The generalized Riemann hypothesis for Dirichlet L-functions

27 November 2026 · Edition 930

Volume XIII

CM theta derivatives and Frobenius translates

Abstract

We construct the CM theta derivatives, compute local divisibility and follow Frobenius through the prescribed rows. Interpolation at split primes gives integral and archimedean estimates for the marked elliptic jets.

The guide in Volume I lists all twenty-seven volumes.

Contents

XIII CM theta derivatives and Frobenius translates 1
64 Complex multiplication and integral sections . . . 3
64.1 Complex multiplication and the local prime-power count . . . 3
64.1.1 An integral bound for an invariant derivative . . . 3
64.1.2 The same quadratic field and the same weights . . . 4
64.1.3 Algebraic jets over a common number field . . . 5
64.2 The exact ideal of scalar CM derivatives . . . 6
64.3 Realizing the derivative by global theta sections . . . 10
64.4 The trace polarization and integral Fourier components . . . 12
64.5 Frobenius and mixed derivatives in CM eigendirections . . . 15
64.6 Reduction of polynomial differential operators at an inert prime . . . 17
65 Elliptic derivatives on definite classes . . . 21
65.1 The norm of the prescribed products of maximal minors . . . 21
65.2 Arithmetic of the normalized elliptic theta derivatives . . . 24
65.3 Conjugate class sums for the normalized theta vacua . . . 27
65.4 Split representatives and the finite Weil action . . . 31
65.5 An inert-prime congruence for the prescribed class sums . . . 34
65.6 Higher powers in the prescribed class sums . . . 37
65.7 The elliptic normalization on the common interval . . . 39
65.8 The two-torsion point prescribed by the split prime . . . 42
65.9 A Gram matrix comparison for the analytic theta section . . . 44
66 Frobenius translates and higher derivatives . . . 46
66.1 The Frobenius count in a single list of minor degrees . . . 46
66.2 Nonzero translated class sums at one definite step . . . 49
66.3 The cost of the prescribed derivatives . . . 51
66.4 The first inert-prime congruence in the Hermitian frame . . . 54
66.5 Higher powers at an inert prime . . . 56
66.6 Odd powers of Frobenius in the class-section derivatives . . . 58
66.7 Exact coefficients at the odd powers of Frobenius . . . 61
66.8 Individual Frobenius translates in the theta derivatives . . . 62
66.9 One minor projection for the translates at primes split in the second field . . . 64
66.10 Composing the polynomial maps through the class sums . . . 67

66.11 The factorial and field norm of the composed value . . . 69
66.12 A finite torsion level for simultaneous nonvanishing . . . 72
66.13 Differentiating torsion translates at primes dividing the order . . . 74
67 Signed theta periods and CM derivatives . . . 75
67.1 Congruences for a prescribed signed theta period . . . 75
67.2 Real sizes and prime-power congruences for the same theta periods . . . 77
67.3 From the adelic theta distribution to CM derivatives . . . 80
67.4 Local divisibility of the prescribed compact coefficient . . . 82
67.5 CM derivatives on the prescribed final row . . . 84
67.6 The marked elliptic derivatives at every prime . . . 85
67.7 Finite valuations of the CM splitting characters . . . 86
68 Marked elliptic jets and their determinants . . . 87
68.1 Joint row degrees on the even Frobenius cycles . . . 87
68.2 Elliptic theta derivatives at a split prime . . . 89
68.3 Simultaneous interpolation on the marked elliptic curve . . . 92
68.4 Positive derivatives of a fixed signed theta section . . . 93
68.5 Common split primes for signed theta derivatives . . . 95
68.6 Integral elementary divisors of the theta derivative table . . . 98
68.7 The archimedean determinant of the same elliptic jets . . . 100
68.8 The rational norm of the marked elliptic determinant . . . 103
68.9 Green energy and signed elliptic determinants . . . 106
68.10 Theta derivatives at ordinary primary torsion . . . 107
68.11 Division functions for normalized theta translates . . . 110
68.12 Independence of prescribed derivatives at split primes . . . 112
68.13 Cyclic terminal Fourier projections on an elliptic curve . . . 114
69 References . . . 117

64 Complex multiplication and integral sections

64.1 Complex multiplication and the local prime-power count

The first binary character of the field in Proposition 6.4 cuts out $K = \mathbb{Q}(\sqrt{-q})$, where $q \equiv 3 \pmod 4$. The three splitting behaviors in this one quadratic field determine which prime powers can contribute at a place. We first prove a bound for derivatives of integral functions on a formal group with complex multiplication by K. It determines the same three local densities, including the factor of one half at q.

64.1.1 An integral bound for an invariant derivative

Let p be a rational prime, let R be the ring of integers of a finite extension of $\mathbb{Q}_p$, and use the valuation $v_p(p) = 1$. Suppose a place v of K over p is nonsplit, so K_v is quadratic. Write e for its ramification index, Q for the size of its residue field, and ϖ for a uniformizer of $\mathcal{O}_{K_v}$. Assume R contains the image of $\mathcal{O}_{K_v}$ under the chosen tangent embedding. Let $\mathcal{F}$ be a smooth commutative one-dimensional formal group over R with an action of $\mathcal{O}_{K_v}$ by formal endomorphisms whose tangent action is that embedding. For $a \geq 1$ define

$$L_{p,K}(a) = v_p(a!) - \frac{1}{e}\left\lfloor \frac{a-1}{Q-1} \right\rfloor .$$

Theorem 64.1 (Integral derivatives on a product of CM formal groups)**.** *Let $g \geq 1$, let D be any invariant derivation defined by an integral tangent vector on $\mathcal{F}^g$, and let f be any integral formal function at the identity. Then*

$$v_p\big((D^a f)(0)\big) \;\geq\; L_{p,K}(a). \tag{64.1}$$

Inert primes have $(e, Q) = (1, p^2)$, and the ramified prime has $(e, Q) = (2, p)$. At a split prime integrality always gives $v_p((D^a f)(0)) \geq 0$. A zero value has valuation $+\infty$.

Proof. Start with any parameter t on the one-dimensional group. For the Teichmüller units $\zeta \in \mu_{Q-1} \subset \mathcal{O}_{K_v}$, the coordinate

$$T = \frac{1}{Q-1} \sum_{\zeta \in \mu_{Q-1}} \zeta^{-1}[\zeta](t)$$

has linear coefficient one and is integral. Here a scalar acting on tangent coordinates is read through the given embedding. Reindexing the sum gives $[\zeta]^*T = \zeta T$. In this coordinate the endomorphism $[\varpi]$ has expansion $P(T) = \varpi T + \sum_{i \geq 2} b_i T^i$ with integral coefficients. Commutativity with the Teichmüller action implies $b_i = 0$ unless $i \equiv 1 \pmod{Q-1}$. Thus every nonlinear term has degree at least Q.

Over the fraction field the formal group admits a logarithm with linear coefficient one. In dimension one, integrate the invariant differential with value dT at zero, taking constant term zero. Translation invariance gives the logarithm addition identity, by differentiating in the second variable and then setting it to zero. Its inverse $E(Z) = Z + \sum_{n \geq 2} c_n Z^n$ is the exponential. The action in logarithm coordinates is its linear part since an additive power series in characteristic zero is linear. Consequently

$$(\varpi^n - \varpi)c_n = \sum_{i=Q}^{n} b_i \sum_{\substack{k_1 + \cdots + k_i = n \\ k_j \geq 1}} c_{k_1} \cdots c_{k_i}, \qquad c_1 = 1.$$

For $n > 1$, the factor on the left has valuation $1/e$. Induction gives $v_p(c_n) \geq -e^{-1}\lfloor (n-1)/(Q-1)\rfloor$. In fact for $i \geq Q$ the sum of the i floors for the indices k_j, plus one, is at most $\lfloor (n-1)/(Q-1)\rfloor$. This accounts for the one division by ϖ at each induction step, also over ramified coefficient rings.

In the product coordinates write the integral tangent vector as $(u_1, \dots, u_g)$. Pull back the function along $Z \mapsto (E(u_1 Z), \dots, E(u_g Z))$. Differentiation in Z on this formal one-parameter subgroup is the invariant derivation D, so its a-th derivative at zero is $a!$ times the coefficient of Z^a. Every term of positive order contributing to this coefficient is a product of at least one exponential coefficient and integral scalars. For indices $k_1 + \cdots + k_i = a$ its denominator valuation is at most $e^{-1}\sum_j \lfloor (k_j - 1)/(Q-1)\rfloor \leq e^{-1}\lfloor (a-1)/(Q-1)\rfloor$. A finite sum of such terms obeys the same bound. This proves (64.1). In all cases an invariant integral derivation on the formal group preserves its integral functions, proving the final assertion. □

The theorem applies also to a section of a line bundle regular in an integral frame near the identity, by applying it to its scalar in that frame. This is a statement about a scalar Taylor coefficient. When lower Taylor coefficients vanish, the first nonzero coefficient changes by a unit under a change of integral frame.

64.1.2 The same quadratic field and the same weights

Fix a common interval and the fields $E_x = E_0(\sqrt{-q}, \sqrt{-d})$, with q, d fixed throughout the interval. Write $B = \mathrm{Gal}(E_x/\mathbb{Q})$, $\Phi = \mathrm{Gal}(E_x/K)$, and use additive notation. The cosets and the bijection $p_t : B \setminus \Phi \to \Phi$, $g \mapsto (1, 1, t) + g$, are those of Volume I. For a lift F_p of Frobenius and the inertia subgroup I_p, the contribution of p to a single count is

$$C_p(t, a, w) = \frac{2\log p}{|I_p|} \sum_{j \geq 1} \sum_{g \in (jF_p + I_p)\setminus \Phi} (a/p^j - w_{p_t(g)})_+. \tag{64.2}$$

The sum over all primes is $C(t, a, w)$. This formula retains the inertia average even at primes ramified in E_0.

Take $b = \exp(x^{\varepsilon})$, $a = \lfloor bx \rfloor$, and define

$$W = 2(1 + \lceil \log_2(a+1) \rceil).$$

Give every distinguished position weight $\lceil b \rceil$ and every other position weight W. For large x, $\lceil b \rceil \geq W$ and $a/W \geq \exp(x^{\varepsilon/3})/3$. Indeed $\log W = O_{\varepsilon}(\log(2x))$, while $\log a \geq x^{\varepsilon} + \log x - o(1)$. These choices satisfy the general integral-weight estimate of Proposition 7.2. In particular they keep the distinguished prime sums and the error budget for discarded characters on the same intervals.

Theorem 64.2 (The local count at every prime and translate)**.** *For all these weights, at every x on a sufficiently distant common interval and for every t, u and stage, the following holds. At a prime nonsplit in K, and for every integral CM jet as in Theorem 64.1,*

$$\frac{C_p(t, a, w)}{2\log p} \;\leq\; v_p((D^a f)(0)).$$

At a split prime $C_p = 0$. These assertions hold also when one replaces the weights by any list of real numbers at least W.

Proof. At an unramified prime of K, inertia lies in Φ. At a split prime so does Frobenius, hence the inner sum is empty. At an inert prime that entire coset lies outside Φ for odd j, and

lies inside for even j. If p ramifies in K, then $I_p \to B/\Phi$ is onto and exactly half the elements of every Frobenius coset are outside Φ. Thus the normalized count is at most

$$U_p = \begin{cases} \displaystyle\sum_{j\ge 1 \text{ odd}} (a/p^j - W)_+, & p \text{ inert}, \\ \displaystyle\frac{1}{2}\sum_{j\ge 1} (a/p^j - W)_+, & p \text{ ramified}. \end{cases}$$

Let S_p denote the corresponding sum of a/p^j without the cutoff and weights, retaining the factor one half in the ramified case. The geometric series give $S_p = ap/(p^2-1)$ and $S_p = a/(2(p-1))$, respectively. Legendre's formula $v_p(a!) = (a - s_p(a))/(p-1)$, with $s_p(a)$ the sum of the base-p digits, gives in both cases

$$L_{p,K}(a) \ge S_p - s_p(a)/(p-1).$$

Here $s_p(a)/(p-1) \le 1 + \lfloor \log_p a \rfloor \le W/2$. If $U_p > 0$, at least one active term loses W at an inert prime and $W/2$ at the ramified prime. All other terms are at most their terms in S_p. Thus $U_p \le S_p - W/2 \le L_{p,K}(a)$. If $U_p = 0$, integrality of the derivative suffices. No bound depends on the translate, the size of the inertia group in E_x, or the number of copies of the formal group. □

64.1.3 Algebraic jets over a common number field

For clarity we realize the local formal groups on the fields of the counts. For each $K = \mathbb{Q}(\sqrt{-q})$ take a CM elliptic curve C with endomorphism ring $\mathcal{O}_K$, over a number field containing K over which all its endomorphisms are defined. The classical algebraicity and integrality of the singular modulus of $\mathbb{C}/\mathcal{O}_K$ give such a curve over $\overline{\mathbb{Q}}$, with integral j-invariant. Its finitely many required endomorphisms are defined over a finite extension. The potential good reduction criterion for elliptic curves then gives good reduction everywhere after a further finite extension. One can take a single extension by first adjoining full torsion of order 3 and 4. Indeed potential good reduction makes the inertia image on a prime-to-residue-characteristic Tate module finite. At each prime use the 3-adic module if the residue characteristic is different from 3 and the 2-adic module otherwise. A finite subgroup of the kernel modulo 3, respectively modulo 4, is trivial by the binomial expansion of a matrix of prime order congruent to the identity. The criterion of Néron, Ogg and Shafarevich gives good reduction. Endomorphisms extend to the abelian scheme by the Néron mapping property. These standard facts are recalled in [1, 2].

Choose one such number field J containing every E_x on the interval. This is possible because q, d, K_ψ are fixed there and the real cyclotomic layers are nested with a largest index on the bounded interval. One may use C^g directly. The CM type given by the embeddings of E_x above the chosen embedding of K also has the integral model

$$\mathcal{A} = \mathcal{O}_{E_x} \otimes_{\mathcal{O}_K} C.$$

Here the notation denotes the direct factor of C^n cut out by an idempotent representing the finite projective $\mathcal{O}_K$-module $\mathcal{O}_{E_x}$ as a summand of $\mathcal{O}_K^n$. The idempotent and its complement add to the identity and their images give the product decomposition. This constructs the abelian scheme, with the indicated action of $\mathcal{O}_{E_x}$. Its tangent space in characteristic zero is $E_x \otimes_K J$ tensored with the tangent line of C, so it has the specified embeddings each with multiplicity one.

At a nonsplit p the action of $\mathcal{O}_K$ on the formal group of C extends to its p-adic completion $\mathcal{O}_{K_v}$. To see continuity, multiplication by p has linear term pT and all other terms have order at least two. Iterating it sends T into $(p, T)^{n+1}$ after n steps. Endomorphisms whose scalars

differ by a multiple of p^n therefore agree modulo $(p,T)^{n+1}$ in formal coordinates, by the formal addition law. Completeness gives the extension. The tangent action is the corresponding embedding of K_v. Over $\mathcal{O}_{K_v}$ a basis adapted to the projective summand conjugates the idempotent to a diagonal projection. This basis change acts integrally on the power of the formal group. Consequently the formal group of $\mathcal{A}$ at every place above p is a power of the formal group in Theorem 64.1.

Corollary 64.3 (An ideal dividing every integral CM jet)**.** *Use an integral invariant tangent vector on $\mathcal{A}$ and a scalar jet of order a at its identity defined integrally over $\mathcal{O}_J$. Let $z \in J$ be its a-th derivative at the identity. For each finite place $w \mid p$ write $e(w/p)$ for its ramification index. The integral ideal*

$$\mathfrak{c}(t,a,w_\bullet) = \prod_p \prod_{w\mid p} \mathfrak{p}_w^{\lceil e(w/p)\, C_p(t,a,w_\bullet)/(2\log p)\rceil}$$

contains z. If $z \neq 0$, then

$$C(t,a,w_\bullet) \le \frac{2}{[J:\mathbb{Q}]} \sum_{\sigma: J\hookrightarrow\mathbb{C}} \log|\sigma z|. \tag{64.3}$$

Products of jets give sums of the corresponding counts whenever the product is nonzero.

Proof. Taylor evaluation to order a depends only on the jet modulo terms of order $a+1$, so it may be computed in any local integral formal frame for the scalar jet. The two preceding theorems give $v_w(z) \ge e(w/p)C_p/(2\log p)$. At a split prime integrality gives the same inequality. The integral valuations give the ceilings, and only finitely many primes contribute. For a nonzero algebraic integer, the sum of its finite valuations times log residue norms equals the sum of its log absolute values over all embeddings. For each p, $\sum_{w\mid p} e(w/p)[\kappa(w):\mathbf{F}_p] = [J:\mathbb{Q}]$. Summing therefore gives (64.3). Valuations and log absolute values add under products. □

For example the canonical theta section of $\mathcal{O}_C([0])$ vanishes simply at the identity. In an integral local frame its a-th tensor power has leading term uT^a with u a unit. The corresponding derivative against a local tangent generator is $a!u$. This gives an actual nonzero theta jet to which the bound applies. The scalar periods of Section 121.15 integrate a chain of Weil kernels and a Bessel test. Using (64.3) on those periods requires an integral identification with the jets, including the factors introduced by projections and normalization. It also requires an archimedean bound after the main term of the count is subtracted.

Locations in the accompanying source. The note's second dated entry on page 3 concerns the odd prime-power series at an inert prime. Related formal coefficients occur in `Development/AbelianVarietyTheory/Proofs/DecoratedLatticeProofs/HeightTwoHondaTypeFirstCoeffNormEqOneStatement.lean`, line 6. Iteration of an invariant derivation occurs in `Development/AbelianVarietyTheory/Proofs/DivisorProofs/ConstantCoeffIterateInvariantDerivationCongr.lean`, line 52.

64.2 The exact ideal of scalar CM derivatives

Let $K = \mathbb{Q}(\sqrt{-q})$ with the primes $q \equiv 3 \pmod 8$ of the common intervals. Its discriminant is $-q$. For $Q = p^f$ and an integer $n \ge 0$ put

$$F_Q(n) = \sum_{j\ge 1} \lfloor n/Q^j \rfloor = \frac{n - s_Q(n)}{Q-1},$$

where $s_Q(n)$ is the sum of the base-Q digits. Define an element of K by

$$H_K(a) = \frac{a!}{\prod_{p \text{ split}} p^{F_p(a)} \prod_{p \text{ inert}} p^{F_{p^2}(a)} (\sqrt{-q})^{F_q(a)}}. \tag{64.4}$$

Only primes at most a occur. The two choices of square root give the same principal ideal. We shall compute the image of a derivative map over a common coefficient field. Its domain consists of all integral scalar jets along the identity of the CM abelian scheme of Section 64.1.

Lemma 64.4 (A factorial bound for the formal exponential)**.** *Let $v_p(p) = 1$, let e be the ramification index of a local scalar field over $\mathbb{Q}_p$, let π be its uniformizer and let $Q = p^f$ be its residue cardinality. In a formal coordinate over the integers of a finite coefficient extension suppose that*

$$[\pi](T) = \pi T + \sum_{i \geq Q} b_i T^i.$$

For the formal exponential $E(Z) = \sum_{n \geq 1} c_n Z^n$ with $c_1 = 1$, one has $v_p(c_n) \geq -F_Q(n)/e$. For any integral scalar jet on a power of this group and any integral invariant tangent vector D,

$$v_p((D^a f)(0)) \;\geq\; v_p(a!) - F_Q(a)/e. \tag{64.5}$$

Proof. Normalize valuations temporarily by $v(\pi) = 1$. Use $[\pi](E(Z)) = E(\pi Z)$ as in Section 64.1. In the coefficient of E^i, group the selections by the multiplicities m_j of indices j, so $\sum m_j = i$, $\sum j m_j = n$. The denominator exponent before division by $\pi^n - \pi$ is at most

$$\sum_j m_j F_Q(j) - e v_p\Big(i! / \textstyle\prod_j m_j!\Big)$$

by induction. Always $F_Q(n) \geq \sum m_j F_Q(j)$ by superadditivity of the floors. We claim that this inequality is strict whenever $i \geq Q$ and the multinomial is a p-adic unit. Indeed the unit condition, by the digit formula for $v_p(i!)$, means that adding the m_j in base p produces no carries. If every $m_j < Q = p^f$, the sum with no carries has no digit in position f or higher. This contradicts $i \geq Q$. Thus some index $j \geq 1$ occurs at least Q times. Adding Q copies of that positive index in base Q produces a carry, and adding the remaining positive indices cannot undo the loss in digit sum. The digit formula for F_Q proves the strict inequality. If the multinomial is a nonunit it supplies at least one unit of the normalized valuation instead. In both cases there is room for division by $\pi^n - \pi$, of valuation one for $n > 1$. Every index on the right is smaller than n. This proves the coefficient bound by induction.

On a product use the parameterization $(E(u_1 Z), \dots, E(u_g Z))$ for the integral coordinates of D. Extract the coefficient of Z^a, multiply by $a!$, and apply superadditivity of F_Q to each product of coefficients. Returning to $v_p(p) = 1$ proves (64.5). □

Lemma 64.5 (The first term after rescaling)**.** *At a place above p the formal group of $\mathcal{A} = \mathcal{O}_{E_x} \otimes_{\mathcal{O}_K} C$ is a power of the elliptic formal group of C. Use the scalar completion of K determined by its tangent action, with index e and residue cardinality Q. There is an integral coordinate as in Lemma 64.4 with b_Q a unit. In an extension choose $\lambda^{Q-1} = \pi$, and put $H(Z) = \lambda^{-1} E(\lambda Z)$. This series is integral and its reduction has the form*

$$\overline{H}(Z) = \sum_{j \geq 0} h_j Z^{Q^j}, \qquad h_0 = 1, \quad h_j \neq 0 \quad (j \geq 0).$$

Proof. The product description at nonsplit places was proved in Section 64.1. At a split prime the continuous action extends to $\mathcal{O}_K \otimes \mathbb{Z}_p = \mathbb{Z}_p \times \mathbb{Z}_p$ by the same continuity argument. Over the

fraction field the logarithm identifies each idempotent with its linear action on the tangent line. One acts by one and the other by zero, and the identities persist integrally since the coefficient ring is torsion-free. The projective module $\mathcal{O}_{E_x}$ has rank $[E_x : K]$ at both factors and is free over the product of these local rings. A change of basis in the idempotent construction of Section 64.1 gives the claimed power also at split primes. The coordinate averaged over the Teichmüller units in the scalar completion gives the displayed form of $[\pi]$ at every prime.

It remains to verify its first nonlinear unit coefficient. An endomorphism of the good elliptic curve extends to the abelian scheme; the degree of a nonzero CM endomorphism with scalar α on every fiber is $|N_{K/\mathbb{Q}}\alpha|$. For example the degree is the degree of the pullback of the origin divisor. This line bundle has constant fiber degree in a smooth proper family, equal in characteristic zero to the lattice index. At an inert prime take $\pi = p$, of degree $p^2 = Q$. At the ramified prime take $\pi = \sqrt{-q}$, of degree $q = Q$. In both cases the reduction has zero linear coefficient. Its local degree at the origin is at most the total degree Q; it is the order of the pulled-back local parameter on the special fiber. Since degrees below Q have no nonzero reduced coefficient, b_Q is a unit.

At a split prime take $\pi = p$. For a positive class number multiple d, choose α generating the d-th power of the prime ideal of K opposite to the tangent place. It is a unit in the tangent completion, and $\alpha\bar{\alpha} = p^d$. The reduction of $[\alpha]$ is separable of degree p^d since its differential is nonzero. Thus the separable degree of $[p^d]$ is at least p^d. The separable degree of $[p]$ is at most p, since its differential is zero and its degree is p^2. By multiplicativity, the separable degree is exactly p. All points of the geometric kernel have the same local multiplicity by translation, which therefore equals p. The local expansion of $[p]$ has its first nonzero reduced term in degree $Q = p$, as required.

The bound on c_n gives $v_p(c_n\lambda^{n-1}) \geq 0$, since $F_Q(n) \leq (n-1)/(Q-1)$ for $n \geq 1$. Substitute $T = \lambda H(Z)$ in the exponential identity and divide by $\pi\lambda$. Modulo the maximal ideal the result is

$$Z = \overline{H} + \bar{b}_Q \overline{H}^{\,Q}.$$

On the left $H(\pi Z)/\pi$ reduces to Z; on the right every term of degree index $i > Q$ has a factor λ^{i-Q}. This equation determines a formal solution uniquely coefficient by coefficient. In characteristic p the displayed series is its solution with $h_j = -\bar{b}_Q h_{j-1}^{Q}$ for $j \geq 1$, so every h_j is nonzero. □

Theorem 64.6 (A global scalar jet with the minimum at every prime)**.** *Fix a sufficiently distant common interval. There is a single finite extension J for that interval such that for each of its fields $E = E_x$ one can fix one integral tangent vector D_E on $\mathcal{A}_E/\mathcal{O}_J$ with the following property. For every order $a = \lfloor x \exp(x^{\varepsilon}) \rfloor$ used on that field, the image of*

$$\{\textit{integral scalar jets to order } a \textit{ at the identity}\} \longrightarrow \mathcal{O}_J, \qquad f \longmapsto (D_E^a f)(0),$$

is exactly $H_K(a)\mathcal{O}_J$. Every integral invariant tangent vector has image contained in this ideal. In particular some single integral jet has derivative $H_K(a)$, simultaneously at every finite and infinite place.

Proof. Section 64.1 supplies an initial common field and abelian schemes. The closed infinitesimal neighborhood of order a of the identity has functions forming a finite locally free $\mathcal{O}_J$-module. Indeed its filtration by powers of the ideal of the identity has graded pieces the symmetric powers of the relative cotangent space, by smoothness. The derivative kills terms of degree above a upon evaluation at zero. It gives an integral linear map on this module and commutes with localization and extension of scalars. Locally the module is the truncated formal power series ring. The valuation of (64.4) over p is precisely the right-hand side of (64.5),

using $v_q(\sqrt{-q}) = 1/2$. These valuations are nonnegative. This proves the universal inclusion and integrality of the generator.

We prove that the bound can be attained locally with a choice of tangent vector. Write $a = \sum a_j Q^j$ with $0 \le a_j < Q$, and set $k = \sum a_j$. Use one distinct factor of the formal group for each nonzero digit. There are enough factors since the rank $g = [E_x : K]$ is at least the degree $2^l \ge x^{2+8\varepsilon}$ of its totally real cyclotomic layer, whereas $1 + \log_2 a = O(x^{\varepsilon} + \log x)$. Use the monomial $\prod_j T_j^{a_j}$ in these coordinates and tangent components u_j. The coefficient of Z^a after pullback is λ^{k-a} times the coefficient of Z^a in $\prod_j H(u_j Z)^{a_j}$. The latter reduces to a homogeneous polynomial of degree a in the components. It is nonzero. Indeed the coefficient of $\prod_j u_j^{a_j Q^j}$ is $\prod_j h_j^{a_j}$: the only way to express $a_j Q^j$ as a sum of precisely a_j powers of Q is to use a_j copies of Q^j. Any carry would lower the digit sum below a_j. At a point where this polynomial is nonzero, the derivative valuation is therefore

$$v_p(a!) + (k - a)v_p(\lambda) = v_p(a!) - F_Q(a)/e.$$

The reduction calculation uses a root λ to detect units; the coefficients h_j lie in the residue field of the original local model by their recurrence. The jet and its tangent vector can be taken in the original formal coordinates after a finite residue extension.

We next make the same tangent vector work globally and at all the orders for each field. Each bounded interval uses finitely many fields and integer orders. Let A be the largest order and fix one of the fields E. Its integral tangent module M is projective of rank $g \ge 2$ over the ring of integers of the initial coefficient field. The structure theorem for projective modules over a Dedekind domain writes it as a sum of $g - 1$ free lines and an invertible ideal. Choose a surjective linear form $L : M \to \mathcal{O}_J$ on one free line and a vector v_0 with $L(v_0) = 1$. At each place above $p \le A$, take the product of the preceding nonzero homogeneous polynomials for the relevant orders. They may be written in the same coordinates on the residue tangent space. Their product times the reduction of L remains a nonzero polynomial. It has a nonvanishing value over a finite extension of the residue field. Scale the resulting vector by a nonzero scalar so that $L = 1$; homogeneity preserves every nonvanishing condition.

All needed finite residue extensions can be included at once in a finite extension of the coefficient field. For each rational $p \le A$ one may adjoin the roots of unity of order $p^b - 1$ with b a common multiple of the finitely many required residue degrees over $\mathbf{F}_p$. At every place above p these roots reduce distinctly and supply $\mathbf{F}_{p^b}$. Take the compositum for all the primes and fields. Over the resulting J, choose the residue directions at every place above $p \le A$; under further extension the local polynomial nonvanishings persist. Subtract v_0 from the chosen directions and apply the Chinese remainder theorem to the projective module $\ker L$. Adding v_0 back gives a global vector D_E with $L(D_E) = 1$ meeting all the prescribed reductions.

For each order and each $p \le A$, the corresponding local monomial now attains equality. Computing in a completion is sufficient, since the image ideal of a linear map of finite modules commutes with flat base change to a completed discrete valuation ring. For $p > A$, the reduction of D_E is also nonzero because $L(D_E) = 1$. A local parameter with unit derivative in that direction, raised to the a-th power, has derivative $a!$ times a unit. It is a unit there since $p > a$. The two ideals thus have identical valuation at every prime of J. They are equal. The image is the image of a linear map on the global module over the affine base $\operatorname{Spec} \mathcal{O}_J$, so its generator itself is attained by a global jet. This proves the assertion for each field over the same J. □

In particular the set of derivatives for the chosen vector, after division by $H_K(a)$, is the whole coefficient ring, and the value one occurs. This computes the full common divisor of scalar jets. The theta periods in Section 121.15 are specified by a kernel, a projection and an

integral. A comparison for those prescribed values must retain restrictions on the jet or on the map to the period.

64.3 Realizing the derivative by global theta sections

We now impose that a scalar jet be the expansion of a global algebraic theta section on the CM abelian scheme. We specify its line bundle, its order, its frame at the identity and its behavior under inversion.

Lemma 64.7 (Jets from a very ample linear system)**.** *Let R be a Dedekind domain, let X/R be smooth and projective with section e, and let L be an invertible sheaf together with an identification $e^{*}L = R$. Suppose a finite projective module V of sections defines a closed immersion $X \hookrightarrow \mathbf{P}_{R}(V)$ with tautological bundle L, using the convention that a point is a rank-one quotient. There exists $s_{0} \in V$ with $s_{0}(e) = 1$. For every $a \geq 1$, all integral scalar jets of order a at e are expansions of s/s_{0}^{a} for sections $s \in H^{0}(X, L^{\otimes a})$. One may use the sections generated by degree-a products from V.*

Proof. Evaluation at e is a surjection $V \to R$, so choose s_{0} above one and put $V_{0} = \ker(V \to R)$. This splits $V = Rs_{0} \oplus V_{0}$. The open set where s_{0} is invertible contains the whole section e. In the corresponding affine chart of the projective bundle, its coordinate algebra is $\operatorname{Sym}_{R} V_{0}$; the linear coordinate belonging to $s \in V_{0}$ restricts on X to s/s_{0}. The ideal of the origin in this chart is the positive-degree ideal. Since X is closed in the chart and contains the origin section, these linear coordinates generate the ideal of e in the induced affine open of X. Its order-a neighborhood is contained in the chart because it has the same underlying space as e. Every element of its coordinate algebra is consequently represented by a polynomial of degree at most a: all monomials of strictly larger degree vanish modulo the $(a+1)$-st power of the ideal. A monomial of degree $j \leq a$ homogenizes to the product of its j sections and $a-j$ copies of s_{0}. Adding these products gives the asserted global section over R. □

Theorem 64.8 (Theta sections attaining the minimum)**.** *On the common fields and intervals of Theorem 64.6, give each CM abelian scheme $\mathcal{A}_{E}$ any relatively ample symmetric rigidified theta line bundle P over the coefficient ring. There exists a frame s_{0}, supplied by a global section of P^{3} which equals one at the identity, such that for the vector D_{E} from that theorem and every required order a,*

$$\left\{ D_{E}^{a}(s/s_{0}^{a})(0) : s \in H^{0}(\mathcal{A}_{E}, P^{3a}) \right\} = H_{K}(a)\mathcal{O}_{J}. \tag{64.6}$$

A product principal polarization P exists over the common field used there. With that choice the positive theta bundle P^{3a} has type $(3a, \ldots, 3a)$ at every complex embedding. In particular the smallest nonzero normalized log norm is the quantity computed in Theorem 6.18. It is attained by one global theta section in the indicated frame.

Proof. On an abelian variety over a field the cube of an ample line bundle is very ample, by the classical very ampleness theorem for abelian varieties. This theorem holds also in positive characteristic. We recall why these fiberwise embeddings give a relative linear system over the entire coefficient ring. For a symmetric ample line bundle L on a geometric fiber and an integer N prime to its characteristic, multiplication by N is finite étale of degree N^{2g}. Pullback on $H^{i}(L)$ is split injective by the trace divided by this degree. By the theorem of the cube $[N]^{*}L \simeq L^{N^{2}}$. Serre vanishing for large such N gives $H^{i}(L) = 0$ for $i > 0$. Apply this to $L = P^{3}$ on every fiber. The Euler characteristic is locally constant in this proper flat family, so $h^{0}(L)$ is constant. Cohomology and base change for the projective abelian scheme gives $V = H^{0}(\mathcal{A}_{E}, P^{3})$ finite projective with its sections spanning the complete system on every

fiber. Evaluation is surjective by Nakayama's lemma. The morphism to the projective bundle is a closed immersion: it is proper with finite geometric fibers, hence finite, and the cokernel of the finite algebra map from the structure sheaf of the projective bundle vanishes on every fiber by the fieldwise closed immersion. Nakayama gives surjectivity. These classical results on linear systems of abelian varieties are given in [3].

Apply Lemma 64.7 to $L = P^3$, rigidified using P. The full domain of the derivative map in Theorem 64.6 is in the image of the global theta sections. The integral inclusion and attainment of the generator from that theorem prove (64.6) for the same vector at every order. A nonzero integral multiple of the generator has norm at least that of the generator, proving the norm assertion.

For the asserted principal polarization we can construct the bundle directly. As a projective module over the Dedekind domain $\mathcal{O}_K$, $\mathcal{O}_E$ is isomorphic to $\mathcal{O}_K^{g-1} \oplus I$ for an invertible ideal I. The construction by idempotents in Section 64.1 respects direct sums and isomorphisms. It identifies $\mathcal{A}_E$ with $C^{g-1} \times C_I$ where $C_I = I \otimes_{\mathcal{O}_K} C$ is an abelian scheme of relative dimension one. Indeed it is a direct factor of a power of C, and its generic tangent space has dimension one. The factors are thus elliptic schemes. On each use the line bundle of its origin, tensoring by a bundle from the base to rigidify it. It is symmetric and induces the principal polarization on each fiber. Their exterior product gives P; its $3a$-th power has the stated type. This product choice uses an $\mathcal{O}_K$-module decomposition of $\mathcal{O}_E$. The equality (64.6) also applies to a different integral polarization prescribed in advance whenever it satisfies the hypotheses. □

There is a direct analytic description of the last construction. At any complex embedding write each elliptic factor as $\mathbb{C}/(\mathbb{Z} + \tau_j\mathbb{Z})$ with $\operatorname{Im}\tau_j > 0$. The odd Jacobi theta function $\vartheta_1(\pi z_j, \tau_j)$ vanishes simply at the lattice and has no other zeros. Its multipliers for $z_j \mapsto z_j + 1$ and $z_j \mapsto z_j + \tau_j$ are -1 and $-\exp(-\pi i\tau_j - 2\pi i z_j)$, respectively. These identities identify the associated bundle with the bundle of the origin. Therefore a section of P^{3a} lifts to a holomorphic function on $\mathbb{C}^g$ with these multipliers raised to the power $3a$ in coordinate j. This is the usual theta transformation law for the product polarization. The ratios in (64.6) are computed in the common frame fixed once over J. Changing that frame can change a higher derivative when lower derivatives are present. [4]

Corollary 64.9 (Theta sections of prescribed parity)**.** *Write $\iota = [-1]$ and let $s_* = s_0\,\iota^* s_0$ in P^6, using the symmetry fixing the rigidification at zero. Use the frame s_*^a for P^{6a}. For global theta sections of parity $(-1)^a$, the image ideal of the order-a derivative is between $2H_K(a)\mathcal{O}_J$ and $H_K(a)\mathcal{O}_J$, inclusive. Consequently it is the full scalar derivative ideal at every place of odd residue characteristic. There is one global section of that parity with derivative exactly $2H_K(a)$.*

Proof. Rigidified symmetry is an involution: its square is an automorphism of the line bundle, hence a scalar from the base since the fibers are proper and geometrically connected, and that scalar is one at the identity. Thus s_* is invariant and has value one. Given the section s with derivative $H_K(a)$ from Theorem 64.8, put $t = s(\iota^* s_0)^a$. Then $t/s_*^a = s/s_0^a$ at the identity. The integral section $t + (-1)^a \iota^* t$ has the stated parity. Inversion acts by -1 on the tangent space and sends the formal one-parameter subgroup for D_E to that for $-D_E$. It therefore multiplies the a-th derivative at zero by $(-1)^a$ in the invariant frame. The derivative of the sum is $2H_K(a)$. The universal divisibility proved in Theorem 64.6 gives the other inclusion. □

The theta sections constructed here have an integral line bundle and a prescribed derivative at every place in one frame. Their coefficients and the frame can depend on the field. The Bessel periods of Section 121.15 are obtained from specified Weil kernels, choices of splittings,

common test vectors and a projection. Comparing those periods to sections subject to these restrictions requires further input; the minimum over all global theta sections alone is given by (64.6).

64.4 The trace polarization and integral Fourier components

Fix a common interval $I = [V, V^{3/2}]$, and take the fields $E = E_x$ of Volume I. Let $K = \mathbb{Q}(\sqrt{-d})$ with $\sqrt{-d} \mapsto i\sqrt{d}$. The source uses the inverse of one factor of the relative different and a purely imaginary scalar to define its CM lattice. We construct this polarization on the same fields. We then compute the denominators of translations in a linear system pulled back by a split CM isogeny. The ideal and scalar occur in `Formalism/LocalRingCardinality/DataHost.lean`, line 149.

Theorem 64.10 (A principally polarized CM lattice over the interval)**.** *Let $\mathfrak{c}$ be a nonzero integral ideal of K and $u = N_{K/\mathbb{Q}}\mathfrak{c}$, the absolute ideal norm. On each E one can choose an integral ideal $\mathfrak{b}$, stable under $\mathrm{Gal}(E/K)$, with $\mathfrak{b}\overline{\mathfrak{b}} = \mathfrak{D}_{E/K}$ and $\mathfrak{b} + \overline{\mathfrak{b}} = \mathcal{O}_E$. Set*

$$M = \mathfrak{c}\mathcal{O}_E\,\mathfrak{b}^{-1}, \qquad \xi = -1/(u\sqrt{-d}), \qquad e(x,y) = \mathrm{Tr}_{E/\mathbb{Q}}(\xi x \bar{y}).$$

The form e gives a principal polarization on the complex torus of M with CM embeddings extending the chosen embedding of K. Its Rosati involution restricts to conjugation on E. For one choice of $\mathfrak{c}$ per field all the resulting tori and polarizations have abelian scheme models and relatively ample symmetric rigidified line bundles over the integers of one number field J on I.

Proof. Outside primes dividing $2Fqd$, the field E is unramified over $\mathbb{Q}$, where F is the conductor of ψ. At d, the extension obtained by adjoining $K_\psi, C_l, \sqrt{-q}$ to $\mathbb{Q}$ is unramified. Base change of its local unramified algebras to K_d (here the completion at d) is unramified. Every remaining rational prime in the support of the relative different splits in K. Indeed $-d \equiv 1 \bmod 8$, and $-d \equiv 1 \bmod p$ for $p = q$ and for every odd $p \mid F$ on sufficiently distant intervals. For each such split p, choose one of its two primes in K and put into $\mathfrak{b}$ the full part of $\mathfrak{D}_{E/K}$ over that prime. Conjugation exchanges the two parts and $\mathrm{Gal}(E/K)$ preserves each. This proves all the assertions about $\mathfrak{b}$.

Transitivity of the different and the quadratic discriminant give $\mathfrak{D}_{E/\mathbb{Q}} = \mathfrak{D}_{E/K}(\sqrt{-d})$. Also $\mathfrak{c}\bar{\mathfrak{c}} = (u)$, hence $\xi M\overline{M} = \mathfrak{D}_{E/\mathbb{Q}}^{-1}$. By the defining trace-duality property of the inverse different, $\{x \in E : e(x, M) \subset \mathbb{Z}\} = M$. The trace form is alternating since $\bar{\xi} = -\xi$. In the coordinates of the CM type the real extension of e satisfies

$$e(v, iv) = \frac{2}{u\sqrt{d}} \sum_{\tau \mid K} |v_\tau|^2 > 0 \quad (v \neq 0), \qquad e(iv, iw) = e(v, w).$$

The Riemann bilinear relations consequently give a polarization, which is principal by trace duality. The identity $e(ax, y) = e(x, \bar{a}y)$ gives the asserted involution. [1]

Choose the elliptic scheme C_d after finite extension as in Section 64.1, with the complex uniformization $\mathbb{C}/\mathcal{O}_K$. The finite projective $\mathcal{O}_K$-module M gives the abelian scheme $\mathcal{A} = M \otimes_{\mathcal{O}_K} C_d$. Its complex lattice and tangent action are exactly those above. The complex polarizing homomorphism is defined over a number field. For example, after isogenies the source and target are powers of C_d, and their rational homomorphisms are matrices in K; homomorphisms descend under algebraically closed extension in characteristic zero. A line bundle representing the polarization can be chosen over $\overline{\mathbb{Q}}$ in the corresponding component of the Picard scheme. It can be made symmetric by twisting with a degree-zero bundle, since multiplication by two on the dual is surjective. These finite data descend after a finite extension.

