of periods* $\mathbf{B}_{\text{crys}}$. Since this ring of periods contains a certain copy of $\mathbf{Z}_p(1)$ which may be thought of as a "p-adic analogue of π," it is thus natural to suspect that in a p-adic analogue of the theory of this paper some "square root of this copy of $\mathbf{Z}_p(1)$" — and, in particular, its *invertibility* — should play an analogously important role to the role played by the invertibility of Gauss sums in the present paper. We hope to develop such a p-adic theory in a future paper (cf. also [HAT], Introduction, §5.1).

Finally, we explain the contents of the various §'s of this paper. In §1, we define and discuss the elementary properties of the Fourier transform of a finite flat group scheme. In §2, we discuss the "discrete Gaussians" and their "integrals" (Gauss sums) that arise in the computations of this paper. In §3, we formalize the necessary technical details concerning the Fourier transform of an algebraic theta function. This formalization results in the appearance of various degrees of line bundles and divisors on the moduli stack of elliptic curves which were computed in [HAT]; in §3, we review these computations. In §4, 5, we estimate the degree of vanishing of the norm of the Fourier transform of an algebraic theta function in a neighborhood of infinity. It turns out that these computations differ somewhat depending on the "position" of certain auxiliary torsion subgroups of the elliptic curve that are necessary in order to define our Fourier transform. Roughly speaking, the necesssary computations may be separated into two cases or parts, depending on the position of these auxiliary torsion subgroups. The two cases constitute, respectively, the content of §4, 5. In §6, we investigate when the norm of the Fourier transform is *generically zero.* In §7, we perform certain complicated but elementary computations that we use in §8. These computations are at the level of high-school mathematics and, in particular, have nothing to do with arithmetic geometry. In §8, we combine the estimates of §4, 5, with the computations of §7 to show the important "coincidence of degrees" discussed above. In §9, we record the consequences of this coincidence of degrees, i.e., our first main result (Theorem 9.1). In §10, we apply Theorem 9.1 to construct the *theta-convoluted comparison isomorphism* (whose realization was, as explained above, the main motivation for the theory of this paper).

§1. The Scheme-Theoretic Fourier Transform

In this §, we extend the well-known theory of *Fourier analysis on finite abelian groups* to its "schematic analogue," Fourier analysis on finite, flat commutative group schemes.

Let S be a scheme. Let

$$G \to S$$

be a *finite, flat commutative group scheme* over S. Write $\widehat{G} \to S$ for the *Cartier dual* of G ([Shz], §4). Thus, if T is an S-scheme, the T-valued points of $\widehat{G}$ are the homomorphisms G_T ($\stackrel{\text{def}}{=} G \times_S T$) $\to (\mathbf{G}_{\mathrm{m}})_T$.

Let $f \in \Gamma(G, \mathcal{O}_G)$ be a function on G. Then we define its *Fourier transform* $\widehat{f} \in \Gamma(\widehat{G}, \mathcal{O}_{\widehat{G}})$ as follows: The value of $\widehat{f}$ on a T-valued point $\widehat{\gamma} \in \widehat{G}(T)$ (where T is an S-scheme) is given by:

$$\widehat{f}(\widehat{\gamma}) \stackrel{\text{def}}{=} \int_{G_T/T} f \cdot (\widehat{\gamma})^{-1}$$

Here, we think of $\widehat{\gamma}$ as an (invertible) function on G_T, and denote by "$\int_{G_T/T}$" the *trace morphism* $\mathcal{O}_{G_T} \to \mathcal{O}_T$ (which is well-defined since $G \to S$ is finite and flat). Since this definition is functorial in T, we thus obtain a well-defined element $\widehat{f} \in \Gamma(\widehat{G}, \mathcal{O}_{\widehat{G}})$. This completes the definition of the Fourier transform of f. In the following, we shall also write

$$\mathcal{F}_G(f)$$

(or $\mathcal{F}(f)$, when the choice of G is clear) for $\widehat{f}$.

Next, let $f, g \in \Gamma(G, \mathcal{O}_G)$ be two functions on G. Then in addition to the *usual product* $f \cdot g \in \Gamma(G, \mathcal{O}_G)$, we also have the *convolution (product)*

$$f * g \in \Gamma(G, \mathcal{O}_G)$$

of f, g, defined by:

$$(f * g)(\gamma) \stackrel{\text{def}}{=} \int_{\gamma' \in G} f(\gamma \cdot (\gamma')^{-1}) \cdot g(\gamma')$$

(for T-valued points $\gamma \in G(T)$). Finally, let us write $\mathcal{I}(f)$ for the function obtained by pulling f back via the inversion morphism $[-1] : G \to G$ on G.

Proposition 1.1. *Suppose that $G \to S$ is of* constant rank $|G|$, *and that the integer $|G|$ is a* nonzero divisor *on S. Then we have:*

(i.) $|G| \cdot \mathcal{I}(f) = \mathcal{F}_{\widehat{G}}(\mathcal{F}_G(f))$.

(ii.) $|G| \cdot \mathcal{F}_G(f \cdot g) = \mathcal{F}_G(f) * \mathcal{F}_G(g)$.

(iii.) $\mathcal{F}_G(f * g) = \mathcal{F}_G(f) \cdot \mathcal{F}_G(g)$. *for any $f \in \Gamma(G, \mathcal{O}_G)$.*

Proof. Since $|G|$ is a nonzero divisor on S, we may assume without loss of generality that $|G|$ is invertible on S, and hence that $G \to S$ is *étale* ([Shz], §4, Corollary 3). Then by replacing S by a finite étale cover of S, we may assume that $G \to S$ is of the form $\Gamma \times S$, where Γ is a finite abelian group (in the category of sets). In this case, the stated identities are well-known (cf., e.g., [DyMc], §4.5). ○

Now let us suppose that we have an exact sequence

$$0 \to H \to G \to K \to 0$$

of finite, flat commutative group schemes over S. Taking Cartier duals, we obtain an exact sequence

$$0 \to \widehat{K} \to \widehat{G} \to \widehat{H} \to 0$$

If $f \in \Gamma(K, \mathcal{O}_K)$ is a function on K, then by pull-back, we obtain a function $f|_G \in \Gamma(G, \mathcal{O}_G)$, which we also denote by $\mathrm{Res}^G_K(f)$.

Now suppose that $K \to S$ is of constant rank $|K|$, and that the integer $|K|$ is a nonzero divisor on S. Then it follows that over $S_K \stackrel{\mathrm{def}}{=} S[|K|^{-1}]$, $K|_{S_K} \to S_K$ is *étale*, hence that $H|_{S_K}$ is open and closed in G_{S_K}. Now suppose that $f \in \Gamma(H, \mathcal{O}_H)$ is a function on H, and that $\widetilde{f} \in \Gamma(G, \mathcal{O}_G)$ is a function on G such that $\widetilde{f}|_H = f$, and, moreover, that $\widetilde{f}|_{S_K}$ vanishes on the open and closed subscheme $G_{S_K} \backslash H_{S_K} \subseteq G_{S_K}$. Then we shall write

$$\mathrm{Ind}^G_H(f)$$

for $\widetilde{f}$. Thus, $\mathrm{Ind}^G_H(f)$ is the result of "extending f by zero" to a function on G. Note that such an $\widetilde{f}$ is necessarily *unique* (since S_K is schematically dense in S, and $\widetilde{f}$ is uniquely determined on H_{S_K} and $G_{S_K} \backslash H_{S_K}$).

Proposition 1.2. *Suppose that* $G \to S$ *is of* constant rank $|G|$, *and that the integer* $|G|$ *is a* nonzero divisor *on* S. *Then:*

(i.) For any $f \in \Gamma(K, \mathcal{O}_K)$, *we have:* $\mathcal{F}_G(\mathrm{Res}^G_K(f)) = |H| \cdot \mathrm{Ind}^{\widehat{G}}_{\widehat{K}}(\mathcal{F}_K(f))$.

(ii.) For any $f \in \Gamma(H, \mathcal{O}_H)$ *such that* $\mathrm{Ind}^G_H(f)$ *exists, we have:* $\mathcal{F}_G(\mathrm{Ind}^G_H(f)) = \mathrm{Res}^{\widehat{G}}_{\widehat{H}}(\mathcal{F}_H(f))$.

(iii.) In particular, if 1_G *is the constant function* 1 *on* G, *and* $\delta_{0,G}$ *is the "delta distribution at the origin" (i.e., the function – defined after one inverts* $|G|$ *– which is* 1 *at the origin and* 0 *elsewhere), then* $\mathcal{F}_G(1_G) = |G| \cdot \delta_{0,\widehat{G}}$, *and* $\mathcal{F}_G(\delta_{0,G}) = 1_{\widehat{G}}$.

Proof. Just as in the proof of Proposition 1.1, it suffices to verify the result under the assumption that G is of the form $\Gamma \times S$, where Γ is a finite abelian group of order invertible on S. But in this case, the result is well-known (cf., e.g., [DyMc], §4.5). ○

§2. Discrete Gaussians and Gauss Sums

One of the key fundamental results in classical Fourier analysis on the real line is that the *Fourier transform of a Gaussian is* (up to a factor which typically involves $\sqrt{\pi}$) *a Gaussian.* In this §, we examine the *discrete analogue* of this phenomenon. Here, the discrete analogue of a classical Gaussian is a *"discrete Gaussian,"* while the discrete analogue of the factor that appears when one applies the Fourier transform is a *Gauss sum.*

We maintain the notations of §1. Here, we assume further that the group scheme G is (noncanonically) isomorphic to $\mathbf{Z}/N\mathbf{Z}$, for some positive integer N which is *invertible* on S. In the following, we assume that some particular isomorphism

$$G \cong (\mathbf{Z}/N\mathbf{Z}) \times S$$

has been chosen. Note that the choice of such an isomorphism endows G with a structure of "*ring scheme*" (i.e., arising from the ring structure of $\mathbf{Z}/N\mathbf{Z}$). In particular, if $\gamma \in G(S)$, then we shall write (for $i \in \mathbf{Z}_{\geq 1}$) $i \cdot \gamma$ (respectively, γ^i) for the result of adding (respectively, multiplying) — i.e., relative to this ring scheme structure — γ to (respectively, by) itself a total of i times. Often, by abuse of notation, we shall simply write $\gamma \in G$ for the N elements of $G(S)$ defined by $\mathbf{Z}/N\mathbf{Z}$. Let

$$\chi : G \to \mathbf{G}_{\mathrm{m}}$$

be a *faithful* character of the group scheme G. Then consider the function

$$\psi : G \to \mathbf{G}_{\mathrm{m}}$$

defined by $\psi(\gamma) \stackrel{\mathrm{def}}{=} \chi(\gamma^2)$.

Definition 2.1. Such a function ψ on G (defined for some χ as above) will be referred to as a *discrete Gaussian (on G)*.

In the following, we would like to consider the *Fourier transform of a discrete Gaussian* and show that this Fourier transform is essentially another discrete Gaussian (times a certain Gauss sum).

Let us first observe that since χ is *faithful*, the characters of G are all of the form $\gamma \mapsto \chi(c \cdot \gamma)$, for some $c \in \mathbf{Z}/N\mathbf{Z}$. Let us then compute the Fourier coefficient of ψ for the character χ_c corresponding to an *even* $c = 2c'$ (where $c' \in \mathbf{Z}/N\mathbf{Z}$):

$$\begin{aligned}\int_{\gamma \in G} \psi(\gamma) \cdot \chi(-c \cdot \gamma) &= \int_{\gamma \in G} \chi(\gamma^2 - 2c' \cdot \gamma) \\ &= \chi(-(c')^2) \cdot \int_{\gamma \in G} \chi((\gamma - c')^2) \\ &= \chi(-(c')^2) \cdot \int_{\gamma \in G} \chi(\gamma^2)\end{aligned}$$

Write

$$\mathcal{G}(\chi, N) \stackrel{\mathrm{def}}{=} \int_{\gamma \in G} \chi(\gamma^2)$$

for the Gauss sum defined by χ. Then the above calculation shows in particular that for N *odd* (in which case all c may be written as $c = 2c'$), the Fourier transform $\mathcal{F}(\psi)$ is the function $\chi_c \mapsto \mathcal{G}(\chi, N) \cdot \chi(-\frac{1}{4} \cdot c^2)$. This function is clearly a constant ($= \mathcal{G}(\chi, N)$) multiple of a discrete Gaussian.

Next, we consider the more complicated case when N is *even*. When N is even, we shall write $N = 2M$. First, let us suppose that N is *divisible by* 4. In this case, every $\gamma \in \mathbf{Z}/N\mathbf{Z}$ satisfies:

$$(\gamma + M)^2 \equiv \gamma^2 + 2M \cdot \gamma + M^2 \equiv \gamma^2$$

(modulo N). Thus, it follows that the function ψ on $G \cong \mathbf{Z}/N\mathbf{Z}$ is obtained by pulling back a function on $G/M \cdot G \cong \mathbf{Z}/M\mathbf{Z}$ via the natural projection $G \to G/M \cdot G$. In particular, it follows from Proposition 1.2, (i.), that the Fourier coefficients of ψ are zero for odd c (i.e., c which cannot be written in the form $c = 2c'$). Thus, we see that the above calculation implies that the Fourier transform $\mathcal{F}(\psi)$ in this case is the result of extending by zero a constant ($= \mathcal{G}(\chi, N)$) multiple of a function on $\mathbf{Z}/M\mathbf{Z} \cong 2 \cdot \widehat{G} \subseteq \widehat{G}$ whose pull-back to $\mathbf{Z}/N\mathbf{Z}$ is a discrete Gaussian on $\mathbf{Z}/N\mathbf{Z}$.

Definition 2.2. If N is divisible by 4, and $\widetilde{\psi}$ is a function on G/MG whose pull-back to G is a discrete Gaussian ψ on G, then we shall refer to $\widetilde{\psi}$ as a *reduced discrete Gaussian on* G/MG. If N is odd, then we will also refer to arbitrary discrete Gaussians (as in Definition 2.1) as *reduced discrete Gaussians.*

Finally, we consider the case of *odd* M. In this case, every $\gamma \in \mathbf{Z}/N\mathbf{Z}$ satisfies:

$$(\gamma + M)^2 \equiv \gamma^2 + 2M \cdot \gamma + M^2 \equiv \gamma^2 + M$$

(modulo N). In particular, it follows from Proposition 1.2, (i.), that the Fourier coefficients of ψ are *zero for even* c (i.e., c which can be written in the form $c = 2c'$). Thus, we must compute the coefficients for odd $c = 2c' + M$ (where we note that since M is odd, we may take c' to be *even*):

$$\begin{aligned}
\int_{\gamma \in G} \psi(\gamma) \cdot \chi(-c \cdot \gamma) &= \int_{\gamma \in G} \chi(\gamma^2 - 2c' \cdot \gamma - M \cdot \gamma) \\
&= \chi(-(c')^2) \cdot \int_{\gamma \in G} \chi((\gamma - c')^2 + M \cdot \gamma) \\
&= \chi(-(c')^2) \cdot \int_{\gamma \in G} \chi(\gamma^2 + M \cdot \gamma)
\end{aligned}$$

Moreover,

$$\begin{aligned}
\int_{\gamma \in G} \chi(\gamma^2 + M \cdot \gamma) &= \int_{\gamma \in 2 \cdot G} \chi(\gamma^2) - \int_{\gamma \in 2 \cdot G} \chi((\gamma + M)^2) \\
&= \int_{\gamma \in 2 \cdot G} \chi(\gamma^2) - \int_{\gamma \in 2 \cdot G} \chi(\gamma^2 + 2M \cdot \gamma + M^2) \\
&= 2 \cdot \int_{\gamma \in 2 \cdot G} \chi(\gamma^2) \\
&= 2 \cdot \mathcal{G}(\chi^2, M)
\end{aligned}$$

(where we note that since χ is faithful, we have $\chi(M^2) = \chi(M) = -1$).

Next, let us recall from the computations of Gauss sums in [Lang], pp. 86-87, that we have

$$\mathcal{G}(\chi^2, M) = \epsilon_{\chi^2, M} \cdot \sqrt{M} \neq 0$$

where $\epsilon^4_{\chi^2,M} = 1$. Similarly, if N is *odd*, then we have

$$\mathcal{G}(\chi, N) = \epsilon_{\chi,N} \cdot \sqrt{N} \neq 0$$

where $\epsilon^4_{\chi,N} = 1$. Finally, if N is *even*, then we have

$$\mathcal{G}(\chi, N) = \epsilon_{\chi,N} \cdot (1+i) \cdot \sqrt{N} \neq 0$$

where $\epsilon^4_{\chi,N} = 1$, $i = \sqrt{-1}$. Thus, we see that we have proven the following result:

Proposition 2.3. *Let $\chi : G \to \mathbf{G}_\mathrm{m}$ be a* faithful *character. Let $\psi(\gamma) \stackrel{\mathrm{def}}{=} \chi(\gamma^2)$ be the* discrete Gaussian *on G associated to χ. For $c \in \mathbf{Z}/N\mathbf{Z}$, write χ_c for the character $G \to \mathbf{G}_\mathrm{m}$ defined by $\chi_c(\gamma) \stackrel{\mathrm{def}}{=} \chi(c \cdot \gamma)$. Then:*

(i.) Suppose that N is odd. *Then*

$$\{\mathcal{F}(\psi)\}(\chi_c) = \mathcal{G}(\chi, N) \cdot \chi(-\frac{1}{4} \cdot c^2)$$

where $\mathcal{G}(\chi, N) \stackrel{\mathrm{def}}{=} \sum_{\gamma \in G} \chi(\gamma^2) = \epsilon_{\chi,N} \cdot \sqrt{N} \neq 0$ (and $\epsilon^4_{\chi,N} = 1$). Thus, $\mathcal{F}(\psi)$ is equal to a nonzero multiple of a discrete Gaussian on $\widehat{G}$.

(ii.) Suppose that $N = 2M$ is even, *but M is* odd. *Then $\{\mathcal{F}(\psi)\}(\chi_c) = 0$ if $c \in 2\mathbf{Z}/N\mathbf{Z}$. If $c = 2c' + M$ for $c' \in 2\mathbf{Z}/N\mathbf{Z}$, then*

$$\{\mathcal{F}(\psi)\}(\chi_c) = 2 \cdot \mathcal{G}(\chi^2, M) \cdot \chi(-(c')^2)$$

where $\mathcal{G}(\chi^2, M) \stackrel{\mathrm{def}}{=} \sum_{\gamma \in 2\mathbf{Z}/N\mathbf{Z}} \chi(\gamma^2) = \epsilon_{\chi^2,M} \cdot \sqrt{M} \neq 0$ (and $\epsilon^4_{\chi^2,M} = 1$). Thus, $\mathcal{F}(\psi)$ is equal to a nonzero multiple of the translate by $M \in \mathbf{Z}/N\mathbf{Z} \cong \widehat{G}$ of the extension by zero of a discrete Gaussian on $2 \cdot \widehat{G}$ ($\subseteq \widehat{G}$).

(iii.) Suppose that $N = 2M$ and M are even. *Then $\{\mathcal{F}(\psi)\}(\chi_c) = 0$ if $c \in (2\mathbf{Z} + M)/N\mathbf{Z}$. If $c = 2c'$ for $c' \in \mathbf{Z}/N\mathbf{Z}$, then*

$$\{\mathcal{F}(\psi)\}(\chi_c) = \mathcal{G}(\chi, N) \cdot \chi(-(c')^2)$$

where $\mathcal{G}(\chi, N) \stackrel{\mathrm{def}}{=} \sum_{\gamma \in G} \chi(\gamma^2) = \epsilon_{\chi,N} \cdot (1+i)\sqrt{N} \neq 0$ (and $\epsilon^4_{\chi,N} = 1$, $i = \sqrt{-1}$). Thus, $\mathcal{F}(\psi)$ is equal to a nonzero multiple of the extension by zero of a function on $2 \cdot \widehat{G} \cong \mathbf{Z}/M\mathbf{Z}$ whose pull-back to $\mathbf{Z}/N\mathbf{Z}$ is a discrete Gaussian on $\mathbf{Z}/N\mathbf{Z}$.

Thus, in summary, "the Fourier transform of a reduced discrete Gaussian is itself a nonzero multiple (i.e., by a certain Gauss sum) of a reduced discrete Gaussian."

Remark. Frequently, we will work with finite, flat group schemes G of order N over bases where N is not necessarily invertible, or with finite, étale group schemes which are étale locally, but not necessarily globally, isomorphic to $\mathbf{Z}/N\mathbf{Z}$. In these cases, we shall also refer to functions on G as *(reduced) discrete Gaussians* if they become (reduced) discrete Gaussians as in Definition 2.2 after N is inverted, and a suitable isomorphism with $\mathbf{Z}/N\mathbf{Z}$ is chosen over some étale covering of the original base.

§3. Review of Degree Computations in [HAT]

The purpose of this § is to review various aspects of the theory of [HAT] in characteristic 0, and to explain the fundamental set-up of the theory of the present paper.

Let $S^{\log}$ be a *$\mathbf{Z}$-flat fine noetherian log scheme*. Let us assume that we are given a *log elliptic curve* (cf. [HAT], Chapter III, §1.1)

$$C^{\log} \to S^{\log}$$

over $S^{\log}$ which is smooth over a schematically dense open subscheme of S. It thus follows that the "divisor at infinity" (i.e., the pull-back via the associated classifying morphism of the divisor at infinity of $(\overline{\mathcal{M}}_{1,0})_{\mathbf{Z}}$) is a Cartier divisor $D \subseteq S$. Thus, just as in [HAT], Chapter IV, §4,5, we have a stack S_∞ obtained from S by adjoining the roots of the q-parameters at the locus $D \subseteq S$ over which $C^{\log} \to S^{\log}$ degenerates. Over S_∞, we have the smooth group scheme

$$f : E_{\infty,S} \to S_\infty$$

whose connected components at the points of bad reduction are in natural one-to-one correspondence with $\mathbf{Q}/\mathbf{Z}$. The metrized line bundles of [Zh] may be thought of as living on $E_{\infty,S}$.

Let m, d be positive integers such that m *does not divide* d. Let

$$\eta \in E_{\infty,S}(S_\infty)$$

be a torsion point of order m. Then in [HAT], Chapter V, §1, we associated to this data *certain metrized line bundles*

$$\overline{\mathcal{L}}_{\mathrm{st},\eta}, \quad \overline{\mathcal{L}}^{\mathrm{ev}}_{\mathrm{st},\eta}$$

In the following discussion, we will denote by

$$\overline{\mathcal{L}}$$

the metrized line bundle $\overline{\mathcal{L}}_{\mathrm{st},\eta}$ (respectively, $\overline{\mathcal{L}}^{\mathrm{ev}}_{\mathrm{st},\eta}$) if d is *odd* (respectively, *even*). Note that the *push-forward* $f_*\overline{\mathcal{L}}$ of this metrized line bundle to S_∞ defines a metrized vector bundle on S_∞. Moreover, this metrized line bundle admits the action of a certain natural *theta group scheme* $\mathcal{G}_{\overline{\mathcal{L}}}$ (cf. [HAT], Chapter IV, §5).

Next, let us assume that we are given finite, flat (i.e., over S_∞) *subgroup schemes*

$$G, H \subseteq E_{\infty,S}$$

which are étale locally isomorphic to $\mathbf{Z}/d\mathbf{Z}$ in characteristic 0 (i.e., after tensoring with $\mathbf{Q}$), and which satisfy

$$H \times G = {}_dE_{\infty,S} \subseteq E_{\infty,S}$$

(where ${}_dE_{\infty,S}$ is the kernel of multiplication by d on $E_{\infty,S}$). We shall refer to G as the *restriction subgroup* (since its principal use will be as a collection of points to which we will restrict sections of $\overline{\mathcal{L}}$), and H as the *Lagrangian subgroup* (since its primary use will be to descend $\overline{\mathcal{L}}$ — cf. [HAT], Chapter IV, Theorem 1.4).

In the following discussion, we would like to consider *the Fourier transforms of restrictions of sections of* $\overline{\mathcal{L}}$ *to* G. If d is *odd*, then the datum of G is sufficient for this purpose. If, however, d is *even*, then in order to take the Fourier transform of a restricted section, we need a canonical *trivialization* of the restriction $\overline{\mathcal{L}}|_G$. Recall, however, from [HAT], Chapter IV, Theorem 1.6, that we only have such a canonical trivialization over $2 \cdot G$, not over all of G. Thus, in the case that d is *even*, we must assume that we are also given the following data: First of all, let us write $\widetilde{E}_{\infty,S} \stackrel{\mathrm{def}}{=} E_{\infty,S}/(d_0 \cdot G)$, where $d_0 \stackrel{\mathrm{def}}{=} \frac{1}{2}d$. Thus, the multiplication by 2 morphism on $\widetilde{E}_{\infty,S}$ factors into a composite of two morphisms of degree 2:

$$\widetilde{E}_{\infty,S} \to E_{\infty,S} \to \widetilde{E}_{\infty,S} = E_{\infty,S}/(d_0 \cdot G)$$

Moreover, the 2-torsion of $\widetilde{E}_{\infty,S}$ surjects onto $d_0 \cdot G \subseteq E_{\infty,S}$. Thus, it follows by elementary group theory that $G \subseteq E_{\infty,S}$ is contained in the image of the d-torsion of $E_{\infty,S}$. Write $\widetilde{G} \subseteq \widetilde{E}_{\infty,S}$ for the inverse image of $G \subseteq E_{\infty,S}$ in $\widetilde{E}_{\infty,S}$, and $G_{\widetilde{E}/E} \stackrel{\mathrm{def}}{=} \mathrm{Ker}(\widetilde{E}_{\infty,S} \to E_{\infty,S}) \subseteq \widetilde{E}_{\infty,S}$. Then we have an exact sequence

$$0 \to G_{\widetilde{E}/E} \to \widetilde{G} \to G \to 0$$

of finite, flat group schemes over S_∞ which are annihilated by d. Then in the *even case*, we assume that we given the following *additional data*:

a subgroup scheme $G_{\mathrm{spl}} \subseteq \widetilde{G}$ *that splits the above exact sequence* (i.e., maps isomorphically onto G).

If we pull the metrized line bundle $\overline{\mathcal{L}}$ back to $\widetilde{E}_{\infty,S}$, the resulting metrized line bundle $\overline{\mathcal{L}}|_{\widetilde{E}_{\infty,S}}$ has degree $2d$, hence *admits* (by [HAT], Chapter IV, Theorem 1.6) *a canonical trivialization over any subgroup scheme of* $\widetilde{E}_{\infty,S}$ *annihilated by* d *— in particular, over* G_{spl}.

Moreover, it follows (from [HAT], Chapter IV, Theorem 1.6, (2)) that *if we modify the splitting* G_{spl} *by some homomorphism* $\alpha : G \to G_{\widetilde{E}/E}$*, then the resulting trivialization differs from the trivialization corresponding to the given* G_{spl} *by a factor given by the function* $\beta \circ \alpha : G \to \boldsymbol{\mu}_2$, for some fixed homomorphism $\beta : G_{\widetilde{E}/E} \to \boldsymbol{\mu}_2$ (which is independent of α).

Remark. Suppose just for the remainder of this Remark that S is of *characteristic* 0. Since $G_{\widetilde{E}/E}$ is a finite étale group scheme of rank 2 over S_∞, $G_{\widetilde{E}/E}$ is abstractly isomorphic to $\{\pm 1\} \cong \boldsymbol{\mu}_2$ (where the "$\cong$" holds since we are in characteristic zero). Moreover, I *claim* that β *is the unique isomorphism between* $G_{\widetilde{E}/E}$ *and* $\boldsymbol{\mu}_2$. Indeed, if this were not the case, then β would be trivial, and we would obtain that the trivialization of $\overline{\mathcal{L}}|_{G_{\mathrm{spl}}} = \overline{\mathcal{L}}|_G$ is *independent* of the choice of splitting G_{spl}. Moreover, if the trivialization is independent of the splitting for this particular choice of G, then it follows (by considering the action of Galois on G in the universal case, i.e., finite étale coverings of the moduli stack $(\mathcal{M}_{1,0})_{\mathbf{Q}}$) that this holds for all G. On the other hand, if this holds for all G, then it would follow that the canonical section of [HAT], Chapter IV, Theorem 1.6, extends to a section defined over $K_{\overline{\mathcal{L}}}$ (i.e., not just $2 \cdot K_{\overline{\mathcal{L}}}$) whose image is contained in the subscheme $\mathcal{S}_{\overline{\mathcal{L}}}$ of symmetric elements. Also, let us observe that since the image of this extended section lies in $\mathcal{S}_{\overline{\mathcal{L}}}$, it follows (by the same argument as that used to prove the latter part of [HAT], Chapter IV, Theorem 1.6, (2)) that the formula "$\{\sigma(a+b)\cdot\sigma(a)^{-1}\cdot\sigma(b)^{-1}\}^2 = [a,b]$" of [HAT], Chapter IV, Theorem 1.6, (2), also applies to this extended section. But this implies that the *Weil pairing* $[-,-]$ on d-torsion points of the universal elliptic curve over $(\mathcal{M}_{1,0})_{\mathbf{Q}}$ *admits a square root*, which is absurd. (Indeed, the field of constants in (i.e., algebraic closure of $\mathbf{Q}$ in) the field of definition of these d-torsion points in the universal case is $\mathbf{Q}(e^{2\pi i/d})$, but *the existence of such a square root would imply that* $\mathbf{Q}(e^{2\pi i/2d}) \subseteq \mathbf{Q}(e^{2\pi i/d})$, which is false, since d is *even*.) This completes the proof of the *claim*.

The purpose of the above Remark was to convince the reader that the *introduction of the splitting* G_{spl} *is, in fact, unavoidable.* Thus, one way to summarize the above discussion in a fashion which is independent of the choice of splitting G_{spl} is the following: There is a natural $\mathrm{Hom}(G, \boldsymbol{\mu}_2)$-*torsor*

$$\mathcal{T}_2 \to S_\infty$$

determined by $E_{\infty,S}$, G, which is *nontrivial in general.* Moreover, over $\mathcal{T}_2$, the restriction $\overline{\mathcal{L}}|_G$ admits a *canonical trivialization.*

Thus, at any rate, if we assume that we are given a splitting G_{spl} whenever d is even, then regardless of the parity of d, we obtain (cf. [HAT], Chapter IX, §3) a natural isomorphism

$$\overline{\mathcal{L}}|_G \cong \mathcal{O}_G \otimes_{\mathcal{O}_{S_\infty}} \mathcal{K}$$

where $\mathcal{K} \stackrel{\mathrm{def}}{=} \overline{\mathcal{L}}|_e$ is the restriction of $\overline{\mathcal{L}}$ to the identity section $\in E_{\infty,S}(S_\infty)$. Similarly, (since our assumptions on G and H are *identical*) if we assume that we are given a splitting H_{spl} of the analogous exact sequence for H

$$0 \to H_{\widetilde{E}/E} \to \widetilde{H} \to H \to 0$$

whenever d is even, then regardless of the parity of d, we obtain (cf. [HAT], Chapter IX, §3) a natural *subgroup scheme*

$$\mathcal{H} \subseteq \mathcal{G}_{\overline{\mathcal{L}}}$$

which is *Lagrangian* in the sense of [MB], Chapitre V, Définition 2.5.1. Note that:

(1) After possibly replacing S by a finite flat cover, such an H_{spl} always exists.

(2) Unlike in [HAT], Chapter IV, §1, we do *not* assume that $\mathcal{H}$ is isomorphic either to $\mathbf{Z}/d\mathbf{Z}$ or $\boldsymbol{\mu}_d$ over S.

Let us write

$$E_{\infty_H,S} \stackrel{\mathrm{def}}{=} E_{\infty,S}/H$$

for the quotient of $E_{\infty,S}$ by H. Thus, we have a natural isogeny $E_{\infty,S} \to E_{\infty_H,S}$. Moreover, since we have a lifting $\mathcal{H} \subseteq \mathcal{G}_{\overline{\mathcal{L}}}$ of H, we also get a natural metrized line bundle $\overline{\mathcal{L}}_H$ on $E_{\infty_H,S}$ that descends $\overline{\mathcal{L}}$. Write $f_H : E_{\infty_H,S} \to S_\infty$ for the structure morphism of $E_{\infty_H,S}$. Note that the relative degree (i.e., with respect to f_H) of $\overline{\mathcal{L}}_H$ is 1. Thus, it follows that $(f_H)_*\overline{\mathcal{L}}_H$ is a *metrized line bundle* on S_∞. Write

$$\mathcal{M} \stackrel{\mathrm{def}}{=} \{(f_H)_*\overline{\mathcal{L}}_H\}^{-1}$$

Next, let us observe that if we compose the *Fourier transform* $\mathcal{F}_G$ (tensored with $\mathcal{K}$) discussed in §1 with the trivialization isomorphism $\overline{\mathcal{L}}|_G \cong \mathcal{O}_G \otimes_{\mathcal{O}_{S_\infty}} \mathcal{K}$ reviewed above, we get a morphism

$$\overline{\mathcal{L}}|_G \to \mathcal{O}_{\widehat{G}} \otimes_{\mathcal{O}_{S_\infty}} \mathcal{K}$$

If we then compose this morphism with the morphism obtained by restricting sections of $\overline{\mathcal{L}}_H$ (first to $E_{\infty,S}$ and then) to G, we obtain a morphism

$$\mathcal{E} : \mathcal{M}^{-1} \to \mathcal{O}_{\widehat{G}} \otimes_{\mathcal{O}_{S_\infty}} \mathcal{K}$$

which maps a section of $\overline{\mathcal{L}}_H$ to the *Fourier expansion of the corresponding algebraic theta function*. This "theta Fourier expansion morphism" is the main topic of the present paper.

Note that since $\mathcal{O}_{\widehat{G}}$ has a natural $\mathcal{O}_{S_\infty}$*-algebra structure*, it makes sense to speak of the norm of a section of $\mathcal{O}_{\widehat{G}}$. Thus, this norm will form a section of $\mathcal{O}_{S_\infty}$. In particular, if we *take the norm of* $\mathcal{E}$, we obtain a section

$$\nu \in \Gamma(S_\infty, \mathcal{M}^{\otimes d} \otimes \mathcal{K}^{\otimes d})$$

The main technical goal of the present paper is to show that ν *is invertible on the interior* $U_S \subseteq S_\infty$ *of* S_∞ (i.e., the open subscheme where the log structure is trivial). This goal will be achieved by computing the order of the zeroes of ν at the points at infinity, and *comparing the sum of these orders to the degree of the metrized line bundle* $\mathcal{M}^{\otimes d} \otimes \mathcal{K}^{\otimes d}$ (in the universal case, i.e., when the base is given by the moduli stack of log elliptic curves — note that over such a base, the notion of "degree" makes sense), which is given by Propositions 3.1, 3.2, below. It turns out that these two numbers *coincide*. This will suffice to show that ν is *invertible on the interior* $U_S \stackrel{\text{def}}{=} S - D$.

Remark. If we change the *choice of splitting* G_{spl}, then the resulting trivialization gets multiplied (cf. the above discussion) by some character $G \to \boldsymbol{\mu}_2$. The effect of such a multiplication on the Fourier transform (cf. Proposition 1.1, (ii.)) is given by the automorphism of $\mathcal{O}_{\widehat{G}}$ induced by translation by this character $G \to \boldsymbol{\mu}_2$ (regarded as an element of $\widehat{G} = \text{Hom}(G, \mathbf{G}_{\text{m}})$). Clearly, the norm is unaffected by such automorphisms. In particular, *the norm* ν *is independent of the choice of splitting*. One way to summarize this observation in a way that does not involve G_{spl} explicitly is the following: The $\text{Hom}(G, \boldsymbol{\mu}_2)$-torsor $\mathcal{T}_2 \to S_\infty$ discussed above defines (via the natural inclusion $\text{Hom}(G, \boldsymbol{\mu}_2) \hookrightarrow \text{Hom}(G, \mathbf{G}_{\text{m}}) = \widehat{G}$) a natural $\widehat{G}$*-torsor*

$$\mathcal{T}_{\widehat{G}} \to S_\infty$$

Moreover, *the Fourier transform of a section of* $\overline{\mathcal{L}}|_G$ *is naturally given by an element of* $\mathcal{O}_{\mathcal{T}_{\widehat{G}}} \otimes_{\mathcal{O}_{S_\infty}} \mathcal{K}$.

For the remainder of this §, let us assume that S is a *smooth, proper* (not necessarily connected) *one-dimensional scheme over* $\mathbf{C}$ (the complex number field — in fact, any field of characteristic zero will do). Also, let us assume that the log structure of $S^{\log}$ arises from a finite number of points. For simplicity, we assume that $C^{\log} \to S^{\log}$ degenerates at all the points at which the log structure of $S^{\log}$ is nontrivial. Recall from [HAT], Chapter IV, §5, that, under these assumptions, it makes sense to consider the *degree* of a metrized vector bundle on S_∞, and from [HAT], Chapter V, Proposition 1.1, that:

Proposition 3.1. *We have:* $\deg(\mathcal{M}) = \frac{1}{24d}(d-1) \cdot \log(q)$.

Remark. Just as in [HAT], degrees will always be expressed in "$\log(q)$" units, i.e., those units for which the divisor at infinity of the moduli stack $(\overline{\mathcal{M}}_{1,0})_{\mathbf{C}}$ has degree 1.

Proof. Since we are working here with "H-invariants" (cf. [HAT], Chapter IV, Theorem 1.4) of the push-forward that appears in [HAT], Chapter V, Proposition 1.1, the degree of $\mathcal{M}^{-1}$ is $\frac{1}{d}$ times the degree appearing in *loc. cit.* ○

Proposition 3.2. *We have:* $\deg(\mathcal{M}^{\otimes d} \otimes \mathcal{K}^{\otimes d}) = \frac{1}{24}(d-1) \cdot \log(q) + d \cdot [\overline{\mathcal{L}} \cdot e]$. *Moreover,* $[\overline{\mathcal{L}} \cdot e] = 0$ *if d is* odd, *and*

$$= -\frac{1}{d} \cdot \sum_{\iota} \{\phi_1(-d \cdot \eta_\iota + \frac{1}{2}) \cdot \log(q) = -\frac{1}{d} \cdot \sum_{\iota} \{\phi_1(-d \cdot \eta_\iota + \frac{1}{2}) - \phi_1(-d \cdot \eta_\iota)\} \cdot \log(q)$$

if d is even. *(Here, η_ι denotes the element of $\mathbf{Q}/\mathbf{Z}$ (i.e., the connected component of the special fiber of $E_{\infty,S} \to S_\infty$) defined at the point at infinity ι by the torsion point $\eta \in E_{\infty,S}(S_\infty)$, and $\phi_1(\theta) = \frac{1}{2}\theta^2 - \frac{1}{2}|\theta| + \frac{1}{12}$ (for $|\theta| \leq \frac{1}{2}$) is the function of [HAT], Chapter IV, Proposition 4.4.)*

Proof. It remains only to remark that the computation of $[\overline{\mathcal{L}} \cdot e]$ follows from [HAT], Chapter V, Proposition 1.2. ○

The computation underlying the *coincidence of degrees* referred to above is quite complicated and forms the topic of §4-8. One of the ingredients that we will need in this computation is (a certain consequence of) the rather complicated degree computation carried out in [HAT], Chapter VI, §3. For d' a positive integer $\leq d$, let us consider the sums (cf. the computation in the proof of [HAT], Chapter VI, Theorem 3.1, which corresponds to the case $d' = d$)

$$\mathcal{Z}(d, d', m) \stackrel{\text{def}}{=} \sum_{\iota} \sum_{j=1}^{d'} \frac{1}{d} \cdot c_j(\text{Case } X_\iota) \cdot \log(q)$$

(where, just as in [HAT], sums over ι are to be interpreted as *averages*, in keeping with the principle that everything is to be in "$\log(q)$ units"). Put another way, this number is the sum of the d' smallest exponents of q that appear in the q-expansion of the theta functions that arise at the various points ι at infinity. It is not difficult to see that this number is determined uniquely by d, d', and m.

Proposition 3.3. *If d' is* odd*, then*

$$\mathcal{Z}(d, d', m) = \frac{d'}{24d}((d')^2 - 1) \cdot \log(q)$$

If d, d' are even*, then*

$$\begin{aligned}\mathcal{Z}(d, d', m) &= \frac{d'}{24d}((d')^2 - 1) \cdot \log(q) - \frac{d'}{d} \cdot \sum_{\iota} \phi_1(-d \cdot \eta_\iota + \frac{1}{2}) \cdot \log(q) \\ &= \frac{d'}{24d}((d')^2 - 1) \cdot \log(q) - \frac{d'}{d} \cdot \sum_{\iota} \{\phi_1(-d \cdot \eta_\iota + \frac{1}{2}) - \phi_1(-d \cdot \eta_\iota)\} \cdot \log(q)\end{aligned}$$

Here, η_ι denotes the element of $\mathbf{Q}/\mathbf{Z}$ (i.e., the connected component of the special fiber of $E_{\infty,S} \to S_\infty$) defined at the point at infinity ι by the torsion point $\eta \in E_{\infty,S}(S_\infty)$, and $\phi_1(\theta) = \frac{1}{2}\theta^2 - \frac{1}{2}|\theta| + \frac{1}{12}$ (for $|\theta| \leq \frac{1}{2}$) is the function of [HAT], Chapter IV, Proposition 4.4.