Extend a divisor of this bundle by closure on the regular abelian scheme over the integer ring, and rigidify the resulting bundle P along the identity. A line bundle trivial on the generic fiber is represented by a vertical divisor. All fibers are smooth and geometrically integral, so such divisors are pulled back from the base. Rigidification thus gives the symmetry on the integral model. To see ampleness on every fiber, diagonalize the positive definite K-Hermitian form $u^{-1}\operatorname{Tr}_{E/K}(x\bar{y})$ by orthogonalization. Its diagonal entries are positive rational numbers. After clearing denominators in the coordinate maps, for some positive integer D there are independent maps $\ell_i : M \to \mathcal{O}_K$ and positive integers c_i with

$$Du^{-1}\operatorname{Tr}_{E/K}(x\bar{y}) = \sum_i c_i \ell_i(x)\overline{\ell_i(y)}.$$

The map $\ell = (\ell_i)$ induces an isogeny to a power of C_d on every fiber: a positive integer multiple of its inverse on the rational lattices maps the integral lattices back. Thus its kernel is contained in the torsion of that integer and its image has full dimension. Pull back the product of the elliptic origin bundles with exponents c_i. Its polarization homomorphism agrees with that of P^D on the generic fiber by the displayed equality and the elliptic trace form $-1/\sqrt{-d}$. Equality extends over the base by separatedness. Fiberwise their quotient is algebraically trivial, so P^D is ample on every fiber. The fiberwise criterion for relative ampleness now applies. Taking a compositum works for all the finitely many fields on I. □

Lemma 64.11 (Two principal split primes of controlled size)**.** *For $T \geq \max(d, 3)$ there exist primes $T < g_1 < g_2$ and $\pi_i \in \mathcal{O}_K$ with $\pi_i\bar{\pi}_i = g_i$, $(\pi_i) + (\bar{\pi}_i) = \mathcal{O}_K$, and $\log(g_1 g_2) \ll \log(2T)$ with an absolute implied constant. On I both primes can be fixed above every integer order $\lceil xe^{x^{\varepsilon}} \rceil$, all rational primes ramified in any E_x, and all the dimensions $2(2n)(r + t_{\mathrm{r}}) + 1$ from Section 92.1. Then $\log(g_1 g_2) \ll_{\psi,\varepsilon} x^{3\varepsilon/2} + \log(2x)$ for every $x \in I$.*

Proof. Let $\omega = (1 + \sqrt{-d})/2$, and take $c = 2\lceil \sqrt{T/d} \rceil + 2$. The binary integral form

$$N_{K/\mathbb{Q}}(u + cv\omega) = (u + cv/2)^2 + dc^2v^2/4$$

is primitive, positive definite, and has discriminant $-dc^2$. Thorner and Zaman's unconditional theorem gives a prime represented by it of size at most an absolute constant times $(dc^2)^{694}$. In any such representation $v \neq 0$ since a square cannot be prime. Hence $g \geq dc^2/4 > T$, while $dc^2 \ll T$. The representing element has norm g; as $g > d$ it is unramified and its two conjugate prime ideals are distinct. Apply this argument first at T and then at g_1. [5, Thm. 1.2]

For the interval take T larger by one than the largest bound specified in the statement. The ranks are polynomial in V, the largest order has logarithm $O(V^{3\varepsilon/2} + \log(2V))$, and the quadratic prime selection gives $\log(qd) \ll_{\psi,\varepsilon} V^{\varepsilon/5}(\log(2V))^2$. The remaining ramified primes divide $2F$. Since $x \geq V$, this gives the required bound at every point on the interval. □

Theorem 64.12 (Integral Fourier components of split CM translations)**.** *For one of these primes write $g = \pi\bar{\pi}$. Take a product $\mathcal{V}$ of copies of $\mathcal{A}$ with the indicated $\mathcal{O}_K$-action on some factors and the conjugate action on the others. Let G_+, G_- be the sums of their dimensions and $G = G_+ + G_-$. Write $f = [\pi]$, $h = [\bar{\pi}]$, $B = \ker f$. After a common finite extension all generic g-torsion points and roots of unity of order g are defined. For any relatively ample integral bundle P_0 on $\mathcal{V}$, consider global sections of $f^*P_0^N$. Translations by B act using $f \circ t_z = f$.*

At a place $w \mid g$ normalize $v_w(g) = 1$, and let G_{et} be G_+ if π is a unit at w, and G_- otherwise. For every character λ of $B(J)$, the Fourier projector

$$e_\lambda = g^{-G} \sum_{z \in B(J)} \lambda(z)^{-1} t_z^*$$

preserves the integral lattice of sections after multiplication by $g^{G_{\mathrm{et}}}$. The same bound holds for $\sum_\lambda u_\lambda e_\lambda$ for any w-integral u_λ. On the full lattice of sections, the denominator for each single projector is sharp for all sufficiently large N. Away from g all these single projectors preserve the integral lattice.

Proof. On a single factor the kernel of $[\pi]$ has generic order $g^{\dim \mathcal{A}}$ by its index on M. It is killed by g; both $[\pi]$ and its conjugate are isogenies of abelian schemes, since their composite is $[g]$ and they have finite kernels and full image on every fiber. When the tangent scalar is a unit the isogeny is étale at the identity and hence everywhere by translation. At the other places over g, its dual is étale because the Rosati involution from Theorem 64.10 exchanges $\pi, \bar\pi$. The kernel of the dual isogeny is the Cartier dual of the original kernel. The same argument applies with the two roles exchanged on a factor with conjugate action. [6]

Over the completed integer ring R_w, the finite étale kernel factors and the finite étale dual factors are constant since all their generic geometric points are rational. Indeed each point extends by properness and the closures are disjoint sections of a finite étale scheme over a normal local domain with split generic algebra. Thus $B = B_{\mathrm{et}} \times B_{\mathrm{mult}}$, where B_{et} is constant of order $g^{G_{\mathrm{et}}}$, and B_{mult} is the diagonalizable group of the character group $\Gamma \simeq (\mathbb{Z}/g)^{G - G_{\mathrm{et}}}$.

The identity $f \circ t = f$ on $B \times \mathcal{V}$ linearizes $f^* P_0^N$ integrally; the group law gives the compatibility of successive translations. For the diagonalizable factor, write a section's coaction as $\sum_{\gamma \in \Gamma} s_\gamma \otimes X^\gamma$ in the group algebra $R_w[\Gamma]$. Coassociativity and the counit give respectively that s_γ has weight γ and that $\sum s_\gamma = s$. Each s_γ is integral since X^γ is an integral basis. On the generic fiber this decomposition equals ordinary finite Fourier projection by character orthogonality. The remaining projection averages over the constant group of order $g^{G_{\mathrm{et}}}$ with coefficients roots of unity. This proves the claimed exponent, the bound for linear combinations, and integrality away from g.

For sharpness restrict to the finite flat fiber $B = f^{-1}(0)$, where the pullback bundle has one frame from the origin. Its functions are $\mathrm{Map}(B_{\mathrm{et}}(J), R_w) \otimes R_w[\Gamma]$. For the given λ take the point mass at the identity of the first factor times the corresponding weight character of the second. Its projected value at the identity is $1/g^{G_{\mathrm{et}}}$. For N sufficiently large this finite-fiber section extends to a global section over R_w. In fact f^*P_0 is relatively ample, and relative Serre vanishing for the ideal sheaf of B tensored with $(f^*P_0)^N$ gives the surjectivity of restriction over the affine base. It follows that the denominator cannot be decreased on that lattice. On the bounded interval all fields and g_i used here form finite lists, so a common finite coefficient extension suffices. □

Corollary 64.13 (Pullback of the projected integral jet)**.** *Use a frame of P_0^N near the origin and the frames it induces under f and fh. Let D be a product of integral invariant derivations in the two groups of factors, of orders a_+, a_-. Write J_D for evaluation of the resulting scalar derivative at zero and e'_λ for the B-projector on $(fh)^*P_0^N$. For integral $s \in H^0(\mathcal{V}, f^*P_0^N)$ one has*

$$J_D(e'_\lambda h^* s) = \bar\pi^{\,a_+} \pi^{a_-} J_D(e_{\lambda \circ h^{-1}} s).$$

Here h^{-1} in the character denotes the inverse on $B(J)$. Consequently at $w \mid g$,

$$v_w\big(J_D(e'_\lambda h^* s)\big) \ge a_+ v_w(\bar\pi) + a_- v_w(\pi) - G_{\mathrm{et}}.$$

For $r(r + t_{\mathrm{r}})$ copies and total dimension $G = 2n\, r(r + t_{\mathrm{r}})$, the logarithm of the full worst-case denominator at the two primes is bounded by $G \log(g_1 g_2) = o(b/x)$, uniformly at every x on I.

Proof. Since $(\pi, \bar\pi) = 1$, a Bézout identity in $\mathcal{O}_K$ gives an inverse to h on B. For every $z \in B(J)$ one has $t_z^* h^* = h^* t_{h(z)}^*$ with the canonical pullback actions and frames. Reindexing the Fourier

average gives $e'_\lambda h^* = h^* e_{\lambda\circ h^{-1}}$. Differentiating $h \circ t_v = t_{h(v)} \circ h$ at the identity gives the chain rule for an invariant direction everywhere. Its scalar is $\bar\pi$ on the first factors and π on the conjugate factors. Iterating yields the formula with no lower-order term because the frame is pulled back as well. Integral invariant derivations preserve integral functions, so Theorem 64.12 gives the valuation bound. Finally $G = O(n^3)$ by the rank choice, and Lemma 64.11 bounds the logarithms by a fixed power of x. This proves the asymptotic claim. □

The dimension in the corollary gives exactly the group order g^{frn_V} specified in `Formalism/SharpRestriction/Divisibility/CanonicalTranslateJets.lean`, line 84, where $f = 2n$ and $n_V = r+t_{\mathrm{r}}$. Lines 176–188 and 198–210 of that file specify further identities between translated sections, automorphic evaluations and jets in matched frames. The theorem gives the integral Fourier and isogeny calculation for the explicit polarized CM lattice. Identifying an individual restricted automorphic lift with one of these sections, with the same integral frame and a bound for its projected global norm, remains open in this manuscript.

64.5 Frobenius and mixed derivatives in CM eigendirections

The minimum for a single scalar derivative in Section 64.2 depends on the quadratic splitting type of the prime. For mixed derivatives the individual CM embeddings can affect the answer. We work on the principally polarized abelian scheme of Theorem 64.10, with $\mathfrak{c} = \mathcal{O}_K$, $K = \mathbb{Q}(\sqrt{-d})$, and with the fields of Proposition 6.28. Fix a rational prime p inert in K and unramified in E. Let R be a completed integer ring of a common coefficient field containing E, with good reduction as above. Normalize $v_p(p) = 1$. Write $Q = p^2$, $\Sigma = \mathrm{Hom}_K(E, J)$, and $\sigma\tau = \tau \circ \mathrm{Frob}_p^2$ for $\tau \in \Sigma$, with arithmetic Frobenius in $\mathrm{Gal}(E/\mathbb{Q})$. For nonnegative integers a_τ put

$$A = \sum_\tau a_\tau, \qquad B_p(\boldsymbol{a}) = \sum_\tau \bigl(v_p(a_\tau!) - F_Q(a_\tau)\bigr).$$

In $a_\tau = \sum_{j\ge 0}(l_{\tau j} + p h_{\tau j})Q^j$, both $l_{\tau j}$ and $h_{\tau j}$ are between zero and $p-1$. Define

$$L_\nu = \sum_{j\ge 0} l_{\sigma^{-j}\nu, j}, \qquad H_\nu = \sum_{j\ge 0} h_{\sigma^{-j}\nu, j} \qquad (\nu \in \Sigma).$$

Theorem 64.14 (An orbit-dependent divisibility bound)**.** *Let D_τ be invariant derivations generating the integral tangent eigenlines of $\mathcal{O}_E$ at p. For every integral scalar jet f through order A at the identity,*

$$v_p\left(\left(\prod_\tau D_\tau^{a_\tau} f\right)(0)\right) \;\ge\; B_p(\boldsymbol{a}) + \sum_{\nu\in\Sigma} \lfloor L_\nu/p \rfloor. \tag{64.7}$$

If $L_\nu < p$ and $H_\nu < p$ for every ν, some integral jet attains exactly $B_p(\boldsymbol{a})$. In the frame of Theorem 64.8, this minimum is attained by a global section of P^{3A} at the chosen place, for $A \ge 1$.

Proof. Locally the CM ideal M is free of rank one over the semilocal algebra $\mathcal{O}_E \otimes_{\mathcal{O}_K} \mathcal{O}_{K,p}$, which is finite étale over $\mathcal{O}_{K,p}$. Choose its generator and a basis of this algebra over $\mathcal{O}_{K,p}$. The formal group is then a power of the elliptic formal group used in Section 64.2. After base change to R the primitive idempotents of the étale algebra give tangent vectors v_τ, the columns of an invertible matrix V. These are integral generators of the tangent eigenlines in the product coordinates of the elliptic group. Their entries lie in an unramified extension of $\mathcal{O}_{K,p}$, since they are the columns of the inverse of the evaluation matrix of the chosen algebra basis. In particular,

$$v_\tau^{[Q^j]} \equiv v_{\sigma^j\tau} \pmod p, \tag{64.8}$$

where brackets raise each coordinate to that power. To see this, the row at μ of the evaluation matrix times v_τ is $\mathbf{1}_{\mu=\tau}$. Raising this equality to Q on the residue field replaces row μ by row $\sigma\mu$, and the matrix remains invertible there. The congruence holds modulo p in the unramified coefficient ring, hence also in pR if R itself is ramified. Iteration proves (64.8). We may prove the result using these generators, since rescaling any one by a unit only rescales the final derivative by a unit.

Let $\mathcal{E}(Z) = \sum_{s\ge1} c_s Z^s$, $c_1 = 1$, be the formal exponential in the elliptic coordinate of Lemma 64.5. The normalized invariant operators

$$T_{\tau,b} = \frac{p^{F_Q(b)}}{b!} D_\tau^b$$

preserve integral formal functions. At the identity this follows by extracting the coefficient of degree b after substituting $\mathcal{E}(v_{i\tau}Z)$ for the i-th coordinate and using Lemma 64.4. For the operator statement apply the same extraction to $f(X +_{\mathcal{A}} Y)$ in Y, with the coefficients now in $R[[X]]$. Translation invariance identifies the result with $T_{\tau,b}f(X)$.

For $b = Q^j$, every positive splitting $b = s_1 + \cdots + s_k$ with $k \ge 2$ satisfies $F_Q(b) > \sum_i F_Q(s_i)$. Indeed the base-Q digit sum of b is one and the sum of the digit sums on the right is at least two. Their difference is a positive multiple of $Q-1$. Thus, after multiplying by $p^{F_Q(b)}$, each contribution from a monomial of degree at least two is divisible by p. The linear term contributes $u_j v_\tau^{[Q^j]}$ with $u_j = p^{F_Q(Q^j)} c_{Q^j} \in R^\times$, a unit by Lemma 64.5 and $F_Q(Q^j) = (Q^j - 1)/(Q-1)$. Using (64.8) and translating once more gives a congruence of operators on integral formal functions,

$$T_{\tau,Q^j} \equiv u_j D_{\sigma^j\tau} \pmod p. \tag{64.9}$$

Factor T_{τ,a_τ} as a unit times the product of $l_{\tau j}$ copies of T_{τ,Q^j} and $h_{\tau j}$ copies of T_{τ,pQ^j} at each j. The exponents F_Q add exactly by the digit formula. The remaining factor is a unit because the multinomial coefficient that combines these base-p digits has valuation zero, by Legendre's formula for factorials. After this factorization, group the first kind of operator according to $\nu = \sigma^j\tau$. Any p in a group have product congruent modulo p to a unit times D_ν^p by (64.9). Since $p < Q$, the integral operator $T_{\nu,p}$ equals $D_\nu^p/p!$. Thus each such product sends integral functions into $pR[[X]]$. These constant multiples of invariant derivatives commute. After dividing each disjoint group of p operators by p, their composition and all unused factors still preserve integral functions. Restoring the factorials proves (64.7).

For attainment, use the integral linear coordinates T'_ν obtained from the elliptic parameters T_i by V^{-1}. Let $d_{\tau j} = l_{\tau j} + p h_{\tau j}$, $k_\nu = \sum_j d_{\sigma^{-j}\nu,j}$, and $k = \sum_\nu k_\nu$. Test the jet of the monomial $\prod_\nu (T'_\nu)^{k_\nu}$. Introduce independent variables Z_τ in the tangent space and adjoin temporarily $\lambda^{Q-1} = p$. The reduction of $\lambda^{-1}\mathcal{E}(\lambda Z)$ is $\sum_{j\ge0} h_j Z^{Q^j}$ with every $h_j \ne 0$, by Lemma 64.5. After inserting $\lambda \sum_\tau v_{i\tau} Z_\tau$ in coordinate i and applying V^{-1}, the reduction of the resulting T'_ν/λ is

$$\sum_{j\ge0} h_j Z_{\sigma^{-j}\nu}^{Q^j}.$$

To obtain $\prod Z_\tau^{a_\tau}$ from the k linear-coordinate factors after this substitution, exactly $d_{\tau j}$ choices of $Z_\tau^{Q^j}$ must occur. Indeed the least number of powers of Q summing to a_τ is its base-Q digit sum. The sum of these minima is already k, so no carries in base Q are possible. The indicated coefficient is the product of nonzero powers of h_j times the multinomials at each ν for the groups of sizes $d_{\sigma^{-j}\nu,j}$. The assumptions $L_\nu, H_\nu < p$ say exactly that addition within these

groups has no base-p carry. Every multinomial is therefore a unit. Undoing the rescaling and multiplying by $\prod_\tau a_\tau!$ gives valuation $\sum_\tau v_p(a_\tau!) + (k-A)/(Q-1) = B_p(\boldsymbol{a})$.

The bundle P of Theorem 64.10 is relatively ample, symmetric and rigidified. The argument of Theorem 64.8 therefore gives a relatively very ample P^3 and an integral section s_0 of P^3 with value one at the origin on this K-scheme. Lemma 64.7 gives a surjection from the degree-A products of its global sections onto the integral jets in the frame s_0^A. Its base change to R is also onto. If every global section had valuation strictly greater than this minimum then so would the whole image of their R-span, contrary to the monomial just constructed. This proves the last assertion. □

Corollary 64.15 (Two mixed derivatives of the order in the prime count)**.** *At every sufficiently large x in the common intervals there is an unramified prime p, split in $K_q = \mathbb{Q}(\sqrt{-q})$ and inert in K, and there are two lists of exponents on the same polarized scheme with the same multiset of entries and total order $A = \lceil x e^{x^{\varepsilon}} \rceil$, with the following property. At the chosen place over p, for the first list some global theta section of P^{3A} has derivative valuation B_p. For the second list every integral section has derivative valuation at least $B_p + 1$. Here B_p has the same value for both lists, and the tangent directions and frame are fixed for the comparison.*

Proof. In the Galois coordinates (i, j, z) of Volume I choose $g = (0, 1, z)$ with z of order four in A_0. This exists at large x since the cyclic order $|A_0|$ tends to infinity. The restriction map from the units modulo $N = \operatorname{lcm}(F, 2^{l'+2})qd$ to $\operatorname{Gal}(E/\mathbb{Q})$ is onto. Use Linnik's theorem in any preimage residue class to take a prime $p \ll N^C$ with Frobenius g. It is unramified in E and has the stated two signs. Since $\log N = o(x^{\varepsilon})$ uniformly, $p^2 + p - 1 < A$ for large x. The permutation $\sigma = g^2$ on Σ consists of disjoint pairs, since it is a nonidentity translation of order two on the torsor of embeddings over K. [5, Thm. 1.1]

Fix an embedding ν for the exponent $p - 1$. For the first list give the exponent p^2 to an embedding in a different σ-orbit. For the second move only this exponent to $\sigma^{-1}\nu$. To complete both lists write

$$A - (p^2 + p - 1) = \sum_{j \ge 0} c_j Q^j, \quad 0 \le c_j < Q.$$

For each nonzero c_j, give the exponent $c_j Q^j$ to an embedding in a fresh orbit, identical for the two lists. At most $1 + \log_2 A$ such orbits are needed and there are $|\Sigma|/2 = n \gg 1 + \log_2 A$. Give every other embedding exponent zero. In the first list no two contributions from different embeddings reach the same ν' in the digit sums of the theorem. There is no carry in either kind of digit, hence the minimum is attained. In the second list the $p - 1$ low digits at ν and the one low digit from the p^2-term now give $L_\nu = p$. Apply (64.7). The list of exponents has only been permuted, which leaves B_p unchanged. □

This comparison detects an individual Frobenius action in the divisibility of genuine global theta derivatives at the required total order. The two multidegrees in the corollary are chosen to exhibit that action. To apply it to the automorphic periods one must determine the multidegrees of their prescribed harmonic coefficients, control the sum over the period classes in the same integral frame and bound the projected global norms. Section 6.6 still requires these estimates and the remaining odd-primary cohomology bound.

64.6 Reduction of polynomial differential operators at an inert prime

The polynomials occurring in a theta evaluation can have several monomials with the same total order. To decide whether a power of a prime divides every value, one must also detect

cancellations among these monomials. We compute the algebra of the normalized invariant differential operators modulo the maximal ideal. Its multiplication keeps track of the permutation of the CM embeddings by Frobenius.

Use the scheme and prime p of Section 64.5. More generally, we allow any finite product of copies of that scheme. In this case Σ is the disjoint union of the sets of tangent eigendirections of the factors. A factor with conjugate CM action has its embeddings relabeled by complex conjugation, which commutes with $\sigma = \mathrm{Frob}_p^2$. Frobenius acts within each factor. Let R be the completed integer ring at the chosen place, with residue field k, and put $Q = p^2$. We use the integral local generators of the tangent lines constructed in the proof of Theorem 64.14. Write

$$T_{\tau,c} = \frac{p^{F_Q(c)}}{c!} D_\tau^c, \qquad X_\tau = D_\tau, \qquad Y_\tau = D_\tau^p / p!.$$

These are commuting operators on integral formal functions. A bar denotes their action after reduction to k. The same notation for a scalar denotes its image in k.

Theorem 64.16 (The algebra of the reduced operators)**.** *The k-algebra generated by all $\overline{T}_{\tau,c}$ is*

$$k[y_\tau : \tau \in \Sigma] / (y_\tau^{p^2} : \tau \in \Sigma), \qquad y_\tau \longmapsto \overline{Y}_\tau. \tag{64.10}$$

In this presentation $\overline{Y}_\tau^{\,p} = \overline{w}_\tau \, \overline{X}_{\sigma\tau}$ for a unit w_τ. For the digits and the integers L_ν, H_ν of Section 64.5, the image of $\prod_\tau T_{\tau,a_\tau}$ is the monomial

$$\prod_{\nu \in \Sigma} y_\nu^{H_\nu + pL_{\sigma\nu}}$$

times a unit. The proof gives the unit for each monomial.

Proof. By (64.9) are units $u_{\tau,j}$ such that

$$T_{\tau,Q^j} \equiv u_{\tau,j} X_{\sigma^j\tau} \pmod{p}, \qquad u_{\tau,0} = 1.$$

In the product coordinates of that proof one can take the coefficient $p^{F_Q(Q^j)}[Z^{Q^j}]\mathcal{E}(Z)$ of the elliptic exponential on the factor containing τ. The congruence means that the difference maps integral formal functions into $pR[[T]]$, even when R is ramified. Define the rational unit at p

$$c_j = \frac{p! \, ((Q^j)!)^p}{(pQ^j)!}.$$

Legendre's formula gives $v_p((pQ^j)!) = 1 + p\, v_p((Q^j)!)$. Also $F_Q(pQ^j) = pF_Q(Q^j)$, so the exact identity in characteristic zero is $T_{\tau,pQ^j} = c_j T_{\tau,Q^j}^p / p!$. Write $T_{\tau,Q^j} = u_{\tau,j} X_{\sigma^j\tau} + pB$, with B integral. The two terms commute since B is a linear combination of commuting invariant operators. In the binomial expansion of their p-th power every term containing B is divisible as an operator by p^2. For the last term this uses p^p, including when $p = 2$, and for an intermediate term it uses the binomial coefficient and the factor p. Since $v_p(p!) = 1$,

$$T_{\tau,pQ^j} \equiv c_j u_{\tau,j}^p Y_{\sigma^j\tau} \pmod{p}. \tag{64.11}$$

On the other hand

$$Y_\tau^p = \frac{(p^2)!}{p(p!)^p} \, T_{\tau,Q}.$$

The rational factor is a unit. Thus we may take $w_\tau = ((p^2)!/(p(p!)^p))u_{\tau,1}$. The exact equality $X_\tau^p = p! Y_\tau$ and the preceding congruence give $\overline{Y}_\tau^{\,p^2} = 0$.

For each $a_\tau = \sum_j (l_{\tau j} + p h_{\tau j}) Q^j$, factor T_{τ, a_τ} into the Q^j and pQ^j operators with the indicated multiplicities, as in Theorem 64.14. The unit multiplying their product is

$$\frac{\prod_j ((Q^j)!)^{l_{\tau j}} ((pQ^j)!)^{h_{\tau j}}}{a_\tau!}.$$

Apply the two operator congruences and then replace $\overline{X}_\nu$ by $\overline{w}^{-1}_{\sigma^{-1}\nu} \overline{Y}^{\,p}_{\sigma^{-1}\nu}$. These substitutions give the stated exponents and all scalar factors. They show that (64.10) maps onto the operator algebra.

To prove injectivity use the monomials $\prod_\nu \overline{X}_\nu^{b_\nu} \overline{Y}_\nu^{d_\nu}$, where $0 \le b_\nu, d_\nu < p$. By the relation for $\overline{Y}_\nu^{\,p}$, these monomials differ by units from the proposed basis of monomials in the y_ν with exponents below p^2, each occurring once. Put $e_\nu = b_\nu + p d_\nu$ and $s = \sum_\nu e_\nu$. Choose integral linear formal coordinates T'_ν dual to the D_ν in the tangent space at zero. For this operator, its value on a monomial of total degree s at zero comes only from applying each differentiation to a coordinate. All terms where a derivative acts on the coefficients of a vector field have order below s on the test monomial, so they vanish. As a result the value on $\prod_\nu (T'_\nu)^{e_\nu}$ is $\prod_\nu e_\nu!/(p!)^{d_\nu}$, a unit since $e_\nu < p^2$ and $v_p(e_\nu!) = d_\nu$. It is zero on every other monomial of that same total degree. These assertions follow in characteristic zero before reduction, where division by the factorials is legitimate. An operator of lower order vanishes on every monomial of degree s at zero as well. In any proposed nonzero linear relation, choose a term with s maximal among those with nonzero coefficient. Its test monomial therefore isolates a nonzero value in k, a contradiction. This proves independence, including independence of the resulting distributions evaluated at zero. □

Corollary 64.17 (An exact test for additional divisibility)**.** *For any list of orders on these factors and any integral scalar jet through their total order one has*

$$v_p\left(\left(\prod_\tau D_\tau^{a_\tau} F \right)(0) \right) \;\ge\; B_p(\boldsymbol{a}) + \sum_{\nu \in \Sigma} \left\lfloor \frac{H_\nu + p L_{\sigma\nu}}{p^2} \right\rfloor. \tag{64.12}$$

The minimum over integral jets equals $B_p(\boldsymbol{a})$ if and only if every exponent $H_\nu + p L_{\sigma\nu}$ is below p^2.

Proof. Group the factors from (64.11) for a common ν. Any p of them together are congruent modulo p to a unit times $X_{\sigma\nu}$, by the computation of Y_ν^p. At a position μ this gives $\lfloor H_{\sigma^{-1}\mu}/p \rfloor$ disjoint groups congruent to unit multiples of X_μ, in addition to the L_μ original factors of that kind. Any p such groups together are divisible by p as operators because $X_\mu^p = p! Y_\mu$. All the groups are disjoint and commute. Dividing their products by the powers of p so obtained leaves integral operators. The number of powers obtained at μ is $\lfloor (H_{\sigma^{-1}\mu} + p L_\mu)/p^2 \rfloor$. Restoring the original factorials proves (64.12). If all these terms are zero, the reduced monomial of Theorem 64.16 is nonzero and its test monomial gives the scalar minimum. Its degree is at most $\sum a_\tau$. Indeed replacing p occurrences of Y_ν by $X_{\sigma\nu}$ lowers the order, while the initial replacement of each T_{τ, Q^j} or T_{τ, pQ^j} has order at most that of the replaced factor. If some term is positive, (64.12) excludes the scalar minimum. □

For example, fix ν and prescribe one high digit at each $(\sigma^{-j}\nu, j)$ for $0 \le j < p$, all other digits zero. Then $H_\nu = p$ gives $y_\nu^p \neq 0$, and the scalar minimum is attained. Now add $p - 1$ low units at $(\sigma\nu, 0)$. The same exponent becomes $p + p(p-1) = p^2$, so every integral section acquires at least one extra power of p.

Theorem 64.18 (Polynomial coefficients in a projected theta section)**.** *Use both auxiliary primes and the common interval of Theorem 6.36. Keep p unramified in E, inert in K and*

distinct from those two primes, and put $a = \lceil x \exp(x^{\varepsilon}) \rceil$. *Let* $\mathcal{P}(\boldsymbol{D}) = \sum_{\boldsymbol{a}} c_{\boldsymbol{a}} \prod_{\tau} D_{\tau}^{a_{\tau}}$ *be a nonzero polynomial over* $\operatorname{Frac} R$, *of total degree at most* a. *For its nonzero coefficients form*

$$b_{\boldsymbol{a}} = c_{\boldsymbol{a}} \prod_{\tau} \frac{a_{\tau}!}{p^{F_Q(a_{\tau})}}.$$

Choose β *of smallest valuation among these numbers. In the algebra* (64.10) *form*

$$W_{\mathcal{P}} = \sum_{\boldsymbol{a}} \overline{b_{\boldsymbol{a}}/\beta} \prod_{\tau} \overline{T}_{\tau, a_{\tau}}.$$

In every translation character the minimum valuation at zero of $\mathcal{P}(\boldsymbol{D})$ *on the integral projected sections in the frame of Theorem 6.36 equals* $v_p(\beta)$ *precisely when* $W_{\mathcal{P}} \neq 0$. *When* $W_{\mathcal{P}} = 0$ *every value has valuation at least* $v_p(\beta) + 1/e_w$, *where* e_w *is the absolute ramification index of* R. *This test applies to any integral harmonic polynomial expressed in the chosen directions.*

Proof. Dividing the operator by β gives exactly a sum of the integral normalized operators with coefficients $b_{\boldsymbol{a}}/\beta$. If $W_{\mathcal{P}} = 0$, this operator vanishes after reduction, so its image lies in the maximal ideal of R. If $W_{\mathcal{P}} \neq 0$, collect its monomials using the units in Theorem 64.16. The maximal-order test in that proof gives an integral jet with unit value. Its required degree is at most a by the order calculation in Corollary 64.17. Theorem 6.36 shows that each λ-component supplies every such jet in the specified frame. This argument also holds for the product of factors in the present section. In fact the product isogeny is still finite étale at p, its character lines on the target are torsion, and the cube of its ample symmetric polarization is relatively very ample, exactly the hypotheses used in that proof. Flat base change identifies the local sections with the span of the global integral sections. If all projected global sections gave values in β times the maximal ideal, their R-span would too. Thus when $W_{\mathcal{P}} \neq 0$ some global section attains the minimum in that character at the chosen place. □

Corollary 64.19 (The full local image ideal)**.** *In the setting of Theorem 64.18, choose elliptic formal parameters* T_i *on the product and write* $v_{i\tau}$ *for the coordinates of* D_{τ} *on the tangent space. Let* $\mathcal{E}_i(Z)$ *be the elliptic formal exponential in coordinate* i, *with linear term* Z. *For* $0 \leq |\boldsymbol{k}| \leq a$ *set*

$$j_{\boldsymbol{k}} = \sum_{\boldsymbol{a}} c_{\boldsymbol{a}} \left(\prod_{\tau} a_{\tau}! \right) [\boldsymbol{Z}^{\boldsymbol{a}}] \prod_{i} \mathcal{E}_i \left(\sum_{\tau} v_{i\tau} Z_{\tau} \right)^{k_i}.$$

For each λ, *the image of evaluation at zero on all* R*-integral projected sections is the nonzero fractional ideal* $\sum_{|\boldsymbol{k}| \leq a} R j_{\boldsymbol{k}}$. *In particular the smallest valuation is* $\min_{|\boldsymbol{k}| \leq a} v_p(j_{\boldsymbol{k}})$, *also when the first reduction* $W_{\mathcal{P}}$ *vanishes.*

Proof. In characteristic zero the formal exponential takes addition on the tangent space to the formal group law. Differentiating the displayed product in the variables Z_{τ} thus evaluates $\mathcal{P}(\boldsymbol{D})$ on the monomial $\prod_i T_i^{k_i}$ at the origin. These monomials form an R-basis of the relative jets through order a. Their evaluations therefore generate exactly the asserted image by the surjectivity for each character. The polynomial is nonzero in characteristic zero. Among its terms of maximum degree, a monomial in dual tangent coordinates with the matching exponents pairs nontrivially with one term and annihilates the others at zero. Thus at least one generator is nonzero.

Only finitely many coefficients are needed in this formula. In an elliptic coordinate of Section 64.2, write $[p](T) = pT + \sum_{m \geq Q} d_m T^m$ and $\mathcal{E}_i(Z) = \sum_{s \geq 1} h_s Z^s$. Starting with $h_1 = 1$, comparison of $[p](\mathcal{E}_i(Z))$ and $\mathcal{E}_i(pZ)$ gives for $2 \leq s \leq a$

$$(p^s - p) h_s = \sum_{m=Q}^{s} d_m \sum_{\substack{j_1 + \cdots + j_m = s \\ j_i \geq 1}} h_{j_1} \cdots h_{j_m}.$$

Every index on the right is smaller than s and the scalar on the left is nonzero. This supplies the required coefficients from the group law through order a. □

In the source, the homogeneous harmonic coefficient and the evaluation on a translated section appear in `Formalism/SharpRestriction/Divisibility/CanonicalTranslateJets.lean`, line 165. The criterion computes the first possible local valuation once the coefficient is specified. The isomorphism (64.10) determines cancellation between its monomials. To bound the arithmetic periods of Section 6.6, the coefficients selected by the global lifts, their sum over the period classes and their archimedean normalization still require a comparison.

65 Elliptic derivatives on definite classes

65.1 The norm of the prescribed products of maximal minors

The auxiliary norm in the source uses an ordered product of maximal minors at every CM embedding. Its definition fixes both the polynomials and the position of the class sum. We compute the norm with these choices. Let Σ be the CM type over $K=\mathbb{Q}(\sqrt{-d})$ on the fields of Section 6.6, and write $f=|\Sigma|=[E:K]$. Take ranks $1\le r\le s$, weights $b_\tau\in\mathbb{Z}_{\ge 0}$, and write $Z=(Z_\tau)_{\tau\in\Sigma}$ for s-by-r complex matrix variables. Set $k_\tau=rb_\tau$, $k=\sum_\tau k_\tau$ and $D=frs$. For an r-element subset I of row indices, write $\Delta_I(Z_\tau)$ for its minor in increasing row order. For every ordered choice $T=(I_{\tau j}:1\le j\le b_\tau)$ put

$$P_T(Z)=\prod_{\tau,j}\Delta_{I_{\tau j}}(Z_\tau).$$

Empty products are one. Let c,h range over the source and target classes for the two compact levels, with weights m_c,m'_h equal to the reciprocals of the respective stabilizer orders. Write $F_{ch}(Z)$ for the holomorphic theta function at that pair of representatives, including the prescribed finite Weil action on the chosen vector. The quantity computed here at a complex embedding is

$$\mathcal{N}=\sum_h m'_h\sum_T\left|\sum_c m_c P_T(\partial)F_{ch}(0)\right|^2. \tag{65.1}$$

These are the minors, derivatives and two class sums of `Development/AbelianVarietyTheory/Definitions/Foundations/NormSumPairRankZeroOfCurveCoordNorm.lean`, line 105 and lines 153–162 there. The ordinary derivative convention is specified in `Formalism/SharpRestriction/GlobalSchurBounds/GL3Theta.lean`, line 533.

On polynomials in the matrix entries give distinct monomials orthogonal Fischer inner products and let $\|Z^\alpha\|_{\mathrm F}^2=\alpha!=\prod_i\alpha_i!$. For a germ F let $J_{\boldsymbol k}F$ be its Taylor component homogeneous of degree k_τ in each block. Denote by Π the orthogonal projection onto the span of all P_T in that component.

Theorem 65.1 (An exact archimedean norm for the class sums)**.** *Define*

$$C_{r,b}=\prod_{j=0}^{r-1}\frac{(b+j)!}{j!}.$$

For the functions in (65.1) *one has*

$$\mathcal{N}=\left(\prod_\tau C_{r,b_\tau}\right)\sum_h m'_h\left\|\Pi J_{\boldsymbol k}\left(\sum_c m_c F_{ch}\right)\right\|_{\mathrm F}^2. \tag{65.2}$$

In particular this identity keeps the cross terms between distinct source classes mapping to the same target class.

Proof. First use one matrix variable and one integer b. The Cauchy–Binet determinant identity, raised to the b-th power, gives

$$\det(W^{*}Z)^{b}=\sum_{T}P_{T}(Z)\overline{P_{T}(W)}.$$

Ordered choices in this sum count each term with its multinomial multiplicity. Take the Fischer inner product conjugate-linear in the first entry. Define $SH=\sum_{T}P_{T}\langle P_{T},H\rangle_{\mathrm{F}}$. This is self-adjoint and positive. Its range is the span V_{b} of the P_{T}, since its kernel is their common orthogonal complement. It commutes with unitary changes of the s rows. Indeed the displayed kernel is unchanged by the same unitary change of rows in both matrices, and the Fischer inner product is invariant. For the latter assertion its integral representation is the ordinary Gaussian inner product for independent entries with density $\pi^{-1}e^{-|z|^{2}}$. Integration of the monomials in polar coordinates verifies this representation. The kernel determines S by pairing its second polynomial variable with H.

Let P_{0} be the b-th power of the minor on the first r rows. If $b>0$, any of the other indexed polynomials uses a row outside the first r, with positive degree in that row in every monomial. Thus $SP_{0}=\|P_{0}\|_{\mathrm{F}}^{2}P_{0}$. For $b=0$ this also holds since the sole index gives the constant one. The unitary row translates of P_{0} span V_{b}. To see this, the kernels $\det(W^{*}Z)^{b}$ as W varies span V_{b}. Orthogonality to all of them implies that the polynomial SH vanishes at every W. For full-rank W, orthonormalizing its columns writes this kernel as a scalar multiple of a unitary translate of P_{0}. For deficient rank the kernel is zero when $b>0$. Hence $S=\|P_{0}\|_{\mathrm{F}}^{2}\Pi$.

It remains to compute the scalar. For an r-by-r matrix of independent standard complex Gaussian entries it is $\mathbb{E}|\det Z|^{2b}$. Orthonormalize the columns in order. The squared determinant is the product of the squared lengths of their components normal to the preceding columns. Given these columns, in complex codimension j the squared length of the next component is a sum of j independent variables of density e^{-t} on $t\geq 0$, by unitary invariance. Its b-th moment is $(b+j-1)!/(j-1)!$, obtained by integrating the gamma density $t^{j-1}e^{-t}/(j-1)!$. Successive conditional expectation gives $C_{r,b}$. For several embeddings the operators, their spans, and their inner products tensor. Finally P_{T} has real coefficients, so $P_{T}(\partial)F(0)=\langle P_{T},J_{\boldsymbol{k}}F\rangle_{\mathrm{F}}$. Apply the tensor identity to the sum of the F_{ch} at each h. □

Proposition 65.2 (The Gaussian bound after summing all minors)**.** *Write* $|Z|^{2}=\sum_{\tau}\operatorname{tr}(Z_{\tau}^{*}Z_{\tau})$, $M_{\mathrm{in}}=\sum_{c}m_{c}$, $M_{\mathrm{out}}=\sum_{h}m_{h}'$. *If* $|F_{ch}(Z)|^{2}\leq S\exp(\pi|Z|^{2}/A)$ *for every* c,h,Z *with* $A>0$, *then*

$$\mathcal{N}\leq M_{\mathrm{out}}M_{\mathrm{in}}^{2}\,S\,2^{D}(2\pi/A)^{k}\prod_{\tau}C_{r,b_{\tau}}. \tag{65.3}$$

The factorial in this bound satisfies

$$0\leq\log C_{r,b}-r\log(b!)=\sum_{j=0}^{r-1}\log\binom{b+j}{j}\leq\tfrac{1}{2}r(r-1)\log(1+b+r).$$

Proof. Set $G_{h}=\sum_{c}m_{c}F_{ch}$. The triangle inequality gives

$$|G_{h}(Z)|^{2}\leq M_{\mathrm{in}}^{2}S\exp(\pi|Z|^{2}/A).$$

Integrate with the probability density $(t/\pi)^{D}\exp(-t|Z|^{2})$, where $t=2\pi/A$. The integral is at most $2^{D}M_{\mathrm{in}}^{2}S$. Independent scalar rotations of the matrix blocks act unitarily for this Gaussian. The Fourier projection under these rotations onto multidegree $\boldsymbol{k}$ is $J_{\boldsymbol{k}}$ by the Taylor expansion, and is a contraction by Cauchy–Schwarz. Gaussian scaling gives $\int|J_{\boldsymbol{k}}G_{h}|^{2}=t^{-k}\|J_{\boldsymbol{k}}G_{h}\|_{\mathrm{F}}^{2}$. The further projection Π is also a contraction. Substitute in (65.2). The last inequality follows from $\binom{b+j}{j}\leq(1+b+r)^{j}$. □

Theorem 65.3 (A class-independent bound for the CM theta metric)**.** *For a class pair let L, L' be self-dual Hermitian $\mathcal{O}_E$-lattices in the definite standard spaces of ranks r, s. Take $\mathfrak{b}$ from Theorem 64.10, and write $\Phi(X) = (\tau X)_{\tau\in\Sigma}$. For a nonzero scalar $\delta \in \mathbb{C}$, set*

$$\Lambda = \delta\Phi\Big(\mathfrak{b}^{-1}\operatorname{Hom}_{\mathcal{O}_E}(L, L')\Big), \qquad A = |\delta|^2\sqrt{d}/2, \qquad H(Z, Z) = |Z|^2/A.$$

In this metric the lattice has real covolume one and each nonzero vector has squared length at least $2f/\operatorname{rd}(E)$, where $\operatorname{rd}(E) = |\operatorname{disc} E|^{1/[E:\mathbb{Q}]}$. If Θ is a holomorphic theta section for this lattice in the Hermitian frame, let $\|\Theta\|_2^2$ be the average of $|\Theta(Z)|^2 e^{-\pi H(Z,Z)}$ on the torus. Then

$$\sup_Z |\Theta(Z)|^2 e^{-\pi H(Z,Z)} \le \left[e\max\left(1, \frac{2rs\,\operatorname{rd}(E)}{\pi}\right)\right]^D \|\Theta\|_2^2. \tag{65.4}$$

Proof. The module $M_0 = \operatorname{Hom}_{\mathcal{O}_E}(L, L')$ is self-dual for $h(X, Y) = \operatorname{tr}(Y^*X)$. Indeed it is the tensor product of the dual source lattice with the target lattice, and the tensor product of their perfect Hermitian pairings is exactly h. This can be checked on free bases after localization. On $\mathfrak{b}^{-1}M_0$ the trace form $\operatorname{Tr}_{E/\mathbb{Q}}(-h(X, Y)/\sqrt{-d})$ is unimodular by the inverse different as in Theorem 64.10. On Λ it is $-\operatorname{Im} H$. Its top exterior power divided by $D!$ is the Euclidean volume form for H, up to sign. A symplectic lattice basis therefore has volume one.