Proof. For d' *odd*, the result follows (even when d is even) from the computations in [HAT], Chapter VI, the portion of the proof of Theorem 3.1 entitled "Computation of the Degree in the Odd Case" (which reduce, essentially, to [HAT], Chapter V, Lemma 4.2). For d, d' *even*, the result follows from the computations in [HAT], Chapter VI, the portion of the proof of Theorem 3.1 entitled "Computation of the Degree in the Even Case." ○

Remark. Often, when the entire discussion consists of degrees "in $\log(q)$ units," we will omit the symbol "$\log(q)$," as in [HAT].

Finally, before proceeding, we would like to introduce some more notation. Let us write

$$m' \stackrel{\mathrm{def}}{=} \frac{m}{(m, d)}$$

Thus, put another way, m' is the *order of the torsion point $d \cdot \eta$*. Note that $\mathcal{Z}(d, d', m)$ depends only on d, d', and m', i.e., it may be thought of as a *function of these three variables*. When we wish to think of it that way, we shall write:

$$\mathcal{Z}'(d, d', m')$$

for $\mathcal{Z}(d, d', m)$.

§4. The Fourier Transform of an Algebraic Theta Function: The Case of an Étale Lagrangian Subgroup

In this §, we would like to estimate the order of vanishing of the section ν of §3 at those points at infinity where the Lagrangian subgroup $H \subseteq E_{\infty,S}$ is "*of étale type*," i.e., maps *injectively* into the group of connected components $\mathbf{Q}/\mathbf{Z}$ in the special fiber.

We maintain the notation of §3, except that in the present §, we work in a *neighborhood of infinity*, i.e., we assume that

$$S \stackrel{\text{def}}{=} \operatorname{Spec}(\mathbf{C}[[q^{\frac{1}{2md}}]])$$

(equipped with the log structure defined by the divisor $V(q^{\frac{1}{2md}})$) and that the one-dimensional semi-abelian scheme in question $E \to S$ (i.e., the one-dimensional semi-abelian scheme whose logarithmic compactification is $C^{\log} \to S^{\log}$) is the *Tate curve* "$\mathbf{G}_{\mathrm{m}}/q^{\mathbf{Z}}$." Write U for the standard multiplicative coordinate on the $\mathbf{G}_{\mathrm{m}}$ that uniformizes E. Since we chose the base S so that q admits a $2d$-th root in $\mathcal{O}_S$, it follows that our *Lagrangian and restriction subgroups* $H, G \subseteq E_{\infty,S}$, as well as the *splittings* $G_{\mathrm{spl}}, H_{\mathrm{spl}} \subseteq \widetilde{E}_{\infty,S}$ when d is *even*, are all defined over S (i.e., not just over S_∞). Let us denote the unique *"point at infinity"* (i.e., the special point of S) by ∞_S. Also, we set $n \stackrel{\text{def}}{=} 2m$ (as in [HAT], Chapter IV, §2,3).

Let us denote by $E'_{\infty,S}$ *another copy* of $E_{\infty,S}$. In the following, we would like to think of $E'_{\infty,S}$ as a covering of $E_{\infty,S}$, by means of the isogeny given by the morphism *"multiplication by n"*:

$$E'_{\infty,S} \xrightarrow{[n]} E_{\infty,S}$$

Write $\overline{\mathcal{L}}' \stackrel{\text{def}}{=} \overline{\mathcal{L}}|_{E'_{\infty,S}}$. Note that since $\overline{\mathcal{L}}'$ has degree $n^2 \cdot d$, it follows that

$$K_{\overline{\mathcal{L}}'} = {}_{n^2 \cdot d}E'_{\infty,S}$$

We would like to think of $E'_{\infty,S}$ as admitting a Schottky uniformization by "another copy of $\mathbf{G}_{\mathrm{m}}$," which we shall denote by $\mathbf{G}'_{\mathrm{m}}$. The standard multiplicative coordinate on $\mathbf{G}'_{\mathrm{m}}$ will be denoted by U'. Thus, $(U')^n = U$. Also, for various natural numbers N, we shall denote the copy of $\boldsymbol{\mu}_N$ that sits naturally inside $\mathbf{G}'_{\mathrm{m}}$ by $\boldsymbol{\mu}'_N$.

Next, let us observe that the natural action of $\mathbf{G}'_{\mathrm{m}}$ on the Schottky uniformization of $(E'_{\infty,S}, \overline{\mathcal{L}}')$ (cf., e.g., the discussion of [HAT], Chapter IV, §2,3) induces a natural action of $\boldsymbol{\mu}'_{n^2 \cdot d}$ on $\overline{\mathcal{L}}'$ (cf., e.g., the discussion at the beginning of [HAT], Chapter IV, §2) — that is, we get a homomorphism:

$$i_{\mathrm{Sch}} : \boldsymbol{\mu}'_{n^2 \cdot d} \hookrightarrow \mathcal{G}_{\overline{\mathcal{L}}'}$$

On the other hand, let us observe that since $\overline{\mathcal{L}}$ is defined by translating a symmetric line bundle by a torsion point of order m (and then readjusting the integral structure/metric — cf. the definitions of $\overline{\mathcal{L}}_{\mathrm{st},\eta}$, $\overline{\mathcal{L}}^{\mathrm{ev}}_{\mathrm{st},\eta}$ in [HAT], Chapter V, §1), it follows that if we forget about the adjustment of the metric, then $\overline{\mathcal{L}}'$ is *totally symmetric* (i.e., equal to the square of a symmetric line bundle). Moreover, it follows from the discussion preceding [HAT], Chapter V, Proposition 1.1, that the curvature of $\overline{\mathcal{L}}'$ is symmetric, which implies that $\overline{\mathcal{L}}'$ is, in fact, *totally symmetric as a metrized line bundle.* Thus, since n is *even*, it follows from [HAT], Chapter IV, Theorem 1.6, that the canonical section "σ" of *loc. cit.* defines a homomorphism:

$$i_{\sigma'} : \boldsymbol{\mu}'_{n \cdot d} \hookrightarrow \mathcal{G}_{\overline{\mathcal{L}}'}$$

(the fact that the content of [HAT], Chapter IV, Theorem 1.6, is still valid when we consider metrics follows as in the discussion of [HAT], Chapter IX, §3). Thus, it is natural to ask whether or not these two homomorphisms coincide on $\boldsymbol{\mu}'_{n \cdot d}$:

Lemma 4.1. *We have:* $i_{\sigma'} = i_{\mathrm{Sch}}|_{\boldsymbol{\mu}'_{n \cdot d}}$.

Proof. Recall that $\overline{\mathcal{L}}'$ is *totally symmetric as a metrized line bundle*, and that the action of $\mathbf{G}'_{\mathrm{m}}$ on the Schottky uniformization of the pair $(E'_{\infty,S}, \overline{\mathcal{L}}')$ is also *symmetric* (cf. [HAT], Chapter IV, §2). Thus, it follows that i_{Sch} maps into $\mathcal{S}_{\overline{\mathcal{L}}'}$. Then it follows from the definition of the canonical section "σ" in [HAT], Chapter IV, §1, (together with the fact that i_{Sch} is a *homomorphism*) that $i_{\mathrm{Sch}}|_{\boldsymbol{\mu}'_{n \cdot d}} = i_{\sigma'}$, as desired. ○

Next, let us recall that the push-forward $(f_H)_*(\overline{\mathcal{L}}_H)$ is generated by a section whose corresponding theta function is given by (cf. [HAT], Chapter V, Theorem 4.8; [HAT], Chapter VII, §6):

$$\sum_{k \in \mathbf{Z}} q^{\frac{1}{d}(\frac{1}{2} \cdot k^2 + (i_\chi/n) \cdot k)} \cdot U^k \cdot (U')^{i_\chi} \cdot \chi(k) \cdot \theta^m$$

for some character $\chi : \mathbf{Z} \to \boldsymbol{\mu}_n$ (where $n \stackrel{\mathrm{def}}{=} 2m$), and some integer $i_\chi \in \{-m, -m+1, \ldots, -1, 0, 1, \ldots, m-1\}$. Since "$(U')^{i_\chi} \cdot \theta^m$" essentially amounts to the trivialization in question, we see that the "actual theta *function*" is given by:

$$\Theta \stackrel{\mathrm{def}}{=} \sum_{k \in \mathbf{Z}} q^{\frac{1}{d}(\frac{1}{2} \cdot k^2 + (i_\chi/n) \cdot k)} \cdot U^k \cdot \chi(k)$$

Let us first consider the case where G is of *multiplicative type*, i.e., $G = \boldsymbol{\mu}_d \subseteq \mathbf{G}_{\mathrm{m}}$. This is in some sense the most *fundamental and important case* of the various cases (relative to the "position" of G, H inside ${}_dE_{\infty,S}$) that will be considered in this and the following §.

(As we saw in the Remark following Proposition 3.2, the norm ν is *independent* of the choice of G_{spl}. Moreover, let us note that since $d_0 \cdot G$ is *multiplicative*, the isogeny $\widetilde{E}_{\infty,S} \to E_{\infty,S}$ of §3 is "of étale type," i.e., it lies between $E_{\infty,S}$ and its Schottky uniformization. Put another way, this means that $\widetilde{E}_{\infty,S}$ is Schottky-uniformized by the same $\mathbf{G}_{\mathrm{m}}$ as $E_{\infty,S}$. Thus, it makes sense to stipulate that we take $G_{\mathrm{spl}} \stackrel{\mathrm{def}}{=} \boldsymbol{\mu}_d \subseteq \mathbf{G}_{\mathrm{m}}$.) In this case, restriction to G amounts to identifying U^k and $U^{k'}$ whenever $k \equiv k$ modulo d. Now according to the theory of [HAT], Chapter VIII, §2,3,4, there is a certain special set of d consecutive integers K_{Crit} such that the result of restricting the above theta function to $G = \boldsymbol{\mu}_d$ is given by:

$$\Theta_{\boldsymbol{\mu}} \stackrel{\mathrm{def}}{=} \sum_{k_0 \in \mathbf{Z}/d\mathbf{Z}} (U|_{\boldsymbol{\mu}_d})^{k_0} \cdot \Big(\sum_{k \in \mathbf{Z},\ k \equiv k_0 (\mathrm{mod}\ d)} q^{\frac{1}{d}(\frac{1}{2}\cdot k^2 + (i_\chi/n)\cdot k)} \cdot \chi(k) \Big)$$

$$= \sum_{k \in K_{\mathrm{Crit}}} q^{\frac{1}{d}(\frac{1}{2}\cdot k^2 + (i_\chi/n)\cdot k)} \cdot (U|_{\boldsymbol{\mu}_d})^k \cdot (\chi(k) + \epsilon_k) \cdot \{1 + (\text{smaller powers of } q)\}$$

where ϵ_k is a certain n-th root of unity if k is *exceptional* (cf. [HAT], Chapter VIII, Lemmas 4.3, 4.4), and $\epsilon_k = 0$ otherwise (i.e., if k is not exceptional). There is at most one exceptional k in the set K_{Crit}. Moreover, the exponents of q appearing in the above sum are precisely the d numbers $\frac{1}{d}\cdot c_j$ (for $j = 1, \ldots, d$) appearing in the definition of $\mathcal{Z}(d, d, m)$. Moreover, since the set K_{Crit} consists of k *consecutive* integers, it follows that the above function on $\boldsymbol{\mu}_d$ is essentially the *Fourier expansion* of the restriction of the theta function in question to $G = \boldsymbol{\mu}_d$. Thus, we obtain that the degree of vanishing at ∞_S of the norm ν constructed in §3 — which we shall denote by $\deg(\nu)$ — is $\geq$ the "ι portion" of the sum in the definition of $\mathcal{Z}(d, d, m)$, where ι corresponds to the point at infinity ∞_S where we have localized in the present discussion. (Here, we say "$\geq$," rather than "$=$" since we dot know whether or not the coefficient $\chi(k) + \epsilon_k$ which appeared above is nonzero.) In particular, if we average over all the possible ι's (which corresponds to all possible torsion points η of order precisely m, weighted in the proper fashion), we obtain that the resulting average $\mathrm{Avg}_\eta(\deg(\nu))$ satisfies the following:

Lemma 4.2. *We have:*

$$\mathrm{Avg}_\eta(\deg(\nu)) \geq \mathcal{Z}(d, d, m)$$

for any G of multiplicative type *(i.e., for which $G = \boldsymbol{\mu}_d \subseteq \mathbf{G}_{\mathrm{m}}$).*

Thus, it remains to consider the case when G is *not necessarily of multiplicative type*. Let us first observe that since $\mathrm{Im}(G) = \mathrm{Im}({}_dE_{\infty,S}) \subseteq E_{\infty_H,S}$ is *independent of* G, it follows that even in the case where G is not necessarily of multiplicative type, we are in effect restricting the sections of $(f_H)_*\overline{\mathcal{L}}_H$ to the *same points* as in the case where G is of multiplicative type. The effect of using a different (e.g., a non-multiplicative) G is that a different G results in a *different trivialization* at those points. Thus, in particular, the resulting theta functions differ by a factor given by some function $\psi : \boldsymbol{\mu}_d \rightarrow \mathbf{G}_{\mathrm{m}}$. Since ultimately we are interested in Fourier transforms of theta functions, we thus see that:

> The net effect (of using a non-multiplicative G) on the Fourier transform of the theta function in question is to *convolute by* $d^{-1} \cdot \mathcal{F}(\psi)$ (cf. Proposition 1.1, (ii.)).

Thus, in the following, we propose to compute ψ and its Fourier transform $\mathcal{F}(\psi)$, and then consider the degree of the zero locus at infinity of the convolution of $d^{-1} \cdot \mathcal{F}(\psi)$ with the Fourier transform of the theta function considered above.

To compute the difference ψ in trivializations arising from G, we must introduce some new notation, as follows. First, we write $G_{\boldsymbol{\mu}} \stackrel{\mathrm{def}}{=} \boldsymbol{\mu}_d \subseteq \mathbf{G}_{\mathrm{m}}$. Since H is of étale type, it follows that $G_{\boldsymbol{\mu}} \times H = {}_dE_{\infty,S}$. Note that since H injects into the group of connected components of the special fiber of $E_{\infty,S}$, we get a natural identification

$$H = \mathbf{Z}/d\mathbf{Z}$$

Thus, we shall think of ${}_dE_{\infty,S}$ as $G_{\boldsymbol{\mu}} \times H = \boldsymbol{\mu}_d \times \mathbf{Z}/d\mathbf{Z}$. Then relative to this decomposition, G may be written as the graph of some homomorphism $\alpha_G : \boldsymbol{\mu}_d \rightarrow \mathbf{Z}/d\mathbf{Z}$.

In fact, in order to calculate ψ, we will need to *lift the above data on* $E_{\infty,S}$ *to* $E'_{\infty,S}$. Of course, many of the lifted data on $E'_{\infty,S}$ will not be uniquely determined by the original data on $E_{\infty,S}$, but this will not matter, since different choices of lifts will not affect the end result. Thus, write

$$G'_{\boldsymbol{\mu}} \stackrel{\mathrm{def}}{=} \boldsymbol{\mu}'_{n^2 \cdot d}$$

(so $n \cdot G'_{\boldsymbol{\mu}}$ lifts $G_{\boldsymbol{\mu}}$) and choose an

$$H' = \mathbf{Z}/n^2 \cdot d\mathbf{Z} \subseteq E'_{\infty,S}$$

(where the identification of H' with $\mathbf{Z}/n^2 \cdot d\mathbf{Z}$ is assumed to be given by the natural homomorphism of H' into the group of connected components of the special fiber of $E'_{\infty,S}$) such that $n \cdot H'$ lifts H. Finally, we choose a $G' \subseteq {}_{n^2 \cdot d}E'_{\infty,S}$ defined by some homomorphism

$$\alpha_{G'} : \boldsymbol{\mu}'_{n^2 \cdot d} \rightarrow \mathbf{Z}/n^2 \cdot d\mathbf{Z}$$

such that $n \cdot G'$ lifts G. Let us write

$$\sigma' : 2 \cdot K_{\overline{\mathcal{L}}'} \rightarrow \mathcal{G}_{\overline{\mathcal{L}}'}$$

for the *canonical section* of [HAT], Chapter IV, Theorem 1.6.

We are now ready to *compute* $\psi : \boldsymbol{\mu}_d \to \mathbf{G}_{\mathrm{m}}$. Let $a \in \boldsymbol{\mu}_d = G_{\boldsymbol{\mu}}$. Select a lifting $a' \in n \cdot G'_{\boldsymbol{\mu}}$ of a. Let $a'_1 \in m \cdot G'_{\boldsymbol{\mu}}$ be such that $2 \cdot a'_1 = a'$. Write $b'_1 \stackrel{\mathrm{def}}{=} \alpha_{G'}(a'_1)$; $b' \stackrel{\mathrm{def}}{=} 2b'_1$; b for the image of b' in $E_{\infty,S}$ (i.e., $b = \alpha_G(a)$). Then it essentially follows from the definitions that:

$$\psi(\alpha) = \sigma'((a', b')) \cdot \sigma'(b')^{-1} \cdot \sigma'(a')^{-1} \cdot \chi_{\mathrm{ex}}(a')$$

where $\chi_{\mathrm{ex}} : n \cdot G'_{\boldsymbol{\mu}} \to \mathbf{G}_{\mathrm{m}}$ is a *character*. (Indeed, this essentially follows from the fact that σ', as well as the sections of $\mathcal{G}_{\overline{\mathcal{L}}}$ used in §3 to define the trivialization of $\overline{\mathcal{L}}|_G$ and the subgroup $\mathcal{H} \subseteq \mathcal{G}_{\overline{\mathcal{L}}}$ are all *homomorphisms* on $n \cdot H'$, $n \cdot G'$, G, and H. Thus, the restrictions of two such sections to the same subgroup differ from one another by various characters. This is what leads to the "extra factor" χ_{ex}.) On the other hand, by [HAT], Chapter IV, Theorem 1.6, (2), we have

$$\sigma'((a', b')) \cdot \sigma'(b')^{-1} \cdot \sigma'(a')^{-1} = ([b'_1, a'_1]')^2$$

(where $[-,-]'$ is the pairing associated to $\overline{\mathcal{L}}'$). Clearly, the right-hand side of this equality is a $2d$-th root of unity. Thus, (since $\psi(-)^d = 1$) we obtain that $\chi_{\mathrm{ex}}(-)^{2d} = 1$.

Now suppose that d is *odd*. In this case, we may choose a' and a'_1 to be of *odd order*. This implies that b' and and b'_1 are also of odd order. Since it makes sense to multiply elements of odd order by $\frac{1}{2}$, we thus obtain:

$$([b'_1, a'_1]')^2 = ([b', a']')^{\frac{1}{2}} = [b, a]^{\frac{1}{2}}$$

(where $[-,-]$ is the pairing associated to $\overline{\mathcal{L}}$). In particular, we get $\chi_{\mathrm{ex}}(-)^d = 1$. By abuse of notation, let us write $\chi_{\mathrm{ex}}(a)$ for $\chi_{\mathrm{ex}}(a')$. That is, we have:

$$\psi(a) = [a, \alpha_G(a)]^{-\frac{1}{2}} \cdot \chi_{\mathrm{ex}}(a)$$

for some $\chi_{\mathrm{ex}} : G_{\boldsymbol{\mu}} \to \boldsymbol{\mu}_d$. This completes the case when d is *odd*.

Now suppose that d is *even*. In this case, we obtain:

$$\psi(a) = ([a'_1, \alpha_{G'}(2a'_1)]')^{-1} \cdot \chi_{\mathrm{ex}}(a')$$

Note that a'_1 is well-defined up to the addition of an element $a'' \in m \cdot d \cdot G'_{\boldsymbol{\mu}} = \boldsymbol{\mu}'_{2n}$. Moreover, one checks easily that the pairing $(x, y) \mapsto [x, \alpha_{G'}(y)]'$ on $G'_{\boldsymbol{\mu}} \times G'_{\boldsymbol{\mu}}$ is *symmetric*. Thus,

$$
\begin{aligned}
[a_1' + a'', \alpha_{G'}(2a_1' + 2a'')]' &= [a_1', \alpha_{G'}(2a_1')]' \cdot [a'', \alpha_{G'}(2a_1')]' \cdot [a_1', \alpha_{G'}(2a'')]' \cdot [a'', \alpha_{G'}(2a'')]' \\
&= [a_1', \alpha_{G'}(2a_1')]' \cdot [a'', \alpha_{G'}(a')]' \cdot [a', \alpha_{G'}(a'')]' \cdot [a'', \alpha_{G'}(2a'')]' \\
&= [a_1', \alpha_{G'}(2a_1')]' \cdot [a'', \alpha_{G'}(2a')]' \cdot [a'', \alpha_{G'}(2a'')]' \\
&= [a_1', \alpha_{G'}(2a_1')]' \cdot [??, n \cdot d \cdot \alpha_{G'}(a' + a'')]' \\
&= [a_1', \alpha_{G'}(2a_1')]'
\end{aligned}
$$

where we use that $n \cdot d \cdot a' = 0$; (since d is *even*) $n \cdot d \cdot a'' = 0$. Thus, it follows that $([a_1', \alpha_{G'}(2a_1')]')^{-1}$ *depends only on* a (i.e., not on the choice of lifting a_1'). In particular, (since $\psi(a)$ manifestly only depends on a) we obtain that $\chi_{\mathrm{ex}}(a')$ *depends only on* a. By abuse of notation, we will write $\chi_{\mathrm{ex}}(a)$ for $\chi_{\mathrm{ex}}(a')$. Thus, in summary:

Lemma 4.3. *Let $a \in G_{\boldsymbol{\mu}} = \boldsymbol{\mu}_d$. Then if d is* odd, *then*

$$\psi(a) = [a, \alpha_G(a)]^{-\frac{1}{2}} \cdot \chi_{\mathrm{ex}}(a)$$

for some character $\chi_{\mathrm{ex}} : G_{\boldsymbol{\mu}} \to \boldsymbol{\mu}_d$. If d is even, *and $a_1' \in m \cdot G'_{\boldsymbol{\mu}}$ satisfies $2a_1' \mapsto a$, then*

$$\psi(a) = ([a_1', \alpha_{G'}(2a_1')]')^{-1} \cdot \chi_{\mathrm{ex}}(a)$$

for some character $\chi_{\mathrm{ex}} : G_{\boldsymbol{\mu}} \to \boldsymbol{\mu}_d$. In particular, if the homomomorphism $\alpha_G : \boldsymbol{\mu}_d \to \mathbf{Z}/d\mathbf{Z}$ is of order d_{ord}, *then it follows that (regardless of the parity of d) $\psi : \boldsymbol{\mu}_d \to \mathbf{G}_{\mathrm{m}}$ is — up to a factor given by the character χ_{ex} — the pull-back to $\boldsymbol{\mu}_d$ via the natural projection $\boldsymbol{\mu}_d \to \boldsymbol{\mu}_{d_{\mathrm{ord}}}$ (arising from the fact that d_{ord} divides d) of a* reduced discrete Gaussian *(cf. Definition 2.2) on $\boldsymbol{\mu}_{d_{\mathrm{ord}}}$.*

Proof. It remains only to verify that the bracketed portions of the expressions that we obtained above for $\psi(a)$ are indeed pull-backs of reduced discrete Gaussians as described. But this follows immediately from the definitions. Note that we use here the well-known fact that the pairings $[-,-]$; $[-,-]'$ are *nondegenerate.* (Indeed, if they were degenerate, then the theory of theta groups would imply that that $\overline{\mathcal{L}}'$ descends to some quotient of $E'_{\infty,S}$ by a finite group scheme of order $> n^2 \cdot d$, which is absurd, since $\deg(\overline{\mathcal{L}}') = n^2 \cdot d$.) ○

Thus, by Proposition 1.1, (ii.); Proposition 1.2, (i.); and Proposition 2.3, it follows that

> *The effect on the Fourier expansion of the theta function of the trivialization defined by G is given by translation by an element of $\widehat{G}$ (determined by the character χ_{ex}), followed by convolution by a function on $\widehat{G}$ of the form:*
>
> $$\epsilon \cdot d_{\mathrm{ord}}{}^{-\frac{1}{2}} \cdot \mathrm{Ind}_{\mathbf{Z}/d_{\mathrm{ord}}\mathbf{Z}}^{\mathbf{Z}/d\mathbf{Z}} \xi$$

where ϵ is a 4-th root of unity (respectively, $\sqrt{2}$ times an 8-th root of unity) if d_{ord} is odd (respectively, even), and ξ is a reduced discrete Gaussian on $\mathbf{Z}/d_{\text{ord}}\mathbf{Z}$.

Let us denote the function $\psi \cdot \Theta_{\boldsymbol{\mu}}$ on $\boldsymbol{\mu}_d$ (whose Fourier expansion is discussed above) by:

$$\Theta_G \stackrel{\text{def}}{=} \psi \cdot \Theta_{\boldsymbol{\mu}}$$

Then if we assume (so that we do not have to deal in the expression below with "exceptional k") that $d_{\text{ord}} \neq 1$ (note: the case $d_{\text{ord}} = 1$ was dealt with above in Lemma 4.2), then since the values of ξ are all $\in \boldsymbol{\mu}_{2d_{\text{ord}}}$, we obtain that (for $k_0 \in \mathbf{Z}/d\mathbf{Z}$) the coefficient of $(U|_{\boldsymbol{\mu}_d})^{k_0+k_{\text{ex}}}$ (where $k_{\text{ex}} \in \mathbf{Z}/d\mathbf{Z}$ is a fixed element determined by χ_{ex}) in the Fourier expansion of Θ_G is of the following form:

$$\begin{aligned}
&\text{Coeff}_{(U|_{\boldsymbol{\mu}_d})^{k_0+k_{\text{ex}}}}(\Theta_G) \\
&= \epsilon \cdot d_{\text{ord}}^{-\frac{1}{2}} \cdot \left\{ \sum_{k \in \mathbf{Z},\ k \equiv k_0 (\text{mod } d_{\text{eff}})} q^{\frac{1}{d}(\frac{1}{2} \cdot k^2 + (i_\chi/n) \cdot k)} \cdot \chi(k) \cdot \xi(\tfrac{k-k_0}{d_{\text{eff}}}) \right\} \\
&= \epsilon \cdot d_{\text{ord}}^{-\frac{1}{2}} \cdot \Big(\text{a } \boldsymbol{\mu}_{n \cdot d_{\text{ord}}}\text{-linear combination of those } q^{\frac{1}{d}(\frac{1}{2} \cdot k^2 + (i_\chi/n) \cdot k)} \\
&\qquad\qquad \text{for which } k \in K_{\text{Crit}},\ k \equiv k_0 \text{ (modulo } d_{\text{eff}}), \\
&\qquad\qquad + \text{ smaller powers of } q \Big)
\end{aligned}$$

where $d_{\text{eff}} \stackrel{\text{def}}{=} d/d_{\text{ord}}$. Since the power of q that appears in the coefficient of $(U|_{\boldsymbol{\mu}_d})^{k_0+k_{\text{ex}}}$ for $\Theta_{\boldsymbol{\mu}}$ is precisely the smallest exponent of q that appears in the q-expansion of the original theta function Θ *among those terms indexed by a k such that* $k \equiv k_0$ (modulo d), it thus follows that the *smallest power of* q that appears in the coefficient of $(U|_{\boldsymbol{\mu}_d})^{k_0+k_{\text{ex}}}$ for Θ_G is precisely the smallest exponent of q that appears in the q-expansion of the original theta function Θ *among those terms indexed by a k such that* $k \equiv k_0$ (modulo d_{eff}). Moreover, this smallest power either appears precisely *once* in $\text{Coeff}_{(U|_{\boldsymbol{\mu}_d})^{k_0+k_{\text{ex}}}}(\Theta_G)$, in which case *its* coefficient (i.e., in the "$\boldsymbol{\mu}_{n \cdot d_{\text{ord}}}$-linear combination" discussed above) is $\in \boldsymbol{\mu}_{n \cdot d_{\text{ord}}}$, or (cf. the "exceptional case" of [HAT], Chapter VIII, Lemmas 4.3, 4.4) it appears *twice* in $\text{Coeff}_{(U|_{\boldsymbol{\mu}_d})^{k_0+k_{\text{ex}}}}(\Theta_G)$, in which case *its* coefficient is the sum of two elements $\in \boldsymbol{\mu}_{n \cdot d_{\text{ord}}}$. Thus, by the same reasoning as that used to prove Lemma 4.2, we obtain the following, which is the main result of this §:

Theorem 4.4. *Assume that the Lagrangian subgroup H is* of étale type. *Then for any restriction subgroup $G \subseteq {}_dE_{\infty,S}$, we have:*

$$\text{Avg}_\eta(\deg(\nu)) \geq d_{\text{ord}} \cdot \mathcal{Z}(d, d_{\text{eff}}, m)$$

where $d = d_{\text{eff}} \cdot d_{\text{ord}}$*, and* d_{ord} *is the order of the difference between* G *and the multiplicative subgroup* $G_{\boldsymbol{\mu}} = \boldsymbol{\mu}_d$*.*

Moreover, the coefficient of the smallest power of q *in* $\text{Coeff}_{(U|_{\boldsymbol{\mu}_d})^{k_0+k_{\text{ex}}}}(\Theta_G)$ *is of the form:*

$$\epsilon \cdot d_{\text{ord}}{}^{-\frac{1}{2}} \cdot \ (\text{an element } \in \boldsymbol{\mu}_{n \cdot d_{\text{ord}}})$$

(where ϵ *is a* 4*-th root of unity (respectively,* $\sqrt{2}$ *times an* 8*-th root of unity) if* d_{ord} *is* odd *(respectively,* even*)), with at most one possible exceptional class of* k_0*'s in* $\mathbf{Z}/d_{\text{eff}}\mathbf{Z}$*. If this exception occurs,* and *the above inequality is an equality, then the coefficient of the smallest power of* q *in* $\text{Coeff}_{(U|_{\boldsymbol{\mu}_d})^{k_0+k_{\text{ex}}}}(\Theta_G)$ *in this case is of the form:*

$$\epsilon \cdot d_{\text{ord}}{}^{-\frac{1}{2}} \cdot \ (\text{a nonzero sum of two elements } \in \boldsymbol{\mu}_{n \cdot d_{\text{ord}}})$$

(where ϵ *is a* 4*-th root of unity (respectively,* $\sqrt{2}$ *times an* 8*-th root of unity) if* d_{ord} *is* odd *(respectively,* even*)).*

Proof. Note that here, we only obtain an inequality

$$\text{Avg}_\eta(\deg(\nu)) \geq d_{\text{ord}} \cdot \mathcal{Z}(d, d_{\text{eff}}, m)$$

because we do not know whether or not (in the "exceptional case" for $d_{\text{ord}} \neq 1$) the sum of the two $(n \cdot d_{\text{ord}})$-th roots of unity is nonzero. The factor of d_{ord} that appears on the right-hand side of this inequality arises because since the coefficient $\text{Coeff}_{(U|_{\boldsymbol{\mu}_d})^{k_0+k_{\text{ex}}}}(\Theta_G)$ depends only on the class of k_0 in $\mathbf{Z}/d_{\text{eff}}\mathbf{Z}$, zeroes occur with multiplicity $d/d_{\text{eff}} = d_{\text{ord}}$. ◯

§5. The Fourier Transform of an Algebraic Theta Function: The Case of a Lagrangian Subgroup with Nontrivial Multiplicative Part

In this §, we would like to estimate the order of vanishing of the section ν of §3 at those points at infinity where the Lagrangian subgroup $H \subseteq E_{\infty,S}$ is "*not necessarily of étale type*," i.e., does not necessarily map injectively into the group of connected components $\mathbf{Q}/\mathbf{Z}$ in the special fiber. In essence, our strategy will be to reduce to the case where H *is* of étale type, which was already dealt with in §4.

In this §, we maintain the notation of §4. However, unlike the situation of §4, *we do not assume that* H *is of étale type.* Write

$$H_{\boldsymbol{\mu}} \stackrel{\text{def}}{=} H \bigcap \boldsymbol{\mu}_d$$

(where $\boldsymbol{\mu}_d \subseteq \mathbf{G}_{\mathrm{m}}$ sits inside the copy of $\mathbf{G}_{\mathrm{m}}$ that uniformizes E). Note that the subgroup $H_{\boldsymbol{\mu}} \subseteq H$ denotes the portion of the Lagrangian subgroup H which is *purely of multiplicative type*. Write H_{et} for the image of H in the group of connected components in the special fiber of $E_{\infty,S}$ (a group which may be identified with $\mathbf{Q}/\mathbf{Z}$). Thus, we have an exact sequence:

$$0 \to H_{\boldsymbol{\mu}} \to H \to H_{\mathrm{et}} \to 0$$

We denote the *orders* of $H_{\boldsymbol{\mu}}$, H_{et} by: $h_{\boldsymbol{\mu}} \stackrel{\mathrm{def}}{=} |H_{\boldsymbol{\mu}}|$; $h_{\mathrm{et}} \stackrel{\mathrm{def}}{=} |H_{\mathrm{et}}|$. Thus, $h_{\boldsymbol{\mu}} \cdot h_{\mathrm{et}} = d$. Also, let us write

$$G_{\mathrm{et}} \stackrel{\mathrm{def}}{=} \mathrm{Ker}([h_{\boldsymbol{\mu}}] : G \to G)$$

for the kernel of multiplication by $h_{\boldsymbol{\mu}}$ on G. Thus, $|G_{\mathrm{et}}| = h_{\mathrm{et}}$.

Next, let us set:

$$E_{\infty_{\boldsymbol{\mu}},S} \stackrel{\mathrm{def}}{=} E_{\infty,S}/H_{\boldsymbol{\mu}}$$

On the other hand, let us recall the quotient $E_{\infty_H,S} \stackrel{\mathrm{def}}{=} E_{\infty,S}/H$ of §3. Since $H_{\boldsymbol{\mu}} \subseteq H$, it follows that the isogeny $E_{\infty,S} \to E_{\infty_H,S}$ factors into a composite of isogenies:

$$E_{\infty,S} \quad \stackrel{H_{\boldsymbol{\mu}}}{\longrightarrow} \quad E_{\infty_{\boldsymbol{\mu}},S} \quad \stackrel{H_{\mathrm{et}}}{\longrightarrow} \quad E_{\infty_H,S}$$

where $H_{\boldsymbol{\mu}} = \boldsymbol{\mu}_{(h_{\boldsymbol{\mu}})}$; $H_{\mathrm{et}} = \mathbf{Z}/h_{\mathrm{et}}\mathbf{Z}$; and the groups above the arrows denote the *kernels* of the homomorphisms corresponding to the arrows. If we denote the respective *"q-parameters"* and *"standard multiplicative coordinates on the respective Schottky uniformizations"* by q, $q_{\boldsymbol{\mu}}$, q_H, and U, $U_{\boldsymbol{\mu}}$, and U_H, respectively, then we have:

$$q^{h_{\boldsymbol{\mu}}} = q_{\boldsymbol{\mu}}; \quad q_{\boldsymbol{\mu}} = q_H^{h_{\mathrm{et}}}; \quad U^{h_{\boldsymbol{\mu}}} = U_{\boldsymbol{\mu}}; \quad U_{\boldsymbol{\mu}} = U_H$$

In the following, we will also write $\mathbf{G}_{\mathrm{m}}$, $(\mathbf{G}_{\mathrm{m}})_{\boldsymbol{\mu}}$, $(\mathbf{G}_{\mathrm{m}})_H$ for the copies of "$\mathbf{G}_{\mathrm{m}}$" that Schottky uniformize $E_{\infty,S}$, $E_{\infty_{\boldsymbol{\mu}},S}$, and $E_{\infty_H,S}$, respectively, (so, in particular, $(\mathbf{G}_{\mathrm{m}})_{\boldsymbol{\mu}} = (\mathbf{G}_{\mathrm{m}})_H$) and $\boldsymbol{\mu}_N \subseteq \mathbf{G}_{\mathrm{m}}$; $\boldsymbol{\mu}_N^{\boldsymbol{\mu}} \subseteq (\mathbf{G}_{\mathrm{m}})_{\boldsymbol{\mu}}$; $\boldsymbol{\mu}_N^H \subseteq (\mathbf{G}_{\mathrm{m}})_H$ for the copies of "$\boldsymbol{\mu}_N$" lying inside these copies of $\mathbf{G}_{\mathrm{m}}$. Finally, observe that since we are given a lifting $\mathcal{H} \subseteq \mathcal{G}_{\overline{\mathcal{L}}}$ of H, we also get natural metrized line bundles $\overline{\mathcal{L}}_{\boldsymbol{\mu}}$ and $\overline{\mathcal{L}}_H$ on $E_{\infty_{\boldsymbol{\mu}},S}$ and $E_{\infty_H,S}$, respectively, that descend $\overline{\mathcal{L}}$.

Note that since H and G generate ${}_dE_{\infty,S}$, it follows that $G \hookrightarrow E_{\infty_{\boldsymbol{\mu}},S}$. Thus, we obtain subgroup schemes

$$H_{\mathrm{et}}, G_{\mathrm{et}} \hookrightarrow E_{\infty_{\boldsymbol{\mu}},S}$$

Note that H_{et} is *tautologically* of étale type. Thus, it follows that the *image* $\mathrm{Im}_{E_{\infty_H,S}}(G_{\mathrm{et}})$ *of* G_{et} *in* $E_{\infty_H,S}$ *is of multiplicative type.* (Indeed, since $E_{\infty_H,S}$ is obtained from $E_{\infty_{\boldsymbol{\mu}},S}$ by forming the quotient by H_{et}, which is of étale type, it follows that the entire image $\mathrm{Im}_{E_{\infty_H,S}}({}_{h_{\mathrm{et}}}E_{\infty_{\boldsymbol{\mu}},S}) = \mathrm{Im}_{E_{\infty_H,S}}(\boldsymbol{\mu}^{\boldsymbol{\mu}}_{h_{\mathrm{et}}})$ in $E_{\infty_H,S}$ is of multiplicative type.)

Next, write

$$G_{\boldsymbol{\mu}} \stackrel{\mathrm{def}}{=} G/G_{\mathrm{et}}$$

Note that $|G_{\boldsymbol{\mu}}| = h_{\boldsymbol{\mu}}$, and that (since the image $\mathrm{Im}_{E_{\infty_H,S}}(G_{\mathrm{et}})$ of G_{et} in $E_{\infty_H,S}$ is of multiplicative type) $G_{\boldsymbol{\mu}}$ *maps naturally into the group of connected components in the special fiber of* $E_{\infty_H,S}$. Moreover, this map is *injective.* (Indeed, this injectivity may be verified for each of the p-primary portions (where p is a prime number) of $G_{\boldsymbol{\mu}}$ independently; thus, it suffices to verify this injectivity in the case where d is a prime power. But then, if injectivity did not hold, then it would follow that $(\mathrm{Im}_{E_{\infty_{\boldsymbol{\mu}},S}}(G)+H_{\mathrm{et}}) \bigcap \boldsymbol{\mu}^{\boldsymbol{\mu}}_d \not\subseteq \boldsymbol{\mu}^{\boldsymbol{\mu}}_{h_{\mathrm{et}}}$, which implies (by multiplying both sides of this non-inclusion by h_{et}) that $\mathrm{Im}_{E_{\infty_{\boldsymbol{\mu}},S}}(G) \bigcap \boldsymbol{\mu}^{\boldsymbol{\mu}}_d \neq \{1\}$ (so, in particular, $G \bigcap \boldsymbol{\mu}_d \neq \{1\}$, hence (since G and H generate ${}_dE_{\infty,S}$) that $h_{\boldsymbol{\mu}} = |H_{\boldsymbol{\mu}}| = 1$, so $G_{\boldsymbol{\mu}} = \{1\}$ — which implies that injectivity holds trivially.) Thus, in summary, this injection induces a *natural identification*

$$G_{\boldsymbol{\mu}} = \frac{1}{h_{\boldsymbol{\mu}}}\mathbf{Z}/\mathbf{Z}$$

Next, let us define

$$h_{\mathrm{eff}} \stackrel{\mathrm{def}}{=} |\mathrm{Im}_{E_{\infty_{\boldsymbol{\mu}},S}}(G_{\mathrm{et}}) \bigcap \boldsymbol{\mu}^{\boldsymbol{\mu}}_d|$$

Note that since H and G generate ${}_dE_{\infty,S}$, it follows that $(h_{\mathrm{eff}}, h_{\boldsymbol{\mu}}) = 1$. Since h_{eff} *divides* h_{et}, let us write $h_{\mathrm{et}} = h_{\mathrm{eff}} \cdot h_{\mathrm{ord}}$. Write

$$H_{\mathrm{eff}} \subseteq H_{\mathrm{et}}; \quad G_{\mathrm{eff}} \subseteq G_{\mathrm{et}}$$

for the respective subgroups given by the kernel of multiplication by h_{ord}. Thus, $|H_{\mathrm{eff}}| = |G_{\mathrm{eff}}| = h_{\mathrm{eff}}$.

The main theme of this § is the following:

> *We would like to apply the theory of §4 to the data*
>
> $$(E_{\infty_{\boldsymbol{\mu}},S}; \overline{\mathcal{L}}_{\boldsymbol{\mu}}; H_{\mathrm{et}}, G_{\mathrm{et}} \hookrightarrow E_{\infty_{\boldsymbol{\mu}},S})$$

where we take the point "η" of §4 to be the given η plus a collection of representatives of the various classes of $G_{\boldsymbol{\mu}} = G/G_{\mathrm{et}}$.