For nonzero $X \in \mathfrak{b}^{-1}M_0$, $v = h(X, X)$ is totally positive and belongs to $\mathfrak{D}_{E/K}^{-1}$, since $\mathfrak{b}\bar{\mathfrak{b}} = \mathfrak{D}_{E/K}$. Thus $|N_{E/\mathbb{Q}}v| \ge 1/N_{E/\mathbb{Q}}\mathfrak{D}_{E/K}$. The latter ideal norm is $|\operatorname{disc} E|/d^f$. The arithmetic–geometric mean inequality over the f places gives

$$\sum_\tau \operatorname{tr}((\tau X)^*(\tau X)) \ge f\,|N_{E/\mathbb{Q}}v|^{1/(2f)} \ge f\sqrt{d}/\operatorname{rd}(E).$$

Multiplication by $|\delta|^2/A$ gives the asserted separation.

For a point z, the translated holomorphic function

$$U_z\Theta(u) = \Theta(u + z)\exp\{-\pi H(u, z) - \pi H(z, z)/2\}$$

has metric squared magnitude equal at u to the original one at $u + z$. Here H is complex-linear in its first variable. Apply the mean-value inequality for the squared absolute value of this function on the open H-ball of radius ρ, where $\rho^2 = \min(D/\pi, f/(2\operatorname{rd}(E)))$. The ball projects injectively up to its boundary by the separation just proved. Inside it the unweighted integral is at most $e^{\pi\rho^2}\|\Theta\|_2^2$, since the metric density descends and the torus has volume one. The ball has volume $\pi^D\rho^{2D}/D!$. Using $D! \le D^D$ proves (65.4). □

Corollary 65.4 (Translation and transport of the vacuum)**.** *Suppose the functions entering (65.1) are the finite Heisenberg translates of a transported theta vacuum, with*

$$F_{ch} = \sum_i q_{i,ch}U_{t_{i,ch}}\Theta_{ch}, \qquad \left(\sum_i |q_{i,ch}|\right)^2 \le Q^{rs}.$$

Unitary character factors may be included in the coefficients. If each Θ_{ch} is obtained from a vacuum of squared norm ν_0 by normalized finite lattice intertwiners for the common Hermitian form, then (65.3) holds with

$$S = Q^{rs}[e\max(1, 2rs\,\operatorname{rd}(E)/\pi)]^D\nu_0.$$

This applies for every list of the prescribed minor weights at the same x, including the ranks in Theorem 6.29.

Proof. For two commensurable self-dual period lattices Λ_1, Λ_2, put $B = \Lambda_1 \cap \Lambda_2$, $q = [\Lambda_2 : B]$. For compatible semicharacters a normalized intertwiner is $q^{-1/2} \sum_{t \in \Lambda_2/B} \epsilon_t U_t$ with $|\epsilon_t| = 1$, the phases chosen for the target automorphy. This is the normalization in `Formalism/LocalToGlobal/KernelLattices/ColumnData.lean`, line 117. Each translate has the same squared norm on the torus for B, using average Haar measure throughout. Distinct translates are orthogonal there. Indeed for $t - t' \notin \Lambda_1$, self-duality gives $w \in \Lambda_1$ such that $\operatorname{Im} H(w, t - t') \notin \mathbb{Z}$. The unitary operator U_w on that common automorphy space has distinct eigenvalues on $U_t\Theta$ and $U_{t'}\Theta$, since its commutator with U_t is $e^{-2\pi i \operatorname{Im} H(w,t)}$. The norm squared of the normalized sum is therefore the original squared norm. For a function with target automorphy its average metric norm is the same over B and Λ_2. Iteration proves $\|\Theta_{ch}\|_2^2 = \nu_0$. Finally the metric supremum is preserved under any U_t. The triangle inequality and (65.4) give the common envelope used in (65.3). □

The last corollary uses the finite translation presentation of the vector. The squared norm ν_0 records its normalization at the complex embedding in question. For an arithmetic application one also needs the normalization at the conjugate embeddings, the integral sections realizing the periods, and the Bessel projection on the row tower. The identity (65.2) concerns the auxiliary norm of the prescribed minors before this last comparison.

65.2 Arithmetic of the normalized elliptic theta derivatives

Use the discriminant-one curve $C = \mathbb{C}/\Lambda$, the differential $dz = dx/y$, and a nonzero point $t \in C[2]$ from Section 6.6. Write A for the area of Λ. For a lift $w \in \mathbb{C}$ put

$$U_w F(z) = e^{-\pi z \bar{w}/A - \pi |w|^2/(2A)} F(z + w).$$

Let Θ_t be the normalized even theta in Proposition 65.21. We use its ordinary complex derivatives in the fixed differential. They determine the Taylor coefficients by division by the corresponding factorials. This convention is specified in `Formalism/SharpRestriction/GlobalSchurBounds/StandardLatticesGL3.lean`, line 45.

Theorem 65.5 (An algebraic formula for every derivative)**.** *For p a rational prime write $v_p(p) = 1$ at each place over p. All the numbers $H_n = \Theta_t^{(n)}(0)$, $n \geq 0$, belong to a single number field. At every complex embedding their images are exactly the derivatives of the normalized theta on the conjugate curve, with the conjugate mark and differential. For $p \geq 5$ they satisfy*

$$v_p(H_n) \geq \begin{cases} 0 & p \neq d, \\ -\frac{1}{2}\lfloor n/2 \rfloor & p = d. \end{cases}$$

Proof. Let $\sigma, \zeta, \wp$ be the Weierstrass functions of Λ, so that $(\log \sigma)' = \zeta$, $\zeta' = -\wp$, $\wp = x$, and $\wp' = y$. The increments $\eta_\Lambda(\lambda) = \zeta(z + \lambda) - \zeta(z)$ are additive on the lattice. Their real-linear extension to $\mathbb{C}$ has the form $u_\Lambda z + v_\Lambda \bar{z}$. If λ_1, λ_2 is a positively oriented basis, the residue of ζ at its single pole in a period parallelogram gives $\eta_\Lambda(\lambda_1)\lambda_2 - \eta_\Lambda(\lambda_2)\lambda_1 = 2\pi i$. Since $\bar{\lambda}_1\lambda_2 - \bar{\lambda}_2\lambda_1 = 2iA$, one gets $v_\Lambda = \pi/A$. These definitions and quasiperiod relations are also given in NIST, Weierstrass functions.

The remaining complex number u_Λ has an algebraic description. Let $\alpha \in \mathcal{O}_K \setminus \mathbb{R}$ and sum over the kernel $C[\alpha]$ of its action. Comparing poles in the elliptic functions $\sum_P \wp(z + P)$ and $\alpha^2 \wp(\alpha z)$ gives

$$\sum_{P \in C[\alpha]} \wp(z + P) = \alpha^2 \wp(\alpha z) + c_\alpha, \qquad c_\alpha = \sum_{P \neq 0} x(P).$$

Their poles have the same principal parts and their difference at zero has the stated constant term. Integrate using $\zeta' = -\wp$ and then take the increment under $z \mapsto z + \lambda$. The additive integration constant drops out and we obtain

$$N_{K/\mathbb{Q}}(\alpha)\eta_\Lambda(\lambda) - \alpha\eta_\Lambda(\alpha\lambda) = -c_\alpha\lambda.$$

The antiholomorphic terms cancel. With $\alpha = \sqrt{-d}$ this gives

$$u_\Lambda = \frac{c_\alpha}{\alpha(\alpha - \bar{\alpha})} = -\frac{1}{2d} \sum_{0 \neq P \in C[\sqrt{-d}]} x(P). \tag{65.5}$$

Multiplication by elements of $\mathcal{O}_K$ on this algebraic CM curve is algebraic over $\overline{\mathbb{Q}}$. For instance a torsion kernel is algebraic, the quotient isogeny is algebraic, and isomorphisms of elliptic curves with prescribed origin between the quotient and C are defined over $\overline{\mathbb{Q}}$. The derivative of the transported endomorphism is the image of α on the transported differential, so its kernel is the corresponding kernel there. In particular replacing $\sqrt{-d}$ by its negative leaves the kernel in (65.5) fixed. The formula proves both algebraicity and transport of u_Λ.

The odd Hermitian theta with derivative one is $e^{-u_\Lambda z^2/2}\sigma(z)$. Indeed the Weierstrass sigma transformation law and the formula for η_Λ give its unitary multipliers, with sign $+1$ on 2Λ and -1 on the other lattice vectors. It has its sole simple zero at the origin. Translate by a lift of t and normalize the value at zero. Oddness of ζ and its increment under $2t$ give $\zeta(t) = \eta_\Lambda(2t)/2$. Hence

$$\Theta_t(z) = e^{-u_\Lambda z^2/2 - \zeta(t) z}\frac{\sigma(z+t)}{\sigma(t)}, \qquad (\log\Theta_t)''(z) = -u_\Lambda - \wp(z+t).$$

The first logarithmic derivative at zero is zero. If L_i denotes the i-th logarithmic derivative there, we have

$$L_2 = -u_\Lambda - x(t), \qquad L_i = -(\partial^{i-2}x)(t) \quad (i \geq 3), \qquad \partial x = y, \quad \partial y = 6x^2 - g_2/2.$$

These identities follow by differentiating the Weierstrass equation. They show that every L_i is algebraic in the same number field and commutes with each embedding. The identity $\Theta_t' = \Theta_t(\log\Theta_t)'$ and Leibniz's rule give

$$H_0 = 1, \qquad H_n = \sum_{i=1}^{n} \binom{n-1}{i-1} L_i H_{n-i}.$$

This proves the assertions about the H_n over number fields.

At $p \geq 5$ the equations $g_2^3 = j/1728$ and $27g_3^2 = g_2^3 - 1$ imply that g_2, g_3 are integral since j is integral. The unit discriminant gives good reduction in this model. A nonzero point of order prime to p cannot reduce to zero, since prime-to-p torsion in good reduction specializes injectively. Its affine coordinates are therefore integral. At $p \neq d$ use (65.5). All its points have order dividing d, giving $v_p(u_\Lambda) \geq 0$. At $p = d$ use the first expression of (65.5) with $\alpha = (1 + \sqrt{-d})/2$. Its norm $(1+d)/4$ is prime to d and $v_d(\alpha(\alpha - \bar{\alpha})) = 1/2$. Thus $v_d(u_\Lambda) \geq -1/2$. The mark t is prime-to-p torsion in both cases, so L_i is integral for $i \geq 3$. Only L_2 can cost a factor of valuation $-1/2$, and every occurrence uses two orders in the recurrence. Induction gives the stated local bounds. □

Theorem 65.6 (Algebraic torsion translates in the Hermitian frame)**.** *Let $w \in \mathbb{C}$ satisfy $mw \in \Lambda$ for an integer $m \geq 1$. The derivatives at zero of $U_w\Theta_t$ lie in one finite extension of the field in Theorem 65.5. At a complex embedding they become the corresponding derivatives of $U_{w'}\Theta_{t'}$ times a single root of unity, independent of the order of differentiation. Here the marked curve is transported and w' lifts the transported point $[w]$. At every $p \geq 5$ prime to m the same valuation bounds as in Theorem 65.5 hold for the translated derivatives.*

Proof. In this proof write $P = [w]$ and $R_w(z) = U_w\Theta_t(z)/\Theta_t(z)$. Under a period translation $\lambda \in \Lambda$, the function R_w is multiplied by a root of unity of order dividing m. This follows by dividing the transformation laws of the numerator and denominator. Their ratio of multipliers is $\exp(\pm 2\pi i\, \mathrm{Im}(\lambda\bar{w})/A)$, whose m-th power is one by integrality of the alternating form on Λ. In particular R_w^m is an elliptic function, with divisor $m([t-P]-[t])$. This degree-zero divisor has trivial class in $\mathrm{Pic}^0(C) = C$ since $mP = 0$. Choose $h \in \overline{\mathbb{Q}}(C)^\times$ with that divisor. Then $R_w^m = ch$ for a nonzero complex constant c.

Successive translations along the same vector have no commutator phase, so $U_w^m = U_{mw}$. More explicitly, the product of the exponential factors at $z + jw$, $0 \le j < m$, is the exponential factor for mw. Consequently

$$\prod_{j=0}^{m-1} R_w(z + jw) = \epsilon_t(mw), \qquad c^m \prod_{j=0}^{m-1} h(z + jP) = \epsilon_t(mw)^m.$$

The multiplier $\epsilon_t(mw)$ is 1 or -1 because the characteristic is a half-characteristic. The product of the translates of h is a nonzero algebraic constant. Its divisor telescopes to zero. Thus c is algebraic.

More precisely $R_w(mz)$ is the uniformization of a rational function on C over $\overline{\mathbb{Q}}$. It is periodic by the multiplier computation and its divisor is $[m]^*([t-P]-[t])$. This divisor is principal over $\overline{\mathbb{Q}}$ because pullback by $[m]$ on Pic^0 is multiplication by m. Divide $R_w(mz)$ by an algebraic function with that divisor. The quotient is constant, and its m-th power is algebraic by $R_w(mz)^m = c\,h([m]z)$. This also gives a finite field for the rational function. For the formal parameter $T = -2x/y$ at zero we have $T = z + O(z^2)$. The expansions $T(z)$ and its formal inverse have coefficients in $\mathbb{Q}(g_2, g_3)$, by formal integration of dx/y in T and reversion of its series with linear term one. They commute with field embeddings. Substituting z/m gives a single finite coefficient field for the germ $R_w(z)$. Multiplying by Θ_t gives one for the translated theta.

At a conjugate embedding transport h and the product formula above. For the genuine translated analytic theta on the new curve use the same transported h and the chosen lift w'. The ratio of the two constants c in these equations has m-th power a sign. Thus the two germs for R_w have quotient a root of unity of order dividing $2m^2$. This follows also at a zero of either germ by removing the common order of vanishing first. Theorem 65.5 gives exact transport for Θ_t. This proves the asserted single phase for the whole translated germ.

For the local assertion take a completed integer ring containing the torsion and fields under consideration and the good Weierstrass model at p. Scale h locally so that its divisor on the smooth proper model consists of its horizontal divisor only. This is possible because the special fiber is geometrically integral, so every vertical divisor is an integer multiple of that fiber. Translation by each torsion section is an automorphism of the model. The product of translates of the rescaled h is a constant of valuation zero by its vertical divisor. Thus its associated c is a unit by the product formula. The pole section t misses the origin in the special fiber. The section $t - P$ also misses it unless $P = t$, by injectivity of prime-to-p specialization. It follows that in the completed local ring at zero one has $ch = T^{me}b(T)$ with b an integral unit and $e = 1$ if $P = t$, $e = 0$ otherwise. Here the case $P = 0$ simply has zero divisor. After adjoining a chosen root of $b(0)$, the equation for the root of $b(T)$ has a unique power series solution with that constant term by Hensel's lemma, since m is a unit. In particular R_w is integral in the formal parameter T. The invariant vector field dual to dx/y acts on this completed ring by an integral unit times d/dT. Every undivided derivative of R_w at zero is therefore integral. Apply Leibniz's rule and the bounds on H_n to $R_w\Theta_t$ to finish. □

Corollary 65.7 (Simultaneous finite translates on a product)**.** *Let $a \ge 1$, and on C^a let $\Theta = \prod_{j=1}^{a} \Theta_t(z_j)$. Choose finitely many torsion vectors w_i killed by m and algebraic weights b_i. The derivatives of $F = \sum_i b_i U_{w_i} \Theta$ lie in one number field. At each complex embedding the Taylor series is the Taylor series of $\sum_i \rho(b_i)\xi_{i,\rho} U_{w_i'} \Theta'$ for roots of unity $\xi_{i,\rho}$. Consequently*

$$\|F^{\rho}\|_2^2 \le \Big(\sum_i |\rho(b_i)| \Big)^2 \nu_{\rho}^{a},$$

where the norm uses a common period sublattice and normalized Haar measure. At every $p \ge 5$ prime to m where all weights are integral, $v_p(\partial^{\boldsymbol{n}} F(0)) \ge 0$ for $p \ne d$. At $p = d$ it is at least $-\frac{1}{2}\sum_j \lfloor n_j/2 \rfloor$ under the same hypotheses.

Proof. The Hermitian translation factors over the product. Apply Theorem 65.6 to every component and take the compositum of the finitely many fields. The phases multiply. The metric norm of each translated product over the common sublattice is the product of the one-factor norms, since its metric magnitude is a torus translate of the original product. The triangle inequality proves the bound. At a finite place each mixed derivative of a product is the product of its indicated one-variable derivatives. The valuation bounds follow term by term. □

These results identify the analytic elliptic normalization and its arithmetic derivatives for the actual function used in the source. The torsion level matters in the local statement. At a prime dividing that level the Hensel argument does not apply. For an iterated theta lift the effects of passage between lattices and of the class and Bessel sums must also be accounted for.

65.3 Conjugate class sums for the normalized theta vacua

We apply Sections 65.1 and 65.2 at all embeddings of one coefficient field. Throughout $C = \mathbb{C}/(\delta\mathcal{O}_K)$ is the discriminant-one curve, t_* is the two-torsion mark on which both idempotents act nontrivially, and E/K is the field belonging to x in the common interval. Put $W = \mathrm{Mat}_{s\times r}(E)$, $f = [E : K]$, $D = frs$, and write Φ for the CM embedding of W into the D matrix entries of Section 65.1. The trace Hermitian form on W is

$$h_K(X, Y) = \mathrm{Tr}_{E/K} \operatorname{tr}(Y^{*} X).$$

For a pair of Hermitian lattice classes set $M_0 = \mathfrak{b}^{-1} \operatorname{Hom}_{\mathcal{O}_E}(L, L')$. This is self-dual for h_K by the inverse relative different and the perfect Hermitian pairing on $\operatorname{Hom}(L, L')$. In particular $h_K(M_0, M_0) \subset \mathcal{O}_K$.

Lemma 65.8 (The theta construction in an orthonormal basis)**.** *Suppose rs is even. The space W has a K-orthonormal basis $v_1, \dots, v_D$. Let V have columns $\Phi(v_i)$; it is unitary with algebraic entries. In coordinates $z = V^{*} Z$ let $\Gamma = \delta\mathcal{O}_K^{D}$ and $\Gamma_M = \delta M$, where $M \subset K^D$ is M_0 written in this basis. These lattices admit compatible theta multipliers. On the product lattice the section with this multiplier is $\Theta(z) = \prod_j \Theta_{t_*}(z_j)$, up to scalar. The normalized intertwiner from Γ to Γ_M sends this section to a nonzero vacuum.*

Proof. Diagonalize the positive form $\mathrm{Tr}_{E/K}(u\bar{v})$ on E over K by Gram–Schmidt. The diagonal entries are positive rational numbers, since they are fixed by conjugation in K. Each occurs rs times on W. For a diagonal pair a, a one can choose $\lambda, \mu \in K$ with $|\lambda|^2 + |\mu|^2 = 1/a$. Indeed Meyer's theorem that every indefinite rational quadratic form in at least five variables has a nontrivial rational zero applies to $X^2 + dY^2 + U^2 + dT^2 - S^2/a$. At such a zero $S \ne 0$ by positivity of the first four terms. Division by S^2 gives the two required norms. The two

columns (λ,μ) and $(-\bar\mu,\bar\lambda)$ are orthonormal for the diagonal pair. This proves existence of the basis. For the even-by-even ranks of the column tower there is also a direct construction in groups of four repeated entries. Write $1/a$ as a sum of four rational squares by Lagrange's four-square theorem applied after multiplying by a denominator squared. Left multiplication by the resulting rational quaternion has transpose times itself equal to $a^{-1}I_4$. Finally $V^{*}V = I_D$ by the trace formula for h_K.

On either lattice define a sign at the point with coordinates δb by $(-1)^{\sum_i b_i\bar b_i}$. The exponent is an integer because both lattices before multiplication by δ are integral for the K-Hermitian form. For $h\in\mathcal O_K$ the integers $2\operatorname{Re}h$ and $2\operatorname{Im}h/\sqrt{d}$ have the same parity, as follows on writing $h=u+v(1+\sqrt{-d})/2$. Expanding the exponent of the sign on a sum therefore gives precisely the sign required by the unitary translation law for the alternating form $\operatorname{Im}H$. The two signs coincide on the intersection of the lattices by their definition. In one product coordinate $t_{*}=[\delta/2]$, which corresponds to $1\in\mathcal O_K/2$. The odd theta has sign -1 on the two periods $\delta,\delta(1+\sqrt{-d})/2$. Translation by $\delta/2$ preserves the first sign and reverses the second, by the commutator formula in Corollary 65.4. The signs thus obtained agree with $(-1)^{b\bar b}$ on these generators since $(1+d)/4$ is even. The multiplication law extends agreement to all periods. The product has the asserted multiplier. The space of sections for the product of the degree-one bundles is one-dimensional by the product formula for sections.

Both lattices are self-dual for the alternating form of the metric, by Theorem 65.3 for Γ_M and directly in each product coordinate for Γ. Multiply each $U_w\Theta$ by the sign of $w\in\Gamma_M$, sum over $\Gamma_M/(\Gamma\cap\Gamma_M)$ and divide by the square root of its order. The summands are independent of the chosen lifts after multiplying by the sign, by the multiplication law and the compatibility on the intersection. Translation by any member of Γ_M permutes the sum with the required sign. Corollary 65.4 shows that its norm is that of Θ, which is positive. □

This construction is the finite expression in `Formalism/SharpRestriction/GlobalSchurBounds/StandardLatticesGL3.lean`, line 197. We allow successive normalized intertwiners through any finite list of such trace lattices, and multiplication by algebraic scalars all of whose complex conjugates have magnitude one. All statements below apply to a single intertwiner as well.

Theorem 65.9 (Metric and lattice after arithmetic conjugation)**.** *Let G be a vacuum constructed in Lemma 65.8, including the allowed successive transports. Its Taylor coefficients in Z belong to one number field. At an embedding ρ the transported Taylor series represents an entire function G^{ρ}. Write $\Lambda_\rho=\delta_\rho\mathfrak c$ for the period lattice of the conjugate elliptic differential, where $\mathfrak c$ is an integral ideal of K. In product coordinates for $\rho(V)$ the metric magnitude of G^{ρ} descends to the lattice*

$$\Gamma_{M,\rho}=\delta_\rho\mathfrak c\,\rho(M).$$

Here $\rho(M)$ applies the restriction of ρ to K coordinatewise. With the Hermitian metric of scale $A_\rho=\operatorname{area}(\Lambda_\rho)$, one has

$$\|G^{\rho}\|_2^2=\nu_\rho^{D},$$
$$\sup_{Z}|G^{\rho}(Z)|^2e^{-\pi|Z|^2/A_\rho}\le[e\max(1,2rs\ \operatorname{rd}(E)/\pi)]^{D}\,\nu_\rho^{D}. \tag{65.6}$$

Finite torsion translates of G conjugate to the corresponding translates of G^{ρ} up to roots of unity.

Proof. Fix an integer n such that every period lattice in the construction lies between $n\Gamma$ and $n^{-1}\Gamma$; enlarge it to put all translation vectors under consideration in $n^{-1}\Gamma$. Work first in product coordinates. For $w\in n^{-1}\Gamma$ write $R_w=U_w\Theta/\Theta$. The proof of Theorem 65.6 shows in

each coordinate that $R_w(nz)$ is an algebraic rational function on the elliptic curve. Thus the product is rational on C^D over a number field. The calculation also covers a larger multiple n of the torsion order by composition with integer multiplication. Every finite expression in intertwiners consequently has the form

$$G(Vz) = \Theta(z)\, S([z/n]), \qquad S \in \overline{\mathbb{Q}}(C^D).$$

Here $[z/n]$ denotes the point of C^D represented by z/n. For example, for a translate of this expression its ratio to Θ is $R_w(z)S([z/n]+[w/n])$, again rational on the same cover. This proves the assertion by induction, including the normalization factors. Finitely many rational functions and torsion points suffice. Their fields together with the field of Theorem 65.5 and the entries of V lie in one finite Galois extension $J/\mathbb{Q}$. One may include the full n^2-torsion and the CM endomorphisms. In a finite sum, products of the U_w may equally be combined into single translations. Their commutator and composition phases are roots of unity since the alternating pairing is rational on δK^D. Corollary 65.7 then proves the entire convergence of every conjugate series, even at a possible pole of the displayed ratio. Entries of V lie in the abelian CM field E as embedded in $\mathbb{C}$. Its automorphisms commute with conjugation, so $\rho(V)$ is unitary and conjugation transports the linear change of variables.

More precisely, select w' so that $[w'/n] = \rho([w/n])$ on the conjugate product curve. By the rational-function description, conjugation sends $R_w(z)$ to $R'_{w'}(z)$ up to the constant root of unity in Theorem 65.6. It carries translation of S by $[w/n]$ to translation of S^ρ by $[w'/n]$. This proves the last assertion of the theorem, and proves that a unitary multiplier which is a root of unity at w transports to a unitary multiplier at w'. For any further translate one may enlarge n and J for this assertion.

We identify all the transported periods. In the quotient $n^{-1}\Gamma/n\Gamma$ the map $w \mapsto [w/n]$ identifies the group with $C[n^2]^D$. The scalar torsion is a free rank-one $\mathcal{O}_K/n^2\mathcal{O}_K$-module. Transport by ρ is semilinear for $\rho|_K$ because the scalar CM endomorphisms transport with their tangent multipliers. Hence the generator $[\delta/n^2]$ is sent to $[\delta_\rho a/n^2]$, where $a \in \mathfrak{c}$ generates $\mathfrak{c}/n^2\mathfrak{c}$ over $\mathcal{O}_K/n^2\mathcal{O}_K$. For clarity, the module representing $\Gamma_M/n\Gamma$ in $(\mathcal{O}_K/n^2\mathcal{O}_K)^D$ is $nM/n^2\mathcal{O}_K^D$. Its image is

$$n\mathfrak{c}\,\rho(M)/n^2\mathfrak{c}^D \;\subset\; (\mathfrak{c}/n^2\mathfrak{c})^D.$$

Indeed at each prime over n, a generates $\mathfrak{c}$ locally by Nakayama's lemma. At every other prime these quotient modules vanish. This proves the equality and gives the displayed lattice in the theorem. The lattice $\delta_\rho\mathfrak{c}$ exists since the conjugate curve has CM by the same maximal order, so its period lattice is homothetic to an invertible ideal. On $n\Lambda_\rho^D$ the periodicity of the ratio and the theta law already give a unitary multiplier. Hence $\Gamma_{M,\rho}$ is a lattice of metric periodicity.

For the first normalized intertwiner its conjugated sum consists of translates of the conjugate product section by distinct elements modulo the conjugate product lattice. Its coefficients have magnitude equal to the inverse square root of their number. All translations have norm squared ν_ρ^D on the common period lattice, with Haar probability measure. They are orthogonal by the commutator proof of Corollary 65.4, giving the first equality of (65.6). To iterate the argument we verify self-duality and separation for each intermediate lattice. For the trace lattice with the ideal $\mathfrak{c}$ inserted, $A_\rho = |\delta_\rho|^2 N\mathfrak{c}\sqrt{d}/2$. The trace pairings used in Theorem 65.3 are divided by $N\mathfrak{c}$, and $\mathfrak{c}\bar{\mathfrak{c}} = (N\mathfrak{c})$ exactly cancels this divisor. Thus the real alternating form is still unimodular. For a nonzero matrix in $\mathfrak{c}\,\mathfrak{b}^{-1}\operatorname{Hom}(L,L')$, the quantity $\operatorname{tr}(X^*X)/N\mathfrak{c}$ is totally positive in $\mathfrak{D}_{E/K}^{-1}$. The same statements hold in the transported coordinates, since the trace and all ideal relations are preserved under field embeddings. Applying the arithmetic–geometric mean argument of that theorem gives the same squared separation $2f/\operatorname{rd}(E)$. Consequently

every subsequent normalized sum again preserves the norm. Indeed the preceding section now has unitary multipliers on its transported self-dual lattice, and the transported cosets are distinct modulo that lattice by the torsion-group identification above. This is exactly the orthogonality argument for the first intertwiner. The mean-value proof of Theorem 65.3 applies with this separation and covolume one, giving the supremum bound. □

Theorem 65.10 (The field norm of the auxiliary class sum)**.** *At each class pair c, h of Section 65.1, take a vacuum G_{ch} as just constructed and a finite section*

$$F_{ch} = \sum_i a_{i,ch} U_{w_{i,ch}} G_{ch}, \qquad \left(\sum_i |\rho(a_{i,ch})| \right)^2 \le Q^{rs} \quad \text{at every embedding } \rho.$$

The $w_{i,ch}$ are rational torsion vectors and the coefficients are algebraic. Let $J/\mathbb{Q}$ be a finite Galois field containing the coefficients of these data and their expansions, including the fields used in Theorem 65.9. The number $\mathcal{N}$ of (65.1) belongs to J. If one class coordinate is nonzero, set $\mathfrak{h} = [J : \mathbb{Q}]^{-1} \log |N_{J/\mathbb{Q}} \mathcal{N}|$. Use the weights, $M_{\mathrm{in}}, M_{\mathrm{out}}, k, D$ from Proposition 65.2. Then

$$\begin{aligned} \mathfrak{h} \le\ & \log(M_{\mathrm{out}} M_{\mathrm{in}}^2) + rs \log Q + D \log\bigl(2e \max(1, 2rs \operatorname{rd}(E)/\pi)\bigr) \\ & + \sum_\tau \log C_{r,b_\tau} + k\bigl(\log(\sqrt{d}/\pi) - \gamma + D_{\xi_d}\bigr) \\ & + D\bigl(\tfrac{1}{4} \log d - \tfrac{1}{2}\gamma + \tfrac{1}{2} D_{\xi_d}\bigr). \end{aligned} \tag{65.7}$$

The bound is independent of the indices of the intertwining lattices, the choice of an orthonormal basis, and the auxiliary coefficient field. It holds at every x on the common interval with the same choice of d.

Proof. Write $v_{h,T} = \sum_c m_c P_T(\partial) F_{ch}(0)$. These coordinates lie in J by Theorem 65.9. The rational mass weights and the stability of J under complex conjugation put $\mathcal{N} = \sum_{h,T} m'_h v_{h,T} \bar{v}_{h,T}$ in J. At the original embedding it is positive under the stated nonvanishing assumption. Define

$$B_\rho = \sum_{h,T} m'_h |\rho(v_{h,T})|^2.$$

This is positive at every embedding. At an arbitrary embedding complex conjugation on J need not commute with ρ. Writing ι for the original complex conjugation on J, Cauchy–Schwarz gives

$$|\rho(\mathcal{N})| \le \sqrt{B_\rho B_{\rho\iota}}.$$

The map $\rho \mapsto \rho\iota$ permutes the embeddings. Hence $\mathfrak{h} \le [J : \mathbb{Q}]^{-1} \sum_\rho \log B_\rho$.

The minors have integer coefficients, so B_ρ is the sum of squares of exactly the prescribed derivatives of the conjugated sections with exactly the given weights. Each translated section has the same metric supremum as its vacuum. Theorem 65.9 makes the possible conjugation phases immaterial in the triangle inequality for F_{ch}. The envelope in Proposition 65.2 at this embedding can therefore be taken as

$$S_\rho = Q^{rs} [e \max(1, 2rs \operatorname{rd}(E)/\pi)]^D \nu_\rho^D.$$

Insert this into (65.3), take logarithms, and average. The exact mean of $k \log(2\pi/A_\rho) + D \log \nu_\rho$ is equation (65.17) of Theorem 65.25. This proves (65.7). □

The coefficient bound used here is the arithmetic finite translation bound in `Development/AbelianVarietyTheory/Definitions/Foundations/NormSumPairRankZeroOfCurveCoordNorm.lean`, line 114. Formula (65.7) applies to the explicit vacuum and class-section presentations in its

hypotheses. In the iterated automorphic lift, one must identify the Weil translates at the class representatives with such presentations, prove the required finite-place divisibilities, and identify a nonzero global Bessel projection. The field norm estimate alone does not provide those identifications or the odd-primary strict cohomology bound.

65.4 Split representatives and the finite Weil action

We now start with one finite vector in a theta lift and follow it through the two sets of class representatives. The local calculation can be performed at split primes outside the level of that vector. Put $k = E^+$ and let U_n be the unitary group of the standard positive definite Hermitian space E^n over k. All adelic groups in this section use the finite adeles.

Theorem 65.11 (Class representatives supported at split primes)**.** *Let $J \subset U_n(\mathbb{A}_{k,f})$ be an open compact subgroup and let S be any finite set of rational primes. Every class in*

$$U_n(k)\backslash U_n(\mathbb{A}_{k,f})/J$$

has a representative whose components are the identity except over at most two rational primes that split completely in E and lie outside S. For $n \geq 2$ one of the two primes can be fixed for all the classes. For $n = 1$ one prime suffices.

Proof. Shrink J to a product of local subgroups which is full integral at almost all places. A representative for a class at the finer level also represents its image at the stated level. For $T = U_1$ the diagonal first entry splits the determinant $U_n \to T$. For $g \in U_n(\mathbb{A}_{k,f})$ put $t = \det g$. Write $t = z/\bar{z}$ for a finite idele z of E by local Hilbert 90. At almost every place the extension is split or unramified and t is a unit. In the split case take the pair $(t_1, 1)$. In the unramified field case a Hilbert 90 solution can be multiplied by a power of a uniformizer of k_v to have valuation zero. These choices give an idele.

Choose a positive integer M such that for all integral unit ideles u congruent to 1 modulo M at primes over M we have $\mathrm{diag}(u/\bar{u}, 1, \dots, 1) \in J$. Such an M exists by openness and the full level away from finitely many primes. The ray class of z for $M\mathcal{O}_E$ contains a prime $\mathfrak{P}$ over a rational prime p splitting completely in E, outside any prescribed finite set. Indeed let H be the ray class field and take its normal closure over $\mathbb{Q}$. Extend the desired ray automorphism to an element of the normal closure fixing E. Chebotarev over $\mathbb{Q}$ supplies a rational prime and a prime of the normal closure with precisely this Frobenius. Its restriction to E is trivial and $E/\mathbb{Q}$ is Galois. The Frobenius over E is therefore the same element, and its restriction to H gives the chosen class by reciprocity. We use the convention in which uniformizers give arithmetic Frobenius. Thus $z = a z_{\mathfrak{P}} u$ with $a \in E^\times$, $z_{\mathfrak{P}}$ supported at $\mathfrak{P}$, and u in the indicated ray unit group. Removing $\mathrm{diag}(a/\bar{a})$ on the left and $\mathrm{diag}(u/\bar{u})$ on the right leaves a representative g_1 with determinant supported over p. In these diagonal matrices all other entries on the diagonal are one. This proves the result for $n = 1$.

For $n \geq 2$ fix another rational prime $p_0 \notin S$ splitting completely in E, excluding it when choosing p. Fix a place v_0 of k above p_0. The group SU_n is simply connected and absolutely almost simple over k, since it becomes SL_n over E. Its points over k_{v_0} are $\mathrm{SL}_n(k_{v_0})$ and are noncompact. The strong approximation theorem for simply connected almost simple groups therefore makes $SU_n(k)$ dense in its finite adeles away from v_0. Apply it to $g_1 \,\mathrm{diag}(\det(g_1)^{-1}, 1, \dots, 1) \in SU_n(\mathbb{A}_{k,f})$. At every place away from p, p_0, choose approximation modulo $J_v \cap SU_n(k_v)$. This specifies an open set in the restricted product since the subgroup is full integral almost everywhere. The rational element so obtained, acting inversely on the left of g_1, puts all these components in J_v. Remove them on the right using the product subgroup. Only the two split primes remain. □

Lemma 65.12 (The split oscillator on a lattice vector)**.** *Let X be a finite-dimensional vector space over a nonarchimedean local field, $X^\vee$ its frequency space with a perfect additive pairing, and $U \subset X$ a compact open lattice. Its annihilator is denoted by $U^\circ \subset X^\vee$. In the position realization take the unit vector $\varphi_U = \mathrm{vol}(U)^{-1/2}\mathbf{1}_U$. For $A \in \mathrm{GL}(X)$ the normalized change of variables*

$$f(y) \longmapsto |\det A|^{-1/2} f(A^{-1}y)$$

sends it to φ_{AU}. In a unitary lattice realization of the same Heisenberg representation this change on the vacuum is the positive square-root normalized finite intertwiner from $U \oplus U^\circ$ to $AU \oplus (AU)^\circ$, with trivial vacuum characters in the position realization.

Proof. The first identity follows by transformation of Haar measure. Position translations by U and frequency modulations by U° fix φ_U. Their common invariant line consists of functions supported on U and constant there. The first statement about support follows from the fact that U is the annihilator of U°, using all its modulations. The same description holds for AU. Let $b = [U : U \cap AU]$ and $c = [AU : U \cap AU]$. The target period lattice modulo its intersection with the source period lattice has order bc. Indeed the index in the frequency component is b by annihilator duality. The normalized finite sum over these bc cosets is on the target line, has norm one, and has inner product $1/\sqrt{bc}$ with the source vacuum. For the inner product only the zero coset contributes by commutator orthogonality, exactly as in Corollary 65.4. Direct integration also gives

$$\langle \varphi_U, \varphi_{AU} \rangle = \frac{\mathrm{vol}(U \cap AU)}{\sqrt{\mathrm{vol}(U)\,\mathrm{vol}(AU)}} = (bc)^{-1/2}.$$

The nonzero positive inner product on this line fixes the scalar. This proves the asserted compatibility of normalizations. A unitary splitting character multiplying the change of variables multiplies the answer by its own scalar. □

We specify the global finite Heisenberg realization used in applying the lemma. Identify the holomorphic vacuum G_0 on the standard matrix lattice with the finite vacuum. Here all vector equalities are transported with this fixed choice of scale. For $a \in W = \mathrm{Mat}_{s\times r}(E)$ write $q(a) = h_K(a,a) \in \mathbb{Q}$ and

$$W(a) = e^{\pi i q(a)} U_{\delta\Phi(a)}.$$

These operators fix G_0 on the integral period module $M = \mathfrak{b}^{-1}\,\mathrm{Mat}_{s\times r}(\mathcal{O}_E)$, by the sign computed in Lemma 65.8. For $z \in K$ define the rational functional $\lambda(z) = \mathrm{Re}\, z + \mathrm{Im}\, z/\sqrt{d}$ in the chosen embedding. Multiplying the exponentials in the definition gives

$$W(a)W(b) = e^{-2\pi i \lambda(h_K(a,b))}\, W(a+b).$$

Moreover $\lambda(\mathcal{O}_K) \subset \mathbb{Z}$. Extend this cocycle to finite adeles by the product of the local additive characters which on rational arguments gives $e^{-2\pi i u}$. It is trivial on $\widehat{M} \times \widehat{M}$. This describes the usual lattice realization without choosing complex representatives for finite adelic vectors. Indeed

$$W/M \;\simeq\; (W \otimes_{\mathbb{Q}} \mathbb{A}_{\mathbb{Q},f})/\widehat{M}.$$

To check the isomorphism, choose a $\mathbb{Z}$-basis of M. After clearing a common denominator surjectivity is the Chinese remainder theorem, and a rational number integral everywhere is an integer. For one rational lift of each coset the vectors $W(a)G_0$ are orthogonal of the same norm by the commutator argument. Changing the lift multiplies by the cocycle with a period, a root of unity. On this basis adelic translations act by changing cosets with precisely the cocycle just displayed. For instance if $y = a + u$, $u \in \widehat{M}$, the action on the vacuum is the inverse of the cocycle of (a,u) times $W(a)G_0$. Independence of the lift follows from the cocycle identity

and its triviality on periods. The same construction works with the period module of any class vacuum.

The description factors into local descriptions since the cosets are a restricted product of local cosets and the cocycle factors. At a prime completely split in E outside $2\,\mathrm{disc}(E)$, the two conjugate components of the matrix space are a position space X and its frequency space $X^\vee$. Each is totally isotropic. The standard matrix module at this prime is $U \oplus U^\circ$, by self-duality and the splitting. In particular the local vacuum above is identified with φ_U. For detail, translate φ_U by the local position and frequency vectors. Position cosets give disjoint supports, and distinct frequency characters on a given coset are orthogonal. Fourier expansion on the compact group U makes their span all locally constant compactly supported functions. Taking the phase convention of $W(a)$ amounts to multiplying the product of a position and a frequency operator by the scalar determined by the displayed cocycle. The scalar is one for integral components and thus fixes the same vacuum. These formulas give the isometry on the coset bases and identify the operators. The split pair action is $A : y \mapsto g'yg^{-1}$ on the position component and the contragredient action on its frequency component. It preserves h_K, hence preserves the chosen phase convention. This is the change-of-variables action of the split oscillator, with the prescribed splitting character if one is used. See also the position formulas in [7, 8].