Next, we consider *metrized line bundles.* Note that the metrized line bundle $\overline{\mathcal{L}}_H$ on $E_{\infty_H,S}$ has degree 1 and *curvature* (cf. [HAT], Chapter V, §1) given by:

$$\frac{1}{h_{\boldsymbol{\mu}}} \cdot \sum_{i=0}^{(h_{\boldsymbol{\mu}})-1} \delta_{[i/h_{\boldsymbol{\mu}}]}$$

(where $\delta_{[i/h_{\boldsymbol{\mu}}]}$ denotes the delta distribution on $\mathbf{S^1}$ concentrated at the point $[i/h_{\boldsymbol{\mu}}] \subseteq \mathbf{S^1}$). Let

$$\overline{\mathcal{L}}'_H \stackrel{\mathrm{def}}{=} \overline{\mathcal{L}}_H(\psi)$$

where $\psi : \mathbf{S^1} \to \mathbf{R}$ is the unique piecewise smooth function such that the *curvature* of $\overline{\mathcal{L}}'_H$ is equal to $\delta_{[0]}$, and $\int_{\mathbf{S^1}} \psi = 0$. Then, as reviewed in §4, $\overline{\mathcal{L}}'_H$ is generated by the section defined by the *theta function*:

$$\Theta_H \stackrel{\mathrm{def}}{=} q_H^{-\frac{1}{2}k_\eta^2} \sum_{k \in \mathbf{Z}} q_H^{\frac{1}{2}(k+k_\eta)^2} \cdot U_H^k \cdot \chi(k)$$

where we write $k_\eta \stackrel{\mathrm{def}}{=} i_\chi/n$ (so $|k_\eta| \leq \frac{1}{2}$). Observe that as a function on $\mathbf{Z}$, the function $k \mapsto \frac{1}{2}(k+k_\eta)^2$ assumes its *minimum* at $k = 0$. Moreover, if we restrict Θ_H to $\boldsymbol{\mu}^H_{h_{\mathrm{et}}}$, then the highest power of q_H appearing in the coefficient of $(U_H|_{\boldsymbol{\mu}^H_{h_{\mathrm{et}}}})^{k_0}$ is given by:

$$\begin{aligned} -\frac{1}{2}k_\eta^2 \ + \ & \mathrm{Min}_{k \equiv k_0 \text{ mod } h_{\mathrm{et}}} \ \{\frac{1}{2}(k+k_\eta)^2\} \\ &= -\mathrm{Min}_{k \in \mathbf{Z}} \ \{\frac{1}{2}(k+k_\eta)^2\} \ + \ \mathrm{Min}_{k \equiv k_0 \text{ mod } h_{\mathrm{et}}} \ \{\frac{1}{2}(k+k_\eta)^2\} \end{aligned}$$

Now to consider such coefficients of $(U_H|_{\boldsymbol{\mu}^H_{h_{\mathrm{et}}}})^{k_0}$ amounts to considering the Fourier transform of the restriction of the theta function in question to $\boldsymbol{\mu}^H_{h_{\mathrm{et}}}$. More generally — cf. *the theory of §4*, which we think of as being applied to the data

$$(E_{\infty_{\boldsymbol{\mu}},S}; \overline{\mathcal{L}}_{\boldsymbol{\mu}}; H_{\mathrm{et}}, G_{\mathrm{et}} \hookrightarrow E_{\infty_{\boldsymbol{\mu}},S})$$

— we would like to consider *the Fourier coefficients of the convolution of* $\Theta_H|_{\boldsymbol{\mu}^H_{h_{\mathrm{et}}}}$ with some reduced discrete Gaussian (times a character) on $\boldsymbol{\mu}^H_{h_{\mathrm{ord}}}$ (regarded as a quotient of $\boldsymbol{\mu}^H_{h_{\mathrm{et}}}$). (Note that $h_{\mathrm{ord}} = h_{\mathrm{et}}/h_{\mathrm{eff}}$ appears here since $h_{\mathrm{eff}} = |\mathrm{Im}_{E_{\infty_{\boldsymbol{\mu}},S}}(G_{\mathrm{et}}) \bigcap \boldsymbol{\mu}^{\boldsymbol{\mu}}_d|$.) Then the highest power of q_H appearing in the coefficient of $(U_H|_{\boldsymbol{\mu}^H_{h_{\rm et}}})^{k_0+k_{\rm ex}}$ (for such a convolution, where $k_{\rm ex}$ is a constant determined by the character) is given by:

$$-\frac{1}{2}k_\eta^2 \; + \; \mathrm{Min}_{k \equiv k_0 \text{ mod } h_{\rm eff}} \; \{\frac{1}{2}(k+k_\eta)^2\}$$
$$= -\mathrm{Min}_{k \in \mathbf{Z}} \; \{\frac{1}{2}(k+k_\eta)^2\} \; + \; \mathrm{Min}_{k \equiv k_0 \text{ mod } h_{\rm eff}} \; \{\frac{1}{2}(k+k_\eta)^2\}$$

Note that for an appropriate choice of reduced discrete Gaussian, *this convolution amounts precisely to the restriction of the theta function in question to* $G_{\rm et}$.

Of course, ultimately, we wish to consider the Fourier coefficients of the restriction of the theta function in question to G. This amounts to restricting Θ_H to $G_{\rm et}+\gamma$, for various $\gamma \in G_{\boldsymbol{\mu}} = G/G_{\rm et}$. Write $k_\gamma \in \frac{1}{h_{\boldsymbol{\mu}}}\mathbf{Z}$ for a representative of $\gamma \in G_{\boldsymbol{\mu}} = \frac{1}{h_{\boldsymbol{\mu}}}\mathbf{Z}/\mathbf{Z}$. Also, let us define a *metrized line bundle on* $E_{\infty_H,S}$

$$\overline{\mathcal{L}}''_H \stackrel{\rm def}{=} \overline{\mathcal{L}}_H(\psi(0))$$

(where $\psi : \mathbf{S^1} \to \mathbf{R}$ is the function appearing in the definition of $\overline{\mathcal{L}}'_H$). Thus, $\overline{\mathcal{L}}_H$, $\overline{\mathcal{L}}'_H$, and $\overline{\mathcal{L}}''_H$ have the same restriction to the generic fiber of $E_{\infty_H,S}$; $\overline{\mathcal{L}}_H$ and $\overline{\mathcal{L}}''_H$ have the *same curvature*; and $\overline{\mathcal{L}}'_H$ and $\overline{\mathcal{L}}''_H$ have the same metric structure at the connected component of the identity (in the special fiber of $E_{\infty_H,S}$). Let us write $\widehat{\mathbf{G}}_{\rm m}$ for the *q-adic formal completion of* $(\mathbf{G}_{\rm m})_{S_\infty}$. Then it follows from the *determination of the metric* given in, e.g., [HAT], Chapter VII, Lemma 6.4 (cf. also the discussion following this lemma), together with the *well-known explicit form of theta functions* on $(\mathbf{G}_{\rm m})_H/q_H^{(1/(h_{\boldsymbol{\mu}}\cdot n))\cdot\mathbf{Z}}$ (cf. [HAT], Chapter V, Theorem 4.8), that if we regard Θ_H as a *section of* $\overline{\mathcal{L}}''_H$, then its restriction to the copy of $\widehat{\mathbf{G}}_{\rm m}$ corresponding to γ will be given (up to a possible factor $\in \boldsymbol{\mu}_\infty$) by:

$$\Theta''_H[\gamma] \stackrel{\rm def}{=} q_H^{-\frac{1}{2}k_\eta^2} \cdot \sum_{k \in \mathbf{Z}} \; q_H^{\frac{1}{2}(k+k_\eta+k_\gamma)^2} \cdot U_H^{k+k_\gamma} \cdot \chi(k)$$

(where, in the above expression, the factor $U_H^{k_\gamma}$ may be thought of as part of the trivialization in use; moreover, since this same factor multiplies *all* the terms in the above expression, it may be ignored — i.e., we essentially have a function in *integral powers* of U_H). Thus, if we write

$$\frac{1}{2}k_H^2 \stackrel{\rm def}{=} \mathrm{Min}_{k \in \mathbf{Z}, \; \gamma \in G_{\boldsymbol{\mu}}} \; \{\frac{1}{2}(k+k_\eta+k_\gamma)^2\} \le \frac{1}{2}k_\eta^2$$

then

$$\Theta_H[\gamma] \stackrel{\rm def}{=} q_H^{\frac{1}{2}k_\eta^2 - \frac{1}{2}k_H^2} \cdot \Theta''_H[\gamma] = q_H^{-\frac{1}{2}k_H^2} \cdot \sum_{k \in \mathbf{Z}} \; q_H^{\frac{1}{2}(k+k_\eta+k_\gamma)^2} \cdot U_H^{k+k_\gamma} \cdot \chi(k)$$

is *the theta function associated to a generator of* $(f_H)_*\overline{\mathcal{L}}_H$. Moreover, if we then *convolute* $\Theta_H[\gamma]|_{\boldsymbol{\mu}^H_{h_{\mathrm{et}}}}$ with some *reduced discrete Gaussian* (times a character) pulled back from the quotient $\boldsymbol{\mu}^H_{h_{\mathrm{et}}} \to \boldsymbol{\mu}^H_{h_{\mathrm{ord}}}$, then it follows that *the highest power of* q_H *appearing in the coefficient of* $(U_H|_{\boldsymbol{\mu}^H_{h_{\mathrm{et}}}})^{k_0+k_{\mathrm{ex}}}$ (where $k_0 \in \mathbf{Z}$) for such a convolution is given by:

$$-\frac{1}{2}k_H^2 \ + \ \mathrm{Min}_{k \equiv k_0 - k_\gamma \mod h_{\mathrm{eff}}} \ \{\frac{1}{2}(k + k_\eta + k_\gamma)^2\}$$

(where $k \in \mathbf{Z}$, and the congruence symbol "$\equiv$" is well-defined since, as remarked above, $(h_{\mathrm{eff}}, h_{\boldsymbol{\mu}}) = 1$). Thus, *if we allow* γ *to vary*, then we obtain that *the highest power of* q_H *appearing in the coefficient of* $(U_H|_{\boldsymbol{\mu}^H_{h_{\mathrm{et}}}})^{k_0+k_{\mathrm{ex}}}$ (where $k_0 \in \mathbf{Z}$) for such a convolution is given by:

$$\begin{aligned} -\frac{1}{2}k_H^2 \ &+ \ \mathrm{Min}_{j/h_{\boldsymbol{\mu}} \equiv k_0 \mod h_{\mathrm{eff}}} \ \{\frac{1}{2}((j/h_{\boldsymbol{\mu}}) + k_\eta)^2\} \\ &= -\frac{1}{2}k_H^2 \ + \ \frac{1}{h_{\boldsymbol{\mu}}^2} \cdot \mathrm{Min}_{j \equiv h_{\boldsymbol{\mu}} \cdot k_0 \mod h_{\mathrm{eff}}} \ \{\frac{1}{2}(j + h_{\boldsymbol{\mu}} \cdot k_\eta)^2\} \end{aligned}$$

(where $j \in \mathbf{Z}$, and the congruence symbol "$\equiv$" is well-defined since, as remarked above, $(h_{\mathrm{eff}}, h_{\boldsymbol{\mu}}) = 1$).

The above analysis thus implies — by the same reasoning as that used to derive Theorem 4.4 in §4 — the following generalization of Theorem 4.4, which is the *main result of this* §:

Theorem 5.1. *For any Lagrangian subgroup* H *and any restriction subgroup* $G \subseteq {}_dE_{\infty,S}$, *we have:*

$$\mathrm{Avg}_\eta(\deg(\nu)) \geq (d/h_{\mathrm{eff}}) \cdot \mathcal{Z}'(d, h_{\mathrm{eff}}, m')$$

where $h_{\mathrm{eff}} = |\mathrm{Im}_{E_{\infty \boldsymbol{\mu}},S}(G_{\mathrm{et}}) \bigcap \boldsymbol{\mu}_d^{\boldsymbol{\mu}}|$.

Proof. The sums $\mathcal{Z}'(-,-,-)$ are defined as sums of minima such as

$$\mathrm{Min}_{j \equiv h_{\boldsymbol{\mu}} \cdot k_0 \mod h_{\mathrm{eff}}} \ \{\frac{1}{2}(j + h_{\boldsymbol{\mu}} \cdot k_\eta)^2\}$$

regarded as powers of $q^{\frac{1}{d}}$. Here, we wish to regard such minima as powers of $q_H^{1/h_{\boldsymbol{\mu}}^2}$. But in fact, $q = q_{\boldsymbol{\mu}}^{1/h_{\boldsymbol{\mu}}}$, $q_{\boldsymbol{\mu}} = q_H^{h_{\mathrm{et}}}$ implies $q = q_H^{h_{\mathrm{et}}/h_{\boldsymbol{\mu}}}$, hence

$$q^{\frac{1}{d}} = q^{1/(h_{\mathrm{et}} \cdot h_{\boldsymbol{\mu}})} = q_H^{1/h_{\boldsymbol{\mu}}^2}$$

so we see that we do not need to multiply the $\mathcal{Z}'(-,-,-)$'s by any factor in our estimate of the degree of vanishing of the product of the Fourier coefficients corresponding to a *single* collection of representatives in $\mathbf{Z}/d\mathbf{Z}$ of the set of "equivalence classes" $(\mathbf{Z}/d\mathbf{Z})/h_{\text{eff}} \cdot (\mathbf{Z}/d\mathbf{Z}) = \mathbf{Z}/h_{\text{eff}}\mathbf{Z}$. Since, for a given class of $\mathbf{Z}/d\mathbf{Z}$ modulo h_{eff}, we must contend with a total of d/h_{eff} Fourier coefficients, we thus obtain a factor of d/h_{eff} in our final estimate.

Finally, note that the term $h_{\boldsymbol{\mu}} \cdot k_\eta$ appearing in the minima above corresponds precisely to the image "$d \cdot \eta_\iota$" of $\eta_\iota \in \mathbf{S^1}$ (where this $\mathbf{S^1}$ is the $\mathbf{S^1}$ corresponding to the special fiber of the original $E_{\infty,S}$) in $\mathbf{S^1}/(\frac{1}{d}\mathbf{Z}/\mathbf{Z})$. Indeed, k_η corresponds to the image of η_ι in $\mathbf{S^1}/(\frac{1}{h_{\text{et}}}\mathbf{Z}/\mathbf{Z}) = (\mathbf{S^1})_H$ (i.e., the $\mathbf{S^1}$ corresponding to the special fiber of $E_{\infty_H,S}$), so the image "$d \cdot \eta_\iota$" of η_ι in $\mathbf{S^1}/(\frac{1}{d}\mathbf{Z}/\mathbf{Z})$ is given by multiplying k_η by $d/h_{\text{et}} = h_{\boldsymbol{\mu}}$, as desired. ○

Theorem 5.2. *In the situation of Theorem 5.1, write* $h_{\boldsymbol{\mu}} \stackrel{\text{def}}{=} |H \bigcap \boldsymbol{\mu}_d|$; $d = h_{\boldsymbol{\mu}} \cdot h_{\text{et}}$; $h_{\text{et}} = h_{\text{eff}} \cdot h_{\text{ord}}$. *Then the coefficient of the smallest power of q in the Fourier coefficients of the algebraic theta function in question on G (cf. the discussion of §3) are of the form:*

$$\epsilon \cdot h_{\text{ord}}{}^{-\frac{1}{2}} \cdot \ (\text{an element } \in \boldsymbol{\mu}_{n \cdot h_{\boldsymbol{\mu}} \cdot h_{\text{ord}}})$$

(where ϵ is a 4-th root of unity (respectively, $\sqrt{2}$ times an 8-th root of unity) if h_{ord} is odd *(respectively,* even*)), with at most one possible exceptional class of coefficients in $\widehat{G}/h_{\text{eff}} \cdot \widehat{G}$. If this exception occurs,* and *the inequality of Theorem 5.1 is an equality, then the coefficient of the smallest power of q in this coefficient is of the form:*

$$\epsilon \cdot h_{\text{ord}}{}^{-\frac{1}{2}} \cdot \ (\text{a nonzero sum of two elements } \in \boldsymbol{\mu}_{n \cdot h_{\boldsymbol{\mu}} \cdot h_{\text{ord}}})$$

(where ϵ is a 4-th root of unity (respectively, $\sqrt{2}$ times an 8-th root of unity) if h_{ord} is odd *(respectively,* even*)).*

Proof. This follows essentially from the above analysis, together with the following remarks: First of all, it follows from the fact that the function

$$j \mapsto (j + h_{\boldsymbol{\mu}} \cdot k_\eta)^2$$

(on integers j such that $j \equiv h_{\boldsymbol{\mu}} \cdot k_0 \bmod h_{\text{eff}}$) is "essentially" injective (i.e., either injective or, if it is not injective, then the fiber consists of two elements) that *the minima discussed above are achieved for "essentially" only one value of j* (where "essentially" means that there is at most one exception, in which case the minimum is achieved for precisely of two values of j). Thus, by considering the class of this j modulo $h_{\boldsymbol{\mu}}$, we see that we need only consider the restriction of Θ_H to $G_{\text{et}} + \gamma$, for *fixed* $\gamma \in G_{\boldsymbol{\mu}}$. But since (by definition) $G_{\boldsymbol{\mu}} = G/G_{\text{et}}$, it follows that then we are essentially in the situation of §4, *applied to the data*

$$(E_{\infty_{\boldsymbol{\mu}},S}; \overline{\mathcal{L}}_{\boldsymbol{\mu}}; H_{\text{et}}, G_{\text{et}} \hookrightarrow E_{\infty_{\boldsymbol{\mu}},S})$$

(so "d_{ord}" of §4 becomes $h_{\text{et}}/h_{\text{eff}} = h_{\text{ord}}$ in the notation of the present discussion). Thus, Theorem 5.2 follows from Theorem 4.4. Note that here, when we apply Theorem 4.4, the "n" of Theorem 4.4 becomes $n \cdot h_{\boldsymbol{\mu}}$ (in the notation of the present discussion) since in addition to translating by η, we are also translating by γ whose order in G/G_{et} divides $h_{\boldsymbol{\mu}}$. This completes the proof of Theorem 5.2. ○

§6. Generic Properties of the Norm

In this §, we maintain the notation of §4. (In particular, we continue to assume that *the Lagrangian subgroup is of étale type.*) The goal of the present § is to determine in which cases the *norm* ν (of the Fourier transform of an algebraic theta function) is *generically nonzero* (on the moduli space of elliptic curves in characteristic zero).

Recall the notation

$$m' \stackrel{\text{def}}{=} \frac{m}{(m,d)}$$

Thus, put another way, m' is the *order of the torsion point $d \cdot \eta$.*

Definition 6.1. If our data satisfies the conditions:

(1) d is even;

(2) $m' = 2$;

(3) $d \cdot \eta \in G$ (where G is the *restriction subgroup*);

then we shall say that our data is *of null type.* If our data is not of null type, then we shall say that it is *of general type.*

Remark. In fact, condition (1) of Definition 6.1 is implied by conditions (2) and (3).

The main result of this § is the following:

Proposition 6.2. *The norm ν (introduced in §3) is generically zero on S if and only if our data is of null type.*

Proof. If we work over a *global* S as in §3, then it is immediate that every connected component of S contains points at infinity at which the restriction subgroup G is *of multiplicative type* (cf. §4). Thus, it suffices to prove Proposition 6.2 in the case where G is *of multiplicative type*.

Now we return to a *local* S (as in §4, 5). Since G is *of multiplicative type*, we know the explicit form of the restriction to G of the theta function in question (cf. §4):

$$\Theta_{\boldsymbol{\mu}} \stackrel{\text{def}}{=} \sum_{k_0 \in \mathbf{Z}/d\mathbf{Z}} (U|_{\boldsymbol{\mu}_d})^{k_0} \cdot \Big(\sum_{k \in \mathbf{Z},\ k \equiv k_0 (\text{mod } d)} q^{\frac{1}{d}(\frac{1}{2}\cdot k^2 + (i_\chi/n)\cdot k)} \cdot \chi(k) \Big)$$

$$= \sum_{k \in K_{\text{Crit}}} q^{\frac{1}{d}(\frac{1}{2}\cdot k^2 + (i_\chi/n)\cdot k)} \cdot (U|_{\boldsymbol{\mu}_d})^k \cdot (\chi(k) + \epsilon_k) \cdot \{1 + (\text{smaller powers of } q)\}$$

Thus, *if ν is generically zero*, then it follows that we are "in the exceptional case," and that "$\chi(k) + \epsilon_k$" is zero. In this case, $\chi(k) + \epsilon_k$ is equal (up to a possible factor $\in \boldsymbol{\mu}_\infty$) to $\chi(d) + 1$. Thus, we obtain:

$$\chi(d) = -1$$

In particular, $\chi(d)^2 = 1$.

Now, relative to the notation of [HAT], Chapter V, §4, the character χ may be identified with a character "$\chi_{\mathcal{M}}$," and "$\chi_{\mathcal{M}}$" is related to another character $\chi_{\mathcal{L}}$ by:

$$\chi_{\mathcal{M}} = \chi_{\mathcal{L}} \cdot \chi_\theta$$

(where χ_θ is a fixed character which is independent of the particulars of the data under consideration). Note that all of these characters are characters $\boldsymbol{\mu}_n \times \mathbf{Z}_{\text{et}} \to \boldsymbol{\mu}_n$. Next, recall that $\chi_{\mathcal{L}}$, $\chi_{\mathcal{M}}$ (cf. the discussion at the beginning of [HAT], Chapter V, §4) *faithfully capture the twist induced on $\overline{\mathcal{L}}$ by translation by η.* More precisely,

> *If d is odd (respectively, even), then the order of $\chi_{\mathcal{L}}$ (respectively, $\chi_{\mathcal{M}}$) restricted to $\boldsymbol{\mu}_n \times (d \cdot \mathbf{Z}_{\text{et}})$ is equal to the order of $d \cdot \eta$*, i.e., to m'.

(Here the factor of d arises since the discussion of [HAT], Chapter V, concerns, in effect, degree one line bundles on the *étale quotient* $E_{\infty,S} \to E_{\infty,S}/(\mathbf{Z}/d\mathbf{Z})$, relative to our notation in the present discussion.) Thus, in summary, we obtain that

$$\chi_{\mathcal{M}}{}^2|_{\boldsymbol{\mu}_n \times (d\cdot\mathbf{Z}_{\text{et}})} = \chi_{\mathcal{L}}{}^2|_{\boldsymbol{\mu}_n \times (d\cdot\mathbf{Z}_{\text{et}})} = 1$$

(where we use the fact that since we are in the "exceptional case" (cf. [HAT], Chapter VIII, Lemma 4.3), we are in "Cases I or II" of [HAT], Chapter V, §4, which implies that the restriction of $\chi_{\mathcal{L}}{}^2$, $\chi_{\mathcal{M}}{}^2$ to $\boldsymbol{\mu}_n$ is trivial). Thus, we obtain that:

$$2 \cdot (d \cdot \eta) = 1$$

i.e., that $m' = 2$. Also, since we are "in the exceptional case" (cf. [HAT], Chapter VIII, proof of Lemma 4.3), it follows that *either* we are in "Case I" (cf. [HAT], Chapter V, §4) and d is *odd*, *or* we are in "Case II" (cf. [HAT], Chapter V, §4) and d is *even*.

Suppose that we are in "Case I" (cf. [HAT], Chapter V, §4) and d is *odd*. First, observe that since $m' = 2$ and d is *odd*, it follows that we may assume that $m = 2$. Since we are in "Case I," it follows that $\chi_{\mathcal{L}}|_{\boldsymbol{\mu}_n} = 1$. Also, since d is odd, and $n = 4$, it follows (from $\chi(d) = -1$) that $\chi_{\mathcal{M}}{}^2|_{\mathbf{Z}_{\mathrm{et}}} = 1$ (but $\chi_{\mathcal{M}}|_{\mathbf{Z}_{\mathrm{et}}} \neq 1$, since $\chi_{\mathcal{M}}(d) = \chi(d) = -1$), hence (by the explicit description of χ_θ in [HAT], Chapter IV, Theorem 2.1) that $\chi_{\mathcal{M}}|_{\mathbf{Z}_{\mathrm{et}}} = \chi_\theta|_{\mathbf{Z}_{\mathrm{et}}}$, so $\chi_{\mathcal{L}}|_{\mathbf{Z}_{\mathrm{et}}} = 1$. Thus, we obtain that $\chi_{\mathcal{L}}$ is *trivial*. But since, as remarked above, the order of $\chi_{\mathcal{L}}$ is equal to m', we thus obtain that $m' = 1$, which is absurd.

Thus, we conclude that *the hypothesis that ν is generically zero implies that we are in "Case II" (cf. [HAT], Chapter V, §4); that d is even; and that $m' = 2$*. I *claim* that $d \cdot \eta$ lies in G. Indeed, this follows from the fact that the portion of $\chi_{\mathcal{M}}$ which governs the "étale portion" of $d \cdot \eta$ (i.e., the connected component of the special fiber of $E_{\infty,S}$ in which $d \cdot \eta$ lies), namely, $\chi_{\mathcal{M}}|_{\boldsymbol{\mu}_n}$, is *trivial* (since we are in "Case II"). Thus, the image in the special of $E_{\infty,S}$ of the point $d \cdot \eta$ lies in the connected component of the identity, so $d \cdot \eta \in G$ (recall that we have assumed in this discussion that G is "of multiplicative type"!), as claimed. This completes the proof of the assertion that *if ν is generically zero, then our data is of null type*.

Thus, it remains to show that: *if our data is of null type, then ν is generically zero*. But this follows immediately from substitution into the explicit expression for $\Theta_{\boldsymbol{\mu}}$ given above (i.e., one uses the fact that $\chi(-)$ of any *odd* multiple of d is equal to -1 to show that the coefficient of $(U|_{\boldsymbol{\mu}_d})^{\frac{d}{2}}$ vanishes). This completes the proof of Proposition 6.2. ○

§7. Some Elementary Computational Lemmas

In the following discussion, we assume that we are given a finite collection

$$p_1, p_2, \ldots, p_r$$

(where $r \geq 1$) of (distinct) *prime numbers*, together with a collection of positive integers $e_1, e_2, \ldots, e_r$. Write

$$d \stackrel{\text{def}}{=} p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_r^{e_r}$$

If $\mathcal{A} \subseteq \{1, 2, \ldots, r\}$ is a nonempty subset, let us write

$$\mathcal{F}(\mathcal{A})$$

for the set of functions $\psi : \mathcal{A} \to \mathbf{Z}$ (whose value at $j \in \mathcal{A}$ we write ψ_j) such that for each $j \in \mathcal{A}$, we have $1 \leq \psi_j \leq e_j$.

Lemma 7.1. *We have:*

$$d - 1 = \sum_{\mathcal{A} \subseteq \{1,\ldots,r\}} \Big\{ \sum_{\psi \in \mathcal{F}(\mathcal{A})} \{(\prod_{j \in \mathcal{A}} p_j^{2\psi_j}) - 1\} \cdot \frac{(\prod_{j \notin \mathcal{A}} p_j)}{\{\prod_{j=1}^{r} (p_j + 1)\}} \cdot \Big(\prod_{j \in \mathcal{A}} p_j^{-\psi_j} \cdot (p_j - 1 + \delta_{\psi_j, e_j}) \Big) \Big\}$$

where $\delta_{x,y}$ is 1 if $x = y$ and 0 otherwise.

Proof. It is immediate that it is equivalent to verify:

$$(p_1^{e_1} \cdot \ldots \cdot p_r^{e_r} - 1) \cdot \prod_{j=1}^{r} (p_j + 1) = \sum_{\emptyset \neq \mathcal{A} \subseteq \{1,\ldots,r\}} (\prod_{j \notin \mathcal{A}} p_j) \cdot \Big\{ \sum_{\psi \in \mathcal{F}(\mathcal{A})} \{(\prod_{j \in \mathcal{A}} p_j^{2\psi_j}) - 1\} \cdot \Big(\prod_{j \in \mathcal{A}} p_j^{-\psi_j} \cdot (p_j - 1 + \delta_{\psi_j, e_j}) \Big) \Big\}$$

Let us first *fix* $\mathcal{A}$, and consider the sum over $\psi \in \mathcal{F}(\mathcal{A})$. This sum may be thought of as consisting of two sums, corresponding to the two terms "$\prod_{j \in \mathcal{A}} p_j^{2\psi_j}$" and "$-1$." The first sum may be evaluated as follows:

$$\begin{aligned}
&\sum_{\psi \in \mathcal{F}(\mathcal{A})} \{\prod_{j \in \mathcal{A}} p_j^{2\psi_j}\} \cdot \Big(\prod_{j \in \mathcal{A}} p_j^{-\psi_j} \cdot (p_j - 1 + \delta_{\psi_j, e_j}) \Big) \\
&= \sum_{\psi \in \mathcal{F}(\mathcal{A})} \Big(\prod_{j \in \mathcal{A}} p_j^{\psi_j} \cdot (p_j - 1 + \delta_{\psi_j, e_j}) \Big) \\
&= \prod_{j \in \mathcal{A}} \Big\{ \sum_{\psi_j = 1}^{e_j} p_j^{\psi_j} \cdot (p_j - 1 + \delta_{\psi_j, e_j}) \Big\} \\
&= \prod_{j \in \mathcal{A}} \Big\{ p_j (p_j - 1) \cdot \frac{(p_j^{e_j - 1} - 1)}{(p_j - 1)} + p_j^{e_j + 1} \Big\} \\
&= \prod_{j \in \mathcal{A}} \Big\{ p_j^{e_j} - p_j + p_j^{e_j + 1} \Big\} = \prod_{j \in \mathcal{A}} \Psi_j
\end{aligned}$$

where we write $\Psi_j \stackrel{\text{def}}{=} p_j^{e_j} - p_j + p_j^{e_j+1}$. On the other hand,

$$
\begin{aligned}
-\Big\{ \sum_{\psi \in \mathcal{F}(\mathcal{A})} \Big(\prod_{j \in \mathcal{A}} p_j^{-\psi_j} \cdot (p_j - 1 + \delta_{\psi_j, e_j}) \Big) \Big\} \\
&= - \prod_{j \in \mathcal{A}} \Big\{ \sum_{\psi_j = 1}^{e_j} p_j^{-\psi_j} \cdot (p_j - 1 + \delta_{\psi_j, e_j}) \Big\} \\
&= - \prod_{j \in \mathcal{A}} \Big\{ p_j^{-1} \cdot (p_j - 1) \cdot \frac{(1 - p_j^{-e_j+1})}{(1 - p_j^{-1})} + p_j^{-e_j+1} \Big\} \\
&= - \prod_{j \in \mathcal{A}} \Big\{ (1 - p_j^{-e_j+1}) + p_j^{-e_j+1} \Big\} = -1
\end{aligned}
$$

Thus, in summary, it suffices to show that:

$$
(p_1^{e_1} \cdot \ldots \cdot p_r^{e_r} - 1) \cdot \prod_{j=1}^{r} (p_j + 1) = \sum_{\emptyset \neq \mathcal{A} \subseteq \{1, \ldots, r\}} (\prod_{j \notin \mathcal{A}} p_j) \cdot \Big\{ \Big(\prod_{j \in \mathcal{A}} \Psi_j \Big) - 1 \Big\}
$$

To do this, we use induction on r. The result is clear for $r = 1$. Thus, let us prove it for $r \geq 2$, assuming the result known for strictly smaller r. First, let us note that the above sum over $\mathcal{A} \neq \emptyset$ may be split into *three sums*: the first (respectively, second; third) corresponding to the case where $\mathcal{A} = \{1\}$ (respectively, $1 \in \mathcal{A}$ (but $\mathcal{A} \neq \{1\}$); $1 \notin \mathcal{A}$). Note that there is a natural bijective correspondence between the second and third types of $\mathcal{A}$ given by appending/deleting the element "1." Thus, we obtain:

$$
\begin{aligned}
\sum_{\emptyset \neq \mathcal{A} \subseteq \{1, \ldots, r\}} (\prod_{j \notin \mathcal{A}} p_j) \cdot \Big\{ \Big(\prod_{j \in \mathcal{A}} \Psi_j \Big) - 1 \Big\} \\
&= -\Big\{ \sum_{\emptyset \neq \mathcal{A} \subseteq \{1, \ldots, r\}} (\prod_{j \notin \mathcal{A}} p_j) \Big\} + \sum_{\emptyset \neq \mathcal{A} \subseteq \{1, \ldots, r\}} (\prod_{j \notin \mathcal{A}} p_j) \cdot \Big\{ \prod_{j \in \mathcal{A}} \Psi_j \Big\} \\
&= -\Big\{ \sum_{\emptyset \neq \mathcal{A} \subseteq \{1, \ldots, r\}} (\prod_{j \notin \mathcal{A}} p_j) \Big\} + (\prod_{j=2}^{r} p_j) \cdot \Psi_1 \\
&\quad + \sum_{1 \in \mathcal{A} \subseteq \{1, \ldots, r\},\ |\mathcal{A}| \geq 2} (\prod_{j \notin \mathcal{A}} p_j) \cdot \Big\{ \prod_{j \in \mathcal{A}} \Psi_j \Big\} + \sum_{\emptyset \neq \mathcal{A}' \subseteq \{2, \ldots, r\}} (\prod_{j \notin \mathcal{A}'} p_j) \cdot \Big\{ \prod_{j \in \mathcal{A}'} \Psi_j \Big\}
\end{aligned}
$$

$$
\begin{aligned}
&= -\Big\{ \sum_{\emptyset \neq \mathcal{A} \subseteq \{1,\ldots,r\}} \big(\prod_{j \notin \mathcal{A}} p_j\big)\Big\} - \big(\prod_{j=1}^{r} p_j\big) + \big(\prod_{j=2}^{r} p_j\big) \cdot p_1^{e_1} \cdot (p_1+1) \\
&\quad + \sum_{\emptyset \neq \mathcal{A}' \subseteq \{2,\ldots,r\}} \big(\prod_{1 \neq j \notin \mathcal{A}'} p_j\big) \cdot (\Psi_1 + p_1) \cdot \Big\{ \prod_{j \in \mathcal{A}'} \Psi_j \Big\} \\
&= -\Big\{ \sum_{\mathcal{A} \subseteq \{1,\ldots,r\}} \big(\prod_{j \notin \mathcal{A}} p_j\big)\Big\} + \big(\prod_{j=2}^{r} p_j\big) \cdot p_1^{e_1} \cdot (p_1+1) \\
&\quad + (p_1+1) \cdot p_1^{e_1} \cdot \sum_{\emptyset \neq \mathcal{A}' \subseteq \{2,\ldots,r\}} \big(\prod_{1 \neq j \notin \mathcal{A}'} p_j\big) \cdot \Big\{ \prod_{j \in \mathcal{A}'} \Psi_j \Big\} \\
&= -\Big\{ \prod_{j=1}^{r} (p_j+1)\Big\} + \big(\prod_{j=2}^{r} p_j\big) \cdot p_1^{e_1} \cdot (p_1+1) \\
&\quad + (p_1+1) \cdot p_1^{e_1} \cdot \sum_{\emptyset \neq \mathcal{A}' \subseteq \{2,\ldots,r\}} \big(\prod_{1 \neq j \notin \mathcal{A}'} p_j\big) \cdot \Big\{ \prod_{j \in \mathcal{A}'} \Psi_j \Big\}
\end{aligned}
$$

Next, let us write

$$d' \stackrel{\text{def}}{=} p_2^{e_2} \cdot \ldots \cdot p_r^{e_r}$$

so $d = p_1^{e_1} \cdot d'$. Then we have

$$
\begin{aligned}
(d-1) \cdot \prod_{j=1}^{r} (p_j+1) &= (d - p_1^{e_1} + p_1^{e_1} - 1) \cdot \prod_{j=1}^{r} (p_j+1) \\
&= p_1^{e_1}(d'-1) \cdot \prod_{j=1}^{r} (p_j+1) + (p_1^{e_1}-1) \cdot \prod_{j=1}^{r} (p_j+1)
\end{aligned}
$$

Thus, by dividing by (p_1+1), we see that it suffices to show that:

$$
\begin{aligned}
&(p_1^{e_1}-1) \cdot \prod_{j=2}^{r} (p_j+1) + p_1^{e_1}(d'-1) \cdot \prod_{j=2}^{r} (p_j+1) \\
&\quad = -\Big\{ \prod_{j=2}^{r} (p_j+1)\Big\} + p_1^{e_1} \cdot \big(\prod_{j=2}^{r} p_j\big) + p_1^{e_1} \cdot \sum_{\emptyset \neq \mathcal{A}' \subseteq \{2,\ldots,r\}} \big(\prod_{1 \neq j \notin \mathcal{A}'} p_j\big) \cdot \Big\{ \prod_{j \in \mathcal{A}'} \Psi_j \Big\}
\end{aligned}
$$

But by the induction hypothesis on r, we have

$$
\begin{aligned}
&-\Big\{\prod_{j=2}^{r}(p_j+1)\Big\}+p_1^{e_1}\cdot(\prod_{j=2}^{r}p_j)+p_1^{e_1}\cdot\sum_{\emptyset\neq\mathcal{A}'\subseteq\{2,\ldots,r\}}(\prod_{1\neq j\notin\mathcal{A}'}p_j)\cdot\Big\{\prod_{j\in\mathcal{A}'}\Psi_j\Big\}\\
&\quad=-\Big\{\prod_{j=2}^{r}(p_j+1)\Big\}+p_1^{e_1}\cdot(\prod_{j=2}^{r}p_j)+p_1^{e_1}\cdot\sum_{\emptyset\neq\mathcal{A}'\subseteq\{2,\ldots,r\}}(\prod_{1\neq j\notin\mathcal{A}'}p_j)\\
&\qquad\quad+p_1^{e_1}\cdot(d'-1)\cdot\Big\{\prod_{j=2}^{r}(p_j+1)\Big\}\\
&\quad=-\Big\{\prod_{j=2}^{r}(p_j+1)\Big\}+p_1^{e_1}\cdot\Big\{\prod_{j=2}^{r}(p_j+1)\Big\}+p_1^{e_1}\cdot(d'-1)\cdot\Big\{\prod_{j=2}^{r}(p_j+1)\Big\}\\
&\quad=(p_1^{e_1}-1)\cdot\Big\{\prod_{j=2}^{r}(p_j+1)\Big\}+p_1^{e_1}\cdot(d'-1)\cdot\Big\{\prod_{j=2}^{r}(p_j+1)\Big\}
\end{aligned}
$$

as desired. This completes the proof of Lemma 7.1. ○

Next, we shift gears and write $\mathbf{S^1}$ for the *unit circle* $\mathbf{R}/\mathbf{Z}$, equipped with the standard coordinate θ (arising from the standard coordinate on $\mathbf{R}$). Write

$$f:\mathbf{S^1}\to\mathbf{R}$$

for the unique continuous, piecewise linear function on $\mathbf{S^1}$ which is linear except at $\theta=0,\frac{1}{2}$, and satisfies:

$$f(0)=+1;\quad f(\frac{1}{2})=-1$$

Note that f satisfies the property:

$$f(\theta+\frac{1}{2})=-f(\theta)$$

and that $\frac{df}{d\theta}=-4$ for $\theta\in[0,\frac{1}{2}]$ and $\frac{df}{d\theta}=4$ for $\theta\in[\frac{1}{2},1]$.

Next, let us define, for N a *positive integer*:

$$\Phi(N)\stackrel{\mathrm{def}}{=}N\cdot\sum_{i=0}^{N-1}f(\frac{i}{N})\in\mathbf{R}$$

and (by induction on N, starting with $\Phi^{\mathrm{exact}}(1)\stackrel{\mathrm{def}}{=}\Phi(1)$)

$$\Phi^{\mathrm{exact}}(N) \stackrel{\mathrm{def}}{=} \Phi(N) - \sum_{a|N,\ a<N} \Phi^{\mathrm{exact}}(a)$$

where in the sum, a ranges over all positive integers $< N$ which divide N. In the following, *we would like to compute* $\Phi(N)$ *and* $\Phi^{\mathrm{exact}}(N)$ *explicitly.*

Lemma 7.2. *If* N *is an* odd *positive integer, then* $\Phi(N) = 1$. *If* N *is an* even *positive integer, then* $\Phi(N) = 0$.