Theorem 65.13 (The single-step class sections from one finite vector)**.** *Use rs even, the standard normalized vacuum G_0, and begin with a single vector of the form*

$$F = \sum_i a_i W(b_i) G_0, \qquad Qb_i \in M, \qquad \left(\sum_i |\rho(a_i)| \right)^2 \le Q^{rs}$$

at all embeddings. Take the usual finite oscillator action of the unitary pair, with normalized change of variables at split places. One may multiply that action there by unitary algebraic determinant characters of the norm-one torus, or by the unitary Hecke factors on finite ideles of E with integral circle weights in the source splitting. At both levels choose representatives by Theorem 65.11, avoiding the primes dividing $2Q\,\mathrm{disc}(E)$. For every such pair of representatives the finite Weil translate of F has a presentation as in Theorem 65.10, with the same bound Q^{rs}. Its translation vectors can be taken to have order dividing Q relative to the new period lattice. Consequently the field norm estimates of Section 6.6 of Theorem 66.9 and Corollary 66.11 apply to the nonzero auxiliary class sum formed from these representatives.

Proof. Let g, g' be the chosen pair and write $B(y) = g'yg^{-1}$ on the adelic matrix space. The old adelic period module $\widehat{M}$ moves to $B\widehat{M}$. It is the completion of the rational period module $M' = \mathfrak{b}^{-1} \mathrm{Hom}_{\mathcal{O}_E}(L, L')$ for the two moved lattices, by localizing the definition of Hom. At the moving places Lemma 65.12 identifies the new vacuum with the normalized lattice intertwiner up to the indicated character factors. At all other places the action is the identity. The finite intertwining sum globally is the product of these local sums. Indeed its coset quotient is the product of the local quotients, its square-root normalization is the product of their positive square-root normalizations, and in the W-convention each summand is translation by a new period. The old and new vacua have trivial corrected-period characters. For rational periods this last statement follows from $e^{\pi i q(a)} = (-1)^{q(a)}$ and extends to their finite completions in the coset model. Hence this is exactly a vacuum allowed by Theorem 65.9.

The permitted character factors have magnitude one under every complex embedding. To check this, on the finite norm-one ideles the character has an open unit kernel and on the archimedean circles it has integral weights. The norm-one torus class quotient at this kernel is finite, for instance by the ray-class argument in the first proof. Some positive power of a given

finite idele therefore equals a rational norm-one element times a member of the kernel. The corresponding power of its character value is the inverse archimedean character of that rational element by automorphy. Each conjugate of an element $u \in E^\times$ with $u\bar{u} = 1$ has absolute value one since E is CM. Its products to integral powers have the same property. Taking roots proves both algebraicity and the required magnitudes. For a Hecke character on the ideles of E as specified in `Formalism/SharpRestriction/GlobalSchurBounds/StandardLatticesGL3.lean`, line 409, use the finite ray class group of E instead. A finite idele raised to some positive power is a principal idele a times a ray unit in the kernel. The square of its archimedean character at a is a product of integral powers of $\tau(a)/\overline{\tau(a)}$, by the integral circle weights. Again all conjugates have absolute value one. This applies in particular to the determinant lifts at split places in lines 463–470 of the same source.

Conjugating $W(b_i)$ by the split change of variables translates by Bb_i in the new model. This follows on position and frequency operators separately. The correcting phase is preserved because the pair preserves h_K. As $QBb_i \in B\widehat{M}$, the adelic coset of Bb_i has order dividing Q modulo $\widehat{M'}$. Choose its rational representative b_i' by the quotient isomorphism above, now with lattice M'. Then $Qb_i' \in M'$. Acting on the moved vacuum changes this adelic translation to $W(b_i')$ times a root of unity, since the additive cocycle at finite places has finite-order values. Finally $W(b_i')$ and the Hermitian translation $U_{\delta\Phi(b_i')}$ differ by $e^{\pi i q(b_i')}$, also a root of unity. Absorb these scalars and the common character factor in a_i. All the absolute coefficient sums over embeddings are preserved. This gives exactly the hypotheses of Theorem 65.10 at every pair of representatives and proves the consequence. □

The theorem follows a prescribed single-step vector through the finite class sums. For the iterated lift the successive inputs, their finite integral divisibility, and the nonzero Bessel period extracted at the final rank still require a comparison on the same interval.

65.5 An inert-prime congruence for the prescribed class sums

Fix x on the common interval, $r \le s$ with rs even, and the single-step construction of Theorem 65.13. Keep the same δ, K, E, M, and standard elliptic mark t_*. Let S be any finite set of primes $p \ge 5$ inert in K, unramified in E, and prime to Q. We choose one vacuum for the entire set. The archimedean estimate of Theorem 66.9 applies to this choice. At each $p \in S$ and each coefficient place above it use the integer ring R of a sufficiently large finite extension. Congruences modulo pR are normalized by $v_p(p) = 1$.

Lemma 65.14 (One orthonormal basis for the specified primes)**.** *One can choose the K-orthonormal basis of Lemma 65.8 so that it is an $\mathcal{O}_K \otimes \mathbb{Z}_p$-basis of $M \otimes \mathbb{Z}_p$ simultaneously at every $p \in S$. At all places above these primes its CM embedding matrix V and its inverse have integral entries.*

Proof. At $p \in S$, $K_p/\mathbb{Q}_p$ is the unramified quadratic extension. The trace Hermitian lattice M_p is self-dual. Its reduction modulo p is therefore a nondegenerate Hermitian space over $\mathbb{F}_{p^2}$. It has a vector of nonzero norm. Indeed if all norms vanished, polarization of $h(v+aw, v+aw)$ for every $a \in \mathbb{F}_{p^2}$ would give $\mathrm{Tr}_{\mathbb{F}_{p^2}/\mathbb{F}_p}(ah(w,v)) = 0$ for every a, v, w, contrary to nondegeneracy. A lift has unit norm. The norm on units of $\mathcal{O}_{K_p}$ is onto $\mathbb{Z}_p^\times$. It is onto on residue fields by cyclicity, and a unit in $1+p\mathbb{Z}_p$ has a square root in $\mathbb{Z}_p$ by Hensel's lemma, which is also a norm from K_p. Rescale the lift to length one, split off its orthogonal complement integrally by its pairing, and repeat. This gives a local orthonormal basis at every selected prime.

Relative to any initial rational orthonormal basis, the local bases are matrices in the unitary group of the identity form over K_p. The condition that such a matrix give a basis of M_p is

open. The Cayley transform $X \mapsto (1-X)(1+X)^{-1}$ parametrizes the unitary matrices away from eigenvalue -1 by an open part of the rational vector space of skew-Hermitian matrices. Its inverse has the same formula. To reach this open part within each local condition, multiply the selected matrix by a central norm-one unit arbitrarily close to one, avoiding the finitely many forbidden eigenvalues. The values $(1+c\sqrt{-d})/(1-c\sqrt{-d})$ with $c \in \mathbb{Q}_p$ close to zero supply such units. Approximate the inverse Cayley parameters at all $p \in S$ by a single rational point of the vector space, using weak approximation on its rational coordinates. Its transform exists and lies in all the specified open sets. For the empty set simply use the initial basis.

The primes in S do not divide the relative different, so $\mathfrak{b}$ is a unit there. Thus every entry of every v_i is integral at all places of E above S. The same is true for its conjugates, and $V^{-1} = V^{*}$ gives the assertion for the inverse. □

To construct the vacuum of Lemma 65.8, start in the basis of Lemma 65.14 with the product of the marked elliptic sections, then use the normalized intertwiner to the standard trace lattice, with scalar one. For the input weights impose the source condition that $Q^{rs}a_i$ is an algebraic integer. Choose the split representatives of Theorem 65.13. A matrix-coordinate index $\nu = (\tau, i, j)$ specifies a CM embedding, row, and column. Let c_E denote complex conjugation on E and σ_p the arithmetic Frobenius of $E/\mathbb{Q}$ at p. Its value is independent of the place because $E/\mathbb{Q}$ is abelian. Define

$$\pi_p(\tau, i, j) = (\sigma_p c_E \circ \tau, i, j).$$

Here each image of E in $\mathbb{C}$ is identified with the same normal field. The new embedding again belongs to the CM type since both σ_p and c_E induce conjugation on K. Write $\kappa = -(\partial^{p-1}x)(t_*)$ for the elliptic unit of Lemma 66.12, with x the Weierstrass function.

Theorem 65.15 (Reduction of the actual class-section derivatives)**.** *For each F_{ch} obtained from the single input vector and the indicated representatives, all undivided derivatives in the matrix coordinates are integral at every place over S. At $p \in S$ set $H_\alpha = \partial^\alpha F_{ch}(0)$. Writing e_ν for the unit multi-index, one has*

$$H_{\alpha + p e_\nu} \equiv \kappa\, \alpha_{\pi_p(\nu)} H_{\alpha - e_{\pi_p(\nu)}} \pmod{pR}. \tag{65.8}$$

The right side is zero if $\alpha_{\pi_p(\nu)} = 0$. Also $H_{\alpha + p^2 e_\nu} \equiv 0 \bmod pR$ for every α, ν. The same assertions hold for all classes using the single basis of the lemma.

Proof. At each prime in S, the product period lattice and the standard trace lattice agree in the coordinates of the lemma. The class representatives move lattices only at split primes, so all the moved trace lattices also agree with them locally at p. Every index in the two normalized intertwiners is therefore prime to p, as can be checked on the finite quotient of each target lattice by its intersection with the source. Their square-root normalization factors are units. In producing the finite sums of translates of the original elliptic product, each translation has order prime to p in the product torus. Indeed all representatives of the intertwining cosets belong locally to the product lattice, and the further vectors have order dividing Q in the new period lattice. The two lattices again agree locally at p. Composing translations only introduces roots of unity. The weights a_i are integral here by the assumption on $Q^{rs}a_i$.

The determinant factors in Theorem 65.13 are units at all places above S. In its ray class proof take the finite idele lifts to be supported at the moving split primes. Whenever a power of a lift equals a principal idele times units, the principal generator is a unit at all primes above S. The formula for a power of the character value as a product of conjugates and their inverses then proves the assertion, also for the norm-one torus. We have thus expressed F_{ch}, in product

coordinates, as a sum of products of prime-to-p translates of Θ_{t_*} with integral coefficients. All their undivided derivatives are integral by Corollary 65.7.

In the ring of undivided derivative sequences use the multivariable product rule, with a binomial coefficient in each coordinate. For a product coordinate z_j denote its shift derivation by D_j. Theorem 66.13, gives $D_j^p F = \kappa z_j F$ in this ring over R/pR for every one of the translated products, hence also for the sum. The matrix coordinates are related by $z_j = \sum_\mu \overline{V}_{\mu j} Z_\mu$. Since V^* is integral, the chain rule preserves integrality of all undivided derivatives. More explicitly, each derivative in a matrix direction is a linear combination of the D_j with integral coefficients, and the same holds on iterating. Coefficientwise substitution of the linear forms respects the sequence product by the chain and product rules.

The commuting derivations give $\partial_\nu^p = \sum_j \overline{V}_{\nu j}^{\,p} D_j^p$ after this substitution modulo pR. Since $E/\mathbb{Q}$ is unramified at p, every p-integral entry satisfies $\overline{V}_{\nu j}^{\,p} \equiv V_{\pi_p(\nu),j} \bmod pR$. This congruence first holds in the unramified integer ring at each place of E and remains valid after extension to R. Consequently

$$\partial_\nu^p F_{ch} \equiv \kappa \sum_{\mu,j} V_{\pi_p(\nu),j} \overline{V}_{\mu j}\, Z_\mu F_{ch} = \kappa Z_{\pi_p(\nu)} F_{ch} \pmod{pR},$$

where the last equality is $VV^* = 1$. Taking the α-th entry proves (65.8). The derivation ∂_ν^p kills the linear coordinate $Z_{\pi_p(\nu)}$. Its p-fold iteration therefore multiplies F_{ch} by $\kappa^p Z_{\pi_p(\nu)}^p = 0$ in the sequence ring. This gives the remaining congruence. □

Corollary 65.16 (Two divisibility tests on the prescribed minor weights)**.** *Fix $p \in S$. Suppose that at least one embedding τ satisfies one of the following two conditions.*

$$b_\tau > s(p^2-1),$$
$$\pi_p(\tau) \neq \tau, \qquad b_\tau > p b_{\pi_p(\tau)} + s(p-1).$$

Here π_p on embeddings omits the row and column, which it fixes. Then every prescribed $P_T(\partial)F_{ch}(0)$ belongs to pR, at every place over p.

Proof. Each monomial of the determinant product has exponent sum b_τ in each column at τ. Under the first condition some entry in a column has exponent at least p^2, and Theorem 65.15 applies. For the second condition, fix a column and denote the row exponents at τ by a_i, and those at $\pi_p(\tau)$ by a_i'. Apply (65.8) in row i at τ $\lfloor a_i/p \rfloor$ times. Each application consumes one exponent from the other embedding in that same row, or gives zero. The two embeddings are distinct so reducing the second set of exponents leaves the first set untouched except for the prescribed subtractions of p. Nonzero reduction would require $\sum_i \lfloor a_i/p \rfloor \le \sum_i a_i' = b_{\pi_p(\tau)}$. But $\sum_i a_i \le p \sum_i \lfloor a_i/p \rfloor + s(p-1)$. The assumed strict inequality contradicts this requirement. Thus each monomial gives zero modulo pR, and the determinant coefficients are integers. This proves the claim. □

Theorem 65.17 (Finite divisibility and the archimedean estimate for one class sum)**.** *Let $S_* \subset S$ be the primes passing either test of Corollary 65.16. Put $e = [E:\mathbb{Q}]$, $A_r = |\mathrm{GL}_{re}(\mathbb{F}_3)|$, $A_s = |\mathrm{GL}_{se}(\mathbb{F}_3)|$, and*

$$Y = A_s A_r^2 \mathcal{N}, \qquad \mathcal{N} = \sum_{h,T} m_h' \left| \sum_c m_c P_T(\partial) F_{ch}(0) \right|^2 .$$

At every place above every $p \in S_*$, $v_p(Y) \ge 2$. If a class coordinate is nonzero, define

$$B_-(Y) = \frac{1}{[J:\mathbb{Q}]} \sum_{p \notin S_*} \log p \sum_{v \mid p} [J_v : \mathbb{Q}_p] \max(0, -v_p(Y)).$$

Only finitely many primes occur in this denominator term. With the same coefficients, class representatives and number field J in both bounds,

$$2\sum_{p\in S_*}\log p - B_-(Y) \le \log(A_sA_r^2) + \frac{\log|N_{J/\mathbb{Q}}\mathcal{N}|}{[J:\mathbb{Q}]}. \tag{65.9}$$

The second term on the right has the upper bound of Theorem 66.9, on the same $E = E_x$ and power interval.

Proof. Every source stabilizer acts faithfully on its integral lattice of $\mathbb{Z}$-rank re, and the target stabilizers act on lattices of rank se. They are finite by definiteness. Reduction modulo three is injective on every finite subgroup of $\mathrm{GL}_n(\mathbb{Z})$. Indeed a nontrivial element in the congruence kernel of prime order would have the form $1+3^jB$ with some unit entry of B and $j \ge 1$. Raising to a prime other than three preserves this first valuation, and raising to three increases it by exactly one, by the binomial expansion. Thus the reciprocal stabilizer orders have common denominators A_r and A_s respectively.

Write $v_{h,T}$ for the inner class sum. By Corollary 65.16, $A_rv_{h,T}$ lies in pR for every place over any $p \in S_*$. Its complex conjugate satisfies the same condition since conjugation permutes the places above p in the common Galois field. As $A_sm'_h$ is integral, every term of Y has valuation at least two there. When one class coordinate is nonzero, $Y \neq 0$ since the original archimedean sum has positive weights. For a nonzero element of a number field the logarithm of the absolute rational norm, divided by the degree, is the sum of $v_p(Y)[J_v:\mathbb{Q}_p]\log p/[J:\mathbb{Q}]$ over all finite places. It has finite support. Retain the positive lower bounds above S_* and the negative contributions elsewhere. This gives (65.9). All the presentations used above have the archimedean coefficient bounds in Theorem 65.13, which proves the final assertion. □

The finite-place bound here records one factor of p in every class coordinate at primes satisfying either test. The weighted prime count in Volume I requires higher valuations, control of the denominator term, and a nonzero Bessel projection of the iterated lifts. These requirements and the odd-primary strict cohomology estimate remain open.

65.6 Higher powers in the prescribed class sums

Fix the fields $K, E = E_x$, the ranks r, s, the weights b_τ, the level Q and the interval of Section 65.5. Write $f = [E:K]$ and $D = frs$. Choose any one finite set S as there and the one basis of Lemma 65.14 for all its primes. We keep the same input, class representatives, and archimedean normalization as in Theorem 65.17. At each $p \in S$ use

$$F_p(n) = v_p(n!), \qquad \omega_p = p/(p^2-1), \qquad \alpha! = \prod_{\nu=1}^{D}\alpha_\nu!, \qquad |\alpha| = \sum_{\nu=1}^{D}\alpha_\nu.$$

Theorem 65.18 (A bound for every matrix derivative)**.** *For every pair of classes c, h, every place over $p \in S$, and every multi-index α, one has*

$$v_p(\partial^\alpha F_{ch}(0)) \;\ge\; \max\left\{0, \sum_\nu F_p(\alpha_\nu) - \lfloor\omega_p|\alpha|\rfloor\right\}. \tag{65.10}$$

Proof. For a power series in any finite number of variables over the local coefficient field, impose the condition that its ordinary coefficient of total degree n at each monomial belongs to $p^{-\lfloor\omega_p n\rfloor}R$. Sums with integral coefficients and products preserve this condition. For a product, the two degrees add and the sum of their floors is at most the floor of their sum. An integral

linear change of variables also preserves it. Indeed the expansion of a monomial of degree n has integral coefficients in that degree.

In product coordinates every local elliptic factor $U_w\Theta_{t_*}$ satisfies the condition by the ordinary coefficient estimate proved in Theorem 66.16. The expression for F_{ch} in the proof of Theorem 65.15 is a finite sum with integral coefficients of products of these factors. All its translates have order prime to the selected p. To recover matrix coordinates one substitutes the linear forms given by the integral matrix V^*. Thus the stated condition holds for F_{ch} in those coordinates. Multiplication by $\alpha!$ takes its coefficient at Z^α to $\partial^\alpha F_{ch}(0)$. Theorem 65.15 supplies integrality of the latter, also when the second bound is negative. □

For a determinant term, the available information in a column is its total degree. The cheapest possible factorial valuation for that column has an exact expression.

Lemma 65.19 (Distribution of a column degree)**.** *For integers $b \ge 0$, $s \ge 1$, define*

$$M_p(b,s) = \sum_{j \ge 1} \max\left(0, \left\lceil \frac{b - s(p^j - 1)}{p^j} \right\rceil\right).$$

The sum is finite. It equals the minimum of $\sum_{i=1}^{s} F_p(n_i)$ over all tuples of nonnegative integers with $\sum_i n_i = b$.

Proof. Write each n_i as a multiple of p^j plus its remainder. The sum of the remainders is at most $s(p^j - 1)$, so each sum of quotients is at least the indicated summand. Summing gives the lower bound. To attain the bound at all levels together, start with $b_0 = b$ and set

$$b_{j+1} = \max\{0, \lceil (b_j - s(p-1))/p \rceil\}, \qquad d_j = b_j - p b_{j+1}.$$

Here $0 \le d_j \le s(p-1)$. In fact, if $b_j > s(p-1)$, then $s(p-1) - p < d_j \le s(p-1)$; in the other case $d_j = b_j$. Whenever $b_j > 0$ the next quotient is smaller, so this process terminates. Independently at each position j, distribute d_j as a sum of s digits between zero and $p-1$, by filling successive slots up to $p-1$. Use these digits as the base-p digits of $n_1, \dots, n_s$. They then sum to b, and the sum of their quotients on division by p^j is exactly b_j. To evaluate the recursion, the integer b_j is the least nonnegative integer q such that $b \le p^j q + s(p^j - 1)$. This holds at $j = 0$. At the next step the requirement is $b_j \le pq + s(p-1)$, which is equivalent to $b \le p^{j+1} q + s(p^{j+1} - 1)$ by the induction hypothesis. This gives precisely the ceilings in the assertion. □

Theorem 65.20 (Higher finite valuations on the common interval)**.** *Let $k = r \sum_\tau b_\tau$, $B = \max_\tau b_\tau$, and let δ_p be one if either condition in Corollary 65.16 holds and zero otherwise. Put*

$$m_p = \max\left\{ \delta_p,\ r \sum_{\tau} M_p(b_\tau, s) - \lfloor \omega_p k \rfloor \right\}. \tag{65.11}$$

At every place above every $p \in S$, the integer p^{m_p} divides every local scalar $P_T(\partial) F_{ch}(0)$ in R and every cleared coordinate $A_r v_{h,T}$. With the normalization of Theorem 65.17, $v_p(Y) \ge 2m_p$ there. If at least one coordinate is nonzero, then, with $B_-^{(S)}(Y)$ the normalized sum of the negative valuations outside S as in that theorem,

$$2 \sum_{p \in S} m_p \log p - B_-^{(S)}(Y) \ \le\ \log(A_s A_r^2) + \frac{\log |N_{J/\mathbb{Q}} \mathcal{N}|}{[J : \mathbb{Q}]}. \tag{65.12}$$

For fixed p, the explicit exponent also satisfies

$$m_p \ \ge\ \frac{k}{p^2 - 1} - D(1 + \log_p(1 + B)).$$

Proof. Every monomial of P_T uses one matrix entry per column per minor. At each embedding and in each of the r columns the s exponents therefore sum to b_τ. Apply Lemma 65.19 to each column and insert the result in Theorem 65.18. Every monomial has degree k and every determinant coefficient is integral. The other bound δ_p is Corollary 65.16. Multiplication of a class sum by A_r clears all its stabilizer weights. The bounds hold at every place above p, and hence also for the conjugate class coordinates. Clearing the outer weights by A_s proves the bound on $Y = \sum_{h,T} A_s m'_h |A_r v_{h,T}|^2$. At the distinguished embedding the sum is positive when some coordinate survives. Apply the rational norm to this nonzero Y and take logarithms, as in Theorem 65.17, to obtain (65.12).

Finally $F_p(n) = (n - s_p(n))/(p-1)$. For $0 \le n \le B$ the digit sum is at most $(p-1)(1+\log_p(1+B))$. Every admissible column distribution thus has factorial valuation at least $b_\tau/(p-1) - s(1+\log_p(1+B))$. Sum these inequalities and use $1/(p-1) - \omega_p = 1/(p^2-1)$. □

The right side of (65.12) has the upper bound in Theorem 66.9 and Corollary 66.11, with the same Y, E_x, Q and classes. The bound on m_p is uniform for that choice of data. Its leading coefficient $1/(p^2-1)$ has a convergent sum against $\log p$ over the primes, by comparison with $\sum_{n\ge 2} \log n/(n^2-1)$. This part of the estimate alone therefore supplies only a bounded multiple of k in the prime sum. The factorial terms at infinity can grow as $r\sum_\tau b_\tau \log b_\tau$. Recovering the weights of the distinguished Frobenius classes, controlling the remaining denominator and passing to the nonzero iterated Bessel period are still necessary for the proposed proof.

65.7 The elliptic normalization on the common interval

Keep d, $K = \mathbb{Q}(\sqrt{-d})$, the CM field E over K, and the interval I of Section 6.6. Take $\Lambda = \delta\mathcal{O}_K$ with $g_2(\Lambda)^3 - 27 g_3(\Lambda)^2 = 1$. Such a δ exists by the scaling law of weight twelve for the lattice discriminant. Write $C = \mathbb{C}/\Lambda$, with differential dz and model

$$y^2 = 4x^3 - g_2 x - g_3, \qquad dz = dx/y.$$

Here $j = 1728 g_2^3$. The classical theorem of complex multiplication for the maximal order says that j is an algebraic integer and its distinct conjugates over $\mathbb{Q}$ are the j-invariants of the ideal classes of K, each occurring once in its minimal polynomial. In particular g_2, g_3 are algebraic. We use the theorem precisely in this form. For the modular identities below we use the usual normalization $q = e^{2\pi i \tau}$. Milne, Complex Multiplication.

Let J be any number field containing g_2, g_3 and the coordinates of a chosen nonzero two-torsion point t. At each embedding $\rho : J \hookrightarrow \mathbb{C}$ take the period lattice of dx/y on the conjugate model. Write it as $\Lambda_\rho = \omega_\rho(\mathbb{Z} + \tau_\rho \mathbb{Z})$ with τ_ρ in the usual closed modular fundamental domain. Put $y_\rho = \operatorname{Im} \tau_\rho$, $A_\rho = |\omega_\rho|^2 y_\rho$ and $t_\rho = \rho(t)$ as an elliptic curve point. Boundary choices in the fundamental domain have the same height.

Proposition 65.21 (The metric norm of the marked elliptic theta)**.** *In the Hermitian frame of metric factor $e^{-\pi|z|^2/A_\rho}$, let Θ_ρ be the theta section with simple zero at t_ρ normalized by $\Theta_\rho(0) = 1$. Its squared norm ν_ρ, taken with probability Haar measure, satisfies*

$$A_\rho = 4\pi^2 y_\rho |\eta(\tau_\rho)|^4, \qquad \nu_\rho = \frac{1}{\sqrt{2y_\rho}\,|\vartheta[\epsilon,\beta](0,\tau_\rho)|^2}. \tag{65.13}$$

The characteristic is one of the three even characteristics and is determined by t_ρ. For an absolute constant c,

$$\log^+(A_\rho^{-1}) + \log^+ \nu_\rho \le c(1 + y_\rho), \qquad \log^+ u = \max(0, \log u).$$

This includes the point used to define the normalized vacuum in `Formalism/SharpRestriction/GlobalSchurBounds/GL3Theta.lean`*, line 198.*

Proof. Suppress the subscript ρ. The modular discriminant formula for the lattice is $g_2^3-27g_3^2 = (2\pi)^{12}\omega^{-12}\eta(\tau)^{24}$, where $\eta(\tau) = q^{1/24}\prod_{n\geq 1}(1-q^n)$. Taking absolute values proves the area formula. NIST, Modular Functions.

For $w = z/\omega$ use the convention

$$\vartheta[\epsilon,\beta](w,\tau) = \sum_{m\in\mathbb{Z}} e^{\pi i(m+\epsilon)^2\tau+2\pi i(m+\epsilon)(w+\beta)}.$$

The odd characteristic has one zero, at the origin modulo periods. Indeed pairing opposite half-integers gives the zero, and the argument principle on a translated period parallelogram gives one zero counting multiplicity. For the count, the logarithmic derivative is periodic under $w \mapsto w+1$ and decreases by $2\pi i$ under $w \mapsto w+\tau$, as follows by reindexing the series. Translation by the three nonzero half-periods therefore gives the three even characteristics, with simple zero at the corresponding marked point. For the appropriate one the Hermitian theta is

$$e^{\pi w^2/(2y)}\frac{\vartheta[\epsilon,\beta](w,\tau)}{\vartheta[\epsilon,\beta](0,\tau)}.$$

Its metric magnitude is periodic by the same transformation laws. It agrees with the unitary translate of the odd Hermitian theta, divided by its value at zero, as in the source definition. Indeed the ratio has no zeros or poles, and the logarithm of its magnitude is a periodic harmonic function, hence constant. The normalization fixes the constant ratio.

Integrate over $w = u+v\tau$, $0\leq u,v<1$, with measure $du\,dv$. The exponential factor and the metric contribute $e^{-2\pi y v^2}$ to the squared magnitude. Integration in u kills the distinct Fourier modes. The remaining numerator is

$$\sum_{m\in\mathbb{Z}}\int_0^1 e^{-2\pi y(m+\epsilon+v)^2}\,dv = \int_{\mathbb{R}} e^{-2\pi y v^2}\,dv = (2y)^{-1/2}.$$

Absolute convergence on the period parallelogram justifies the calculation. This proves the formula for ν.

Since $y\geq\sqrt{3}/2$, $|q|\leq e^{-\pi\sqrt{3}}<1$. Jacobi's product formulas show that the two even constants with $\epsilon=0$ are bounded above and below by positive absolute constants in magnitude. The remaining one has magnitude comparable to $e^{-\pi y/4}$. In each product, after extracting the leading factor, the upper and lower bounds follow from convergence of the products of $1+|q|^{n/2}$ and $1-|q|^{n/2}$ uniformly in this range. The product for η gives $\log|\eta(\tau)| = -\pi y/12+O(1)$ by the same argument. Substitution yields the asserted bounds. NIST, Jacobi products. □

Theorem 65.22 (The mean area in the discriminant-one normalization)**.** *For the quadratic character ξ_d of K, let $D_{\xi_d} = L'(1,\xi_d)/L(1,\xi_d)$. Taking all embeddings of J with equal weight gives*

$$\frac{1}{[J:\mathbb{Q}]}\sum_{\rho}\log(A_\rho/\pi) = \gamma+\log(2\pi/\sqrt{d})-D_{\xi_d}. \tag{65.14}$$

Moreover the embedding means of y_ρ, $\log^+(A_\rho^{-1})$ and $\log^+\nu_\rho$ are each $O(1+\log d+|D_{\xi_d}|)$, with an absolute implied constant.

Proof. Complex multiplication and the equal number of extensions of every embedding of $\mathbb{Q}(j)$ to J identify the mean of every function of the reduced lattice shape with its ideal class mean. The discriminant-one condition fixes the area within a similarity class by Proposition 65.21. The mark can vary above the same j. The bounds of that proposition hold for all three choices.

For $\tau = u + iy$, define the full Epstein sum

$$Z(\tau, s) = \sum_{(m,n)\neq(0,0)} y^s |m + n\tau|^{-2s}, \qquad \operatorname{Re} s > 1.$$

For an integral ideal $\mathfrak{a}$ of reduced shape τ, its area in $\mathbb{C}$ is $\sqrt{d}\, N\mathfrak{a}/2$. Sending $z \in \mathfrak{a} \setminus \{0\}$ to $(z)\mathfrak{a}^{-1}$ enumerates the integral ideals in the inverse class, with multiplicity $w_K = |\mathcal{O}_K^\times|$. Since $N((z)\mathfrak{a}^{-1}) = |z|^2/N\mathfrak{a}$, summing over the h ideal classes proves

$$\frac{1}{h} \sum_{[\mathfrak{a}]} Z(\tau_{\mathfrak{a}}, s) = \frac{w_K}{h} (\sqrt{d}/2)^s \zeta(s) L(s, \xi_d).$$

Here the factorization follows either by comparing the three splitting types at each rational prime or from Section 4.1.

We compute the constant term of Z at one. The terms with $n = 0$ give $2y^s\zeta(2s)$. For $n \neq 0$ apply the Mellin integral for the inverse power and Poisson summation in m to the Gaussian centered at $-nu$. The zero Fourier mode summed over n is

$$2\sqrt{\pi}\, \frac{\Gamma(s - \frac{1}{2})}{\Gamma(s)} y^{1-s} \zeta(2s - 1).$$

Its expansion is $\pi/(s-1) + 2\pi\gamma - 2\pi\log 2 - \pi \log y + O(s-1)$. This follows from the Laurent expansion of ζ and the gamma duplication formula at one.

The mode with $nk \neq 0$ has Mellin integral proportional to

$$e^{2\pi i k n u} \int_0^\infty v^{s-3/2} e^{-(ny)^2 v - \pi^2 k^2 / v}\, dv.$$

The double sum is locally normally convergent near $s = 1$. Indeed substituting $v = \pi|k|t/(|n|y)$ leaves a power factor times $e^{-\pi|nk|y(t+1/t)}$. One half of this exponential gives $e^{-\pi|nk|y}$, the other makes the integral uniformly finite on compact sets of s. At $s = 1$ the Fourier transform of $1/(v^2 + a^2)$ at k is $(\pi/a)e^{-2\pi|k|a}$, by a residue calculation. With the factor y and both signs of n, k, the nonzero modes sum to

$$4\pi \sum_{n,k\geq 1} \frac{e^{-2\pi nky} \cos(2\pi nku)}{n} = -4\pi \sum_{k\geq 1} \log|1 - e^{2\pi i k\tau}|.$$

Adding $2y\zeta(2) = \pi^2 y/3$ from $n = 0$ proves

$$Z(\tau, s) = \frac{\pi}{s-1} + 2\pi(\gamma - \log 2) - \pi \log(y|\eta(\tau)|^4) + O_\tau(s-1).$$

The residue in the ideal class identity fixes the scalar on its right to have residue π. Its constant term divided by π is therefore $\gamma + D_{\xi_d} + \log(\sqrt{d}/2)$. Comparing constants and using (65.13) gives (65.14).

Finally the eta product gives $-\log(y|\eta|^4) = \pi y/3 - \log y + O(1) \geq c_1 y - c_2$ with $c_1 > 0$ absolute. Average this inequality and apply the identity just proved. The bounds for the other two means follow from Proposition 65.21. □

Corollary 65.23 (The elliptic factors at every point of the same interval)**.** *Take the d selected for I in Theorem 5.1. For all $x \in I$ the embedding mean of $\log^+(A_\rho^{-1}) + \log^+ \nu_\rho$ is $O_{\psi,\varepsilon}(x^{\varepsilon/4})$. For integers $k, m \geq 0$, even when they vary with x, one has*

$$\frac{1}{[J : \mathbb{Q}]} \sum_\rho \log^+\Big((2\pi/A_\rho)^k \nu_\rho^m\Big) \ll_{\psi,\varepsilon} (k + m) x^{\varepsilon/4}.$$

Proof. The selected character satisfies $|D_{\xi_d}| \le 3\log x$ and $\log d \le Y^{\varepsilon/5}(\log Y)^2$ with $Y \le x$. For fixed $\varepsilon > 0$ both quantities are $O_\varepsilon(x^{\varepsilon/4})$. Apply Theorem 65.22 and use subadditivity of $\log^+$ on products. □

The source prescribes a vacuum of squared norm $\nu_\rho^{[E:K]rs}$ at ranks r, s, as recorded in `Formalism/SharpRestriction/GlobalSchurBounds/StandardLatticesGL3.lean`, line 496. Equation (65.14) proves the elliptic area identity appearing in `Development/AbelianVariety Theory/Proofs/FoundationProofs/MeanLogPeriodConjugatesEqChowlaSelbergStatement.lean`, line 8. The corollary controls the cost of those two elliptic factors in the estimate of Section 65.1. To use that estimate on an algebraic global period one must still identify the conjugates of its section in the indicated normalization and compare its class sum with the specified Bessel projection.

65.8 The two-torsion point prescribed by the split prime

There is an exact identity for the second elliptic factor of Corollary 65.23 when the mark is the one used in the source. Write $\omega_K = (1+\sqrt{-d})/2$. Since $d \equiv 7 \bmod 16$, the ring $\mathcal{O}_K/2\mathcal{O}_K = \mathbb{F}_2 \times \mathbb{F}_2$ has complementary idempotents given by $\omega_K, \bar{\omega}_K$. Indeed their sum is one and their product $(1+d)/4$ is even. On $C[2]$ the action is the regular module for this ring, as is seen from $(\frac{1}{2}\mathcal{O}_K)/\mathcal{O}_K$. There is exactly one point t_* on which both idempotents act nontrivially. It is the sum of the two points generating the distinct summands. This characterizes the point under every embedding, including those which exchange the summands.

Lemma 65.24 (The difference of the other two roots)**.** *Let P, Q be the two nonzero points of $C[2]$ different from t_*, and define the nonzero algebraic number*

$$B_* = (x(P) - x(Q))^2$$

in the discriminant-one model of Proposition 65.21. At every finite place over a rational prime p, normalized by $v_p(p) = 1$, one has

$$v_p(B_*) = \begin{cases} -4 & p = 2, \\ 0 & p \text{ odd.} \end{cases}$$

At every complex embedding ρ the squared metric norm of the elliptic vacuum with mark t_* is

$$\nu_\rho = \frac{\pi}{\sqrt{2A_\rho}\,|\rho(B_*)|^{1/4}}. \tag{65.15}$$

Proof. The CM j-invariant is integral. By the criterion for potentially good reduction of elliptic curves, after finite extension at any chosen place take an integral Weierstrass equation with unit discriminant. Enlarge the field to contain $C[2]$ and the CM endomorphisms. In comparing x with the affine coordinate X of this good model, the coordinate change has the form $x = u^2X + r$. The original equation in the variables $(x, y/2)$ also has discriminant one. The change scales the discriminant by u^{12}, so u is a unit even if r has a denominator. It follows that the valuation of $x(P) - x(Q)$ is that of $X(P) - X(Q)$.

For $p \neq 2$ the distinct two-torsion points have distinct reductions by good reduction. The two nonzero points have integral affine coordinates. On a smooth Weierstrass cubic two points of the same X-coordinate coincide or are negatives, since the vertical line meets the cubic in that pair and the origin. Each of the points is its own negative. Hence their reduced X-coordinates differ and their difference is a unit.

For $p = 2$, the action of $\mathcal{O}_K \otimes \mathbb{Z}_2 = \mathbb{Z}_2 \times \mathbb{Z}_2$ on the 2-divisible group of the good model splits it into two factors. The endomorphisms extend to the good elliptic scheme by the extension property for abelian schemes over a discrete valuation ring. Each factor has height one, as can be read from the order 2^n of its generic 2^n-torsion using the CM lattice. The ranks are preserved in the special fiber by finite flatness. In the special fiber the two dimensions add to one. The dimension-zero factor is étale, and the dimension-one factor of height one is connected. Indeed its connected formal group has positive height, leaving height zero for an étale quotient. Thus exactly one of P, Q reduces to the origin. Write it as P, so that $X(Q)$ is integral.

In a parameter T of the good formal group, multiplication by two is $2T + aT^2 + O(T^3)$ with a a unit. To see the unit, reduce modulo the maximal ideal. The kernel at the origin in the special fiber has length two by the connected height-one factor. This length is exactly the order of the first nonzero term of $[2](T)$ there. Now $v_2(T(P)) > 0$ and $[2](T(P)) = 0$. If $v_2(T(P)) < 1$ the quadratic term has strictly least valuation. If $v_2(T(P)) > 1$ the linear term does. Thus $v_2(T(P)) = 1$. For the Weierstrass parameter $T = -X/Y$, the expansion of X is T^{-2} times an integral unit series with constant one. It follows that $v_2(X(P)) = -2$. Since $X(Q)$ is integral, squaring the difference gives the asserted -4.

At a complex place write the first full period as ω. The classical half-period identities express the square of the even theta constant in Proposition 65.21 by

$$|\vartheta[\epsilon, \beta](0, \tau)|^4 = |\omega/\pi|^2 \, |x(P) - x(Q)|.$$

For the mark $\omega/2$, the constant is $\vartheta_2(0, \tau)$ and the difference is $e_2 - e_3$, where $e_1 = \wp(\omega/2)$, $e_2 = \wp(\omega(1 + \tau)/2)$, $e_3 = \wp(\omega\tau/2)$. For the other two marks the ϑ_3, ϑ_4 identities give the differences of the other respective pair. The coefficient uses the full period ω, twice the half-period ω_1 in the classical notation. Substitute this identity into (65.13) and use $A = |\omega|^2 \operatorname{Im} \tau$. This gives (65.15). NIST, Weierstrass roots and Jacobi constants. □

Theorem 65.25 (Exact mean norm of the prescribed elliptic vacuum)**.** *For the paired fields and the unique mark t_*, one has*

$$\frac{1}{[J : \mathbb{Q}]} \sum_{\rho} \log \nu_\rho = \frac{1}{4} \log d - \frac{\gamma}{2} + \frac{1}{2} D_{\xi_d}. \tag{65.16}$$

In particular, with $k, m \geq 0$ and the same embeddings,

$$\frac{1}{[J : \mathbb{Q}]} \sum_{\rho} \log\Big((2\pi/A_\rho)^k \nu_\rho^m \Big) = k\big(\log(\sqrt{d}/\pi) - \gamma + D_{\xi_d} \big) + m\big(\tfrac{1}{4} \log d - \tfrac{1}{2}\gamma + \tfrac{1}{2} D_{\xi_d} \big). \tag{65.17}$$

Proof. One may enlarge J to contain all the points above since this repeats each embedding the same number of times. Lemma 65.24 implies that $16 B_*$ has valuation zero at every finite place. It is an algebraic unit. Its field norm has absolute value one, and therefore $[J : \mathbb{Q}]^{-1} \sum_\rho \log |\rho(B_*)| = -4 \log 2$. Average the logarithm of (65.15). This gives

$$\frac{1}{[J : \mathbb{Q}]} \sum_{\rho} \log \nu_\rho = \log(\sqrt{2}\, \pi) - \frac{1}{2[J : \mathbb{Q}]} \sum_{\rho} \log A_\rho.$$

Theorem 65.22 now gives (65.16). The same theorem gives the mean of $\log(2\pi/A_\rho)$. Linearity gives (65.17). □

This evaluates the actual elliptic metric factors with their signs in the product formula. A source statement on means for the marked vacuum is `Development/AbelianVarietyTheory/Pro`

`ofs/DecoratedLatticeProofs/ThetaZeroMeanLogNormConjugatesOfWeberStatement.lean`, line 13. The proof here uses only the classical half-period identities, the valuation of the difference of two roots, and the class mean in Theorem 65.22. Applying the identity to a higher-rank period requires an arithmetic identification of its transported section at the same embeddings.