Proof. First, assume that N is *odd.* Write

$$(\mathbf{S^1})' \stackrel{\mathrm{def}}{=} \mathbf{S^1}/(\frac{1}{N}\mathbf{Z}/\mathbf{Z})$$

for the quotient of $\mathbf{S^1}$ by the subgroup $\frac{1}{N}\mathbf{Z}/\mathbf{Z} \subseteq \mathbf{S^1}$. Thus, $(\mathbf{S^1})'$ is also naturally isomorphic to a copy of $\mathbf{S^1}$. Write θ' for the standard coordinate on $(\mathbf{S^1})'$. Thus, $\theta' = N \cdot \theta$. Let

$$g(\theta') \stackrel{\mathrm{def}}{=} \sum_{i=0}^{N-1} f(\theta + \frac{i}{N})$$

for the "push-forward" of f to $(\mathbf{S^1})'$. (Thus, $g : (\mathbf{S^1})' \to \mathbf{R}$.) Note that g is itself *continuous and piecewise linear* on $(\mathbf{S^1})'$. Moreover,

$$\int_{\mathbf{S^1}} f = \int_{(\mathbf{S^1})'} g = 0$$

Finally, the derivative of g for "generic" (i.e., all but finitely many exceptional values) θ' may be computed as follows:

$$\begin{aligned} N \cdot \frac{dg}{d\theta'}(\theta') = \frac{dg}{d\theta}(\theta') &= \sum_{i=0}^{N-1} (\frac{df}{d\theta})(\theta + \frac{i}{N}) \\ &= 4 \cdot \sum_{i=0}^{N-1} \chi_{[\frac{1}{2},1]}(\theta + \frac{i}{N}) - \chi_{[0,\frac{1}{2}]}(\theta + \frac{i}{N}) \\ &= 4 \cdot \{\chi_{[\frac{1}{2},1]}(\theta') - \chi_{[0,\frac{1}{2}]}(\theta')\} \end{aligned}$$

where (for an interval $[a,b] \subseteq \mathbf{R}$) $\chi_{[a,b]}$ denotes the *indicator function* on this interval (i.e., it is $= 1$ on $[a,b]$ and $= 0$ outside of $[a,b]$), and, in the final equality, we make essential use of the fact that N is *odd.*

But note that these properties imply that $N \cdot g$ on $(\mathbf{S^1})'$ "looks just like" f on $\mathbf{S^1}$. Thus, in particular, it follows that

$$\Phi(N) = N \cdot g(0) = f(0) = 1$$

as desired.

Now assume that N is *even*. Then observe that $\Phi(N)$ is defined as (essentially) the sum of the values of the function f over a certain finite set of points of $\mathbf{S^1}$. Moreover, *since N is even*, it follows that this set is *invariant with respect to the automorphism of $\mathbf{S^1}$ given by $\theta \mapsto \theta + \frac{1}{2}$*. Since $f(\theta + \frac{1}{2}) = -f(\theta)$, we thus obtain $\Phi(N) = 0$, as desired. ○

Lemma 7.3. *We have: $\Phi^{\text{exact}}(1) = 1$, $\Phi^{\text{exact}}(2) = -1$. Moreover, if N is any positive integer $\neq 1, 2$, then $\Phi^{\text{exact}}(N) = 0$.*

Proof. By definition $\Phi^{\text{exact}}(1) = \Phi(1) = 1$, and $\Phi^{\text{exact}}(2) = \Phi(2) - \Phi(1) = 0 - 1$ (by Lemma 7.2). The final assertion is proven by induction on N. This assertion is vacuous for $N = 1, 2$. Thus, assume that $N \geq 3$, and that the assertion in question is known for strictly smaller N.

We begin with the case of N *odd*. In this case, 2 does not divide N, so, by the induction hypothesis, we obtain (from the definition of $\Phi^{\text{exact}}(N)$):

$$\Phi^{\text{exact}}(N) = \Phi(N) - \Phi(1) = 1 - 1 = 0$$

(by Lemma 7.2). This completes the case when N is odd.

Now assume that N is *even*. In this case, for all a as in the sum appearing in the definition of $\Phi^{\text{exact}}(N)$, we have $\Phi^{\text{exact}}(a) = 0$, unless $a = 1, 2$. Moreover, in this case, $a = 1, 2$ both appear, so we get:

$$\Phi^{\text{exact}}(N) = \Phi(N) - \{\Phi^{\text{exact}}(1) + \Phi^{\text{exact}}(2)\} = 0 - \{1 - 1\} = 0$$

(by Lemma 7.2), as desired. ○

§8. The Various Contributions at Infinity

In this §, we piece together the results of §5, 6, and 7, to obtain the *main result of this paper concerning degrees.* This result concerning degrees is the main technical result underlying the theory of this paper. In particular, the theorems of §9, 10, below, will essentially be formal consequences of this result concerning degrees.

The main point is that the various computations performed in §5, 6, and 7 are sufficient to *compute the total degree of vanishing of the norm* ν *of* §*3*, as follows. In this §, we use the notation of the latter part of §3 (i.e., we assume that S is a curve in characteristic 0). As usual, degrees will always be expressed in $\log(q)$ *units*. The total degree of vanishing of ν will be a *weighted sum/average* over all the possibilities for H (*the Lagrangian subgroup*) and G (*the restriction subgroup*). In the following discussion, we shall write (cf. §7)

$$d \stackrel{\mathrm{def}}{=} p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_r^{e_r}$$

(where $p_1, \ldots, p_r$ are distinct prime numbers; and $e_1, \ldots, e_r$ are positive integers).

First, let us observe that the estimate (from below) for $\deg(\nu)$ in Theorem 5.1 (as a function of G, H) *depends only on* h_{eff}. For a given G, H, we shall refer to the primes that divide $h_{\mathrm{eff}} = |\mathrm{Im}_{E_{\infty_{\boldsymbol{\mu}}},S}(G_{\mathrm{et}}) \bigcap \boldsymbol{\mu}_d^{\boldsymbol{\mu}}|$ (cf. Theorem 5.1) as *active primes*. Thus, the set of active primes forms a subset

$$\mathcal{A} \subseteq \{1, \ldots, r\}$$

For each active prime p_j, the p_j-primary part of the resulting h_{eff} (cf. §5) is equal to some $p_j^{\psi_j}$. Thus, we obtain a function

$$\psi : \mathcal{A} \to \mathbf{Z}$$

given by $j \mapsto \psi_j$, and (by definition) we have:

$$h_{\mathrm{eff}} = \prod_{j \in \mathcal{A}} p_j^{\psi_j}$$

Next, let us observe that the *probability* that, at a given point at infinity, the p_j-primary part of h_{eff} has order $p_j^{\psi_j}$ for all $j \in \mathcal{A}$, and order 1 for all $j \notin \mathcal{A}$, is given by:

$$\Big\{ \prod_{j \in \mathcal{A}} \Big(\frac{p_j - 1 + \delta_{\psi_j, e_j}}{(p_j + 1)p_j^{\psi_j}} \Big) \Big\} \cdot \Big\{ \prod_{j \notin \mathcal{A}} \Big(\frac{p_j}{p_j + 1} \Big) \Big\}$$

Indeed, clearly what happens for one p_j is *independent* of what happens for the other p_j's. Thus, the probability in question is equal to the product of the probabilities for each individual p_j. On the other hand, to compute the probability for a given p_j, we make use of the following lemma (where we think of "$\mathcal{M}$" as the module of d-torsion points in the Tate curve; "$(\mathbf{Z}/p^e\mathbf{Z}) \oplus 0$" as the submodule defined by "$\boldsymbol{\mu}_{p_j^{e_j}}$"; "$\mathcal{N}$" as the submodule defined by the restriction subgroup G; "p" as p_j; "e" as e_j; and "e'" as ψ_j):

Lemma 8.1. *Let p be a prime number, and e, e' positive integers such that $e' \leq e$. Write $\mathcal{M} \stackrel{\text{def}}{=} (\mathbf{Z}/p^e\mathbf{Z}) \oplus (\mathbf{Z}/p^e\mathbf{Z})$. Then the fraction of rank one free $\mathbf{Z}/p^e\mathbf{Z}$-submodules $\mathcal{N} \subseteq \mathcal{M}$ which are equal to the module $(\mathbf{Z}/p^e\mathbf{Z}) \oplus 0$ modulo $p^{e'}$ but not modulo $p^{e'+1}$ (if $e' < e$) is given by:*

$$\frac{p - 1 + \delta_{e',e}}{(p+1)p^{e'}}$$

On the other hand, the fraction of rank one free $\mathbf{Z}/p^e\mathbf{Z}$-submodules $\mathcal{N} \subseteq \mathcal{M}$ which are not *equal to the module $(\mathbf{Z}/p^e\mathbf{Z}) \oplus 0$ modulo p is given by $\frac{p}{p+1}$.*

Proof. Indeed, the computation of the second fraction is immediate, so let us concentrate on the computation of the first fraction. First of all, the fraction of rank one free $\mathbf{Z}/p^e\mathbf{Z}$-submodules $\mathcal{N} \subseteq \mathcal{M}$ which are equal to the module $(\mathbf{Z}/p^e\mathbf{Z}) \oplus 0$ modulo p is given by

$$\frac{1}{p+1}$$

Such $\mathcal{N}$ admit a *unique generator* of the form $\gamma = (1, a_\gamma)$, where $a_\gamma \in p\mathbf{Z}/p^e\mathbf{Z}$. Thus, the first fraction in the statement of Lemma 8.1 is equal to $\frac{1}{p+1}$ times the fraction of a_γ which are $\equiv 0$ modulo $p^{e'}$ but not modulo $p^{e'+1}$ (if $e' < e$). The fraction of such a_γ is given by:

$$\begin{aligned}
\frac{|p^{e'}\mathbf{Z}/p^e\mathbf{Z}| - |p^{e'+1}\mathbf{Z}/p^e\mathbf{Z}|}{|p\mathbf{Z}/p^e\mathbf{Z}|} &= \frac{p^{e-e'} - p^{e-e'-1}}{p^{e-1}} \\
&= \frac{p^{e-e'}(1-p^{-1})}{p^{e-1}} \\
&= \frac{p^{-e'}(1-p^{-1})}{p^{-1}} = p^{-e'}(p-1)
\end{aligned}$$

if $e' < e$, and

$$\frac{|p^{e'}\mathbf{Z}/p^e\mathbf{Z}|}{|p\mathbf{Z}/p^e\mathbf{Z}|} = \frac{p^{e-e'}}{p^{e-1}} = p^{1-e'}$$

if $e' = e$. Thus, multiplying by $\frac{1}{p+1}$ gives the desired result. ○

Now let us recall the estimate (for a *fixed* G, H) of Theorem 5.1:

$$\mathrm{Avg}_\eta(\deg(\nu)) \geq (d/h_{\mathrm{eff}}) \cdot \mathcal{Z}'(d, h_{\mathrm{eff}}, m')$$

On the other hand, $\mathcal{Z}'(d, h_{\mathrm{eff}}, m')$ has been computed in Proposition 3.3. Note, moreover, that by Lemma 7.3, the "$\phi_1(-)$" term in the expressions of Proposition 3.3 *vanishes if*

d is odd or $m' \neq 2$. (Indeed, up to a nonzero factor, one computes that the differences $\phi_1(\theta + \frac{1}{2}) - \phi_1(\theta)$ are equal (as functions on $\mathbf{S^1}$) to the function "f" studied in the latter portion of §7. Thus, the asserted vanishing follows from the equality $\Phi^{\text{exact}}(m') = 0$ proven in Lemma 7.3.) Thus, in the following, we shall *assume first that either d is odd, or (if d is even, then) $m' \neq 2$.* We will return later to the exceptional case where d is even and $m' = 2$.

Thus, under the present assumptions on d and m', we obtain (by Proposition 3.3):

$$(d/h_{\text{eff}}) \cdot \mathcal{Z}'(d, h_{\text{eff}}, m') = \frac{1}{24}((h_{\text{eff}})^2 - 1)$$

(where we omit the "$\log(q)$" since we will always work in $\log(q)$ units). Thus, substituting the expression for h_{eff} given above, and then taking the *weighted sum* (relative to the probabilities for various types of G, H computed above), we obtain the following estimate for the *total degree of vanishing* $\deg_{\text{tot}}(\nu)$ *of the norm ν at the various points at infinity of S*:

$$\begin{aligned}
\deg_{\text{tot}}(\nu) \geq \sum_{\mathcal{A} \subseteq \{1,\ldots,r\}} \Big\{ \sum_{\psi \in \mathcal{F}(\mathcal{A})} & \frac{1}{24}\{(\prod_{j \in \mathcal{A}} p_j^{2\psi_j}) - 1\} \cdot \\
& \Big\{ \prod_{j \in \mathcal{A}} \Big(\frac{p_j - 1 + \delta_{\psi_j, e_j}}{(p_j + 1)p_j^{\psi_j}}\Big)\Big\} \cdot \Big\{ \prod_{j \notin \mathcal{A}} \Big(\frac{p_j}{p_j + 1}\Big)\Big\}\Big\} \\
= \frac{1}{24}(d - 1) & \\
= \deg(\mathcal{M}^{\otimes d} \otimes \mathcal{K}^{\otimes d}) - d \cdot [\overline{\mathcal{L}} \cdot e] & \\
= \deg(\mathcal{M}^{\otimes d} \otimes \mathcal{K}^{\otimes d}) &
\end{aligned}$$

where in the first equality (respectively, second; third), we apply Lemma 7.1 (respectively, Proposition 3.2; Proposition 3.2 and the above discussion concerning $\phi_1(-)$). On the other hand, since ν is, by definition, a section of the line bundle $\mathcal{M}^{\otimes d} \otimes \mathcal{K}^{\otimes d}$ (cf. §3), we thus conclude that *all the zeroes of ν have been accounted for in the estimates of Theorem 5.1*, i.e., that (under the assumption that d is odd or $m' \neq 2$):

> The norm ν is *invertible* away from the points at infinity, and, moreover, the inequalities of Theorem 5.1 are all equalities.

Note that we make use here of the fact that (since d is odd or $m' \neq 2$) ν is *nonzero on a dense open subset of S*, by Proposition 6.2.

It remains to examine *the case where d is even, and $m' = 2$.* By the theory of §6, if our data is *of null type* (cf. Definition 6.1), then ν will be *generically zero* (cf. Proposition 6.2). Thus, we assume that our data is *of general type* (cf. Definition 6.1). Note that the estimate from below for $\deg_{\mathrm{tot}}(\nu)$ will essentially be the same as before, except that we obtain an additional term (cf. Proposition 3.3)

$$-\phi_1(-d\cdot\eta_\iota+\frac{1}{2})+\phi_1(-d\cdot\eta_\iota)$$

at those points at infinity ι where 2 is an *active prime* (i.e., $2\in\mathcal{A}$). Note that here, since we are not summing over *all* ι, but only *certain special* ι, it is important that we keep *both* of the two terms "$\phi_1(-)$" in the above expression (i.e., it is not the same, in this case, to just compute the sum of the $-\phi_1(-d\cdot\eta_\iota+\frac{1}{2})$ over the specific ι in question) — cf. the computations of [HAT], Chapter VI, proof of Theorem 3.1, in the even case.

Next, note that the probability that $2\in\mathcal{A}$ is $\frac{1}{2+1}=\frac{1}{3}$. Moreover, at such ι, we have: $d\cdot\eta_\iota\notin G$ (since our data is of general type). But the fact that $2\in\mathcal{A}$ implies that ${}_2G=\boldsymbol{\mu}_2$, so we thus obtain that at such ι, $d\cdot\eta_\iota=\frac{1}{2}$. Thus, the *net contribution* to the estimate from below for $\deg_{\mathrm{tot}}(\nu)$ is:

$$\frac{1}{3}(-\phi_1(-\frac{1}{2}+\frac{1}{2})+\phi_1(-\frac{1}{2}))=\frac{1}{3}(-\phi_1(0)+\phi_1(-\frac{1}{2}))=\frac{1}{3}(-\frac{1}{12}-\frac{1}{24})=-\frac{1}{24}$$

Let us refer to this contribution as the *first new contribution.*

On the other hand, in the present context (where d is even and $m'=2$), the degree of the line bundle $\deg(\mathcal{M}^{\otimes d}\otimes\mathcal{K}^{\otimes d})$ is no longer equal to $\frac{1}{24}(d-1)$, since $-d\cdot[\overline{\mathcal{L}}\cdot e]$ is not necessarily zero (cf. Proposition 3.2). The resulting contribution of this new term — which we shall refer to as the *second new contribution* — is given by:

$$\begin{aligned}-d\cdot[\overline{\mathcal{L}}\cdot e]&=\sum_\iota\ \phi_1(-d\cdot\eta_\iota+\frac{1}{2})=\frac{2}{3}\phi_1(-\frac{1}{2}+\frac{1}{2})+\frac{1}{3}\phi_1(0+\frac{1}{2})\\&=\frac{2}{3}\phi_1(0)+\frac{1}{3}\phi_1(\frac{1}{2})=\frac{2}{3}\cdot\frac{1}{12}-\frac{1}{3}\cdot\frac{1}{24}=\frac{1}{24}\end{aligned}$$

where we note the following:

(1) In the first equality, since this time we are summing over *all* points at infinity ι, we are free to use just the single term "$\phi_1(-d\cdot\eta_\iota+\frac{1}{2})$" (instead of the difference "$\phi_1(-d\cdot\eta_\iota+\frac{1}{2})-\phi_1(-d\cdot\eta_\iota)$").

(2) In the second equality, we use the fact that the probability that $d\cdot\eta_\iota=\frac{1}{2}$ (respectively, $d\cdot\eta_\iota=0$) is $\frac{2}{3}$ (respectively, $\frac{1}{3}$) — cf. Lemma 8.1 in the case $p=2$.

Note, in particular, that *the first and second new contributions cancel* one another out in our estimate from below for $\deg_{\mathrm{tot}}(\nu)$. Thus, by the same reasoning as in the case where

d is odd or $m' \neq 2$, we conclude the following result, which is the *main technical result of this paper*:

Theorem 8.2. *If the given data (i.e., d, m', and η) are* of general type *(cf. Definition 6.1), then the norm ν of §3 is* invertible *away from the points at infinity, and, moreover, the inequalities of Theorem 5.1 are all equalities. If the given data (i.e., d, m', and η) are* of null type *(cf. Definition 6.1), then the norm ν of §3 is* identically zero.

§9. The Main Theorem

So far, our discussion has mainly been in *characteristic zero*. In this present §, we observe that what we have done so far extends immediately to mixed characteristic. This observation allows us to state and prove the *main theorem* of this paper, concerning *the invertibility of the coefficients of the Fourier transform of an algebraic theta function* in mixed characteristic.

Our notation is as at the beginning of §3. To review (cf. §3 for more details): $S^{\log}$ is a $\mathbf{Z}$*-flat fine noetherian log scheme*; $C^{\log} \to S^{\log}$ is a *log elliptic curve* which is smooth over a schematically dense open subscheme of S, hence defines a *"divisor at infinity"* (i.e., the pull-back via the associated classifying morphism of the divisor at infinity of $(\overline{\mathcal{M}}_{1,0})_{\mathbf{Z}}$) $D \subseteq S$. Moreover, we have a *stack* S_∞ obtained from S by adjoining the roots of the q-parameters at the locus $D \subseteq S$ over which $C^{\log} \to S^{\log}$ degenerates, together with a *smooth group scheme* $f : E_{\infty,S} \to S_\infty$ (which is useful for carrying out the constructions of [Zh]).

Let m, d be positive integers such that m *does not divide* d, and $\eta \in E_{\infty,S}(S_\infty)$ be a *torsion point* of order m. Then η defines a certain natural *metrized line bundle* $\overline{\mathcal{L}}$ which — in the notation of [HAT], Chapter V, §1 — is equal to $\overline{\mathcal{L}}_{\mathrm{st},\eta}$ (respectively, $\overline{\mathcal{L}}^{\mathrm{ev}}_{\mathrm{st},\eta}$) if d is odd (respectively, even). The *push-forward* $f_*\overline{\mathcal{L}}$ of this metrized line bundle to S_∞ defines a *metrized vector bundle* on S_∞, equipped with the action of a certain natural *theta group scheme* $\mathcal{G}_{\overline{\mathcal{L}}}$ (cf. [HAT], Chapter IV, §5).

Next, we assume that we are given finite, flat (i.e., over S_∞) *subgroup schemes* $G, H \subseteq E_{\infty,S}$ which are étale locally isomorphic to $\mathbf{Z}/d\mathbf{Z}$ in characteristic 0 (i.e., after tensoring with $\mathbf{Q}$), and which satisfy $H \times G = {}_dE_{\infty,S} \subseteq E_{\infty,S}$. (where ${}_dE_{\infty,S}$ is the kernel of multiplication by d on $E_{\infty,S}$). We shall refer to G as the *restriction subgroup* (since its principal use will be as a collection of points to which we will restrict sections of $\overline{\mathcal{L}}$), and H as the *Lagrangian subgroup* (since its primary use will be to descend $\overline{\mathcal{L}}$). When d is *even*, we also assume that we are given *splittings* G_{spl}, H_{spl} of certain natural surjections $\widetilde{G} \to G$, $\widetilde{H} \to H$ (cf. §3 for more details). With this data, we obtain (regardless of the parity of d) liftings $\mathcal{G}, \mathcal{H} \subseteq \mathcal{G}_{\overline{\mathcal{L}}}$ of $G, H \subseteq {}_dE_{\infty,S}$. Using $\mathcal{H} \subseteq \mathcal{G}_{\overline{\mathcal{L}}}$, we may descend $\overline{\mathcal{L}}$ to a line bundle $\overline{\mathcal{L}}_H$ on $E_{\infty_H,S} \stackrel{\mathrm{def}}{=} E_{\infty,S}/H$.

We are now ready to give the *first main result of this paper*:

Theorem 9.1. (Invertibility of the Coefficients of the Fourier Transform of an Algebraic Theta Function) *Suppose that we are given $C^{\log} \to S^{\log}$, m, d, η, G, G_{spl}, H, and H_{spl}, as above. Let us regard the* **Fourier expansion morphism**

$$\mathcal{E} : (f_H)_* \overline{\mathcal{L}}_H \to \mathcal{O}_{\widehat{G}} \otimes_{\mathcal{O}_{S_\infty}} \mathcal{K}$$

(where $\mathcal{K} \stackrel{\mathrm{def}}{=} \overline{\mathcal{L}}|_e$ is the restriction of $\overline{\mathcal{L}}$ to the identity section e of $E_{\infty,S}$) for the algebraic theta functions obtained by restricting global sections of $\overline{\mathcal{L}}_H$ to G as a "section" *of the $\mathcal{O}_{S_\infty}$-algebra $\mathcal{O}_{\widehat{G}}$ which is well-defined up to scalar multiples. If our data is* of null type *(a condition on d, m, η, and G — cf. Definition 6.1), then the norm ν of $\mathcal{E}$ is* generically zero*. If our data is* of general type *(a condition on d, m, η, and G — cf. Definition 6.1), then $\mathcal{E}$ satisfies the following* **invertibility properties***:*

(1) $\mathcal{E}$ is invertible over $(U_S)_{\mathbf{Q}}$ (where $U_S \stackrel{\mathrm{def}}{=} S - D$; the subscripted $\mathbf{Q}$ denotes "$\otimes_{\mathbf{Z}} \mathbf{Q}$").

(2) Let $\iota \in D$ be a point at infinity. Let

$$h_{\boldsymbol{\mu}} \stackrel{\mathrm{def}}{=} |H \bigcap \boldsymbol{\mu}_d|; \quad h_{\mathrm{et}} \stackrel{\mathrm{def}}{=} d/h_{\boldsymbol{\mu}}; \quad h_{\mathrm{eff}} \stackrel{\mathrm{def}}{=} |\mathrm{Im}_{E_{\infty_{\boldsymbol{\mu}}},S}(G_{\mathrm{et}}) \bigcap \boldsymbol{\mu}_d^{\boldsymbol{\mu}}|; \quad h_{\mathrm{ord}} \stackrel{\mathrm{def}}{=} h_{\mathrm{et}}/h_{\mathrm{eff}}$$

be the local invariants at ι defined in §5. Then in a neighborhood of ι, the endomorphisms of the $\mathcal{O}_{S_\infty}$-algebra $\mathcal{O}_{\widehat{G}}$ defined by multiplying by local generators of the image of $\mathcal{E}$ may be written (for an appropriate basis) as diagonal matrices whose diagonal entries are of the form

$$d \cdot \epsilon \cdot {h_{\mathrm{ord}}}^{-\frac{1}{2}} \cdot \omega \cdot q^{\frac{1}{d} \cdot c_{\mathrm{Rem}(j, h_{\mathrm{eff}})}(\text{Case } X_\iota)} \cdot (\text{a unit } \equiv 1 \text{ modulo } q^{(>0)})$$

where ϵ is a 4-th root of unity (respectively, $\sqrt{2}$ times an 8-th root of unity) if h_{ord} is odd *(respectively,* even*); ω is a sum of either one or two elements of $\boldsymbol{\mu}_{n \cdot h_{\boldsymbol{\mu}} \cdot h_{\mathrm{ord}}}$ (in fact, in all but one exceptional case, $\omega \in \boldsymbol{\mu}_{n \cdot h_{\boldsymbol{\mu}} \cdot h_{\mathrm{ord}}}$); the notation $c_j(\text{Case } X_\iota)$ is as in §3 (cf. [HAT], Chapter V, §4, for more details); j ranges from 1 to d; and $\mathrm{Rem}(j, h_{\mathrm{eff}})$ denotes the unique positive integer $\leq h_{\mathrm{eff}}$ which is $\equiv j$ modulo h_{eff}.*

Proof. The statement of Theorem 9.1 is essentially an amalgamation of Theorems 5.2 and Theorem 8.2. Note, in (2), that the extra factor of d (relative to the expressions in Theorem 5.2) arises from the fact that when we take Fourier expansions (i.e., apply the operator $\mathcal{F}$ of §1), the coefficients of the various characters of G get multiplied by d. Also, we observe that although our computations in §4, 5, were in a characteristic 0 setting, the assertions of (2) still hold, since the various bases of function spaces — i.e., in essence, *q-expansions* — that were used in §4, 5, all still form bases of the corresponding mixed characterstic spaces — cf., e.g., [HAT], Chapter IV, §2,3, where everything is done in mixed characteristic. This completes the proof. ○

Remark. The invertibility of the coefficients of the Fourier expansion of an algebraic theta function may be interpreted as the statement that certain modular functions are, in fact, *modular units*. It would thus be interesting to consider the meaning of Theorem 9.1 from the point of view of the theory of modular units, e.g., to see if one can write these new modular units explicitly in terms of classical modular units such as the *Siegel modular units* (cf., for instance, [KL], Chapter 4).

§10. The Theta Convolution

We maintain the notation of §9. In this §, we apply Theorem 9.1 to study a morphism which we call the *theta convolution*. This morphism is (essentially) the endomorphism of the space of functions on the restriction subgroup G given by convoluting with the algebraic theta function in question. In particular, we observe that the theory of the present paper implies that this theta convolution satisfies certain compatibility properties relative to the *evaluation morphism* studied in [HAT].

In this §, let us write

$$\Theta_{\mathrm{CV}} : \mathcal{M}^{-1} \otimes \mathcal{O}_G \to \mathcal{O}_G \otimes \mathcal{K}$$

(where all tensor products are over $\mathcal{O}_{S_\infty}$; $\mathcal{M} \stackrel{\mathrm{def}}{=} \{(f_H)_* \overline{\mathcal{L}}_H\}^{-1}$; $\mathcal{K} \stackrel{\mathrm{def}}{=} \overline{\mathcal{L}}|_e$; $e \in E_{\infty,S}(S_\infty)$ is the identity section) for the morphism defined as follows: First, recall that restricting sections of $\overline{\mathcal{L}}_H$ to G defines a morphism

$$\mathcal{M}^{-1} \to \overline{\mathcal{L}}|_G \cong \mathcal{O}_G \otimes \mathcal{K}$$

On the other hand, *the convolution operator* $*$ (cf. §1) defines a morphism

$$\mathcal{O}_G \otimes \mathcal{O}_G \to \mathcal{O}_G$$

Thus, if we compose this convolution morphism (tensored with $\mathcal{K}$) with the restriction morphism $\mathcal{M}^{-1} \to \mathcal{O}_G \otimes \mathcal{K}$ (tensored with $\mathcal{O}_G$), we get a morphism Θ_{CV} as above. This morphism will be referred to as the *theta convolution*.

By Proposition 1.1, (iii.), and Theorem 9.1, (1), it follows that Θ_{CV} is *invertible* over $(U_S)_{\mathbf{Q}}$. Since Θ_{CV} is generically invertible, we thus obtain that the image of Θ_{CV} in $\mathcal{O}_G \otimes \mathcal{K} \cong \overline{\mathcal{L}}|_G$, which we denote by

$$\overline{\mathcal{L}}|_G^{\Theta} \subseteq \overline{\mathcal{L}}|_G$$

is a *metrized vector bundle on* S_∞ which satisfies

$$\overline{\mathcal{L}}|_G^{\Theta} \cong \mathcal{M}^{-1} \otimes \mathcal{O}_G$$

Note, moreover, that the inclusion $\overline{\mathcal{L}}|_G^{\Theta} \subseteq \overline{\mathcal{L}}|_G$ is an *isomorphism* over $(U_S)_{\mathbf{Q}}$.

On the other hand, let us recall the object

$$E^{\dagger}_{\infty,[d]}$$

of [HAT], Chapter V, §2. Over $(U_S)_{\mathbf{Q}}$, this object is isomorphic to the *universal extension* of the elliptic curve $E|_{(U_S)_{\mathbf{Q}}} \to (U_S)_{\mathbf{Q}}$ under consideration. Thus, in general, one may think of $E^{\dagger}_{\infty,[d]}$ as a certain extension of this universal extension over the divisor at infinity and the points of positive characteristic. Let us write

$$f_*(\overline{\mathcal{L}}|_{E^{\dagger}_{\infty,[d]}})^{<d}\{\mathrm{et}\}$$

for the push-forward consisting of sections of $\overline{\mathcal{L}}$ over $E^{\dagger}_{\infty,[d]}$ whose torsorial degree (i.e., relative degree for the morphism $E^{\dagger}_{\infty,[d]} \to E_{\infty,S}$) is $< d$, equipped with the *étale-integral structure* (cf. [HAT], Chapter V, §3) at the finite primes. Note that this push-forward forms a metrized vector bundle on S_∞ of rank d^2. Since we are given a subgroup scheme $H \cong \mathcal{H} \subseteq \mathcal{G}_{\overline{\mathcal{L}}}$, we thus obtain a natural action of H on this push-forward. Let us denote by

$$f_*(\overline{\mathcal{L}}|_{E^{\dagger}_{\infty,[d]}})^{<d}\{\mathrm{et}\}^H$$

the metrized vector bundle on S_∞ of rank d consisting of sections that are fixed by H. Then it follows from [HAT], Chapter VI, Theorem 3.1, (1), (2), that we have a natural *evaluation map*

$$\Xi_G : f_*(\overline{\mathcal{L}}|_{E^{\dagger}_{\infty,[d]}})^{<d}\{\mathrm{et}\}^H \to \overline{\mathcal{L}}|_G$$

which is an *isomorphism* over $(U_S)_{\mathbf{Q}}$.

Now we have the following important *application of the theory of this paper* (our second main result):

Theorem 10.1. (The Theta-Convoluted Scheme-Theoretic Comparison Isomorphism) *Suppose that we are in the situation of Theorem 9.1. Let us denote by*

$$\Xi_G : f_*(\overline{\mathcal{L}}|_{E^{\dagger}_{\infty,[d]}})^{<d}\{\mathrm{et}\}^H \to \overline{\mathcal{L}}|_G$$

the evaluation map derived from [HAT], Chapter VI, Theorem 3.1, (1). Write C for the product of all the prime numbers that divide d or n. Then $2d \cdot C \cdot \Xi_G$ factors through $\overline{\mathcal{L}}|_G^{\Theta} \subseteq \overline{\mathcal{L}}|_G$. Moreover, the resulting morphism

$$\Xi_G^{\Theta} : f_*(\overline{\mathcal{L}}|_{E^{\dagger}_{\infty,[d]}})^{<d}\{\mathrm{et}\}^H \to \overline{\mathcal{L}}|_G^{\Theta}$$

satisfies the following properties:

(1) Ξ_G^{Θ} is **invertible** *over $(U_S)_{\mathbf{Q}}$. Moreover, the poles of the inverse of Ξ_G^{Θ} over U_S are annihilated by $2d \cdot C^2$.*

(2) There exists a **natural modification of the integral structure at infinity** *of $f_*(\overline{\mathcal{L}}|_{E^{\dagger}_{\infty,[d]}})^{<d}\{\mathrm{et}\}^H$ analogous to the new integral structure at infinity of [HAT], Chapter VI, §1, with respect to which Ξ_G^{Θ} is both integral and invertible over $S_{\mathbf{Q}}$. (Thus, in particular, relative to this modified integral structure, Ξ_G^{Θ} will be integral over all of S, and invertible over S, except for poles annihilated by $2d \cdot C^2$.) Moreover, just as the new integral structure at infinity of [HAT], Chapter VI, §1, is given by allowing poles on the F^j/F^{j-1}-portion of the push-forward of the form $q^{-\frac{1}{d}c_j(\mathrm{Case}\ X_\iota)}$ (cf. [HAT], Chapter VI, Theorem 3.1, (3)), in the present context, the new integral structure at infinity is* **given by allowing poles** *on the F^j/F^{j-1}-portion of the push-forward of the form*

$$q^{-\frac{1}{d}\{c_j(\mathrm{Case}\ X_\iota) - c_{\mathrm{Rem}(j,h_{\mathrm{eff}})}(\mathrm{Case}\ X_\iota)\}}$$

(where $\mathrm{Rem}(j, h_{\mathrm{eff}})$ is as in Theorem 9.1).

Proof. Over $(U_S)_{\mathbf{Q}}$, everthing is immediate. Let us prove that $2d \cdot C \cdot \Xi_G$ factors through $\overline{\mathcal{L}}|_G^{\Theta} \subseteq \overline{\mathcal{L}}|_G$. First, observe that $2d \cdot C$ is sufficient to cancel the poles of the inverse of the expression "$d \cdot \epsilon \cdot h_{\mathrm{ord}}{}^{-\frac{1}{2}} \cdot \omega$" appearing in Theorem 9.1. This proves the existence of the desired factorization over U_S. Thus, (by working over various appropriate finite, flat coverings of the moduli stack $(\overline{\mathcal{M}}_{1,0})_{\mathbf{Z}}$) one sees that to prove the existence of the desired factorization over S, it suffices to prove its existence at the points of $D_{\mathbf{Q}}$.

To this end, we recall from the theory of [HAT] (cf., especially, [HAT], Chapter V, §4, Theorem 4.8; [HAT], Chapter VI, §4, proof of Theorem 4.1) that to consider the restriction of sections of $f_*(\overline{\mathcal{L}}|_{E^\dagger_{\infty,[d]}})^{<d}\{\text{et}\}^H$ (as opposed to just $(f_H)_*\overline{\mathcal{L}}_H$) to G amounts to considering the various *derivatives* of the theta function in question. In our case, this essentially amounts to considering the various derivatives $(U \cdot \frac{\partial}{\partial U})^j \Theta$ (where Θ is as in §4; $j = 0, \dots, d-1$). If we then restrict such derivatives to G and apply the appropriate trivializations (as discussed in §4, 5), we see that we obtain similar expressions to those obtained in §4, 5 in the case of Θ itself. The only difference is that, in the case of the various derivatives of Θ, the leading terms (i.e., terms involving the smallest powers of q) as in the statement of Theorem 5.2 will be *multiplied by various constant factors.* The point here, however, is that the smallest power of q for these derivatives of Θ will always be $\leq$ the smallest power of q that arises in the case of the original Θ. Thus, even if we divide the Fourier coefficients of the restrictions of the derivatives of Θ by the Fourier coefficients of the corresponding restrictions of Θ itself, the result will remain *integral.* This implies the existence of the factorization stated in Theorem 10.1.

Next, we consider the *invertibility of* Ξ^Θ_G *over* U_S. The fact that the the poles of the inverse of Ξ^Θ_G over U_S are annihilated by $2d \cdot C^2$ follows formally from the fact that the poles of the inverse of Ξ_G are annihilated by C (cf. [HAT], Chapter VI, Theorem 4.1, (2)), together with the fact that $2d \cdot C \cdot \Xi_G$ is (by definition) the composite of Ξ^Θ_G with another morphism.

Finally, we consider the *invertibility of* Ξ^Θ_G *at the points of* $D_{\mathbf{Q}}$. The argument is essentially the same as in the proof above of the existence of the factorization Ξ^Θ_G. Indeed, just as *in the situation of [HAT]* (cf., especially, [HAT], Chapter V, Theorem 4.8; [HAT], Chapter VI, Theorem 4.1, (3)), *a collection of local generators for the new integral structure* is given by the

$$q^{-\frac{1}{d}c_j(\text{Case } X_\iota)} \cdot \zeta^{\text{CG}}_{j-1}$$

(for $j = 1, \dots, d$), *in the present context, a collection of local generators* for the new integral structure is given by the

$$q^{-\frac{1}{d}\{c_j(\text{Case } X_\iota) - c_{\text{Rem}(j,h_{\text{eff}})}(\text{Case } X_\iota)\}} \cdot \zeta^{\text{CG}}_{j-1}$$

(for $j = 1, \dots, d$). That is to say, the "work done by dividing by $q^{\frac{1}{d}c_j(\text{Case } X_\iota)}$" is *partially absorbed by the inverse of the theta convolution*, which results in division by $q^{\frac{1}{d}c_{\text{Rem}(j,h_{\text{eff}})}(\text{Case } X_\iota)}$ (cf. the theory of §4, 5; Theorem 9.1). Thus, in the present "theta-convoluted case," the desired integral structure at infinity is obtained by dividing by "what's left." This completes the proof of Theorem 10.1. ○

Remark 1. In particular, we obtain that at points at infinity ι where $h_{\text{eff}} = d$ — i.e., when the restriction subgroup G is *of multiplicative type* — *no modification of the integral structure at infinity is necessary.* Put another way, at such ι:

The "Gaussian poles" of the "comparison isomorphism" defined by the theta-convoluted evaluation map Ξ_G^{Θ} vanish.

(cf. the discussion of [HAT], Introduction, §5.1). It is this fact/observation that formed *the fundamental motivation* for the author to develop the theory of the present paper.

Remark 2. Just as in [HAT], Chapter IX, §3, we constructed an "arithmetic Kodaira-Spencer morphism" from the "Hodge-Arakelov Comparison Isomorphism" ([HAT], Chapter VIII, Theorem A) of [HAT], one can now construct a *theta-convoluted arithmetic Kodaira-Spencer morphism* from the *theta-convoluted comparison isomorphism* of Theorem 10.1. The procedure is entirely formally analogous to what was done in [HAT], Chapter IX, §3, i.e., one simply transports the natural Galois action on the "étale side" (i.e., the right-hand side) of the comparison isomorphism to the "de Rham-theoretic side" (i.e., the left-hand side) of the comparison isomorphism, and considers the extent to which this Galois action preserves the Hodge filtration. We leave the entirely routine details to the reader. Note that the key technical point here is that:

The range of the theta-convoluted comparison isomorphism, i.e.,

$$\overline{\mathcal{L}}|_G^{\Theta} \cong \mathcal{M}^{-1} \otimes \mathcal{O}_G$$

admits a natural Galois action (arising from the Galois action on G).

Moreover, we would like to emphasize — relative to the context of the theory of [HAT] (cf., especially, the discussion at the end of [HAT], Chapter IX, §3) — that:

The construction of an arithmetic Kodaira-Spencer morphism in which the Gaussian poles have been at least partially eliminated brings us one step closer to the possibility of applying the theory of [HAT] and the present paper to diophantine geometry, as discussed in [HAT], Introduction, §5.1, and [HAT], Chapter IX, §3.

Remark 3. Of course, in order to complete the analogy with the theory of [HAT], one must also study the properties of the theta convolution at *archimedean primes*. Just as in the theory of [HAT], by pulling back the natural metric on the étale side of the theta-convoluted comparison isomorphism one obtains an *étale metric* on the de Rham side of the theta-convoluted comparison isomorphism. The theta-convoluted arithmetic Kodaira-Spencer morphism of Remark 2 will have natural integrality properties with respect to this étale metric. Of course, in order to make use of this machinery, one would like to have more explicit information about the étale metric, in particular, concerning the metrics induced by the étale metric on the various subquotients of the Hodge filtration (on the de Rham side of the theta-convoluted comparison isomorphism). For the Hodge-Arakelov Comparison Isomorphism of [HAT], this sort of computation was carried out in [HAT], Chapters VII and VIII. It is not difficult to compute what happens to the "Hermite, Legendre, and Binomial Models" of the theory of [HAT] when one introduces the theta-convolution. It is the hope of the author to give an explicit exposition of this computation in a future paper.

Bibliography

[DyMc] H. Dym and H. P. McKean, *Fourier Series and Integrals*, Academic Press (1972).

[HAT] S. Mochizuki, *The Hodge-Arakelov Theory of Elliptic Curves: Global Discretization of Local Hodge Theories*, manuscript.

[KL] D. S. Kubert and S. Lang, *Modular Units*, Grundlehren der mathematischen Wissenschaften **244**, Springer-Verlag (1981).

[Lang] S. Lang, *Algebraic Number Theory*, Graduate Texts in Mathematics **110**, Springer-Verlag (1986).

[MB] L. Moret-Bailly, *Pinceaux de variétés abéliennes*, Astérisque **129**, Soc. Math. France (1985).

[Mumf1,2,3] D. Mumford, On the equations defining abelian varieties I, II, III, *Invent. Math.* **1** (1966), pp. 287-354; **2** (1967), pp. 71-135; **3** (1967), pp. 215-244.

[Shz] S. S. Shatz, Group Schemes, Formal Groups, and p-divisible Groups in *Arithmetic Geometry*, edited by G. Cornell and J. H. Silverman, Springer-Verlag (1986).

[Zh] S. Zhang, Admissible pairing on a curve, *Invent. Math.* **112** (1993), pp. 171-193.