65.9 A Gram matrix comparison for the analytic theta section

Fix $p \in S$, let $O = \mathcal{O}_{K_p}$, and use the elliptic curve and nonzero two-torsion mark of Section 65.5. Write $\vartheta = \Theta_{t_*}$, with $\vartheta(0) = 1$. Let T be a good parameter at the origin, with linear term Z in the additive coordinate. By an integral germ in n elliptic parameters we mean a member of $R[[T_1, \dots, T_n]]$. We view this ring inside the characteristic-zero Taylor series by substituting $T_i = T(u_i)$, where u_i are additive coordinates. A row a of length n gives the linear form au. For a matrix A with n columns and entries in O put

$$G_A(u) = \prod_i \vartheta((Au)_i).$$

Conjugation on K_p is its nontrivial automorphism over $\mathbb{Q}_p$, and A^* denotes its conjugate transpose.

Lemma 65.26 (Cancellation of equal integral Hermitian forms)**.** *Let $a_j \in \mathcal{O}_K^n$ be finitely many rows and let $d_j \in \mathbb{Z}$ satisfy $\sum_j d_j a_j^* a_j = 0$. The product $H(u) = \prod_j \vartheta(a_j u)^{d_j}$ is a unit in the ring of integral elliptic germs, with constant coefficient one.*

Proof. A zero row contributes one. For every other row the map $C^n \to C$ given by a_j is a homomorphism of CM abelian varieties. Under translation by $\lambda \in \Lambda^n$ the elliptic theta transformation law multiplies its pullback by a sign times

$$\exp\left(\frac{\pi}{A_0}(a_j u)\overline{a_j \lambda} + \frac{\pi}{2A_0}|a_j \lambda|^2\right),$$

where A_0 is the area of Λ. The sign comes from the two-torsion characteristic. The Gram identity cancels both exponents in the product. Hence H^2 is a meromorphic function on the projective complex variety C^n, with divisor $2\sum_j d_j a_j^*[t_*]$; here the superscript on a divisor means pullback by the row homomorphism. By algebraicity of meromorphic functions on a projective complex variety it is rational. The divisor and the origin are defined over a number field. A rational function with that divisor and value one at the origin descends to its field of definition after a finite extension. Indeed the Riemann–Roch space for the negative of this principal divisor is one dimensional after base change to $\mathbb{C}$, with generator H^2. Global sections of the corresponding line bundle commute with field extension. Choose a generator over the field of definition and normalize its value at the origin. It has the prescribed divisor since its base change is a scalar multiple of H^2.

Pass to the good model over R, enlarging the coefficient field if necessary. All the row morphisms extend to its elliptic scheme, by the extension property for homomorphisms of abelian schemes over a discrete valuation ring with good reduction. Every such homomorphism sends the origin to the origin, and the reduction of t_* is a distinct point since two is a unit. Thus the closures of the horizontal zeros and poles avoid the closed origin. The special fiber of the product is geometrically integral. In the regular local ring at that origin the divisor of H^2 therefore consists only of an integer multiple of the uniformizer divisor. After removing that power of the uniformizer, a rational function with neither zeros nor poles in codimension one is a unit, by normality. Evaluating along the zero section gives a unit of R times the removed power. The normalized value one forces the power to be zero. Thus H^2 is a unit in the completed local ring with value one. Since two is a unit, it has a unique formal square root with constant coefficient one, obtained recursively by degree. This is H. □

Theorem 65.27 (Dependence on the Gram matrix over the local CM integers)**.** *If A, B have entries in O, the same number of columns, and $A^*A = B^*B$, then G_A/G_B is an integral elliptic unit. More generally, a product of such functions with integer exponents and zero signed Gram matrix is an integral elliptic unit. In particular:*

1. *If $A^*A = 0$, then G_A is an integral elliptic unit.*
2. *If $A^*A = \left(\begin{smallmatrix} 0 & I_n \\ I_n & 0 \end{smallmatrix}\right)$ and the coordinates are $u_1, \dots, u_n, v_1, \dots, v_n$, then*

$$G_A(u,v) \prod_{j=1}^{n} \frac{\vartheta(u_j)\vartheta(v_j)}{\vartheta(u_j + v_j)}$$

is an integral elliptic unit.

Proof. The equation for the Gram matrix over O need not hold for arbitrary integral approximations to the rows. We account for their Gram matrices before passing to the limit. Choose $\lambda \in \mathcal{O}_K$ with $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\lambda$. For a fixed number d of columns take the rows

$$e_i \ (1 \le i \le d), \qquad e_i + e_j, \ e_i + \lambda e_j \ (1 \le i < j \le d).$$

Their rank-one matrices a^*a form a $\mathbb{Z}$-basis of the Hermitian matrices over $\mathcal{O}_K$. In the (i,j) position with $i < j$, the last two rows contribute $1, \lambda$; having prescribed all such positions, one corrects the diagonal by integer multiples of the first rows. This argument also proves uniqueness. After completion the same matrices form a $\mathbb{Z}_p$-basis of the Hermitian matrices over O, since p is inert.

For a finite signed list of local rows approximate every entry by elements of $\mathcal{O}_K$. This is possible since its completion at p is O. At each stage expand the signed Gram matrix of the approximating list in the displayed basis, with coefficients $h_a \in \mathbb{Z}$. Multiply the approximating product by $\prod_a \vartheta(au)^{-h_a}$. The resulting signed Gram matrix vanishes exactly. By Lemma 65.26 the corrected product is an integral elliptic unit. The finitely many h_a converge to zero in $\mathbb{Z}_p$, by the assumption on the original Gram matrix and continuity of its basis coordinates.

For each fixed degree the coefficients converge in the local field. Substitution of a linear form is polynomial in its entries in that degree. For any series $1 + U$ with zero constant term in U, the same degree in $(1+U)^m$ involves only finitely many polynomials $\binom{m}{j}$ in the exponent m. These statements remain true after the fixed substitution $u_i = \log_C(T_i)$, inverse to $T(u_i)$. Thus the correcting factors tend coefficientwise to one. The valuation ring is closed and constant coefficients are one. This proves the general assertion. For the hyperbolic Gram matrix, the row $e_i + e_{n+i}$ with exponent one and the two rows e_i, e_{n+i} with exponent minus one give precisely its two off-diagonal unit entries. Sum over i and apply the signed assertion to the resulting ratio. □

Corollary 65.28 (Restriction of each class section)**.** *In product coordinates $z = V^*Z$, write F_{ch} for the class section of Theorem 65.15. For every matrix A with entries in O, the germ $F_{ch}(Au)/G_A(u)$ is integral in the elliptic parameters at every place over the chosen prime. Consequently the restriction $F_{ch}(Au)$ to $A^*A = 0$ is integral in those parameters. In a hyperbolic basis as in Theorem 65.27, multiplying $F_{ch}(A(u,v))$ by the same displayed theta ratios gives an integral elliptic germ.*

Proof. The proof of Theorem 65.15 expresses each class section in the coordinates z as a sum with integral coefficients of translates of the marked product. Dividing by its common factor $\prod_i \vartheta(z_i)$ leaves sums of products of the integral elliptic germs R_w from Theorem 65.6.

Substitution $z_i = (Au)_i$ preserves this elliptic integrality. For integral global rows it is pullback by a morphism of the good elliptic schemes. For a row over O, use global approximations. In each fixed degree the series $T(au)$, after $u_j = \log_C(T_j)$, depends continuously on the entries of a. Its coefficients are therefore still integral. Substituting these into an integral germ at the origin is valid since all their constant terms are zero. Multiplication by the unit of Theorem 65.27 proves the two consequences. □

The factor in the hyperbolic case is explicit in terms of the same marked analytic theta used at infinity. On either of the two isotropic halves it is identically one. This permits the derivative in the other directions to be counted before an integral restriction is made. The source introduces an isotropic condition in `Formalism/SharpRestriction/GlobalSchurBounds/GL3Theta.lean`, line 241 and a hyperbolic basis in the same file at line 296.

66 Frobenius translates and higher derivatives

66.1 The Frobenius count in a single list of minor degrees

We compare the K_d-oriented prime count with the derivatives of Section 65.5. Use one of the common intervals $[V, V^{3/2}]$ in Section 6.6. At each x write

$$E = K_\psi C_l(\sqrt{-q}, \sqrt{-d}), \quad K = \mathbb{Q}(\sqrt{-d}), \quad C_l = \mathbb{Q}(\zeta_{2^{l+2}})^+.$$

Use the index of the chosen fields in Volume I, including its shortened index when that family is used. In both cases $2^l \gg_\psi x^{2+8\varepsilon}$ and $[E:\mathbb{Q}] \ll_\psi x^{2+8\varepsilon}$. Identify the CM embeddings over K with $\Phi = \mathrm{Gal}(E/K)$ by the base embedding, and use additive notation for the abelian Galois group. Complex conjugation is c_E. Let $t \in \Phi$ be the position corresponding to a translate in the count. Set

$$b = e^{x^\varepsilon}, \qquad a = \lceil xb \rceil, \qquad W = \lceil \sqrt{b} \rceil, \qquad B' = \lceil b \rceil, \qquad X = a/W.$$

The list of integer thresholds w_τ, $\tau \in \Phi$, may be any list in $[W, B']$. In particular it may be the distinguished-set list of Volume I for any of the translates. The translate of a Frobenius element outside Φ is $h \mapsto t + c_E + h$. Write $C_d(t, a, w) = \sum_p C_{d,p}$ for that oriented count, with the inertia average of Section 6.1. At an unramified inert prime, with Frobenius σ_p, the exact term is

$$C_{d,p} = 2\log p \sum_{j \ge 1,\ j \text{ odd}} [a/p^j - w_{t+j\delta_p}]_+, \qquad \delta_p = c_E + \sigma_p \in \Phi. \tag{66.1}$$

Indeed even powers restrict trivially to K; at the odd powers one has $c_E + j\sigma_p = j\delta_p$. Use fixed ranks $r \le s$ of a definite single step with rs even, allowing these ranks to vary polynomially with x. Fix the single input, level Q, and class sections F_{ch} of Theorem 65.15.

Lemma 66.1 (Odd multiples in the CM type)**.** *Decompose $\Phi = P \oplus P'$ into its 2-primary and odd-order subgroups. For $\delta = g + y$ with $0 \ne g \in P$ and $y \in P'$, the odd multiples of δ form the set*

$$\mathrm{Gen}(\langle g \rangle) + \langle y \rangle.$$

Here $\mathrm{Gen}(C)$ *denotes the generators of C. The number of nontrivial cyclic subgroups of P is $O_\psi(1 + \log x)$.*

Proof. An odd residue modulo the order of g runs through exactly the units modulo that 2-power. The Chinese remainder theorem allows any such residue together with any residue modulo the odd order of y, giving the stated set. Put $A_0 = \mathrm{Gal}(K_\psi C_l / K_\psi)$, regarded as a

subgroup of Φ fixing the two quadratic factors. Its restriction to C_l is injective, so it is a cyclic 2-group. Its index in Φ is $2o$, with $o = [K_\psi : \mathbb{Q}]$. For $i \geq 1$ there are at most $2o \cdot 2^i$ elements of P killed by 2^i: each fiber in P/A_0 has at most $|A_0[2^i]|$ such elements. Every cyclic subgroup of order 2^i has 2^{i-1} generators, and their sets are disjoint. Thus there are at most $4o$ per order. The degree bound on E bounds the number of possible orders by $O_\psi(1 + \log x)$. □

For each nontrivial cyclic subgroup C of P, choose one generator g_C and set

$$u_{C,t} = \min_{g \in \mathrm{Gen}(C),\, y \in P'} w_{t+g+y}.$$

Use the following minor degrees in (65.1):

$$b_t = a, \qquad b_{t+g_C} = u_{C,t} \quad (C \neq 0), \qquad b_\tau = 0 \quad \text{at all remaining embeddings.} \tag{66.2}$$

The positions in this prescription are all distinct. The list is chosen once for the whole prime sum. Let S contain all primes $p \leq X$ which are inert in K, unramified in E, prime to Q, and at least five. We may take exactly this finite set. Use the common basis of Lemma 65.14 for every prime in S. On a bounded common interval one can also take the union of the relevant good primes for each fixed field, ranks and level, since the integer parameters range over finite sets, and Lemma 65.14 applies to their union at fixed field and lattices.

Theorem 66.2 (Divisibility for the actual weighted count)**.** *For every $p \in S$ with nonzero 2-primary component of δ_p, at every place above p, all the derivatives $P_T(\partial)F_{ch}(0)$ for (66.2) and all their cleared class coordinates $A_r v_{h,T}$ have valuation at least*

$$r \sum_{j \geq 1,\ j \text{ odd}} [d_{p^j}(a,s) - w_{t+j\delta_p}]_+, \qquad d_L(a,s) = \max(0, \lceil (a - s(L-1))/L \rceil).$$

Their common guaranteed lower bound is at least

$$r \left(\frac{C_{d,p}}{2 \log p} - s\, \#\{j \geq 1 : j \text{ odd},\ p^j \leq X\} \right).$$

If the thresholds factor through a quotient of Φ of exponent two, the low half of the cycle in this proof has total degree exactly $w_{t+j\delta_p}$ for every odd j. This includes the dense distinguished set $T_2 = A_0$ for the trivial character and every quadratic ψ.

Proof. In the Frobenius cycle through t, choose as its high half the even translates of t by δ_p. The order of δ_p is even by hypothesis. Write $\delta_p = g + y$ as in Lemma 66.1, and set $C = \langle g \rangle$. The other half is $t + \mathrm{Gen}(C) + \langle y \rangle$. It contains the position $t + g_C$ and no other selected position of (66.2). Indeed a different selected generator belongs to a different cyclic subgroup; the position t is on the even side. The degree sum on the low half is therefore exactly $u_{C,t}$. This is at most $w_{t+j\delta_p}$ at every odd j. If the thresholds factor through an exponent-two quotient, every generator of C has the same image there and P' has zero image. This proves the asserted equality in that case. For $T_2 = A_0$ the list factors through Φ/A_0, which in the coordinates of Volume I is a product of a group of order two with $\mathrm{Gal}(K_\psi/\mathbb{Q})$.

The contribution of the high half to the sum of the $d_{p^j}(b_\tau, s)$ is at least $d_{p^j}(a,s)$. Apply Corollary 66.19 to this cycle. Every other cycle has nonnegative contribution. That corollary estimates the actual determinant monomials before summing the classes and remains valid for the class coordinates after clearing their stabilizer weights. This proves the first bound. Since $d_L(a,s) \geq a/L - s$, replacing it by a/L costs at most s at each active level, by the Lipschitz bound for the positive part. A term with $p^j > X$ is zero in (66.1). The second bound follows. □

Theorem 66.3 (A single-step norm over the full prime range)**.** *Put $Y_t = A_s A_r^2 \mathcal{N}_t$ for the squared class sum (65.1) with degrees (66.2). The divisibility in Theorem 66.2 holds at twice its stated exponents for Y_t. If some scalar class coordinate survives, $Y_t \neq 0$. In a common finite Galois field J of its coefficients one then has*

$$C_d(t,a,w) \le \frac{[J:\mathbb{Q}]^{-1}\log|N_{J/\mathbb{Q}}Y_t| + B_-^{(S)}(Y_t)}{r} + E_Q + O_{\psi,\varepsilon}(b/x), \tag{66.3}$$

$$E_Q = 2a \sum_{\substack{p\mid Q,\ p\le X\\ p \text{ inert in } K}} \frac{\log p}{p-1}.$$

Here the error is uniform for ranks bounded by a fixed power of x, with threshold allowed to depend on that power. The denominator term is the normalized sum of negative valuations outside S as in Theorem 65.17. For Q supported on fixed primes one has $E_Q = 0$ on every sufficiently distant common interval.

Proof. The cleared squared sum has terms $A_s m_h'(A_r v_{h,T})\overline{(A_r v_{h,T})}$ with integral outer weights. Both scalar factors satisfy the lower bound at all places over p, since complex conjugation permutes these places. At the distinguished complex embedding the sum is strictly positive if any coordinate is nonzero. All primes of S have integral coordinates even when the 2-primary component under consideration is zero.

We bound the contributions to the count at primes missed by Theorem 66.2. If δ_p has odd order then it acts trivially on the real 2-power cyclotomic layer C_l. Complex conjugation also acts trivially there, so $p \equiv \pm 1 \pmod M$ with $M = 2^{l+2}$. At an unramified prime the entire count is at most $2a\log p/(p-1)$. Among integers at least two in the two residue classes, all are of the form $jM \pm 1$ with $j \ge 1$. Summing the reciprocal denominators up to X, and bounding each logarithm by $\log(2X)$, gives

$$\sum_{\substack{p\le X\\ p\equiv\pm 1 \bmod M}} C_{d,p} \ll aM^{-1}\log^2(2X) \ll_{\psi,\varepsilon} bx^{-1-6\varepsilon}.$$

The same pointwise bound holds at ramified primes by the normalized inertia average. The size estimates for M and $\log X = O_\varepsilon(x^\varepsilon)$ prove the last inequality.

A prime split in K contributes zero, including when it ramifies in E/K, since its entire inertia-averaged Frobenius coset fixes K. The primes dividing $2\,\mathrm{cond}(\psi)$, as well as 3, split in K on distant intervals by Theorem 5.1. The only other possible ramified primes are q, d. Both grow faster than every fixed power of x there, and their total contribution is at most $2a\sum_{p=q,d}\log p/(p-1) = o(b/x)$. The remaining omitted inert primes dividing the level are covered by E_Q. The same splitting argument shows that this term vanishes for fixed prime support.

Finally the accumulated rounding error in twice the local estimate after dividing by r is at most

$$2s\sum_{p^j\le X}\log p \le 2sX\log(2X) = o(b/x).$$

The inequality uses uniqueness of the prime base of a prime power, and $X \asymp x\sqrt{b}$ gives the last estimate. The field norm formula for Y_t gives an upper bound for the sum of its finite valuations over S after adding all negative contributions outside S to the normalized log norm. Combining these inequalities proves (66.3). □

Proposition 66.4 (The additional degrees in the archimedean estimate)**.** *Uniformly on the same family,*

$$0 \le \sum_{\tau \ne t} b_\tau \ll_\psi b(1+\log x), \qquad 0 \le \frac{1}{r}\sum_{\tau \ne t} \log C_{r,b_\tau} \ll_{\psi,\varepsilon} bx^\varepsilon(1+\log x).$$

In particular the second expression is $o(b\sqrt{x})$. The estimate concerns the explicit factorials in the archimedean norm. Its other factor is the norm of the projected vector.

Proof. There is at most one additional nonzero degree per cyclic subgroup in Lemma 66.1, each at most B'. For a degree $m > 0$, the product defining $C_{r,m}$ in Theorem 65.1 has rm factors at most $m + r$. Since $\log(B' + r) = O_\varepsilon(x^\varepsilon)$ for polynomial ranks on distant intervals, this proves both assertions. □

The scalar Y_t in (66.3) uses a single definite theta step and the displayed auxiliary choice of degrees. Its field norm has the archimedean upper bound of Theorem 66.9. To deduce the centered count estimate needed for Dirichlet GRH one still needs a surviving projection, control of $B_-^{(S)}(Y_t)$, and an upper estimate in the normalization of the full Bessel period. The simultaneous large-prime local cohomology chart on these same fields is in Theorem 32.15.

66.2 Nonzero translated class sums at one definite step

The estimate in Theorem 66.3 involves a norm of a nonzero sum. We now construct such sums at a definite step, for the positive normalization of the split oscillator on the fixed class representatives. We keep all the stabilizer weights. The calculation uses the freedom to translate the finite input.

Let $z = (z_1, \dots, z_D)$ be the matrix coordinates at all CM embeddings, orthonormal for the Euclidean form used in Proposition 65.2. Put $c_0 = \pi/A$, with A the area of the marked elliptic period lattice. The Hermitian metric on functions in this trivialization is $|F(z)|^2 e^{-c_0|z|^2}$. Suppose a full lattice $\Gamma \subset \mathbb{C}^D$ and a common unitary multiplier give all the functions under consideration the transformation law

$$F(z+\gamma) = \epsilon(\gamma)\exp\left(c_0 z\cdot\bar\gamma + c_0|\gamma|^2/2\right)F(z) \qquad (\gamma \in \Gamma).$$

Use Haar probability on the torus $T_\Gamma = \mathbb{C}^D/\Gamma$ and the inner product from this metric, conjugate-linear in the first variable. Write $\|F\|_\Gamma$ for its norm.

Lemma 66.5 (The translation average of a theta derivative)**.** *For every holomorphic section F with this transformation law and every homogeneous polynomial P of degree k in the matrix coordinates,*

$$\int_{T_\Gamma} |P(\partial_z)(U_w F)(0)|^2\, dw = c_0^k \|P\|_{\mathrm{F}}^2 \|F\|_\Gamma^2, \tag{66.4}$$

where $\|P\|_{\mathrm{F}}^2 = \sum_\alpha \alpha! |P_\alpha|^2$ and

$$(U_w F)(z) = e^{-c_0 z\cdot\bar w - c_0|w|^2/2} F(z+w).$$

Proof. On smooth sections put $L_j = \partial/\partial\bar w_j$ and $D_j = \partial/\partial w_j - c_0\bar w_j$. Both preserve the transformation law by direct differentiation. Integration by parts with the metric gives $L_j^* = -D_j$. Indeed the derivative of the metric produces the term $-c_0\bar w_j$ in D_j, and opposite faces of a fundamental parallelepiped cancel since the metric pairings are periodic. The mixed commutator is $[L_i, -D_j] = c_0 \mathbf{1}_{i=j}$. The L_i's commute among themselves, as do the D_j's, and all $L_i F$ vanish.

For $|\alpha| = |\beta| = k$ move the creation operators $(-D)^\alpha$ in the first argument of the inner product to the second using this adjoint identity. Each L_i then commutes to the right, picking up $c_0\beta_i$ when it removes one $-D_i$. A surviving L_i at the far right kills F. This gives

$$\langle D^\alpha F, D^\beta F\rangle_\Gamma = \mathbf{1}_{\alpha=\beta}\, c_0^k \alpha! \|F\|_\Gamma^2.$$

The two signs $(-1)^k$ cancel. Finally differentiating the translation formula at $z = 0$ yields $e^{-c_0|w|^2/2}P(D)F(w)$, since differentiating in w treats $\bar w$ as constant. The last two displays prove (66.4), including the periodicity of its integrand. □

Use now the standard normalized vacuum G_0 on the rational matrix lattice M of Section 65.5. At a pair of class representatives let G_{ch} be its finite Weil transform, using the positive split changes of variables of Lemma 65.12 at the moving places. We take the optional determinant factors at those places to be trivial. Write M_{ch} for the moved rational lattice and set

$$n_{ch} = [M_{ch} : M_{ch} \cap M], \qquad H_h = \sum_c m_c G_{ch}.$$

Take Γ to be the analytic period image of mM for a positive integer m with $mM \subseteq M_{ch}$ at all pairs. The corrected periods $W(\gamma)$ of Section 65.4 fix each corresponding vacuum on its lattice, hence the multipliers for U_γ agree on this common sublattice. It also serves for G_0.

Proposition 66.6 (Positive overlap before differentiation)**.** *At every target class h,*

$$\langle G_0, H_h\rangle_\Gamma = \|G_0\|_\Gamma^2 \sum_c m_c n_{ch}^{-1/2} > 0.$$

For the fixed representatives, define

$$\mathcal{N}_t(w) = \sum_h m'_h \sum_T |P_T(\partial)(U_w H_h)(0)|^2$$

using the degrees of (66.2)*, or any one prescribed list of nonnegative minor degrees. Its mean is exactly*

$$\int_{T_\Gamma} \mathcal{N}_t(w)\, dw = c_0^k \left(\sum_T \|P_T\|_{\mathrm{F}}^2\right) \sum_h m'_h \|H_h\|_\Gamma^2 > 0, \qquad k = r\sum_\tau b_\tau. \tag{66.5}$$

Proof. The positive finite intertwiner taking G_0 to G_{ch} has one translate per coset of $M_{ch} \cap M$ in M_{ch} and a coefficient $n_{ch}^{-1/2}$ on the zero coset. This follows by multiplying the split local intertwiners in Lemma 65.12. Distinct cosets give translates orthogonal to G_0 except at zero. In fact the self-duality of the source period lattice supplies a source period with nontrivial commutator against each nonzero coset. Its unitary translation preserves the common section space on a small enough common period lattice and acts on the two sections by different unitary eigenvalues. Decreasing the common lattice does not affect this inner product, since its periodic integrand has the same average on any finite cover. Equivalently the orthogonality is the computation of Corollary 65.4. The zero coset gives the stated inner product. Positivity follows from $m_c > 0$, $n_{ch} > 0$, and $G_0 \neq 0$. Apply Lemma 66.5 to H_h and sum the finite identities. There is at least one product of minors and every such product is a nonzero polynomial since $r \le s$. This proves the strict inequality. □

Theorem 66.7 (One rational torsion input for all the indicated derivatives)**.** *Fix a rational prime $P_0 \ge 5$ away from the fixed conductor and choose all the class representatives to be the identity there. On sufficiently distant intervals P_0 splits in K_d. At each fixed x, E, r, s there is*

a single finite vector $W(v)G_0$ with $v \in mM[1/P_0]$ for which all the fixed-representative sums $\mathcal{N}_t$ in Section 66.1 are nonzero simultaneously. One may include finitely many additional lists of minor degrees in this choice. For the resulting algebraic numbers $Y_t = A_s A_r^2 \mathcal{N}_t$ the inequality (66.3) holds with $E_Q = 0$.

Proof. Take one product of minors for each of the finitely many lists and one target class h. By Lemma 66.5 and Proposition 66.6 its squared derivative on $U_w H_h$ is a nonnegative real analytic function on the connected torus, with strictly positive mean. Its zero set has empty interior by uniqueness of real analytic continuation. The intersection of the finitely many nonvanishing sets is open and dense. The images of $mM[1/P_0]$ are dense as well, since in a basis of mM they give all grids with mesh P_0^{-e}, $e \geq 0$. Choose one such vector v in the open intersection, and let w be its analytic coordinate. The scalar relating $W(v)$ and U_w is the common root of unity $e^{\pi i q(v)}$ from Section 65.4.

We verify that this translation can be made before the split Weil transforms at the chosen representatives. Call the finite adelic transformation at a pair B_{ch}. The oscillator action conjugates $W(v)$ to $W(B_{ch}v)$, by the position and frequency operators of Section 65.4. At a moving place, which lies away from P_0, the component of v belongs to mM locally. Both v and $B_{ch}v$ therefore belong to the target lattice there, since $B_{ch}M = M_{ch}$ locally. The two corrected local period operators fix the target vacuum. At every other place B_{ch} is the identity. The finite product gives

$$\omega(B_{ch})W(v)G_0 = W(v)G_{ch}$$

in the common realization of Section 65.4, with the same scalar relating its right side to $U_w G_{ch}$ at all pairs. Linearity now gives the stated nonzero class sums for the single input. The existence of representatives avoiding a prescribed finite set is Theorem 65.11. Theorem 5.1, gives $d \equiv -1 \pmod{P_0}$ once its growing cutoff exceeds P_0. Thus the fixed prime splits in K_d.

Some $P_0^e v$ belongs to mM, so take $Q = P_0^e$. This input has a single coefficient one in the finite translation basis. Theorem 65.9 and Theorem 65.6 make its transformed derivatives algebraic. At every selected inert prime the additional translation has order prime to that prime. The reduction, Gram comparison, and divisibility arguments of Sections 65.5, 65.9 and 66.1 therefore apply with the same single basis. The field norm can now be taken at all the chosen translates since their squared sums are positive at the distinguished embedding. The support of Q splits in K_d, giving $E_Q = 0$. □

The choice of torsion point in this theorem is existential. For the fixed representatives the one coefficient has magnitude one at every complex embedding, so the bound for the translated vacuum uses that magnitude in place of $Q^{rs/2}$. Its arithmetic denominator at other places, including P_0, still enters $B_-^{(S)}(Y_t)$. The theorem evaluates the finite sums at the representatives specified before the translation. Identifying these evaluations with an automorphic integral at the originally prescribed levels requires the corresponding level invariance and determinant characters. The nonzero projection of the full iterated row and column lifts and its quantitative normalization remain to be proved.

66.3 The cost of the prescribed derivatives

Use the class sections constructed and transported in Theorem 65.9. The scale in their pointwise estimate is $a_\rho = \pi/A_\rho$. We extract each homogeneous component on a sphere of its own radius. This determines the coefficient of the total derivative order in the averaged estimate.

Lemma 66.8 (A sphere estimate for a homogeneous Taylor component)**.** *Let G be entire on a product of f copies of $\mathbb{C}^l$ and suppose $|G(Z)|^2 \leq S \exp(a \sum_{\tau=1}^{f} |Z_\tau|^2)$, where $a > 0$. Write G_j*

for the Taylor component of degree $j_\tau \ge 0$ in block τ and $j = \sum_\tau j_\tau$. In the Fischer norm, in which $\|Z^\alpha\|^2 = \alpha!$ and monomials are orthogonal,

$$\|G_j\|^2 \le S\, a^j \prod_\tau H_l(j_\tau), \quad H_l(u) = \frac{(u+l-1)!}{(l-1)!}\left(\frac{e}{u}\right)^u \ (u \ge 1), \quad H_l(0) = 1. \tag{66.6}$$

For every $u \ge 1$,

$$\log H_l(u) \le l\log(1+u/l) + u\log(1+l/u) \le l\big(1+\log(1+u/l)\big).$$

Proof. Set the zero-degree blocks to zero throughout. For a homogeneous polynomial P of degree u on $\mathbb{C}^l$, the standard complex Gaussian integral of $|P|^2$ equals $\|P\|^2$. Indeed the coordinate integrals give the factorials. The squared radius of the same Gaussian has density $t^{l-1}e^{-t}/(l-1)!$ by polar integration, and its direction has the uniform probability measure on the unit sphere, independently of the radius. Taking the u-th moment of the squared radius gives

$$\int_{|\omega|=1} |P(\omega)|^2\, d\omega = \frac{(l-1)!}{(u+l-1)!}\,\|P\|^2.$$

Apply the product version to G_j on spheres of radii $R_\tau > 0$. The integral of its square is bounded by the integral of $|G|^2$ there. In fact the homogeneous component is the Fourier projection obtained by rotating each block independently by $e^{i\theta_\tau}$. Orthogonal projection is a contraction on the product of the spheres, whose measure is rotation invariant. Uniform Taylor convergence on this compact product justifies taking that Fourier projection. The pointwise estimate thus gives the factor $\exp(aR_\tau^2)R_\tau^{-2j_\tau}$ from block τ after rescaling to unit spheres. Its minimum occurs at $R_\tau^2 = j_\tau/a$, giving (66.6). For the bound on H_l apply $\sum_{i=0}^{u-1}\log(l+i) \le \int_0^u \log(l+t)\,dt$ to the factorial ratio and use $\log(1+l/u) \le l/u$. □

In the following theorem $r \le s$ are the two ranks with rs even, $l = rs$, $D = fl$, $f = [E:K]$, b_τ are the prescribed minor weights, $k_\tau = rb_\tau$, $k = \sum_\tau k_\tau$, and $B = \max_\tau b_\tau$. Let m_c, m'_h be the rational stabilizer weights, with sums $M_{\mathrm{in}}, M_{\mathrm{out}}$. Write P_T for an ordered product of b_τ maximal minors at each τ. For the prescribed family of sections put

$$v_{h,T} = \sum_c m_c P_T(\partial)F_{ch}(0), \qquad \mathcal{N} = \sum_{h,T} m'_h |v_{h,T}|^2.$$

Precisely, F_{ch} is a finite sum of torsion translates of a normalized vacuum as in Theorem 65.10. Its coefficients $a_{i,ch}$ obey $(\sum_i |\rho(a_{i,ch})|)^2 \le Q^{rs}$ at each embedding. The estimates use the trace lattice for the particular pair c, h. If some $v_{h,T} \ne 0$, write $\mathfrak{h} = [J:\mathbb{Q}]^{-1}\log|N_{J/\mathbb{Q}}\mathcal{N}|$ for a common Galois coefficient field J.

Theorem 66.9 (The signed upper bound at the prescribed weights)**.** *Define*

$$L_d = \log(\sqrt{d}/(2\pi)) - \gamma + D_{\xi_d}, \qquad V_d = \tfrac14\log d - \tfrac12\gamma + \tfrac12 D_{\xi_d}.$$

For every x in the common interval and all the class sections above one has

$$\begin{aligned}\mathfrak{h} \le\ & \log(M_{\mathrm{out}}M_{\mathrm{in}}^2) + rs\log Q + kL_d + DV_d + r\sum_\tau \log(b_\tau!) \\ & + D\log[e\max(1, 2rs\ \mathrm{rd}(E)/\pi)] + \sum_\tau \log H_{rs}(rb_\tau) \\ & + \sum_\tau \sum_{i=0}^{r-1} \log\binom{b_\tau + i}{i}.\end{aligned} \tag{66.7}$$

The last two sums together are at most

$$D\big(1+\log(1+B/s)\big) + \tfrac12 fr(r-1)\log(1+B+r).$$

Proof. Fix an embedding ρ of J. The metric supremum bound in Theorem 65.9, and the coefficient bound give, at each target class h,

$$\left|\sum_{c} m_c F^{\rho}_{ch}(Z)\right|^2 \le M_{\mathrm{in}}^2 Q^{rs}[e\max(1,2rs\ \mathrm{rd}(E)/\pi)]^D \nu_\rho^D\, e^{(\pi/A_\rho)|Z|^2}.$$

The field embeddings act on the indicated Taylor coefficients. For the sum of squared moduli of $\rho(v_{h,T})$, the exact minor identity in Theorem 65.1, gives the product $\prod_\tau C_{r,b_\tau}$ times the square of a Fischer orthogonal projection of this Taylor component. Discard the projection using contraction and apply Lemma 66.8 with $j_\tau = k_\tau$. Sum over h with weights m'_h. Thus the two elliptic factors in the embedding bound are now $(\pi/A_\rho)^k \nu_\rho^D$.

If ι is complex conjugation on J, apply Cauchy–Schwarz to $\rho(\mathcal{N})$ using the two vectors of coordinates at ρ and $\rho\iota$. On averaging logarithms each set of coordinates occurs equally often. This bounds $\mathfrak{h}$ by the mean logarithm of the squared-modulus sum just estimated. Theorems 65.22 and 65.25 give the means L_d and V_d for $\log(\pi/A_\rho)$ and $\log \nu_\rho$. Finally

$$C_{r,b} = (b!)^r \prod_{i=0}^{r-1} \binom{b+i}{i}.$$

This proves (66.7). Use the bound on H_l with $k_\tau/l = b_\tau/s$, and $\log\binom{b+i}{i} \le i\log(1+B+r)$, to obtain the last estimate. □

Corollary 66.10 (The linear term after the factorials are expanded)**.** *With $0\log 0 = 0$, the bound in Theorem 66.9 implies*

$$\begin{aligned}\mathfrak{h} \le\ & \log(M_{\mathrm{out}} M_{\mathrm{in}}^2) + rs\log Q + DV_d + r\sum_\tau b_\tau \log b_\tau + k(L_d - 1) \\ & + O\big(D\log((2+rs\ \mathrm{rd}(E))(2+B+r))\big)\,.\end{aligned}$$

The implied constant is absolute, including when some weights are zero.

Proof. Comparison of $\sum_{j=1}^{b}\log j$ with the integral of $\log t$ gives $\log(b!) = b\log b - b + O(\log(2+b))$ for every $b \ge 0$. The sum of the resulting errors is $O(fr\log(2+B))$. Use $r \le s$, $fr \le D$, and $fr(r-1) \le D$ in the last estimate of Theorem 66.9. □

Corollary 66.11 (Mass and level on the prescribed interval)**.** *Use the ranks of Theorem 6.29 with $r \le s \le x^{402}$. Take the input level to be the full lattice stabilizer and the output level of index at most Q^{s^2+4} in the full stabilizer, as in* `Development/AbelianVarietyTheory/Definitions/Foundations/NormSumPairRankZeroOfCurveCoordNorm.lean`*, line 145. If $B \le 2\lceil\exp(x^{\varepsilon})\rceil$, then uniformly on the interval*

$$\mathfrak{h} \le r\sum_\tau b_\tau\log b_\tau + k(L_d-1) + (rs+s^2+4)\log Q + O_{\psi,\varepsilon}(x^{1630}).$$

For fixed $\varepsilon > 0$ and $A_0 > 0$, the polynomial error is $o(\exp(x^{\varepsilon})/x^{A_0})$.

Proof. For a full-level class with finite stabilizer Γ_c, the finer classes above it correspond to the orbits of Γ_c on the cosets of the finer level in the full level. The reciprocal stabilizer weights over those orbits sum to the index divided by $|\Gamma_c|$, by the orbit–stabilizer formula. The input full mass is bounded above by the number of full-level classes, and the output mass is its own full mass times its level index.

Write $e = [E:\mathbb{Q}]$ and $E \subset \mathbb{Q}(\zeta_N)$ for the conductor multiple chosen earlier in this section. The full-level part of the proof of Lemma 121.17 counts genus classes of rank s and gives the

bound $C(se)^4\log(2seN)$ for their logarithmic number. It applies also in rank r. The result follows there by counting Gram matrices and matrices of one generator of E in a bounded integral basis. Thus

$$\log(M_{\mathrm{out}}M_{\mathrm{in}}^2)\le (s^2+4)\log Q+O\Big((se)^4\log(2seN)\Big).$$

The construction gives $e\ll_\psi x^3$ and $\log N\ll_{\psi,\varepsilon} x^{\varepsilon/5}\log^2(2x)+\log(2x)$. Moreover $\mathrm{rd}(E)\le N$ by the conductor–discriminant formula, and $|V_d|\ll_{\psi,\varepsilon} x^{\varepsilon/4}$ by Theorem 5.1. Therefore $se\ll_\psi x^{405}$, $D\ll_\psi x^{807}$, and each logarithmic factor in the error of Corollary 66.10 is $O_{\psi,\varepsilon}(x)$. Combining these estimates proves the indicated polynomial bound. Finally $x^\varepsilon/(\log x)\to\infty$, which proves the last claim. □

This bound retains the signed term in k needed when comparing upper bounds at infinity with finite divisibilities. To derive (6.3) the comparison must reach the specific integral class sections in the iterated lifts and their nonzero row periods. The complementary odd-prime groups in Proposition 6.11 also require a uniform estimate.

66.4 The first inert-prime congruence in the Hermitian frame

Let $p\ge 5$ be inert in K. Work over the completed integer ring R of a finite extension of $\mathbb{Q}_p$ containing the coefficients and torsion under consideration. Normalize $v_p(p)=1$. The discriminant-one elliptic curve C has good reduction by Theorem 65.5. Let ∂ be the invariant vector field dual to dx/y. For any nonzero $t\in C[2]$, put $\kappa_t=-(\partial^{p-1}x)(t)$. Here the coordinate x in the Weierstrass equation is a function on C.

Lemma 66.12 (A nonzero constant on the supersingular fiber)**.** *On the good model over R/pR, one has $\partial^p=0$ on functions. On the geometric special fiber $\partial^{p-1}x$ is a nonzero constant. In particular $\kappa_t\in R^\times$.*

Proof. In characteristic p the p-fold iterate of a derivation is a derivation, by Leibniz's rule. The iterate of an invariant vector field is invariant, and hence $\partial^p=c\partial$ over R/pR, where $c\in R/pR$. These assertions hold over this ring even when it has nilpotents, because they follow from group translation and the binomial coefficients. Choose a CM scalar $\alpha\in\mathcal{O}_K$ whose residue generates $\mathbb{F}_{p^2}$ over $\mathbb{F}_p$, using inertness. Its isogeny has degree prime to p and extends to the good model after finite extension. Its tangent multiplier is the chosen image λ of α. Pullback of functions intertwines ∂ with $\lambda\partial$. Iterating p times and using $\partial^p=c\partial$ gives $c(\lambda^p-\lambda)=0$. One can evaluate the identity on a parameter at the origin, whose first derivative is a unit. Since $\lambda^p-\lambda$ is a unit, $c=0$.

Pass to the algebraic closure k_0 of the residue field and write $L=k_0(C)$. The constants of ∂ in L are L^p and $[L:L^p]=p$. To see this directly, x is separating, $y=y^p/(4x^3-g_2x-g_3)^{(p-1)/2}$, and $L=L^p(x)$. The element x is not a p-th power since $\partial x=y\neq 0$. In the basis $1,x,\dots,x^{p-1}$ the ordinary derivative in x has kernel L^p, as does $\partial=y\,d/dx$. Thus ∂ on this p-dimensional space is nilpotent with one Jordan block. In particular $\ker(\partial^{p-1})=\mathrm{im}(\partial)$.

Suppose $\partial^{p-1}x=0$. Both 1 and x would then be in $\mathrm{im}(\partial)$, so the differentials dx/y and $x\,dx/y$ would both be exact in L. Use a linear change of x and rescale y to obtain $Y^2=X(X-1)(X-\lambda_0)=f(X)$ with $\lambda_0\neq 0,1$. The two differentials span the same k_0-plane as dX/Y and $X\,dX/Y$. Write $m=(p-1)/2$. Since $1/Y=f(X)^m/Y^p$, exactness for both requires the coefficients of X^{p-1} and X^{p-2} in $f(X)^m$ to vanish. Indeed d/dX on the L^p-basis through X^{p-1} misses precisely the last basis vector, and $\deg(Xf(X)^m)<2p-1$.

Put $P(X) = (X-1)^m(X-\lambda_0)^m = \sum_j a_j X^j$, so the two vanishing coefficients give $a_m = a_{m-1} = 0$. Logarithmic differentiation of this polynomial gives

$$\lambda_0(j+1)a_{j+1} + (m-j)(1+\lambda_0)a_j + (j-1-2m)a_{j-1} = 0.$$

For $1 \le j \le m-1$ the last coefficient is j in k_0. Starting at $j = m-1$ and descending forces $a_0 = 0$, whereas $a_0 = \lambda_0^m \neq 0$. This proves $\partial^{p-1}x \neq 0$. It is a p-th power in L because its derivative is zero. It is regular off the origin and has a pole there of order at most $p+1$, since x has order two and the invariant vector field increases pole orders by at most one. Its p-th root therefore has at most a simple pole at the origin and no other poles. Riemann–Roch in genus one gives only constants with this pole bound. We have proved that $\partial^{p-1}x$ is a nonzero constant. The mark specializes away from the origin, proving the unit assertion. □

Theorem 66.13 (A recurrence for the actual elliptic theta derivatives)**.** *Let $F = U_w\Theta_t$, where w has order prime to p on C, and include $w = 0$. Write $H_n(F) = F^{(n)}(0)$ in the normalized Hermitian frame of Proposition 65.21. For $n \ge 0$, with the right side interpreted as zero at $n = 0$,*

$$H_{p+n}(F) \equiv \kappa_t\, n\, H_{n-1}(F) \pmod{pR}. \tag{66.8}$$

For the unshifted vacuum and all $0 \le j < p$,

$$H_{j(p+1)}(\Theta_t) \equiv j!\,\kappa_t^j \pmod{pR}.$$

In particular $H_{p+1}(\Theta_t)$ is a unit. For every indicated translate, $H_n(F) \in pR$ for every $n \ge p^2$.

Proof. It is important here to distinguish a sequence of undivided derivatives from coefficients of an ordinary power series. We use the ring of sequences over R in which multiplication is

$$(ab)_n = \sum_{i=0}^{n} \binom{n}{i} a_i b_{n-i}.$$

The shift $D(a)_n = a_{n+1}$ is a derivation. Taking all undivided derivatives of a germ at zero respects these operations. Let $Z = (0,1,0,\ldots)$ represent the linear coordinate. Modulo pR the p-th power of a sequence is the constant sequence with value a_0^p. Its shift vanishes by Leibniz's rule, and its degree-zero term has that value.

For $F_0 = \Theta_t$ let $\ell = (\log F_0)'$. All derivatives of both functions are integral at p, by the algebraic formulas of Theorem 65.5. In particular $\ell(0) = 0$, $\ell' = -u_\Lambda - x(z+t)$ with $u_\Lambda \in R$, and F_0 is even. Hence $\ell^{(p-1)}(0) = 0$ and $\ell^{(p)}(0) = \kappa_t$. Every subsequent derivative of ℓ vanishes modulo pR at zero, by the first assertion of Lemma 66.12. In the sequence ring this means $D^{p-1}\ell = \kappa_t Z$ after reduction.

From $DF_0 = \ell F_0$ one obtains

$$D^pF_0 = (D^{p-1}\ell + \ell^p)F_0 \pmod{pR}.$$

For an elementary proof, repeat the product rule. The terms in D^pF_0/F_0 correspond to set partitions of p positions, with a block of size i contributing $D^{i-1}\ell$. This follows by adjoining one position, either in a new block or in an existing block. The cyclic permutation of the p positions groups the terms into orbits of size p, except for the partition into singletons and the partition with one block. Indeed the blocks in any translation-invariant partition of $\mathbb{Z}/p\mathbb{Z}$ are cosets of a subgroup. This proves the formula. Now $\ell^p = 0$ after reduction since $\ell(0) = 0$. Thus $D^pF_0 = \kappa_t Z F_0$ in the reduced sequence ring.

For a translate, the proof of Theorem 65.6, gives $F = R_wF_0$ with R_w integral in a formal parameter of the smooth elliptic model. The invariant derivative ∂^p annihilates this formal ring

modulo pR by Lemma 66.12 and continuity. Every derivative after the first p of R_w, starting at order p, is consequently zero modulo pR. Since D^p is a derivation in characteristic p, we get $D^pF = \kappa_t ZF$. The n-th entry of ZF is $nH_{n-1}(F)$, giving (66.8). Apply it at $n = j(p+1) - p$ and use $j(p+1) - p \equiv j \bmod p$, starting with $F_0(0) = 1$. This gives the factorial congruence. Finally the derivation D^p kills Z, so iterating it p times gives $D^{p^2}F = \kappa_t^p Z^p F = 0$ modulo pR. □

Corollary 66.14 (Failure of a scalar integral frame for this germ)**.** *At every such inert prime the analytically normalized $\Theta_t(z)$, expressed in a good elliptic formal parameter, does not belong to its integral power series ring. Multiplication by any unit in that ring preserves this obstruction.*

Proof. For an integral scalar series every derivative of order at least p is zero modulo pR, by the first part of Lemma 66.12. The order $p+1$ of Θ_t has unit value by Theorem 66.13. Finally a unit and its inverse both preserve the integral power series ring. □

This calculation takes place on the elliptic curve underlying the same class kernels as in Theorem 66.9. It explains why the scalar integral-section estimates in this section cannot be applied directly to the analytic germ of the prescribed vacuum. Equation (66.8) gives a comparison in its actual Hermitian frame.

66.5 Higher powers at an inert prime

Keep the elliptic curve, mark, invariant differential and Hermitian normalization of Theorem 66.13. Write Z for the additive coordinate in which this differential is dZ. For $n \geq 0$ put

$$F_p(n) = v_p(n!) = \sum_{a \geq 1} \lfloor n/p^a \rfloor, \qquad \omega_p = \frac{p}{p^2 - 1}.$$

Throughout, $v_p(0) = +\infty$. We first locate the coefficient of the logarithm which determines the radius of the normalized theta function. All valuations are taken with $v_p(p) = 1$.

Lemma 66.15 (The lowest coefficients of the scaled logarithm)**.** *Put $L_j = (d/dZ)^j \log \Theta_t(0)$, meaning the derivative at zero of the formal logarithm with constant term zero. The odd L_j vanish. For each even $j \geq 2$ set $h_j = \lfloor (j-2)/p \rfloor$. Then $L_j \in p^{h_j} R$, L_{p+1} is a unit, and*

$$h_j - F_p(j) + j\omega_p \;\geq\; \frac{1}{p-1}. \tag{66.9}$$

Equality in the numerical inequality occurs exactly at $j = p+1$.

Proof. Near the marked point, $g = -u_\Lambda - x$ is an integral regular germ and $L_j = (\partial^{j-2} g)(t)$. This follows by differentiating $(\log \Theta_t)''(Z) = -u_\Lambda - x(Z+t)$. The invariant derivation preserves the completed local ring at t. Lemma 66.12 gives $\partial^p R[[T]] \subset pR[[T]]$ in a parameter there. By R-linearity, each block of p derivatives gains a factor of p. The parity follows from evenness, and $L_{p+1} = \kappa_t$ is the unit in the same lemma.

If $2 \leq j < p$, then $F_p(j) = 0$ and $2\omega_p > 1/(p-1)$. For $p+1 \leq j < 2p$ we have $F_p(j) = 1$ and $(p+1)\omega_p - 1 = 1/(p-1)$. For $j \geq 2p$, the base-p digit formula gives $F_p(j) \leq (j-1)/(p-1)$. Also

$$h_j \geq (j - p - 1)/p > j/(p^2 - 1).$$

The last strict inequality holds at $j = 2p$ for $p \geq 5$, and the left side increases faster thereafter. Using $1/(p-1) - \omega_p = 1/(p^2-1)$ proves the strict inequality in this range. □

Theorem 66.16 (Valuations and the radius of the elliptic theta series)**.** *For every prime-to-p torsion point w, including zero, and every $n \geq 0$, the undivided derivatives in the analytic frame satisfy*

$$v_p\big(H_n(U_w\Theta_t)\big) \ \geq \max\{0, F_p(n) - \lfloor \omega_p n \rfloor\}. \tag{66.10}$$

For the marked section itself, put $n_e = (p+1)p^e$, $e \geq 0$. Then

$$v_p\big(H_{n_e}(\Theta_t)\big) = \frac{p^e - 1}{p - 1}. \tag{66.11}$$

In particular its ordinary Taylor series in Z, over the completed algebraic closure of $\mathbb{Q}_p$ with $|p|_p = p^{-1}$, has radius $p^{-\omega_p}$.

Proof. Let $A = \log \Theta_t$. Its constant term is zero and its first possible degree is two. The coefficient of Z^n in $\exp A$ is a finite sum over multiplicities $m_j \geq 0$ with $\sum j m_j = n$, indexed by even $j \geq 2$. The valuation of each summand is at least the integer

$$I = \sum_j m_j(h_j - F_p(j)) - \sum_j F_p(m_j).$$

By (66.9) and $F_p(m) \leq m/(p-1)$, we have $I \geq -\omega_p n$. Thus every summand belongs to $p^{-\lfloor \omega_p n \rfloor} R$, even if R is ramified. Multiplying the coefficient by $n!$ and using the integrality of undivided derivatives in Theorem 66.13 gives (66.10) for $w = 0$.

For a translate write $U_w\Theta_t = R_w\Theta_t$. Theorem 65.6 constructs R_w as an integral series in a good elliptic parameter. It follows from the same block of p derivatives that $v_p(R_w^{(j)}(0)) \geq \lfloor j/p \rfloor$. If $j < p$, $F_p(j) = 0$. For $j \geq p$, putting $a = \lfloor j/p \rfloor$ gives $j \leq pa + p - 1 \leq (2p-1)a \leq (p^2-1)a$. Therefore

$$F_p(j) - \lfloor j/p \rfloor \leq j/(p-1) - j/(p^2-1) = \omega_p j.$$

Its left side is an integer. Coefficient multiplication now gives the same denominator bound for the product, since $\lfloor \omega_p j \rfloor + \lfloor \omega_p (n-j) \rfloor \leq \lfloor \omega_p n \rfloor$. The integrality of the undivided derivatives of the translate completes this part of the proof.

For equality, make a finite extension containing elements a, b of valuations $\omega_p, 1/(p-1)$, respectively. Set $U(Z) = b^{-1}A(aZ)$. By Lemma 66.15 its coefficients are integral and its reduction modulo the maximal ideal is exactly cZ^{p+1} for a nonzero residue c. The equality assertion in that lemma and the unit value of L_{p+1} are both used here. For $m > 0$ the valuation of $b^m/m!$ is $s_p(m)/(p-1)$, where $s_p(m)$ is the sum of the base-p digits. This follows by summing the floors in $F_p(m)$. In degree n_e, expand $\Theta_t(aZ) = \sum_m b^m U(Z)^m/m!$. Only finitely many m occur in this coefficient. A term of valuation $1/(p-1)$ requires m to be a power of p and the coefficient of Z^{n_e} in U^m to be a unit. Its reduction is determined by $c^m Z^{(p+1)m}$, so precisely $m = p^e$ gives that valuation. All other terms have strictly larger valuation. Undoing the scale gives

$$v_p\big(H_{n_e}(\Theta_t)\big) = F_p(n_e) - \omega_p n_e + \frac{1}{p-1}.$$

Here $s_p(n_e) = 2$, which gives (66.11). The lower bound for all ordinary coefficients and equality on this unbounded sequence give $\liminf_{n\to\infty} n^{-1} v_p([Z^n]\Theta_t) = -\omega_p$. The nonarchimedean root test proves the radius claim. □

For example H_{p+1} is a unit, $H_{p(p+1)}$ has valuation one, and $H_{p^2(p+1)}$ has valuation $p+1$. The units and the higher powers occur in the same normalization that defines the archimedean kernel in Theorem 66.9. In several variables an integral change of coordinates preserves an ordinary coefficient bound in the total degree. In contrast, the factorial recovered on taking a derivative depends on the separate coordinate orders.

66.6 Odd powers of Frobenius in the class-section derivatives

Use the data of Sections 65.5–65.9. Fix x in the common interval, one set S of the indicated inert primes and the one elliptic product basis integral at all of them. For $p \in S$ put

$$F_{p^2}(n) = \sum_{j\ge 1} \lfloor n/p^{2j} \rfloor, \qquad B_p(n) = F_p(n) - F_{p^2}(n) = \sum_{j\ge 1,\ j \text{ odd}} \lfloor n/p^j \rfloor.$$

Let Σ be the CM embeddings over $K = \mathbb{Q}(\sqrt{-d})$; arithmetic Frobenius σ_p and complex conjugation c_E give a permutation $\pi = \sigma_p c_E$ of Σ. Each even cycle of π splits into two orbits under π^2. We call these its two halves. For example when K_q splits at p, π interchanges the two restrictions of embeddings to K_q, since c_E acts there as conjugation. In this case every cycle is even.

Lemma 66.17 (Elliptic parameters and a logarithmic derivative)**.** *Let $c_{i\nu} \in R$ and $u_i = \sum_\nu c_{i\nu} Z_\nu$. For an integral germ H in the elliptic parameters T_i the ordinary coefficient of Z^β in $H(T(u_1), \dots, T(u_n))$ has valuation at least $-\sum_\nu F_{p^2}(\beta_\nu)$. Put $\ell = (\log \Theta_{t_*})'$. For one integral linear form u the coefficient of Z^β in $\ell(u)$, for $\beta \neq 0$, has valuation at least*

$$-\sum_\nu F_{p^2}(\beta_\nu) - \min_{\nu:\,\beta_\nu>0} \#\{j \ge 1 :\ j \text{ odd},\ p^j \mid \beta_\nu\}. \tag{66.12}$$

Its constant coefficient vanishes.

Proof. The formal exponential in an integral elliptic parameter with unit linear coefficient has $v_p([Z^m]T(Z)) \ge -F_{p^2}(m)$. We recall the hypotheses of the factorial argument in Lemma 64.4. The formal CM endomorphisms extend from $\mathcal{O}_K$ to $O = \mathcal{O}_{K_p}$ by coefficientwise approximation, as in Corollary 65.28. Choose a parameter of linear coefficient one and average $\zeta^{-1}[\zeta](T)$ over $\zeta \in \mu_{p^2-1} \subset O^\times$, dividing by p^2-1. This gives an integral change with linear coefficient one in which these roots of unity act linearly. Commutation with them forces the first possible nonlinear degree in $[p](T)$ to be p^2. The cited lemma gives the coefficient bound in this coordinate. The functions F_p, F_{p^2}, B_p are superadditive on nonnegative integers, by the floor formulas; in particular integral postcomposition preserves the bound for $T(Z)$. Translation of an integral regular germ at the mark to the origin also gives an integral elliptic germ.

For a monomial of degree $m = |\beta|$ obtained from u^m, the multinomial coefficient adds valuation $F_p(m) - \sum_\nu F_p(\beta_\nu)$. Superadditivity of B_p gives the required lower bound for each $T(u_i)$. Products preserve the bound since each F_{p^2} is superadditive. In any fixed degree only finitely many terms of H enter.

Now $\ell(0) = 0$ and $\ell' = -u_\Lambda - x(Z + t_*)$ is an integral elliptic germ. Consequently $v_p(\ell^{(m)}(0)) \ge B_p(m-1)$ for $m \ge 1$, by the first assertion for this one-variable germ followed by multiplication by $(m-1)!$. For each $\beta_\nu > 0$, write $m-1$ as the sum of the coordinates of $\beta - e_\nu$. Superadditivity gives

$$B_p(m-1) \ge \sum_\mu B_p(\beta_\mu) - \big(B_p(\beta_\nu) - B_p(\beta_\nu - 1)\big).$$

The difference in parentheses counts the odd j with $p^j \mid \beta_\nu$. The coefficient after linear substitution is $\ell^{(m)}(0) c^\beta/\beta!$, which proves (66.12). □

Write $[y]_+ = \max(0, y)$. A matrix coordinate at τ has indices (τ, i, j), with row i and column j. For every even cycle C, and separately for every pair i, j, choose one half H of C and write $L = C \setminus H$. In each expression below, H, L refer to that choice in the indicated block.

Theorem 66.18 (Valuations on the two halves of a Frobenius cycle)**.** *Let F_{ch} be any of the prescribed single-lift class sections in the matrix coordinates. At every place over the chosen p and for every multi-index α, one has*

$$v_p(\partial^\alpha F_{ch}(0)) \ \geq \sum_{i,j} \sum_{C \text{ even}} \sum_{a\geq 1,\ a \text{ odd}} \left[\sum_{\tau\in H} \left\lfloor \frac{\alpha_{\tau ij}}{p^a} \right\rfloor - \sum_{\tau\in L} \alpha_{\tau ij} \right]_+ . \tag{66.13}$$

All choices of halves are allowed in this inequality.

Proof. First decompose the trace lattice at p. The local lattice of the standard vacuum is a copy of $(\mathcal{O}_E \otimes \mathbb{Z}_p)^{rs}$, since E is unramified and the relative different is a unit at p. The chosen orthonormal basis over K gives an integral basis with integral inverse here. The factors of $\mathcal{O}_E \otimes \mathbb{Z}_p$, as an O-algebra, correspond to orbits of $\sigma_p^2 = \pi^2$ on Σ. Indeed $K_p/\mathbb{Q}_p$ is unramified quadratic and its arithmetic Frobenius acts on these embeddings by σ_p^2. After unramified base change splitting E, the homomorphism given by the embeddings identifies each local factor with the product of the coordinate rings in its orbit. This follows from the factorization of a separable residue polynomial and Hensel lifting, or from the integral splitting of a finite unramified algebra. Thus a basis of each local factor gives an invertible integral coordinate change between it and the corresponding matrix variables after that extension.

For fixed i, j, a cycle of π gives an orthogonal block for the trace Hermitian form. On an even cycle its two orbit lattices are isotropic and pair with each other. In fact the form pairs a local field factor only with its conjugate factor. Complex conjugation takes the π^2-orbit to the orbit described on Σ by $\sigma_p c_E = \pi$: the extra Frobenius returns to the fixed embedding of K and fixes the place of the normal extension E. Equivalently for $y \in E$, one has $\tau(c_E y) = \sigma_p^{-1}((\pi\tau)(y))$; substituting this identity in the trace pairing verifies the claim. Distinct matrix entries are orthogonal by the matrix trace.

Choose O-bases of all these orbit lattices, adjoining the two bases within each even block. Write the full matrix of columns in the original elliptic product basis as A; it and its inverse are integral over O. If u denotes the new variables, the product vacuum is $G_A(u) = \prod_i \Theta_{t_*}((Au)_i)$. For a cycle block b consisting of one cycle and one matrix entry, let A_b denote its columns, and write u_b for its variables. Orthogonality says that the Gram matrix of A is the sum of those of the matrices A_b extended by zero outside their own columns. By Theorem 65.27 and Corollary 65.28, the actual section has the factorization

$$F_{ch} = U(T(u)) \prod_b G_{A_b}(u_b), \qquad U \in R[[T_1, \dots, T_D]].$$

Here $D = rs[E : K]$. Each block factor, after the variables in the unchosen half of an even block are set to zero, is an integral elliptic unit. This follows from the zero Gram matrix on the chosen half and the same theorem. The basis change from u to the matrix variables and its inverse preserve each π^2-orbit and are integral after the unramified extension just described.

Differentiate first in all variables of the unchosen halves and in all the variables of the odd cycles, to their prescribed orders. On U any such derivative is an integral linear combination of the invariant derivatives in the elliptic parameters, so it preserves integrality. On an even block write $\ell = (\log \Theta_{t_*})'$. Differentiating its factor once multiplies it by an integral linear combination of $\ell((A_b u_b)_i)$. Successive differentiations of these logarithmic derivatives contribute integral elliptic germs, because ℓ' is such a germ and each row of A_b is over O. Iterating the product rule gives terms with at most $l_b = \sum_{\tau\in L} \alpha_{\tau ij}$ factors of ℓ from this block, times the original G_{A_b} and integral elliptic germs. On an odd block every undivided derivative of G_{A_b} at zero is integral, by Theorem 66.13 and the integral linear change of variables.

Set all the differentiated variables to zero. Every remaining term is now an integral elliptic germ in the chosen halves times at most l_b factors of ℓ in the variables of each even block b. The arguments of these factors are integral linear forms in the matrix variables of that block. Apply Lemma 66.17 and extract the coefficient in the remaining coordinates. The ordinary factorial denominator from all factors together is bounded by $\sum_{b,\tau\in H} F_{p^2}(\alpha_{\tau ij})$, by superadditivity. For fixed odd a, an ℓ-factor contributes one additional unit of denominator in (66.12) at this level only if all its positive monomial exponents are divisible by p^a. It then consumes at least p^a in one chosen coordinate. Since the total in each coordinate is prescribed, the number of such factors is at most

$$\min\left(l_b,\ \sum_{\tau\in H}\lfloor \alpha_{\tau ij}/p^a\rfloor\right).$$

No zero-degree ℓ-factor contributes. Finally multiply by the factorials of the remaining coordinate orders to recover their undivided derivative. Subtraction of the F_{p^2} terms leaves $\sum B_p(\alpha_{\tau ij})$. Subtracting the last display, level by level in each block, gives (66.13). This argument applies to every summand, hence to the full derivative. □

Corollary 66.19 (Truncated prime-power terms in the minor projections)**.** *Put* $d_P(b,s)=\max(0,\lceil (b-s(P-1))/P\rceil)$. *For each even cycle* C *write* C^+, C^- *for its halves. At every place over* p, *the valuation of every actual* $P_T(\partial)F_{ch}(0)$ *and of every* $A_r v_{h,T}$ *is at least*

$$t_p = r\sum_{C\ \text{even}}\ \max_{e\in\{+,-\}}\ \sum_{a\ge 1,\ a\ \text{odd}}\left[\sum_{\tau\in C^e} d_{p^a}(b_\tau,s)-\sum_{\tau\in C^{-e}} b_\tau\right]_+. \tag{66.14}$$

Here $-e$ *denotes the opposite half. The valuation of* $Y=A_sA_r^2\mathcal{N}$ *is at least* $2t_p$. *The lower bound in Theorem 65.20, holds with* m_p *replaced at each prime by* $\max(m_p,t_p)$ *on the same interval.*

Proof. In one column each minor monomial has row sum b_τ at τ. Its sum of quotients on division by P is at least $d_P(b_\tau,s)$, by bounding the s remainders by $P-1$. Choose in every row and column the same orientation of a given cycle that maximizes (66.14). For each level sum the positive parts of (66.13) over rows, using $\sum_i[y_i]_+\ge[\sum_i y_i]_+$. The other half has row sum exactly $\sum_{\tau\in C^{-e}} b_\tau$. Sum over the r columns and the cycles, then take the integral linear combination specified by the minors. Class summation with the cleared weights and complex conjugation at all places over p give the result for Y, as in Theorem 65.20. □

For a two-element cycle, one row and one column, the formula contains $\sum_{a\ \text{odd}}[\lfloor b_+/p^a\rfloor - b_-]_+$. The term at $a=1$ can therefore have order b_+/p, and the higher odd powers retain the same cutoff. Formula (66.14) depends on the actual weights in a single lift. For the full period argument one must still sum the gains after the prescribed maps, compare the resulting nonzero Bessel projection with its archimedean norm, and establish the odd-primary length estimate on these fields.

The supplied source uses a Gram identity to pass to an isotropic family and to a pair of dual isotropic families in `Formalism/SharpRestriction/GlobalSchurBounds/GlobalRankLatticeProofs/UnitTraceSumBounds/PhIsotropicOf.lean`, line 127 and line 132 of that file. The reduction in a dual basis is spelled out in `Formalism/PeriodIntegrals/UnitaryGroupMassFormula/DualGramSubstitution/PhDualGramMain.lean`, line 11. The proof above uses the Gram comparison of Section 65.6 and counts the logarithmic derivatives directly.

66.7 Exact coefficients at the odd powers of Frobenius

Keep a good prime $p \geq 5$ from Theorem 66.18. Put $Q_2 = p^2$, $F_{Q_2}(n) = \sum_{i \geq 1} \lfloor n/Q_2^i \rfloor$ and $\lambda(z) = (\log \Theta_{t_*})'(z)$. Write $g_m = [z^m]\lambda(z)$. For the marked elliptic curve the possible exceptions in Lemma 66.22 can all be evaluated in the same additive coordinate.

Theorem 66.20 (The exceptional coefficients of the marked theta)**.** *For every $i \geq 0$, putting $m = p^{2i+1}$, one has*

$$v_p(g_m) = -F_{Q_2}(m) - 1.$$

For every other positive m, $v_p(g_m) \geq -F_{Q_2}(m)$.

Proof. The second assertion was proved in Lemma 66.22, using the integral elliptic germ $\lambda(u+v)-\lambda(u)-\lambda(v)$. Iterate this addition identity with $u = jz$, $v = z$ for $1 \leq j < p$. Multiplication by any integer is an integral endomorphism of the elliptic formal group. Thus

$$\lambda(pz) - p\lambda(z) = S(T(z))$$

with S an integral series in an elliptic parameter T. Use the parameter in Lemma 64.5, with linear coefficient one. Its inverse under composition is integral through degree p, because the ordinary coefficients of $T(z)$ through that degree are integral by Lemma 66.17. The coefficient in degree m of the left side is $(p^m - p)g_m$. All coefficients in degrees $m < p$ are in pR, including the zero constant term. In degree p the coefficient is a unit, since $p!g_p = \kappa_{t_*}$ by Lemma 66.12 and $(\log \Theta_{t_*})'' = -u_\Lambda - x(z + t_*)$. Composition with the inverse parameter shows that the coefficients of S below degree p lie in pR and $S_p = [T^p]S$ is a unit.

Adjoin ρ with $\rho^{Q_2-1} = p$, and reduce modulo the maximal ideal using a bar. Lemma 64.5 gives

$$H(Z) = T(\rho Z)/\rho \text{ integral}, \qquad \overline{H}(Z) = \sum_{i \geq 0} h_i Z^{Q_2^i}, \qquad h_i \neq 0.$$

This follows from the multiplication-by-p series. In the chosen parameter it begins with $pT + b_{Q_2}T^{Q_2}$, where b_{Q_2} is a unit. Rescaling its exponential identity and reducing gives $Z = \overline{H} + \overline{b}_{Q_2}\overline{H}^{Q_2}$, whose successive coefficients give the displayed series. On substituting $z = \rho Z$, the reduction of $\rho^{-p}S(T(\rho Z))$ is $\overline{S}_p\,\overline{H}^p$. Indeed the coefficients of S below p are divisible by $p = \rho^{Q_2-1}$, and the terms above p are multiplied by positive powers of ρ.

All coefficients of $\rho^{-p}\lambda(p\rho Z)$ have positive valuation. For $m = 1$ this follows by integrality of g_1. For $m \geq 2$ use $F_{Q_2}(m) \leq m/(Q_2 - 1)$ and the bound $v_p(g_m) \geq -F_{Q_2}(m) - 1$ from Volume XIII. After the substitution the valuation is at least $m - 1 - p/(Q_2 - 1) > 0$. Consequently

$$\overline{p\rho^{-p}\lambda(\rho Z)} = -\overline{S}_p \sum_{i \geq 0} h_i^p Z^{pQ_2^i}.$$

Every displayed coefficient is nonzero. At $m = pQ_2^i$, $(m-p)/(Q_2-1) = F_{Q_2}(m)$. Undoing the scale proves the first assertion. □

Corollary 66.21 (A mixed derivative which detects the individual translate)**.** *In one matrix entry let ν, μ lie in opposite halves of an even cycle and $\pi = \sigma_p c_E$. For $m = p^{2i+1}$ put $u_i = p^{F_{Q_2}(m)+1}g_m$, a unit. If F is any of the class sections of Section 65.5, then*

$$\frac{p^{F_{Q_2}(m)+1}}{m!}\,(\partial_\nu^m \partial_\mu F)(0) \equiv u_i F(0)\,\mathbf{1}_{\{\mu = \pi^{2i+1}\nu\}} \pmod{pR}.$$

In particular if $F(0)$ is a unit, the indicated derivative has valuation $v_p(m!) - F_{Q_2}(m) - 1$ at the matching translate and at least $v_p(m!) - F_{Q_2}(m)$ at every other such μ. This holds in particular for the original product vacuum in its orthonormal elliptic coordinates, expressed in the matrix variables.

Proof. On the line $Z_\nu = z$ with all other variables zero, write $A(z)$ for the restriction of F. The factorization in Theorem 66.24, and the product rule give

$$(\partial_\mu F)|_\nu = B(z) + A(z)\sum_k \overline{V}_{\mu k}\lambda(\overline{V}_{\nu k}z).$$

The coefficients of both A and B in degree n have valuation at least $-F_{Q_2}(n)$. For A use isotropy of the chosen half. For B the derivative falls on the integral factor of the block decomposition, and the same restriction applies. These statements also apply directly to the product vacuum, whose value at zero is one.

Multiply the degree m coefficient by $p^{F_{Q_2}(m)+1}$. The term from B and every nonexceptional coefficient in the product vanish modulo pR by superadditivity. If an exceptional coefficient has degree $n = pQ_2^a < m$, the floor at Q_2^{a+1} in $F_{Q_2}(m)$ is strictly larger than the sum of the corresponding floors at n and $m-n$. Indeed $0 < n < Q_2^{a+1}$ and m is divisible by Q_2^{a+1}. That factor of p also makes the term vanish modulo pR. Only $n = m$ remains. Its multiplier is $A(0)$ times the row pairing $\sum_k \overline{V}_{\mu k}\overline{V}^{\,m}_{\nu k}$, which is the stated Kronecker symbol modulo pR by Lemma 66.23. Finally multiplication by $m!$ converts the coefficient into the undivided derivative. □

66.8 Individual Frobenius translates in the theta derivatives

Fix a good prime $p \geq 5$ inert in $K = \mathbb{Q}(\sqrt{-d})$ and unramified in E. Keep the marked even elliptic theta function $\vartheta = \Theta_{t_*}$, the single-step class sections F_{ch} and their matrix coordinates Z_ν from Section 65.5. Write $T(z)$ for the good elliptic parameter in additive coordinate z, normalized to have linear coefficient one. Put

$$Q_2 = p^2, \qquad F_{Q_2}(n) = \sum_{i\geq 1}\lfloor n/Q_2^i\rfloor, \qquad \lambda(z) = \vartheta'(z)/\vartheta(z).$$

All valuations assign one to p. We first determine where a coefficient of λ can have a larger denominator than an integral function of T. This will identify the low direction responsible for each possible loss in a mixed derivative.

Lemma 66.22 (The addition formula and the exceptional degrees)**.** *The difference $\lambda(u+v)-\lambda(u)-\lambda(v)$ is an integral germ in $T(u), T(v)$. If $g_m = [z^m]\lambda(z)$ and $m > 0$, then*

$$v_p(g_m) \;\geq\; -F_{Q_2}(m) - \mathbf{1}_{\{m=p^j \text{ for an odd } j\geq 1\}}. \tag{66.15}$$

Here $g_0 = 0$.

Proof. Consider the germ

$$U(u,v,w) = \frac{\vartheta(u+v+w)\vartheta(u)\vartheta(v)\vartheta(w)}{\vartheta(u+v)\vartheta(u+w)\vartheta(v+w)}.$$

The signed sum of the seven row Gram matrices is zero. Each diagonal entry occurs twice with either sign and each off-diagonal entry occurs once with either sign. Lemma 65.26 therefore makes U a unit in the integral elliptic parameters. The invariant derivative in the third elliptic variable preserves the ring of integral germs. Divide that derivative of U by U and put $w = 0$. Evenness gives $\lambda(0) = 0$, and logarithmic differentiation gives exactly the difference asserted. This three-variable quotient is the local theta expression for the theorem of the cube. See J. S. Milne, *Abelian Varieties*, the section on the theorem of the cube.

The coefficient of $u^k v^{m-k}$ in this difference is $\binom{m}{k}g_m$ for $0 < k < m$. An integral elliptic germ has coefficient valuation at least $-F_{Q_2}(k) - F_{Q_2}(m-k)$ there. Indeed the formal exponential

in a good parameter has degree n coefficient of valuation at least $-F_{Q_2}(n)$, and the floor sum is superadditive. The formal-exponential bound and its invariance under integral change of parameter are proved in Lemma 66.17.

If $m > 1$ is not a power of p, choose $k = p^a < m$ at a nonzero base-p digit of m. The subtraction $m - k$ uses no borrow. Legendre's factorial formula gives $v_p\binom{m}{k} = 0$, and $F_{Q_2}(k) + F_{Q_2}(m-k) = F_{Q_2}(m)$. If $m = p^j$, $j \geq 1$, take $k = p^{j-1}$. There is exactly one carry in the addition, across the boundary p^j. The binomial valuation is one, and the difference $F_{Q_2}(m) - F_{Q_2}(k) - F_{Q_2}(m-k)$ equals one for even j and zero for odd j. This gives (66.15). For $m = 1$, $\lambda'(0) = -u_\Lambda - x(t_*)$ is integral by good reduction at the mark. □

Call a series in a finite set of additive variables Z_ν bounded by the elliptic factorials if its coefficient of Z^β has valuation at least $-\sum_\nu F_{Q_2}(\beta_\nu)$. This condition is preserved by sums and products. It holds for every integral elliptic germ evaluated at $T(L_i(Z))$ for integral linear forms L_i, even with coefficients in an extension of $\mathcal{O}_{K_p}$. In fact the multinomial valuation in L_i^m is $v_p(m!) - \sum_\nu v_p(\beta_\nu!)$. The difference $v_p(n!) - F_{Q_2}(n)$ is superadditive, which gives the stated bound after substitution and multiplication.

Let $\pi = \sigma_p c_E$ act on the embedding index and fix each matrix entry. On an even cycle of this permutation the two orbits of π^2 are denoted by H, L, in either order. Fix one matrix entry in that cycle. Write $c_{\nu i} = \overline{V}_{\nu i}$ for the entries of the change of coordinates $z_i = \sum_\nu c_{\nu i} Z_\nu$ of Section 65.5; the embedding and matrix-entry labels are combined in ν. For $\mu \in L$ define

$$E_\mu(Z_H) = \sum_i c_{\mu i} \lambda\left(\sum_{\nu \in H} c_{\nu i} Z_\nu \right).$$

Lemma 66.23 (The coefficient attached to a specified translate)**.** *The coefficients of E_μ satisfy the elliptic factorial bound, with a possible further loss of one exactly in the following list of positions:*

$$\beta = p^j e_\nu, \qquad j \geq 1 \text{ odd}, \quad \nu \in H, \quad \pi^j \nu = \mu.$$

At each listed position the valuation is at least $-F_{Q_2}(p^j) - 1$.

Proof. Apply the addition formula in Lemma 66.22 to each linear form one summand at a time. The difference between E_μ and $\sum_{\nu,i} c_{\mu i} \lambda(c_{\nu i} Z_\nu)$ satisfies the elliptic factorial bound by integral substitution as above. This treats every coefficient involving two different variables. By (66.15), the remaining possible exception is the pure coefficient at $m = p^j$, j odd. Its multiplier of g_m is

$$\sum_i c_{\mu i} c_{\nu i}^{p^j} \equiv \sum_i \overline{V}_{\mu i} V_{\pi^j \nu, i} = \mathbf{1}_{\{\mu = \pi^j \nu\}} \pmod p.$$

The elements of E in this formula are integral in an unramified local ring at p. Raising to p^j modulo p acts there by σ_p^j. Since j is odd, $\sigma_p^j c_E = \pi^j$. The last equality is row orthogonality $VV^* = 1$. In particular the congruence takes place modulo p itself after any extension of coefficients. When the indices differ it supplies the full missing factor. □

Theorem 66.24 (Divisibility at each odd translate of Frobenius)**.** *In each matrix entry and each even cycle choose a half H. For any multi-index α, at every place over p one has*

$$v_p(\partial^\alpha F_{ch}(0)) \;\geq\; \sum_{\text{entries}} \sum_{C \text{ even}} \sum_{\nu \in H} \sum_{j \geq 1,\ j \text{ odd}} \left[\left\lfloor \frac{\alpha_\nu}{p^j} \right\rfloor - \alpha_{\pi^j \nu} \right]_+ . \tag{66.16}$$

Here ν includes the matrix entry in the outer sum and $[u]_+ = \max(u, 0)$. The same choice of basis and vacuum works at any finite set of the indicated primes.

Proof. Use the integral splitting of the trace lattice in the proof of Theorem 66.18. For clarity, at p the local field factors correspond to the orbits of π^2 in the embeddings. Hermitian duality pairs the two factors in an even cycle, each of which is isotropic. Different cycles and different matrix entries are orthogonal. Choosing integral bases in the local factors, write A_b for the columns of the resulting change of basis in block b. The block here consists of one matrix entry and one cycle. Corollary 65.28 and Theorem 65.27 express F_{ch} as an integral elliptic germ times $\prod_b G_{A_b}(u_b)$. Indeed the full Gram matrix is the sum of its orthogonal block Gram matrices. Each block vacuum on the chosen isotropic half alone is an integral elliptic unit by the same theorem. Passing from a factor basis to its embedding variables is an integral linear substitution in the additive variables. A matrix vector supported on one block has original product coordinates $\sum_{\nu\in b} c_{\nu i} Z_\nu$ in position i.

Apply all derivatives in L and in the odd cycles before extracting coefficients in the chosen halves. For an even block the first logarithmic derivative in direction $\mu \in L$, restricted to H, is precisely E_μ. A logarithmic derivative of order at least two is integral in the local elliptic parameters before passing to embedding coordinates. In fact $\lambda'(z) = -u_\Lambda - x(z + t_*)$ is an integral elliptic germ. Its further invariant derivatives are integral, and the rows of A_b have entries in $\mathcal{O}_{K_p}$, which act integrally on the elliptic formal group. The scalar coefficients introduced by differentiation in embedding directions are integral. The same differentiation of the initial integral factor also preserves integrality. Derivatives of odd block vacua evaluated at zero are integral by Theorem 65.15's undivided-derivative argument for products of marked elliptic thetas.

By the product rule, after setting the differentiated variables to zero, every term is a series satisfying the elliptic factorial bound times a product of E_μ's. There are at most α_μ such factors bearing a given label μ. Indeed each requires one of the derivatives in that direction to act on a block vacuum as a singleton, and an additional derivative on that singleton makes it an integral factor. Any multiplicities from the product rule are integers.

Extract the coefficient of the prescribed monomial in the remaining variables. Superadditivity bounds the common factorial denominator by $\sum_{b,\nu\in H} F_{Q_2}(\alpha_\nu)$. For fixed (ν, j) an exceptional factor must use exactly p^j powers of Z_ν and bear the label $\pi^j\nu$, by Lemma 66.23. Thus it can occur at most $\min(\lfloor \alpha_\nu/p^j \rfloor, \alpha_{\pi^j\nu})$ times. Each such occurrence costs at most one further power of p. On multiplying by the factorials of the remaining orders, the difference $v_p(\alpha_\nu!) - F_{Q_2}(\alpha_\nu)$ is the sum of $\lfloor \alpha_\nu/p^j \rfloor$ over odd j. Subtracting the exceptional losses gives (66.16) in each term, hence in their sum. Lemma 65.14 gives the common basis. □

The source uses two-variable series in a height-two formal group and an odd-power formula in `Formalism/SharpRestriction/GlobalSchurBounds/GL3Theta.lean`, line 382. The calculation above derives the bound directly in the additive coordinates of the marked analytic theta function.

66.9 One minor projection for the translates at primes split in the second field

We apply Section 66.8 on the common intervals of Section 6.6. Write $K_d = \mathbb{Q}(\sqrt{-d})$, $K_q = \mathbb{Q}(\sqrt{-q})$, and $\Phi = \mathrm{Gal}(E/K_d)$. In the coordinates of Theorem 6.23, with the correction for an odd ψ specified there, complex conjugation c_E reverses both quadratic signs. We use only the signs themselves in the proof. Decompose $\Phi = \Phi_0 \sqcup \Phi_1$ according as an embedding fixes K_q or acts on it by conjugation. Their sizes are equal to n. Put the high orders a_t at the embeddings $t \in T \subset \Phi_0$, where $h = |T|$ and $|a_t - xb| \le b$. They are positive integers. The

sparse construction uses $a_t = \lceil xb \rceil$. The low thresholds w_μ equal $B' = \lceil b \rceil$ on the chosen translate of T_2 in Φ_1, of size h_2, and $W = \lceil \sqrt{b} \rceil$ everywhere else. As before $b = \exp(x^\varepsilon)$.

For a list $\mathbf{b}$ of minor degrees let $P_{\mathcal{I}}$ range over products of r-rowed determinants at the embeddings, in the s-by-r matrix variables of (65.1). Write $d_M(b,s) = \max(0, \lceil (b - s(M-1))/M \rceil)$. A place over p has $v_p(p) = 1$.

Corollary 66.25 (Frobenius translates after taking minors)**.** *At each of the good inert primes of Section 65.5, choose a half H_C in each even cycle C on the embeddings. At every place over p the valuations of $P_{\mathcal{I}}(\partial)F_{ch}(0)$ and of its corresponding cleared class coordinates $A_r v_{h',\mathcal{I}}$ are at least*

$$r \sum_{C \text{ even}} \sum_{\nu \in H_C} \sum_{j \ge 1,\ j \text{ odd}} [d_{p^j}(b_\nu, s) - b_{\pi^j \nu}]_+. \tag{66.17}$$

Proof. Use the same half in all entries of a matrix block. In any monomial of a determinant product the sum of the row exponents within each column at ν equals b_ν. The sum of their quotients on division by p^j, rounded down, is at least $d_{p^j}(b_\nu, s)$, since each of the s remainders is at most $p^j - 1$. At $\pi^j \nu$ the row exponents in the same column sum to $b_{\pi^j \nu}$. Sum (66.16) over these rows using $\sum_i [y_i]_+ \ge [\sum_i y_i]_+$. Each of the r columns gives the asserted bound. The determinant polynomials have integer coefficients. Taking their sum and taking a class sum with its integral coefficients $A_r m_c$ both preserve the bound. □

For each translate of the low thresholds use a single list

$$b_\nu = \begin{cases} a_\nu, & \nu \in T, \\ 0, & \nu \in \Phi_0 \setminus T, \\ w_\nu, & \nu \in \Phi_1. \end{cases} \tag{66.18}$$

Let $C_{\mathrm{sp}}(t, a_t, w)$ denote the contribution to $C_d(t, a_t, w)$ from Galois elements which fix K_q and act nontrivially on K_d. At ramified primes use the same inertia average as in (66.1) and the definition preceding it. Let S_{sp} consist of the unramified primes $p \ge 5$ with these two signs up to $X = \max_t a_t / W$, excluding the primes dividing the level. For a nonzero algebraic number Y in a finite Galois field J put

$$\mathcal{H}_S(Y) = \frac{\log |N_{J/\mathbb{Q}} Y|}{[J : \mathbb{Q}]} + \sum_{p \notin S} \sum_{v \mid p} \frac{[J_v : \mathbb{Q}_p]}{[J : \mathbb{Q}]} \max(0, -v_p(Y)) \log p.$$

Theorem 66.26 (Simultaneous divisibility for all high embeddings)**.** *Fix the positive split intertwiners and representatives of Theorem 66.7. Fix $r \le s$ with rs even and s bounded by a fixed power of x. There is one rational torsion input, supported at the fixed split level prime, giving nonzero squared class sums $Y_u = A_s A_r^2 \mathcal{N}_u$ simultaneously for all the lists (66.18) indexed by u. On this field and interval,*

$$\sum_{t \in T} C_{\mathrm{sp}}(t, a_t, w) \ \le \ \frac{\mathcal{H}_{S_{\mathrm{sp}}}(Y_u)}{r} + O_{\psi,\varepsilon}(hb/x). \tag{66.19}$$

The left side uses the list of low thresholds for this u. If a finite family of such lists occurs at the same definite step, it can be included in the same torsion choice.

Proof. For $p \in S_{\mathrm{sp}}$, put $\pi = \sigma_p c_E$. Its action interchanges Φ_0 and Φ_1. Therefore every cycle has even length and its intersection with Φ_0 is one entire half. Choose these halves in Corollary 66.25. For every $t \in T$ and odd j the order at $\pi^j t$ is precisely $w_{\pi^j t}$. At an unramified prime the count in these signs has the exact term $2 \log p \sum_{j \text{ odd}} [a_t / p^j - w_{\pi^j t}]_+$.

Use $d_{p^j}(a_t,s)\ge a_t/p^j-s$ in (66.17). Summing positive parts in that formula keeps every t simultaneously. At most s is lost per t and per active odd exponent. This proves divisibility before any squaring or archimedean estimate.

The cleared squared norm is a sum of products of cleared coordinates and their conjugates with integral outer weights. The lower bound just proved holds at every coefficient place over p, so it doubles on those products and holds on their sum. Theorem 66.7 applies to any finite family of minor lists, in particular (66.18). Its positive translation mean and the density of the common split torsion grid supply the nonzero numbers asserted here. At the level prime the splitting in K_d rules out a contribution. For any other unramified prime, an odd power has the two required signs precisely when the prime itself does. An even power has trivial quadratic signs.

The primes dividing $2\operatorname{cond}(\psi)$, and the prime 3, split in K_d on sufficiently distant intervals. At the remaining ramified primes q,d the normalized count per t is at most $2a_t\log p/(p-1)$, by the inertia average. Their combined contribution is $o(hb/x)$ since both primes exceed every fixed power of x on these intervals. The total rounding loss, after accounting for the square and dividing by r, is at most $2hsX\log(2X)=o(hb/x)$, since $X\asymp x\sqrt{b}$. Finally $\mathcal{H}_S(Y)$ bounds from above the normalized sum of the valuations over S, each weighted by $\log p$, by the product formula. This gives (66.19). □

Proposition 66.27 (The other sign and the cost of the lower degrees)**.** *Let $D_\rho=L'(1,\rho)/L(1,\rho)$ for a nonprincipal primitive character, and write ξ_{qd} for the primitive product of the two quadratic characters. Uniformly for $t\in T$ and u,*

$$C_d(t,a_t,w)-C_{\mathrm{sp}}(t,a_t,w)=M_{\mathrm{both}}(a_t,W)+O_{\psi,\varepsilon}(b/x),$$
$$M_{\mathrm{both}}(a,W)=\frac{a}{2}\{\log(a/W)-1-\gamma+D_{\xi_q}+D_{\xi_d}-D_{\xi_{qd}}\}. \tag{66.20}$$

The lower orders in (66.18) have the following contribution to the exact Fischer factorials of Theorem 65.1.

$$0\le\frac{1}{rh}\sum_{\mu\in\Phi_1}\log C_{r,w_\mu}\ll_{\psi,\varepsilon} bx^{9\varepsilon/8}=o(b\sqrt{x}). \tag{66.21}$$

In (66.21) the field and the sizes of T,T_2 are those of Theorem 6.29, with the optional field shortening of Proposition 6.28.

Proof. In the omitted part the Galois element g reverses both quadratic signs. Thus $t+c_E+g$ fixes K_q and its threshold is W. The sign indicator with the factor two from the count is $(1-\xi_q(g))(1-\xi_d(g))/2$. Average this identity on each inertia coset. A character trivial on inertia takes the value of its primitive Dirichlet character on the prime power. One nontrivial on inertia has average zero and the primitive character also vanishes there. Writing $Y=a_t/W$, the omitted part is consequently

$$\frac{W}{2}\{R_{\mathbf{1}}(Y)-R_{\xi_q}(Y)-R_{\xi_d}(Y)+R_{\xi_{qd}}(Y)\}.$$

Both quadratic fields are distinct and their product character is nonprincipal. Insert the linear and logarithmic main terms of equation 1.1 in the notation R_ρ,G_ρ of its explicit formula. Equivalently these main terms are $Y(\log Y-1-\gamma)$ for the principal character and $-YD_\rho$ for each of the other three. The selected-family estimate at $Y\asymp x\exp(x^\varepsilon/2)$ bounds each of the four remaining terms after multiplication by W by $O_{\psi,\varepsilon}(a_t\exp(-cx^{\varepsilon/8}))=o(b/x)$. See Lemma 7.1. This proves (66.20), including the ramified primes.

At μ the product C_{r,w_μ} contains rw_μ positive integers at most $w_\mu+r$. The sum of the w_μ over Φ_1 is $h_2B'+(n-h_2)W$. Since $h_2\le n$ and $h\ge nx^{-\varepsilon/8}/2$, division by h bounds it by $2B'x^{\varepsilon/8}$. Finally $\log(B'+r)=O_\varepsilon(x^\varepsilon)$ for the stated polynomial ranks. This proves (66.21). □

In particular the centered count at this step is bounded above by

$$\frac{\mathcal{H}_{S_{\mathrm{sp}}}(Y_u)}{r}-\sum_{t\in T}(M_d(a_t,w)-M_{\mathrm{both}}(a_t,W))+O_{\psi,\varepsilon}(hb/x).$$

The bound (66.21) accounts for one explicit factor of this arithmetic norm. The remaining upper estimate concerns the high orders, the projection, and the finite valuations outside S_{sp}. Its required precision is that of equation 6.3, after the sum over all steps.

66.10 Composing the polynomial maps through the class sums

Fix the field, CM type Φ, additive matrix coordinates, positive split intertwiners and definite class representatives of Sections 65.5 and 66.2. We first describe the map on polynomials in the square frame variables. Its coefficients will let us apply Theorem 66.24 to an entire composition.

At rank r put one r-by-r matrix X_τ at each $\tau\in\Phi$. Over an integral domain R, let $V_\lambda(R)$ consist of the polynomials homogeneous of degree $\lambda_{\tau,i}$ in column i of X_τ, invariant under adding an indeterminate multiple of any earlier column to any later one in the same matrix. At each τ the list λ_τ is a decreasing list in the weak sense of r nonnegative integers. Write $|\lambda_\tau|=\sum_i\lambda_{\tau,i}$. These are identities of polynomials in the matrix entries and in the indeterminate. Consequently $V_\lambda(R)=V_\lambda(K)\cap R[X]$ for the fraction field K.

For $r\le s$, introduce s-by-r matrices D_τ and s-by-s matrices Y_τ. Choose nonnegative integers n_τ. If F is a holomorphic theta section in the matrix coordinates, define a linear functional on the monomials in D by $J_F(D^\alpha)=\partial^\alpha F(0)$, with all derivatives undivided. It acts coefficientwise in Y. Let $Y_{\tau,[r]}$ denote the first r columns and put

$$\mathcal{T}_{F,n}(Q)(Y)=J_F\left(Q(X)\prod_{\tau\in\Phi}\det(X_\tau)^{n_\tau}\Big|_{X_\tau=D_\tau^{\mathsf{T}}Y_{\tau,[r]}}\right).\tag{66.22}$$

The transpose in this substitution is the ordinary transpose.

Proposition 66.28 (Column weights and divisibility of every coefficient)**.** *The output of* (66.22) *has column weights* $\lambda'_\tau=(\lambda_{\tau,1}+n_\tau,\dots,\lambda_{\tau,r}+n_\tau,0,\dots,0)$ *and belongs to* $V_{\lambda'}$. *Set* $B_\tau=|\lambda_\tau|+rn_\tau$, *and take* $F=F_{ch}$ *to be one of the translated class sections at a good prime* p *of Theorem 66.24. Choose one half* H_C *in each even cycle* C *of* π_p, *the same half for all matrix entries. If the coefficients of* Q *are integral at a place over* p, *every output coefficient has valuation at least*

$$g_p(\lambda,n;r,s)=\sum_{C\ \text{even}}\ \sum_{\nu\in H_C}\ \sum_{k\ge1,\ k\ \text{odd}}\max(0,L_{\nu,k},M_{\nu,k}),\tag{66.23}$$
$$L_{\nu,k}=rd_{p^k}(n_\nu,s)-B_{\pi_p^k\nu},\qquad M_{\nu,k}=d_{p^k}(B_\nu,rs)-B_{\pi_p^k\nu}.$$

Here $d_l(b,s)=\max(0,\lceil(b-s(l-1))/l\rceil)$.

Proof. Multiplication by the determinant power adds n_τ to each column degree and preserves all the column-addition identities. A column operation on the first r columns of Y_τ induces the identical one on $D_\tau^{\mathsf{T}}Y_{\tau,[r]}$. The later columns of Y_τ do not enter the expression. Taking J_F commutes with these operations, including with scaling a column by an indeterminate. This proves the asserted column conditions over the coefficient field.

Fix a monomial from Q, with row degrees $e_{\tau,i}$ at τ. Each determinant monomial has degree one in each row. Every resulting monomial in D,Y thus has degree $n_\tau+e_{\tau,i}$ in the i-th column of D_τ. Its total degree there, over all columns, is B_τ. The sum of the floors of s

nonnegative integers divided by p^k is at least $d_{p^k}(b,s)$ when their sum is b, by the bound p^k-1 on each remainder. For fixed ν,k in Theorem 66.24, first sum the positive parts over the rs entries. Subtracting all exponents at $\pi_p^k\nu$ costs exactly $B_{\pi_p^k\nu}$. Applying the floor bound in each column gives at least $L_{\nu,k}$, since $e_{\nu,i}\ge 0$. Applying it to all rs entries at once gives at least $M_{\nu,k}$. The sum of positive parts is nonnegative and bounds both quantities for this same monomial. Summing their maximum with zero proves (66.23). Expansion of the substitution introduces integer coefficients, so the bound persists in each resulting coefficient. After dividing by p^{g_p}, the polynomial is still of the asserted weights over the valuation ring by the intersection identity. □

Let the successive ranks be $N_0\le\cdots\le N_m$, with $N_{j-1}N_j$ even. Write $\mathcal{C}_j$ for the finite set of representatives at rank N_j and $m_c>0$ for the inverse stabilizer order. Choose a basis as in Lemma 65.14 at each step, integral at a prescribed finite set of good primes. For every pair at step j choose the positively normalized section $G_{ch}^{(j)}$ of Section 66.2. Apply the same translation U_{w_j} to every such pair at this step. Given an array Q_0 on $\mathcal{C}_0$, define recursively

$$Q_{j,h}(Y)=\sum_{c\in\mathcal{C}_{j-1}} m_c\,\mathcal{T}_{U_{w_j}G_{ch}^{(j)},\,n_j}(Q_{j-1,c})(Y). \tag{66.24}$$

For P_0-power torsion inputs use the corrected rational translations of Theorem 66.7. The correction multiplies the entire j-th map by one common unit complex scalar of finite order.

Theorem 66.29 (Nonvanishing through the intermediate class sums)**.** *Use one nonzero polynomial $Q_0\in V_{\lambda_0}(\overline{\mathbb{Q}})$ at every initial class. For any finite set of such polynomials, degree lists and target classes, there is one tuple of rational translations, supported at the fixed split prime P_0 as in Section 66.2, for which all the values $Q_{m,h}(I)$ in (66.24) are nonzero and algebraic. Here I is the identity frame at every embedding. Put $A_N=|\mathrm{GL}_{N[E:\mathbb{Q}]}(\mathbb{F}_3)|$ and $a_{\mathrm{cl}}=\prod_{j=1}^m A_{N_{j-1}}$. If Q_0 is integral at the chosen coefficient places, then*

$$v_p\big(a_{\mathrm{cl}}Q_{m,h}(I)\big)\ \ge\ \sum_{j=1}^{m} g_p(\lambda_{j-1},n_j;N_{j-1},N_j)$$

at each such place. The successive λ_j are obtained by the column-weight rule of Proposition 66.28.

Proof. Fix one of the data sets and a terminal class h. At each step use a common period lattice Γ_j for its finitely many sections, as in Section 66.2. On the product of the resulting tori form the section

$$\mathcal{G}_h=\sum_{c_0,\dots,c_{m-1}}\left(\prod_{j=1}^m m_{c_{j-1}}\right)\bigotimes_{j=1}^m G_{c_{j-1}c_j}^{(j)},\qquad c_m=h.$$

In the proof of Proposition 66.6 the overlap of each pair section with its step's unshifted vacuum $G_{0,j}$ is $\|G_{0,j}\|^2 n_{ch}^{-1/2}>0$. Pairing $\mathcal{G}_h$ with the tensor of these vacua gives a sum of products of positive numbers, by product integration. In particular $\mathcal{G}_h\neq 0$.

Set $X_{m,\tau}=I$ and work backwards with symbolic matrices $X_{j-1,\tau}=D_{j,\tau}^{\mathsf{T}}X_{j,\tau,[N_{j-1}]}$. Define a single polynomial in the independent matrices D_j by

$$P(D)=Q_0(X_0)\prod_{j=1}^m\prod_{\tau\in\Phi}\det(X_{j-1,\tau})^{n_{j,\tau}}.$$

To see that $P\neq 0$, choose D_j for $j\ge 2$ to be the standard rectangular inclusions at every embedding. Then all X_j, $j\ge 1$, are identity matrices. The top square block of each $D_{1,\tau}$

can give any $X_{0,\tau}$ after transposition. Invertible tuples are Zariski dense in the product of the square matrix spaces, so choose such a tuple with $Q_0(X_0) \neq 0$.

Applying $P(\partial)$ at zero to the product translation of $\mathcal{G}_h$ gives $Q_{m,h}(I)$ with the analytic translations. Indeed, on each path the rule (66.22) first replaces monomials in D_1 by the derivatives of the first section. The next substitution acts on the surviving frame variables and commutes with this replacement. Iterating and evaluating at I gives the displayed P followed by the independent derivative evaluations. Summation over paths gives (66.24). The degree of P in the j,τ block is $B_{j,\tau} = |\lambda_{j-1,\tau}| + N_{j-1}n_{j,\tau}$. Indeed, before applying the j-th substitution the degree in that frame is $B_{j,\tau}$, and all later substitutions leave D_j untouched. Put $b_j = \sum_\tau B_{j,\tau}$.

If $c_j^* = \pi/A_j$ is the metric constant at the j-th step, the product-torus form of Lemma 66.5 is

$$\int |(P(\partial)U_{\boldsymbol{w}}\mathcal{G}_h)(0)|^2 \, d\boldsymbol{w} = \left(\prod_{j=1}^{m} (c_j^*)^{b_j}\right) \|P\|_{\mathrm{F}}^2 \|\mathcal{G}_h\|^2 > 0. \tag{66.25}$$

For details, expand the polynomial into monomials and the section into its finite sum of tensors. For two sections F, F' on one torus and two multi-indices of the same total degree, the adjoint calculation in Lemma 66.5 gives the inner product $\mathbf{1}_{\alpha=\beta}(c_j^*)^{|\alpha|}\alpha!\langle F, F'\rangle$ for their translated derivatives. Integrate separately over the tori and sum. The diagonal monomial factors give exactly the Fischer norm $\sum_\alpha \alpha!|P_\alpha|^2$.

The squared absolute value on the left is a real analytic function on a connected product torus. Its nonvanishing set is open and dense by (66.25). A finite intersection of these sets is open and dense. The product of the P_0-power torsion grids for the common lattices is dense there, so one tuple belongs to that intersection. The translation identity in Theorem 66.7 moves each selected translation to one finite input before all the representatives at that step. Its common phase multiplies the whole path sum by the product of the m phases. The same theorem, using the algebraic addition formulas for rational torsion, gives algebraicity of the corrected derivatives. Finite sums, products and evaluation at I preserve it. Work in one finite normal coefficient field containing the finitely many numbers in question.

For the valuation claim replace every weight m_c at step j by $A_{N_{j-1}}m_c$, an integer by the stabilizer argument in Theorem 65.17. By Proposition 66.28 the cleared map at that step takes an integral input into polynomials divisible coefficientwise by its p^{g_p}. After dividing by that power the inputs for the next step are integral of the new column weights. Induction proves the stated sum in every final coefficient. Evaluation at identity frames preserves the bound. □

The source defines its polynomial substitution and differentiated table in `Formalism/LocalToGlobal/KernelLattices/ThDistC.lean`, line 23 and `Formalism/LocalToGlobal/KernelLattices/ThDistC.lean`, line 60. Multiplying each derivative in direction τ by a scalar $c_{D,\tau}$ multiplies its entire step by $\prod_\tau c_{D,\tau}^{B_{j,\tau}}$ by homogeneity. The distribution in `Formalism/LocalToGlobal/KernelLattices/ThDistC.lean`, line 137 also uses character and frame factors. Theorem 66.29 uses positive split representatives, the additive coordinates of Section 65.5, and evaluation at the identity frame. Comparison at the prescribed levels with the terminal Bessel functional, including its normalization, remains open.

66.11 The factorial and field norm of the composed value

We compute the archimedean polynomial factor for the same scalar as in Section 66.10. Use $Q_0 = 1$, the identity terminal frame, and any nonnegative determinant powers $n_{j,\tau}$. Write $R_j = N_{j-1}$, $s_j = N_j$. Extend each preceding column list by zeros after its last column. The

partition on the first R_j columns after step j is

$$v_{j,\tau,i} = \lambda_{j-1,\tau,i} + n_{j,\tau} \quad (1 \le i \le R_j).$$

Let $b_j = \sum_{\tau,i} v_{j,\tau,i}$, $d_j = |\Phi| R_j s_j$, and let P be the polynomial in the proof of Theorem 66.29. Use $(k)_v = k(k+1)\cdots(k+v-1)$ with $(k)_0 = 1$.

Theorem 66.30 (Exact factorials through successive substitutions)**.** *In the Hermitian additive coordinates the squared Fischer norm is*

$$\|P\|_{\mathrm{F}}^2 = \prod_{j=1}^{m} \prod_{\tau\in\Phi} \prod_{i=1}^{R_j} (R_j - i + 1)_{v_{j,\tau,i}}. \tag{66.26}$$

Proof. Give every entry of the independent matrices $D_{j,\tau}$ the standard complex Gaussian density $\pi^{-1} e^{-|z|^2}$. Polar integration gives $\mathbb{E}[z^k \bar{z}^l] = \mathbf{1}_{k=l} k!$, so the squared Fischer norm is $\mathbb{E}|P(D)|^2$. The embeddings separate because $Q_0 = 1$, and we prove the formula for one embedding.

For a full-rank matrix A with r columns put $H_v(A) = \prod_{i=1}^{r} t_i(A)^{2v_i}$, where $t_i(A)$ is the length left after removing from column i its orthogonal projection on the previous columns. Gram–Schmidt writes $A = UT$ with $U^*U = I_r$ and T upper triangular with positive diagonal $t_i(A)$. For any full-rank B, right multiplication by such a T multiplies its i-th residual length by T_{ii}. Indeed the earlier column spans agree, and the new i-th column modulo this span is T_{ii} times the old one. For square B, $|\det B|^2 = \prod_i t_i(B)^2$.

Hold X_j fixed in the backwards substitutions and put $A = X_{j,[R_j]}$. Conditional on this A, each row of $D_j^{\mathsf{T}} U$ is a standard complex Gaussian row of length R_j. Indeed U extends to a unitary matrix of size s_j, and the Gaussian row in D_j^{T} is invariant under right multiplication by that unitary matrix. The rows are independent. Thus $X_{j-1} = D_j^{\mathsf{T}} A$ has the same conditional distribution as GT for a square standard Gaussian G. These matrices are of full rank almost surely, starting at $X_m = I$ and working backwards.

Given the first $i-1$ columns of G, the random variable $t_i(G)^2$ is the sum of $R_j - i + 1$ independent exponential variables of mean one. Its conditional v_i-th moment is $(R_j - i + 1)_{v_i}$, by integration of the gamma density. The moment is constant in the earlier columns. Taking conditional expectations starting with the last column gives

$$\mathbb{E}_{D_j}\big[H_v(X_{j-1}) \,\big|\, X_j\big] = H_v(X_{j,[R_j]}) \prod_{i=1}^{R_j} (R_j - i + 1)_{v_i}.$$

When H_v is put on the whole next frame, adjoining zeros to v has exactly the effect of restricting to the first R_j columns. Begin with $|\det X_0|^{2n_1}$, integrate D_1 by this formula, and multiply the remaining function by $|\det X_1|^{2n_2}$. This adds n_2 to each current column weight, including the new ones. Repeat to $j = m$. The remaining factor at $X_m = I$ is one, giving precisely (66.26). □

For $d > 0$, $b > 0$ put

$$e(b,d) = b\log(1 + d/b) + d\log(1 + b/d), \qquad e(0,d) = 0.$$

The next estimate allows b to be much larger than the dimension of the derivative variables.

Lemma 66.31 (Gaussian estimate for a multihomogeneous derivative)**.** *Let $H(z)$ be entire on blocks of dimensions d_j. Suppose $|H(z)|^2 \le S \exp(\sum_j c_j |z_j|^2)$ with $S, c_j > 0$. For any polynomial P of block degrees b_j, homogeneous in each block,*

$$|P(\partial) H(0)|^2 \le S \|P\|_{\mathrm{F}}^2 \prod_j c_j^{b_j} \exp(e(b_j, d_j)).$$

Moreover $e(b,d) \le d[1+\log(1+b/d)]$.

Proof. Integrate against independent complex Gaussians of density $(t_j/\pi)^{d_j} e^{-t_j|z_j|^2}$, with $t_j > c_j$. The squared integral norm is at most $S\prod_j (1-c_j/t_j)^{-d_j}$. Rotation of independent blocks is unitary for this measure. Its Fourier projection onto the block degrees b_j is the corresponding Taylor part, by integration of the Taylor series on each compact rotation orbit. It is a contraction in the integral norm. Orthogonality of Gaussian monomials identifies the squared Fischer norm of that Taylor part with its squared integral norm times $\prod_j t_j^{b_j}$. Pair its coefficients with the coefficients of P, using Cauchy–Schwarz with weights $\alpha!$. The resulting product is minimized in each block with $b_j > 0$ at $t_j = c_j(1+d_j/b_j)$, by logarithmic differentiation. With $b_j = 0$ take t_j to infinity. These choices give the asserted factor. The last inequality follows from $\log(1+d/b) \le d/b$. □

Return to one of the torsion tuples supplied by Theorem 66.29. Let $y = a_{\mathrm{cl}} Q_{m,h}(I)$ for a fixed terminal class and put

$$M = \prod_{j=1}^{m} \left(\sum_{c \in \mathcal{C}_{j-1}} m_c \right), \qquad E_j = e \max(1, 2R_j s_j \ \mathrm{rd}(E)/\pi).$$

Here e in E_j is the base of natural logarithms. In the discriminant-one elliptic normalization for K_d set

$$L_d = \log(\sqrt{d}/(2\pi)) - \gamma + D_{\xi_d}, \qquad V_d = \tfrac{1}{4}\log d - \tfrac{1}{2}\gamma + \tfrac{1}{2} D_{\xi_d}.$$

Theorem 66.32 (An upper estimate at infinity for the iterated scalar)**.** *For the nonzero y just defined, in any common finite Galois coefficient field J,*

$$\frac{\log |N_{J/\mathbb{Q}}(y\bar{y})|}{[J:\mathbb{Q}]} \le 2\log(a_{\mathrm{cl}} M) + \log \|P\|_{\mathrm{F}}^2 + \sum_{j=1}^{m} (b_j L_d + d_j(V_d + \log E_j) + e(b_j, d_j)). \tag{66.27}$$

For the balanced degrees of Lemma 94.1, the contribution of the $e(b_j,d_j)$ is $o_{\psi,\varepsilon}(b/x)$ on the common intervals, where $b = \exp(x^{\varepsilon})$.

Proof. At any embedding ρ use the conjugate sections of Theorem 65.9. Each corrected torsion translate has the same metric supremum as its vacuum there. Its squared absolute value in block j is bounded by $(E_j \nu_\rho)^{d_j} \exp(\pi |z_j|^2/A_\rho)$, by (65.6). There is one translate with coefficient of magnitude one per pair. The coefficients of P are integers since the initial polynomial is one. Thus its conjugated derivative is computed by the same P on the sum over all paths of the products of these conjugated sections. Roots of unity have absolute value one at every embedding. The triangle inequality gives a squared envelope for this sum with $S = M^2 \prod_j (E_j \nu_\rho)^{d_j}$ and $c_j = \pi/A_\rho$. Apply Lemma 66.31 and include the factor a_{cl}^2.

For complex conjugation ι at the original embedding, the map $\rho \mapsto \rho\iota$ permutes the embeddings. The normalized logarithm on the left of (66.27) therefore equals the mean of $\log|\rho(y)|^2$. The means of $\log(\pi/A_\rho)$ and $\log \nu_\rho$ are L_d, V_d, respectively, by the elliptic area formula and the formula for the marked two-torsion point in Theorems 65.22 and 65.25. Taking these means and using the exact factorial in (66.26) gives (66.27). On the given intervals $d_j, m, R_j, s_j, |\Phi|$ are bounded by fixed powers of x. The balanced degrees give $b_j \le R_j |\Phi| (a + B' + 1)$, so $\log(1+b_j) = O_\varepsilon(x^\varepsilon + \log x)$. The final assertion now follows from the last bound of Lemma 66.31 and the growth of b. □

For $Z_u = y_u\overline{y_u}/D_x$ in Theorem 94.2, subtract $\log D_x$ from the right of (66.27) to bound its normalized logarithmic field norm. Its $\mathcal{H}_S$ also includes the negative valuations outside S. Equation (66.27) evaluates the archimedean factorial for the same composed and translated scalar as the finite divisibilities. The comparison with the centered main term and the control of those remaining finite valuations are open.

66.12 A finite torsion level for simultaneous nonvanishing

The torsion choice in Theorem 66.29 used density. We now give a sufficient level in terms of the derivative orders and a common period lattice for the fixed representatives. The estimate will apply to the product of all the tests for which nonvanishing is required.

Let $T = \mathbb{C}^n/\Gamma$, $d_0 = 2n$, with Euclidean real inner product. A smooth section f has the multiplier and metric of Section 66.2 with parameter $c > 0$. Its squared metric magnitude $g = |f|^2 e^{-c|z|^2}$ is periodic. Use normalized Haar measure and let $\mu = \int_T g$. For a unit vector $v \in \mathbb{C}^n$ put

$$A_v = \sum_i \bar{v}_i \partial_{\bar{z}_i}, \qquad B_v = -\sum_i v_i(\partial_{z_i} - c\bar{z}_i).$$

Assume $A_v^{K+1} f = 0$ for every such v. Let λ denote the shortest nonzero length in the real dual lattice $\Gamma^\vee = \{u : \langle u, \gamma\rangle_{\mathbb{R}} \in \mathbb{Z} \text{ for every } \gamma \in \Gamma\}$.

Lemma 66.33 (Sampling a squared section at torsion points)**.** *For any positive integer N with $N\lambda \geq 8\sqrt{c(K + 2d_0 + 2)}$, one has*

$$\left| \frac{1}{N^{d_0}} \sum_{w \in N^{-1}\Gamma/\Gamma} g(w) - \mu \right| \leq \frac{\mu}{2}.$$

Proof. If $\mu = 0$, the continuous nonnegative function g is zero everywhere. Assume henceforth $\mu > 0$. Fix v and abbreviate $A = A_v, B = B_v$. Integration by parts on T gives $A^* = B$ and direct differentiation gives $[A, B] = c$, as in Lemma 66.5. On smooth sections killed by A^{k+1} one has an orthogonal expansion into $B^l f_l$, $0 \leq l \leq k$, with $Af_l = 0$. Indeed $A^k f$ is killed by A and $A^k B^k A^k f = c^k k! A^k f$. Subtract $B^k A^k f/(c^k k!)$ and repeat with $k - 1$. Distinct levels are orthogonal by moving the larger power to the other argument and commuting the resulting A's to the right. The same computation gives $\|B^l f_l\|^2 = c^l l! \|f_l\|^2$. It follows by orthogonality that

$$\|Af\| \leq \sqrt{ck}\|f\|, \qquad \|Bf\| \leq \sqrt{c(k+1)}\|f\|.$$

The real covariant derivative $D_v = A - B$ sends these sections into the kernel of A^{k+2}, by the commutator. Thus for $s \geq 1$ $\|D_v^s f\| \leq (2\sqrt{c(K+s)})^s \|f\|$.

In the real direction v, differentiation of a pointwise metric pairing differentiates each argument by D_v. The two connection terms sum to the derivative of the weight $e^{-c|z|^2}$. Apply this product rule s times to g. Cauchy–Schwarz for each integrated absolute product yields $\|\partial_v^s g\|_{L^1} \leq (4\sqrt{c(K+s)})^s \mu$. For $u \neq 0$ in the dual lattice, integrate by parts in the direction $u/|u|$ against the character $\exp(-2\pi i\langle u, z\rangle_{\mathbb{R}})$. Then

$$|\widehat{g}(u)| \leq \mu \left(\frac{2\sqrt{c(K+s)}}{\pi|u|} \right)^s.$$

The dual vectors in $2^l\lambda \leq |u| < 2^{l+1}\lambda$ number at most $5^{d_0} 2^{ld_0}$ for $l \geq 0$. Disjoint balls of radius $\lambda/2$ around them fit in the ball of radius $2^{l+1}\lambda + \lambda/2$, which gives the count by volume. Take $s = 2d_0 + 2$. The Fourier series now converges absolutely, and its finite grid average retains

exactly the frequencies in $N\Gamma^{\vee}$ by finite character orthogonality. Hence the discrepancy is at most

$$2\,5^{d_0}\mu\left(\frac{2\sqrt{c(K+s)}}{\pi N\lambda}\right)^{s} \le 2\,5^{d_0}(4\pi)^{-2d_0-2}\mu < \mu/2.$$

□

Theorem 66.34 (One bounded level for the composed values)**.** *Fix the positive definite class data of Theorem 66.29 and $H \ge 1$ tests on this chain, allowing different initial polynomials, terminal classes and degree lists. For test i let b_{ij} be its degree in the j-th derivative block. Set $K = \sum_{i,j} b_{ij}$, $d_0 = 2\sum_j |\Phi| R_j s_j$. At step j write Λ_j for the period lattice of the standard trace vacuum. Fix a positive integer L_j such that $\Gamma_j = L_j\Lambda_j$ is a common lattice as in Section 66.2, and set $L_* = \max_j L_j$. Let $f_0 = [E : K_d]$. One may choose all the rational translations of Theorem 66.29 with denominator dividing the same P_0-power N, where*

$$N \;\le\; P_0 \max\left(1,\; 8L_*\sqrt{\frac{\pi\,\mathrm{rd}(E)}{2f_0}}\,\sqrt{H(K+2d_0+2)}\right). \tag{66.28}$$

For all the translates of Theorem 94.2 with one terminal class this gives $\log N \le \log L_* + O_{\psi,\varepsilon,P_0}(x^{\varepsilon})$.

Proof. Rescale the j-th block of the product torus by $\sqrt{\pi/A_j}$, so its Gaussian metric becomes the one with parameter one. The derivative evaluation of test i, as a function of the translation, has squared magnitude equal to the squared metric magnitude of the smooth section obtained by applying its derivative polynomial in the raising operators to its holomorphic path sum. This is the differentiated translation formula in Lemma 66.5 applied in every block. The rescaling only multiplies homogeneous derivatives by fixed nonzero constants. Each antiholomorphic directional derivative commutes through the raising operators at the cost of removing one of them or else kills the holomorphic factor. Consequently every direction annihilates this smooth section after $1 + \sum_j b_{ij}$ successive antiholomorphic derivatives.

Take the product of the H sections. Its squared metric magnitude g is the product of the H squared tests, and its metric has parameter H. The ordinary product rule gives $A_v^{K+1} f = 0$ for the product. Each test has positive mean and real analytic squared magnitude by (66.25). Their nonzero sets are open and dense on the same connected torus. The product is positive on a nonempty open set, hence $\int g > 0$.

It remains to bound the real dual minimum after rescaling. In a rescaled standard trace lattice Λ_j', the alternating form $\pi^{-1}\,\mathrm{Im}\langle z, w\rangle$ is unimodular by Theorem 65.3. Hence its real Euclidean dual lattice equals $i\Lambda_j'/\pi$, up to sign. Indeed pairing with iz/π converts the real pairing into the given alternating one, and unimodularity gives both inclusions. The squared minimum of Λ_j' is at least $2\pi f_0/\,\mathrm{rd}(E)$ by the same theorem. Passing to the dual of $L_j\Lambda_j'$ divides its minimum length by L_j. The dual minimum of the orthogonal product therefore satisfies

$$\lambda \;\ge\; L_*^{-1}\sqrt{2f_0/(\pi\,\mathrm{rd}(E))}.$$

Choose the least nonnegative power of P_0 at least the quantity inside the maximum in (66.28), including the lower bound one. Lemma 66.33 makes the average of g on that grid positive, so one grid point makes every test nonzero. Before scaling its j-th component is in $N^{-1}\Gamma_j/\Gamma_j$. This is exactly the grid of rational translations used in Section 66.2, with order dividing N modulo the original lattice. The same commutation with the split representatives gives one input per step and preserves all the previously obtained divisibilities.

For the indicated translates $H \le |\,\mathrm{Gal}(E/\mathbb{Q})|$, and $m, d_0, |\Phi|, R_j, s_j$ are bounded by fixed powers of x. By Lemma 94.1, the total derivative order of one test is at most $\sum_j R_j|\Phi|(a +$

$B'+1$). Thus $\log(H(K+2d_0+2)) = O_\varepsilon(x^\varepsilon + \log x)$. The conductor–discriminant formula gives $\log \mathrm{rd}(E) \le \log \mathrm{cond}(E) = O_{\psi,\varepsilon}(x^{\varepsilon/4})$ on this family. This proves the logarithmic estimate. □

For lattice sampling of polyanalytic functions in the complex plane see L. D. Abreu, *Sampling and interpolation in Bargmann–Fock spaces of polyanalytic functions*. Lemma 66.33 proves directly the estimate for the compact product torus and the lattice used here. Formula (66.28) retains the dependence on the common period indices of the actual representatives. The height of the divided periods in Section 6.6, still requires a sharper estimate.

66.13 Differentiating torsion translates at primes dividing the order

Let $P = [w] \in C$ be a torsion point on the marked elliptic curve of Theorem 67.12. The function $U_w\Theta_{t_*}$ uses the Hermitian translation of Theorem 65.6. Use the complex embedding of K giving its action on the tangent line, and extend its image to the coefficient field. Let $\mathfrak{a}(P) = \{\beta \in \mathcal{O}_K : \beta P = 0\}$ and define

$$\delta_{\mathfrak{p}}(P) = \min_{0 \neq \alpha \in \overline{\mathfrak{a}(P)}} v_{\mathfrak{p}}(\alpha).$$

The minimum is attained since this is a nonzero integral ideal and the local value group of $K^\times$ is discrete. If $mP = 0$, then $0 \le \delta_{\mathfrak{p}}(P) \le v_{\mathfrak{p}}(m)$.

Theorem 66.35 (Torsion translates in the original differential)**.** *At every finite place and every $j \ge 0$, with $\delta = \delta_{\mathfrak{p}}(P)$ and $a_+ = \max(a, 0)$, one has*

$$v_{\mathfrak{p}}\big((U_w\Theta_{t_*})^{(j)}(0)\big) \ge -j\delta - \lfloor j/2 \rfloor (\kappa_p - 2\delta)_+.$$

In particular the value at zero is integral for torsion of arbitrary order. At a split prime the derivative loss due to the translation uses only the component of $\overline{\mathfrak{a}(P)}$ at the chosen place.

Proof. Set $R = U_w\Theta_{t_*}/\Theta_{t_*}$ and fix $m \ge 1$ with $mP = 0$. The transformation law in Theorem 65.6 gives $R^m = ch$ for a rational function h with divisor $m([t_* - P] - [t_*])$. Its proof also gives

$$c^m \prod_{i=0}^{m-1} h(z + iP) = \epsilon_{t_*}(mw)^m, \qquad \epsilon_{t_*}(mw) \in \{1, -1\}.$$

Here the constants and the rational function are algebraic. Over a local field of good reduction, scale h so its order at the generic point of the special fiber is zero and change c inversely. This scaling is possible since the smooth special fiber is reduced and irreducible, so a uniformizer has order one there. Translation by iP extends to an automorphism of the good model. Each factor in the product has vertical order zero. The displayed equation then proves that c is a unit.

Choose $0 \neq \alpha \in \overline{\mathfrak{a}(P)}$ attaining the minimum. For $\lambda \in \Lambda$, the multiplier of R under $\alpha\lambda$ is the exponential of $2\pi i$ times, up to sign, the alternating pairing of λ with $\bar{\alpha}w$. This follows from the adjoint identity for the Hermitian form on the CM line. Since $\bar{\alpha}w \in \Lambda$, the pairing is integral. Consequently $F(z) = R(\alpha z)$ is a meromorphic function on C and $F^m = c\,h \circ [\alpha]$. It is a rational function over a finite number field. Indeed its divisor is the algebraic divisor $[\alpha]^*([t_* - P] - [t_*])$. A degree-zero algebraic divisor which is principal over $\mathbb{C}$ is already principal over $\overline{\mathbb{Q}}$, by base change for global sections of its line bundle. Divide F by an algebraic function with that divisor. The quotient is constant and its m-th power is algebraic by the displayed identity for F^m. Enlarge the local field to contain these data.

The endomorphisms $[\alpha]$ and $[\bar{\alpha}]$ extend over good reduction by the Néron property of the abelian scheme. Their composite on the special fiber is multiplication by the nonzero integer

$N_{K/\mathbb{Q}}(\alpha)$, which is finite and surjective in every characteristic. Thus $[\alpha]$ is dominant on the special fiber. At its generic point h is a unit, so its pullback is a unit there as well. The identity for F^m gives vertical order zero for F. The possible horizontal poles of F are supported in the inverse image of the section t_*. This closed inverse image misses the origin in the special fiber, since $[\alpha](0) = 0$ and t_* has nonzero reduction by Theorem 67.12. Thus F has no pole along any height-one prime of the local ring at the closed origin. The ring is regular and equals the intersection of its localizations at height one. Hence F is regular at that origin. These standard facts are stated in Milne, *Complex Multiplication*, Proposition 6.4, and in the Stacks Project, Tag 0BFG and Tag 031T.

The integral invariant derivation in Theorem 67.12 therefore gives $\partial^i F(0) = \alpha^i R^{(i)}(0)$ integral for every i. In the Leibniz formula for the j-th derivative of $R\Theta_{t_*}$, the term with i derivatives on R has valuation at least $-i\delta - \lfloor (j-i)/2 \rfloor \kappa_p$. The largest possible loss is obtained by maximizing $(j-2a)\delta + a\kappa_p$ over the integers $0 \le a \le \lfloor j/2 \rfloor$. Indeed among the orders with $\lfloor (j-i)/2 \rfloor = a$, the largest i is $j-2a$. The maximum equals the stated expression. This calculation uses ordinary derivatives in dz throughout. □

67 Signed theta periods and CM derivatives

67.1 Congruences for a prescribed signed theta period

There is a second way to choose the two narrow-class representatives of Lemma 72.18. It starts with the original test levels but chooses the representatives jointly with the norm element. This permits simultaneous congruences for a signed sum of columns. We use the fixed splittings and finite-order determinant tuples of Theorem 94.18.

Proposition 67.1 (Two auxiliary prime ideals and prescribed norm congruences)**.** *Fix a period field E/F in the interval of Theorem 19.15, and a finite list of the prescribed split tests and determinant characters. Put $\mathfrak{b} = \mathfrak{d}_F \mathfrak{a}_0^{-1}$. Let $\mathcal{L}$ be a finite set of odd rational primes disjoint from the rational support of $\mathfrak{b}$, with positive integers h_l for $l \in \mathcal{L}$. One can choose the representatives $\mathfrak{p}, \mathfrak{q}$, totally positive β, γ with $(\beta)\mathfrak{d}_F = \mathfrak{p}$, $(\gamma)\mathfrak{a}_0 = \mathfrak{q}$, and $\xi \in E^\times$ so that*

$$u = \xi\bar{\xi} = (d_0\beta\gamma)^{-1}, \qquad \xi \equiv 1 \pmod{l^{h_l}\mathcal{O}_{E,w}} \quad (l \in \mathcal{L},\ w \mid l).$$

At every split place choose a position component, keeping all the original choices. In that component ξ fixes every prescribed split position test away from $\mathfrak{p}$ and all other split lattice indicators. At $\mathfrak{p}$ it acts by a scalar unit in the position space. The determinant characters are unramified there. The only rational primes supporting (ξ) are those under $\mathfrak{b}$, $\mathfrak{p}$, and $\mathfrak{q}$.

Proof. Use the prime selection of Theorem 21.5, to represent the narrow class of $\mathfrak{a}_0$ by a split $\mathfrak{q}$ of norm larger than every prescribed rational prime, including every prime in $\mathcal{L}$. This gives a positive γ. At every v supporting $\mathfrak{b}$ let w_v denote the position prime and set $J = \prod_{v \mid \mathfrak{b}} \bar{w}_v^{v(\mathfrak{b})}$. All these places split by Theorem 110.18. At $\mathfrak{q}$ choose the prime Q opposite its position component. The fractional ideal JQ^{-1} has norm $\mathfrak{b}/\mathfrak{q}$ in F.

At each prescribed nonspherical split place, including $\mathfrak{q}$, and each split divisor of $\mathfrak{b}$, put only its position prime in a ray modulus with a positive exponent large enough that the corresponding scalar units fix the tests. Also include the full ideals $l^{h_l}\mathcal{O}_E$ for $l \in \mathcal{L}$, taking the larger exponent where requirements coincide. This modulus is coprime to JQ^{-1}. Represent the ray class of JQ^{-1} by a prime P of absolute prime norm greater than all the specified rational primes and the rational primes ramified in E or in the determinant characters. The construction over E in Theorem 21.5, gives such a prime. Its rational prime splits completely. Set $\mathfrak{p} = P \cap F$. Equality in the ray class group gives an element ξ congruent to one modulo

the ray modulus with $(\xi) = JQ^{-1}P^{-1}$. Thus $(u) = \mathfrak{b}/(\mathfrak{q}\mathfrak{p})$, and u is totally positive. Defining $\beta = (d_0\gamma u)^{-1}$ gives $(\beta)\mathfrak{d}_F = \mathfrak{p}$ by $\mathfrak{a}_0^2 = (d_0)$. Take the position component at the new $\mathfrak{p}$ to be $\bar{P}$, where ξ is a unit. At other split places outside the modulus both components are units, except at primes opposite those already protected. This proves all the claims. □

Lemma 67.2 (Parity forced by the internal unitary centers)**.** *In an even chain with the splittings fixed, all columns giving nonzero operators have the same $D_{\tau,c} \bmod 2$ at each real place τ. This holds for every choice of the finite-order intermediate determinant characters.*

Proof. Take the norm-one idele equal to -1 at τ and to one elsewhere. Act on every test by this source center. A homogeneous real polynomial on edge i is multiplied by $(-1)^{d_{i,\tau,c}}$ times the vacuum character at -1. Multiplication through the chain gives a fixed phase times $(-1)^{D_{\tau,c}}$. On the other hand, transferring the centers on the odd edges to their targets and changing the odd integration variables, exactly as in Theorem 94.18, gives a phase depending only on the splittings. Each finite-order character is trivial on the connected real scalar circle. Neither endpoint is changed. Comparing the two multiples of any nonzero column proves the assertion at τ. □

Theorem 67.3 (Simultaneous signed Gram congruences at cohomological depth)**.** *Use Proposition 67.1 and retain the original terminal Bessel character and any fixed complex-linear projection. In the fixed-coordinate comparison let G, G' be the Gram matrices before and after the change from β to $\beta' = (d_0\gamma)^{-1}$. For every pair of nonzero operator columns there are totally positive $b_{cc'} \in F^\times$ with*

$$G_{cc'} = b_{cc'}G'_{cc'}, \qquad b_{cc'} \equiv 1 \pmod{l^{h_l}\mathcal{O}_{F,v}} \quad (l \in \mathcal{L},\ v \mid l).$$

Zero operator columns give zero on both sides. In particular, let s be any fixed vector of algebraic coefficients, including a prescribed choice of signs. If G' has algebraic entries, take a number field containing the entries, coefficients, their conjugates and F. At each prime $\mathfrak{l} \mid l$ of this field one has

$$s^*Gs - s^*G's \ \in\ l^{h_l}\sum_{c,c'} \mathcal{O}_{\mathfrak{l}}\,\overline{s_c}s_{c'}G'_{cc'} \qquad (l \in \mathcal{L}).$$

On the interval of Theorem 21.4, one may take every odd $l \le Y$ prime to $2F_\psi$ simultaneously and $h_l = \lceil V^{203} \rceil$. For the original finite levels and polynomial test depths, both representative primes still have logarithmic norms polynomial in x. This depth kills the full groups covered by that theorem on the same fields and intervals.

Proof. The argument of Theorem 94.18, applies to any norm element with the stated local test actions. Here the only possible finite translation is at $\mathfrak{p}$, and it belongs to the central integral units. The intermediate characters are unramified there, so every one has value one on this translation. Their values on the archimedean rotations are also one. All inert lattice vacua are carried to the new vacua since ξ is a unit at every inert place. Thus each operator satisfies $A_c = Ca_cA'_c$ with the same unitary phase and with $a_c = \prod_\tau (\tau u)^{D_{\tau,c}/2}$.

For nonzero columns the lemma gives $(D_{\tau,c} + D_{\tau,c'})/2 \in \mathbb{Z}$ for every τ. The phase cancels in the Gram pairing. Its multiplier is therefore

$$b_{cc'} = \prod_\tau (\tau u)^{(D_{\tau,c}+D_{\tau,c'})/2} \in F^\times.$$

The full congruence modulus at l is Galois stable. Both ξ and $\bar{\xi}$ are one modulo l^{h_l} at all places above l, so every τu is one there to the same depth. Taking integer powers and multiplying proves the first congruence. Expanding the two quadratic forms and subtracting proves the

assertion for the given coefficients, including at places where cancellation increases the valuation of the sum. Explicitly, if any summand is nonzero, put

$$t = \min_{c,c'} v_{\mathfrak{l}}(\overline{s_c} s_{c'} G'_{cc'}) + h_l v_{\mathfrak{l}}(l), \qquad v_{\mathfrak{l}}(0) = +\infty.$$

The difference has valuation at least t. The ultrametric inequality then gives $\min\{v_{\mathfrak{l}}(s^* G s), t\} = \min\{v_{\mathfrak{l}}(s^* G' s), t\}$. In particular, a computed valuation strictly below t on either side establishes nonvanishing of the prescribed projection on both.

For the quantitative choice, $q > V^{401} > Y$ and the support of $\mathfrak{b}$ lies above $2F_\psi q$. Thus all the stated primes are available. The added full rational ideals have log norm at most $[E:\mathbb{Q}]\lceil V^{203}\rceil Y \log(2Y)$, a fixed power of V. The remaining ray modulus also has polynomial logarithmic norm by the finite-level bounds in Theorem 21.5. In its prime-selection argument choose the auxiliary cyclotomic prime above Y and outside the bounded number of other forbidden rational primes. Repeated application of Bertrand's postulate gives such a prime of size $O_\psi(Y)$. The log norm estimate for the ray prime is therefore polynomial in V and hence in x. This proves the simultaneous assertion. □

The modulus in the last theorem controls the difference of the two signed squared norms relative to the indicated fractional ideal. It allows both norms to vanish. A lower bound for the designated projected vector, and a uniform archimedean size estimate for the generators subject to these ray congruences, are separate questions. The next theorem proves the uniform estimate for those generators.

67.2 Real sizes and prime-power congruences for the same theta periods

Theorem 67.4 (Nearly equal conjugates at the full prescribed ray depth)**.** *Keep the fields, intervals, original finite test levels and coefficient primes of Theorem 67.3. Fix $A > 0$ and put $\delta_x = e^{-x^A}$. In Proposition 67.1 one can choose the two auxiliary prime ideals so that the same β, γ, ξ satisfy all its finite congruences and, for $u = \xi\bar{\xi} = (d_0\beta\gamma)^{-1}$,*

$$\max_{\tau} \left|\log \tau\gamma - f^{-1} \log N_{F/\mathbb{Q}}\gamma\right| \le \delta_x,$$
$$\max_{\tau} \left|\log \tau u - f^{-1} \log N_{F/\mathbb{Q}} u\right| \le 2\delta_x,$$
$$\max_{\tau} \left|\log \tau\beta - f^{-1} \log N_{F/\mathbb{Q}}\beta\right| \le 3\delta_x.$$

Here $F = E_x^+$, $f = [F:\mathbb{Q}]$, and τ runs through its real embeddings. For fixed A and polynomial test depths the logarithms of the two prime norms and the absolute logarithms of all conjugates of β, γ, u are bounded by a fixed power of x, uniformly on the interval. In particular this holds with every $l \le Y$, $l \nmid 2F_\psi$, at once, to the depth $h_l = \lceil V^{203}\rceil$ of Theorem 67.3.

Proof. Use the polynomial conductor N_x of Theorem 19.15. Over F there are $f-1$ independent log vectors of totally positive units with Euclidean norm at most $2\sqrt{f}\,\varphi(N_x)\log(2N_x)$, by the proof of Lemma 104.1. Their images in the CM field $E = E_x$ have the same absolute values. Given any finite ray modulus $\mathfrak{m}$, raising all these units to the order of $(\mathcal{O}_E/\mathfrak{m})^\times$ puts them in the ray unit group. This order is at most $N\mathfrak{m}$. Thus the logarithm of the length bound for independent ray-unit vectors is polynomial in x whenever $\log N\mathfrak{m}$ is. The same conclusion holds over F.

Apply Theorem 9.2, to F, with the narrow class of $\mathfrak{a}_0$, finite modulus one, $y = 0$ and $\delta = \delta_x$. Choose its parameter B polynomial in x and large enough that X exceeds all the prescribed primes, the ramified rational primes and any desired $\exp(x^{A_0})$ with A_0 fixed. This

is possible by the original level bounds and $\log d_F \le f \log N_x$, where here d_F denotes the absolute discriminant. We obtain $\mathfrak{q} = (\gamma)\mathfrak{a}_0$ with positive γ and the first asserted inequality. The quadratic character of this narrow class is trivial by Lemma 72.18. Hence $\mathfrak{q}$ splits in E/F.

Form $J, Q, \mathfrak{m}$ exactly as in Proposition 67.1, where Q is the prime over $\mathfrak{q}$ opposite the chosen position component. The log norm of the ray modulus is polynomial in x. The new prime $\mathfrak{q}$ has polynomial log norm, each ordinary test depth is polynomial and the full rational part contributes at most $[E:\mathbb{Q}]\lceil V^{203}\rceil Y \log(2Y)$. Apply the same theorem over E to the fractional ideal JQ^{-1}, with $y = 0$, $\delta = \delta_x$. Increase its polynomial parameter to exclude all primes already specified, including the rational prime under $\mathfrak{q}$. We obtain a prime $P = (s)JQ^{-1}$ of absolute degree one and $s \equiv 1 \bmod \mathfrak{m}$ with $\|\lambda(s)\| < \delta_x$. Its rational prime is unramified and $E/\mathbb{Q}$ is Galois, so that prime splits completely. Set $\mathfrak{p} = P \cap F$, $\xi = s^{-1}$ and $\beta = (d_0\gamma\xi\bar{\xi})^{-1}$. The ideal and ray verifications in Proposition 67.1 now apply to these very elements. At infinity $\log \tau u = -2\log|\sigma s|$ for $\sigma \mid \tau$. Center the identity for $\log \tau\beta$ by subtracting its mean. This proves the other two inequalities. Polynomial bounds for the means follow from $N\mathfrak{a}_0 = d_0^{f/2}$, $N_{F/\mathbb{Q}}u = N\mathfrak{b}/(N\mathfrak{p}\,N\mathfrak{q})$, and $N\mathfrak{b} \le d_F$. The same estimates and prime choices apply for each x on the common cohomology interval. □

Corollary 67.5 (Real comparison for the specified homogeneous tests)**.** *In the fixed-coordinate comparison of Theorem 67.3 put $d_c = \sum_\tau D_{\tau,c}$ and $d_{\max} = \max_c d_c$. For $a_c = \prod_\tau (\tau u)^{D_{\tau,c}/2}$, set $a_c^0 = (N_{F/\mathbb{Q}}u)^{d_c/(2f)}$, taking the positive real root. Then $|\log(a_c/a_c^0)| \le d_c\delta_x$. With the same splittings and the same terminal Bessel character as in that theorem, let v_c, v_c' be corresponding vectors after any common fixed linear projection. For arbitrary complex signs or coefficients s_c, the common phase C of Theorem 94.18, satisfies*

$$\left\| \sum_c s_c v_c - C \sum_c s_c a_c^0 v_c' \right\| \le (e^{d_{\max}\delta_x} - 1) \sum_c |s_c| a_c^0 \|v_c'\|.$$

All the finite signed Gram congruences of Theorem 67.3 hold for these same data whenever its algebraicity hypothesis holds. For the terminal scalar translates of one fixed homogeneous theta operator the factor is exactly Ca_c on their whole signed sum.

Proof. The second bound of the theorem, multiplied by each nonnegative $D_{\tau,c}/2$ and summed over τ, bounds the logarithm of the ratio. For these ray primes the phase contributed by the finite-order intermediate determinant characters is one, by the proof of Theorem 67.3. Thus $v_c = Ca_c v_c'$. The triangle inequality gives the estimate. For one fixed operator the same identity holds on every input, so it applies directly to any linear combination of its terminal input translates. The same reasoning applies to a fixed linear projection on its output.

For the explicit real tests in Theorem 104.28, the factor $d_{\max}$ is at most $x^{C_0}\exp(x^{\varepsilon})$ for a fixed C_0. Indeed the degree on an edge is the sum of the absolute partition entries in that theorem. Their number, the ranks, t_{r}, the number of edges and f are polynomial in x. Each entry is an original row parameter plus splitting and rank shifts. The lists in equation (9.1), and Theorem 72.26, use the B_τ of size $O(x\exp(x^{\varepsilon}))$ and polynomial spacings. At most a polynomial number of these terms occurs in an entry. This proves the bound. For these tests, taking $A > \varepsilon$ makes the relative error factor at most $e^{-x^A/2}$ for large x. This controls the change in real scale. The arithmetic size of a nonzero reference Bessel vector still enters the lower bound in Section 6.6. □

Theorem 67.6 (Cancellation among different degree profiles)**.** *Fix the reference character $\beta' = (d_0\gamma)^{-1}$, one finite family of homogeneous columns, their inputs, a terminal linear projection and complex coefficients s_c. Fix the reference tests before varying the second prime, using*

spherical position tests away from a prescribed finite set. Write v'_c for the projected reference vectors, $\mathbf{d}_c = (D_{\tau,c})_\tau$, and form the vectors

$$U_{\mathbf{d}} = \sum_{\mathbf{d}_c = \mathbf{d}} s_c v'_c.$$

There exists a choice of the second auxiliary prime with nonzero signed projected vector if and only if some $U_{\mathbf{d}} \neq 0$. Here one varies only the norm comparison of Theorem 67.4, using the transported splittings from the common reference, the original Bessel character and the finite congruences of Theorem 67.3. One can retain any prescribed accuracy $0 < \eta \leq 1/10$ in the centered logarithms of u. If the number of distinct profiles, $\log(2 + d_{\max})$, and $\log(1/\eta)$ are polynomial in x, the logarithmic prime norms are still polynomial in x.

Proof. Use $K = E$, $n = 2f$, and fix $A_0 = JQ^{-1}$ and the ray modulus from the proof of Theorem 67.4. For a selected prime $P = (s)A_0$ the signed vector, up to a common unit scalar, is the value of the vector polynomial

$$\sum_{\mathbf{d}} U_{\mathbf{d}} \prod_{\tau} t_\tau^{d_\tau}, \qquad t_\tau = |\sigma s|^{-1}, \quad \sigma \mid \tau.$$

Indeed the real multiplier is exactly a_c. At all protected split tests the chosen component of s^{-1} is one to the prescribed depth. At $P \cap F$ take the unit position component as in Proposition 67.1. Other fresh places carry the reference spherical tests. This proves necessity.

Let h be the number of profiles and set $L = h(h-1)/2$. Choose integers $0 \leq b_\tau \leq L$ such that the numbers $e_{\mathbf{d}} = \sum_\tau b_\tau d_\tau$ are distinct. Each pair of distinct profiles rules out at most a fraction $1/(L+1)$ of the integer box, by fixing all but a coordinate where they differ. The union of the L forbidden sets leaves a choice. Put $D = d_{\max}$, $M = \lceil 4h(1+L)(1+D)/\eta \rceil$, and $z_{\mathbf{d}} = \exp(e_{\mathbf{d}}/M)$. These numbers have mutual spacing at least $1/M$, and $1 \leq z_{\mathbf{d}}^j \leq 2$ for $0 \leq j < h$. For any vectors $W_{\mathbf{d}}$ we have

$$\max_{0 \leq j < h} \left\| \sum_{\mathbf{d}} z_{\mathbf{d}}^j W_{\mathbf{d}} \right\| \geq (3M)^{1-h} \max_{\mathbf{d}} \|W_{\mathbf{d}}\|.$$

To extract a given vector, take the linear combination of the h sums with coefficients of its Lagrange polynomial on the nodes $z_{\mathbf{d}}$. The sum of the absolute coefficients is at most $(3M)^{h-1}$ by multiplying the linear factors.

Choose $\delta = \min(\eta/100, [100h(1+D)(3M)^h]^{-1})$. Select B meeting all the hypotheses of Theorem 9.2, for this accuracy, large enough to exclude the given places and to have $n + h \leq B$. Let $X_0 = \exp((2B)^{20})$, $t_0 = (NA_0/X_0)^{1/n}$, and $\bar{b} = f^{-1} \sum_\tau b_\tau$. For each $j = 0, \dots, h-1$ prescribe

$$X_j = X_0 \exp(-nj\bar{b}/M), \qquad y_{\tau,j} = -j(b_\tau - \bar{b})/M.$$

Use the theorem with parameter $(\log X_j)^{1/20} \geq B$. It gives $|\log(t_\tau/t_0) - jb_\tau/M| \leq 2\delta$. The weighted lower bound $X_j e^{-O(B^2)}$ in its proof dominates the weight $O(hn \log X_j)$ at all earlier choices. Thus the primes can be taken above distinct rational primes, and the position halves at these spherical places can be fixed simultaneously. The centered logarithms of u have modulus at most $2j \max_\tau |b_\tau - \bar{b}|/M + 2\delta < \eta$.

Now take $W_{\mathbf{d}} = t_0^{|\mathbf{d}|} U_{\mathbf{d}}$, where $|\mathbf{d}| = \sum_\tau d_\tau$. Replacing an ideal sample $z_{\mathbf{d}}^j$ by the actual product of the t_τ/t_0 changes each sum in norm by at most $2h(e^{2D\delta} - 1) \max_{\mathbf{d}} \|W_{\mathbf{d}}\|$. This is at most half the lower bound just obtained. Thus one of the actual signed vectors has norm at least $\max_{\mathbf{d}} t_0^{|\mathbf{d}|} \|U_{\mathbf{d}}\|/[2(3M)^{h-1}]$. Finally $\log(1/\delta) \ll h \log(2h(1+D)/\eta)$, so the choices of B and $\log X_j$ have the asserted polynomial bounds. □

All scalar translates of one fixed word have the same degree profile. In that case the vector $U_{\mathbf{d}}$ is the signed reference projection itself, and a change of scale preserves its vanishing exactly. For the normalized Bessel periodization, Theorem 110.4, gives a test at the specified terminal character.

67.3 From the adelic theta distribution to CM derivatives

Fix one of the fields $E = E_x$ of Section 92.1 on the interval of Section 6.6. Put $F = E^+$, $K = \mathbb{Q}(\sqrt{-d_K})$, where d_K is the ramified prime denoted by d_0 in Theorem 110.18, and $f = [E : K]$. Consider two of the standard definite spaces of ranks r, s with rs even. Use all extensions Σ of the chosen embedding of K, the matrix space $W = \mathrm{Mat}_{s\times r}(E)$ over $\mathbb{Q}$, and $D = frs$. Write $h(a, b) = \mathrm{tr}(b^* a)$ and $h_K = \mathrm{Tr}_{E/K} h$. In the marked elliptic differential of Lemma 65.8, put

$$v(a) = \delta\Phi(a), \quad A = |\delta|^2\sqrt{d_K}/2, \quad c = \pi/A, \qquad B(a, b) = \mathrm{Tr}_{E/\mathbb{Q}}(-h(a, b)/\sqrt{-d_K}).$$

Thus $B(a, b) = -\operatorname{Im}(v(a) \cdot \overline{v(b)})/A$. This is the alternating form for the character of Theorem 110.18. Indeed, multiplying the skew scalar $\gamma\sqrt{-d_K}$ by $(d_K\gamma)^{-1}$ gives $-1/\sqrt{-d_K}$, and composing the two traces gives B. Use the symmetric Weyl law with central term $B/2$, and the rational adelic character ψ with $\psi_\infty(t) = e^{-2\pi i t}$. The oriented matrix action and the half factor can also be found in `Formalism/LocalToGlobal/IndefiniteReal/LocalNewformFunction.lean`, line 25. For the original character one transports the actual functions and splittings by Theorem 94.16.

Lemma 67.7 (Mean square of the adelic theta distribution)**.** *Choose a rational polarization of W into a position space X and its dual $X^\vee$. Use the dual adelic measures with both rational quotients of volume one. For a Schwartz–Bruhat vector l, put $\vartheta(l) = \sum_{q\in X(\mathbb{Q})} l(q)$. If $R(w)$ denotes symmetric Weyl translation, then*

$$\int_{W(\mathbb{Q})\backslash W(\mathbb{A})} |\vartheta(R(w)l)|^2\, dw = \|l\|_2^2.$$

If the finite factor of l is an eigenvector for the Weyl translations of a full finite lattice $\widehat{M}$, the left side is also the average on $W_\mathbb{R}/M$ of the same expression with finite argument zero, where $M = W(\mathbb{Q}) \cap \widehat{M}$.

Proof. For $w = (x, y)$ the modulus of the summand after periodizing is the modulus of $\sum_q l(q + x)\psi(\langle q, y\rangle)$. The factors removed are common to the entire sum and have modulus one. Replacing x by a rational translate reindexes q and replacing y by a rational frequency leaves every character on q fixed. These characters of $X^\vee(\mathbb{A})/X^\vee(\mathbb{Q})$ are mutually orthogonal for probability Haar measure. The sum converges absolutely for every x, since the finite support condition puts q in finitely many translates of a real lattice and the real factor decreases rapidly. Integration in y gives $\sum_q |l(q + x)|^2$. Tonelli's theorem and integration over a fundamental domain in x give precisely $\int |l|^2$. For the last assertion the modulus is unchanged by finite translations in $\widehat{M}$, by the eigenvector hypothesis and the Weyl law. Every finite adele is rational modulo $\widehat{M}$, by the Chinese remainder theorem in lattice coordinates. The kernel of the resulting map from $W_\mathbb{R}$ to the double quotient is M. The pushforward of Haar probability to this torus is Haar probability. □

Let $M = \mathfrak{b}^{-1}\,\mathrm{Mat}_{s\times r}(\mathcal{O}_E)$ be the standard module in Lemma 65.8, and ϕ_0 its unit finite vacuum with the corrected period character. Write G_ϕ for the linear realization of a finite vector ϕ in the CM sections of Theorem 65.13. In particular $G_{\phi_0} = G_0$, the image of the product of the marked elliptic theta functions under the normalized lattice intertwiner. Here

ν denotes the averaged squared norm of *one* marked elliptic theta in Proposition 65.21. Use the antiholomorphic Fock realization at infinity. Its vacuum 1 has norm one for Gaussian probability of density $(c/\pi)^D e^{-c|w|^2}$ in the coordinate $w = v(a)$. A polynomial is written $P(\sqrt{c}\,\bar{w})$, so its squared norm is the Fischer norm squared of P.

Theorem 67.8 (The theta functional in the marked elliptic differential)**.** *Fix the Schrödinger–Fock identification once. There is a common scalar C, of absolute value $\nu^{-D/2}$, such that for every smooth finite Schwartz vector ϕ and every homogeneous polynomial P of degree d,*

$$\vartheta(P(\sqrt{c}\,\bar{w}) \otimes \phi) = C\, c^{-d/2}\, P(\partial) G_\phi(0).$$

The same C works for every translate, class representative and degree. The differential operator uses the coefficients of P as written. The phase of C is fixed by the ordinary theta sum on the marked product vacuum.

Proof. Set $K_z(\bar{w}) = \exp(c\,\bar{w}\cdot z)$ and $F_\phi(z) = \vartheta(K_z \otimes \phi)$. This is an entire function. In real position coordinates the inverse Bargmann transform of K_z is a Gaussian times the exponential of an affine function of position with coefficients holomorphic in z. A fixed real symplectic change of polarization acts continuously on Schwartz space. On compact sets of z every derivative is therefore bounded in each Schwartz seminorm. This gives local uniform convergence of the theta sum and its derivatives. These are the Gaussian kernel and intertwining formulas of V. Bargmann, Part I.

Let $U_v H(z) = e^{-cz\cdot\bar{v} - c|v|^2/2} H(z+v)$, and let $\bar{U}_v$ act by the conjugate formula on antiholomorphic functions. The real symmetric Weyl action is $\bar{U}_v$. Indeed $U_v U_{v'}$ has multiplier $e^{\pi i B(v,v')}$ in the real coordinates just chosen, while $\psi_\infty(B/2)$ is its conjugate. The unitary Schrödinger–Fock intertwiner is chosen for these translation operators. For $a \in W(\mathbb{Q})$ the full rational Weyl translation fixes ϑ, by reindexing positions and using the triviality of ψ on $\mathbb{Q}$. The finite corrected translate is $W_f(a) = e^{\pi i h_K(a,a)} R_f(a)$. On rational elements this correction gives exactly the cocycle $e^{-2\pi i(\operatorname{Re} h_K(a,b) + \operatorname{Im} h_K(a,b)/\sqrt{d_K})}$ used in Theorem 65.13. Transferring the real operator across the rational invariance and applying its formula to K_z gives

$$F_{W_f(a)\phi}(z) = e^{\pi i h_K(a,a)} U_{v(a)} F_\phi(z), \qquad \bar{U}_{-v} K_z = e^{-cz\cdot\bar{v} - c|v|^2/2} K_{z+v}.$$

Thus F_{ϕ_0} has the same theta multipliers as G_0 on $v(M)$. This is a principal polarization by Theorem 65.3. Its holomorphic section space has dimension one by Riemann–Roch and vanishing of higher cohomology for an ample line bundle on a complex abelian variety. Hence $F_{\phi_0} = C G_0$. Apply Lemma 67.7 to $1 \otimes \phi_0$. The real translate of 1 at $-z$ is $e^{-c|z|^2/2} K_z$. Consequently $\int_{\mathbb{C}^D/v(M)} e^{-c|z|^2} |F_{\phi_0}(z)|^2\, dz_{\mathrm{prob}} = 1$. The corresponding integral for G_0 is ν^D by Theorem 65.9. This proves the asserted modulus.

In the finite lattice model the translates $W_f(a)\phi_0$, one per coset in $W(\mathbb{A}_f)/\widehat{M}$, form its standard orthonormal basis. One can see finiteness of the expansion of a smooth vector by restricting its period character to a sufficiently small open subgroup of $\widehat{M}$ fixing it. Only the cosets in the annihilator of this subgroup can occur, by the Weyl commutator. There are finitely many, since $\widehat{M}$ is self-dual. Rational representatives exist by the lattice calculation in the lemma. The translation identity and linearity give $F_\phi = C G_\phi$ for every such vector. To recover the phase, apply the reverse normalized lattice sum of Lemma 65.8 to ϕ_0, obtaining ϕ_{prod} on the product lattice. On sections the reverse sum recovers the original section. Averaging over the source periods kills every nonzero coset of the target modulo the intersection, by the commutator. The two indices agree by self-duality, so the zero coset has coefficient one after the two normalizations. Thus $G_{\phi_{\mathrm{prod}}}$ is the marked product section, of value one at zero, and $C = \vartheta(1 \otimes \phi_{\mathrm{prod}})$. Finally $P(\partial_z) K_z|_{z=0} = c^{d/2} P(\sqrt{c}\,\bar{w})$. Applying this identity inside the theta sum proves the formula. □

Theorem 67.9 (A compact theta period with its finite projections)**.** *Write $H = U_r$, $H' = U_s$ for the two definite groups and $[H] = H(F)\backslash H(\mathbb{A}_F)$, with analogous notation for H'. Let a, b be continuous forms of right finite level characters χ, χ' on J, J', respectively. Use their given values, the chosen splitting ω, the polynomial P and the finite test ϕ. For finite class representatives u, v, set*

$$m_u = \frac{\mathrm{vol}(H_\infty \times J)}{|H(F) \cap uJu^{-1}|}, \qquad m'_v = \frac{\mathrm{vol}(H'_\infty \times J')}{|H'(F) \cap vJ'v^{-1}|}.$$

In the denominator only the finite components of a rational element are tested. Use probability Haar measure for the following averages, with k, l denoting the real variables.

$$\phi_{uv} = \omega_f(u, v) \int_{J \times J'} \chi(j)\overline{\chi'(j')}\, \omega_f(j, j')\phi \, dj \, dj',$$
$$P_{uv} = \int_{H_\infty \times H'_\infty} a(k, u)\overline{b(l, v)}\, \omega_\infty(k, l)P \, dk \, dl.$$

Here the real action is written on polynomials in $\sqrt{c}\,\bar{w}$, including its vacuum character. If Θ_P denotes the adelic theta kernel of $P \otimes \phi$ in these coordinates, then

$$\int_{[H]\times[H']} a(g)\overline{b(h)}\, \Theta_P(g, h)\, dg\, dh = Cc^{-d/2} \sum_{u,v} m_u m'_v\, P_{uv}(\partial) G_{\phi_{uv}}(0).$$

The formula includes, by linearity, a finite signed sum of tests. For a lift pairing the kernel with a conjugate input, take a to be that conjugate, with its resulting level character.

Proof. The quotients are compact and have finitely many finite classes. Above u the group $H(F) \cap uJu^{-1}$ acts on $H_\infty \times J$ by left translations, freely, through its real component and its finite component conjugated by u. It is finite since rational points are discrete in the adeles. This gives exactly the mass m_u for normalized averages on this fiber. The same argument gives m'_v. The Weil action factors into its real and finite actions in the chosen splitting. Transforming a and b under j, j' at the finite level gives precisely the two character factors displayed above. This finite average is a finite sum, by smoothness and compactness. At infinity the unitary action preserves the Gaussian and rotates the coordinates, up to its vacuum character. It preserves degree and acts on a finite-dimensional space. Compact integration therefore gives exactly P_{uv}. The theta distributions of these polynomials converge uniformly on the compact groups by the Schwartz estimates in Theorem 67.8. Fubini's theorem and that theorem give the identity with the original measures. □

With $\mathrm{vol}(H_\infty \times J) = \mathrm{vol}(H'_\infty \times J') = 1$, the masses are exactly the rational weights of (65.1). The formula identifies each ordinary derivative and its measure factor before any square or class sum is taken. For a general compact type the polynomial to be differentiated is P_{uv}. A valuation estimate proved for powers of minors applies when those are the polynomials occurring in the sum.

67.4 Local divisibility of the prescribed compact coefficient

Use the rectangular compact period $\mathcal{P} = \langle L(Q), b_* \rangle$ of Theorem 88.2, with b_* the specified terminal test and B_v its covectors there. Take the degrees (66.2) and restrict the target to its standard hyperplane. Let S be the set of good inert primes used in Theorem 66.2. At their finite places the original levels lie in the standard integral groups. Choose representatives away from these primes by Theorem 65.11. Use a common number field containing the arithmetic coefficients and their complex conjugates, with valuations normalized by $v(p) = 1$.

Theorem 67.10 (A local bound for the integral against the fixed test)**.** *Suppose the unaveraged finite tests and their class translates satisfy the CM hypotheses of Theorem 66.2. At every place above S suppose the class values a_u are integral and each B_v is integral on the module generated by the minor products P_T of its branch. This hypothesis refers to algebraic coefficients at the chosen representatives at the original levels. It suffices for the specified terminal compact type to have an integral matrix coefficient presentation as at the end of Theorem 88.2. The finite level characters have finite order.*

Choose open subgroups $J_0 \subset J$, $J_{*,0} \subset J_*$ fixing the incident finite tests and killing the finite level characters. Set $I_0 = [J : J_0][J_* : J_{*,0}]$. Let A_r, A_* be common multiples of the respective stabilizer orders at the original levels. For every $p \in S$ for which the 2-primary component of δ_p is nonzero and every valuation v above p, the algebraic number

$$Y = I_0 A_r A_* \, d_V H \, \frac{c^{k/2}}{\kappa \kappa_* C} \, \mathcal{P}$$

satisfies

$$v(Y) \;\geq\; r \sum_{\substack{j \geq 1 \\ j \text{ odd}}} \left[\, d_{p^j}(a, s) - w_{t + j\delta_p} \, \right]_+ .$$

If the two finite character averages together fix the given test already and the projected sections satisfy the stated CM hypotheses, one can use $I_0 = 1$. The inequality also holds for integral signed combinations at the same degrees, branch and normalization, using common subgroups and stabilizer multiples.

For the ranks of Proposition 92.1, when $r \geq xm$, the entire contribution of the compact representation factor is bounded uniformly by

$$0 \leq \frac{\log(d_V H)}{r} \ll_{\psi, \varepsilon} \frac{b}{\sqrt{x}}, \qquad b = \exp(x^{\varepsilon}).$$

All the assertions use the original fields, intervals and terminal hyperplane.

Proof. The target test b_* is already in the range of its finite orthogonal projector. In its pairing one can therefore integrate the unprojected lift against b_*. Cut up these same source and target quotients at $J_0, J_{*,0}$. The integrals and their original measures do not change. At the refined levels the finite averages of the test are identity operators. The two group-volume factors at those levels multiply to $\kappa \kappa_* / I_0$. Apply the first identity of Theorem 88.2, still using the originally specified a, b_*, Q.

Choose the refined representatives also by Theorem 65.11, supported at primes completely split in E away from the bad places. To compare representatives at the two levels, write a refined representative as $\gamma u j$ with γ rational and j in the old level, and likewise at the target. At every place over $p \in S$ both representatives have component one. Hence γ and its inverse have integral matrices at every such place. This remains true for all their algebraic conjugates at valuations above p, since integrality holds at all places in question. On the source the change of the source coefficient is a value of a determinant character, a unit at those valuations. Indeed the scalar source action on the full-column minor is a determinant power at each real place. Changing variables in the compact definition of a_u gives that very character, together with the finite level factor. On the target the rational change of representative acts on B_v by composition with its compact matrix action or its inverse. Cauchy–Binet expresses each minor of this substitution as an integral linear combination over the local ring of the minors of the same size. The matrices act in the first $s - 1$ rows and preserve the last row, so they preserve the submodule with l_τ occurrences of that row. Products and the determinant character of

the vacuum preserve the resulting module. The finite level multipliers are roots of unity. This proves the asserted integrality at every refined representative, also for complex conjugates of the covector values since all places above p were included.

Every refined stabilizer embeds into its old stabilizer after rational conjugation, so the original A_r, A_* clear its denominator. For each refined pair the full target representative is the block embedding $v \oplus 1$ of the chosen hyperplane representative. It acts at the same good split places. The derivative estimate in Theorem 66.2 is an estimate for each individual minor product on the two moved lattices and therefore also holds on this subset of pairs and minor indices. In the first identity of Theorem 88.2 multiply by $A_r A_*$, and use the refined volume factors. Each derivative is now multiplied by an element integral at v. The nonarchimedean triangle inequality gives the displayed bound even when the signed sum vanishes. If the averaged finite data satisfy the hypothesis at the original levels the same calculation can be made there directly.

For the last assertion $H = \prod_\tau \binom{b_\tau}{l_\tau}$ satisfies $\log H \le (\log 2) \sum_\tau b_\tau$. At the high embedding $b_t = a = \lfloor bx \rfloor$, and at the other embeddings the sum is $O_\psi(b(1+\log x))$ by Proposition 66.4. For a highest weight $\mu = (b_\tau^{r-1}, b_\tau - l_\tau, 0, \dots, 0)$ of length $n = s-1$, the Weyl dimension formula gives $\dim V_\mu = \prod_{i<j} (\mu_i - \mu_j + j - i)/(j-i)$. It follows that $\log d_V \le [E:K]\, n(n-1) \log(1+\max_\tau b_\tau)/2$. The degree and ranks are bounded by fixed powers of x and $\log(1+\max b_\tau) = O_\varepsilon(x^\varepsilon + \log x)$. This logarithm of the dimension is consequently bounded by a fixed power of x and is $o(b/x)$. Finally $r \ge xm$ and $m \asymp \sqrt{x}$ give the claimed estimate. □

The estimate applies to one prescribed integral compact coefficient. It records separately the two finite-level indices and applies with $v(0) = +\infty$. Using a product formula for this value still requires nonvanishing. For the full row of Corollary 83.7, one must also identify the incoming row covectors and control their arithmetic size on this interval.

67.5 CM derivatives on the prescribed final row

Take the last forward pair $U(Y_{m-1}), U(Y_m)$ on the period field of Proposition 9.9. Write $n = n_{m-1}$, $s = n_m$, and $f = [E:K]$, where $K = \mathbb{Q}(\sqrt{-d_K})$ is the marked imaginary quadratic field. Both groups are definite with the standard forms. Their rank difference is odd, so ns is even. At each real place use the actual partition λ_τ of Lemma 104.6, with $L_\tau = |\lambda_\tau|$ and $d = \sum_\tau L_\tau$. Write M for the tensor over these places of the maps in Proposition 95.2, permuting factors into the indicated source and target order. Put

$$P_* = \prod_\tau p_{\lambda_\tau}, \quad \mathfrak{d} = \prod_\tau \dim S_{\lambda_\tau}(\mathbb{C}^n)\, \dim S_{\lambda_\tau}(\mathbb{C}^s).$$

Thus P_* is the prescribed corner polynomial of Proposition 104.8. We use the Gaussian coordinates of Theorem 67.8, with $c = \pi/A$. The original character on the interval and its actual tests are carried to these data by the pointwise transport in Theorem 94.16.

Theorem 67.11 (The period at the full highest weights of the last row)**.** *Use finite class representatives u, v at fixing levels of the source and target. Let γ_u, γ'_v be their stabilizer orders, and κ, κ' the respective volumes of the real groups times these levels. Write G_{uv} for the marked CM section of the actual finite translate at this pair. For a forward lift the source function in the integral is conjugated. Suppose the source and target functions before conjugation, in their matching compact types, have class functions*

$$\sum_a \langle \rho_n(g) x_{ua}, y_{ua} \rangle, \qquad \sum_b \langle \rho_s(h) x'_{vb}, y'_{vb} \rangle.$$

Use the compact actions with their actual splittings. Denote the two unit highest tensors by t_n, t_s, now products over the real places, and set

$$Y_u = \sum_a \langle t_n, x_{ua} \rangle y_{ua}, \qquad Z_v = \sum_b \langle t_s, x'_{vb} \rangle y'_{vb}.$$

For the period $\mathcal{P}_*$ of the forward lift against the target function with test P_*, one has exactly

$$\frac{\mathfrak{d}\, c^{d/2}}{\kappa\kappa' C}\, \mathcal{P}_* = \sum_{u,v} \frac{M(Y_u \otimes Z_v)(\partial) G_{uv}(0)}{\gamma_u \gamma'_v}, \qquad |C| = \nu^{-fns/2}.$$

The complex identity allows the actual incoming class coefficients to have arbitrary size. The right side is an algebraic bilinear form in the tensor entries when the finite test has algebraic coefficients in the lattice model of Theorem 65.13 with its indicated splittings. It applies to signed inputs by linearity in the displayed tensor coordinates.

Proof. At a fixed finite class pair, integrate the polynomial in the archimedean oscillator against each pair of compact matrix coefficients. The source function enters conjugated by the forward convention, and the target function enters conjugated by the Petersson pairing. Proposition 95.2 and its tensor product give exactly $M(Y_u \otimes Z_v)/\mathfrak{d}$. Components of either input of nonmatching type make zero contribution by compact orthogonality. Every compact-finite function in the matching type has such a finite matrix coefficient expansion. The quantity extracted from a class is independent of the expansion, as the one-group matrix-unit integral applied to the highest tensor computes it, after multiplication by the representation dimension.

Apply Theorem 67.8 to the resulting polynomial at each pair. The class measures are κ/γ_u and κ'/γ'_v by Theorem 67.9. This proves the identity. For a prescribed finite character projection one can use the averaged test of that theorem at the original levels. Alternatively, in a pairing with a test in the projected space, refine inside those levels and use the fixing-level formula above. The original integral is the same and the ratio of the two volume products is the index product of Theorem 67.10. For algebraicity choose the fixing-level representatives as in Theorem 65.11. Their finite sections have algebraic derivatives by Theorems 65.13 and 65.9. The determinant expansion and the rational stabilizer weights then give algebraic coefficients of the bilinear form.

For a prescribed homogeneous polynomial P of the same block degrees in place of P_*, apply Proposition 95.2 to each term (a, b) before summing. Its multiplier in the normalized formula becomes $\langle P, M(x_{ua} \otimes x'_{vb}) \rangle_{\mathrm{F}} / \prod_\tau h_{\lambda_\tau}$. In particular the formula keeps the projections and phases of a fixed signed polynomial. When the two right lines are highest and P satisfies the column conditions of Theorem 104.9, the multiplier is its value on the top identity frames. Indeed projecting to the joint highest line retains the one diagonal monomial visible on these frames, and P_* has value one there. □

67.6 The marked elliptic derivatives at every prime

Write d_0 for the prime discriminant parameter of the interval in Section 6.6. Thus $d_0 \equiv 7 \bmod 8$ and $K = \mathbb{Q}(\sqrt{-d_0})$. We use the discriminant-one elliptic curve C, its differential $dz = dx/y$, and the mark t_* of Lemma 65.24. At a place $\mathfrak{p}$ above p let $v_{\mathfrak{p}}(p) = 1$, and put

$$\kappa_p = \begin{cases} 1 & p = 3 \text{ and } 3 \text{ is inert in } K, \\ 1/2 & p = d_0, \\ 0 & \text{otherwise.} \end{cases}$$

Theorem 67.12 (All-prime bound for the marked theta derivatives)**.** *For every $n \geq 0$ and every finite place of a coefficient field,*

$$v_{\mathfrak{p}}\left(\Theta_{t_*}^{(n)}(0)\right) \geq -\kappa_p \lfloor n/2 \rfloor.$$

In particular the ordinary derivatives are integral at 2, including in the fixed discriminant-one differential.

Proof. We may pass to a finite local extension. Normalizing $v_{\mathfrak{p}}(p) = 1$ makes the estimate descend. The CM j-invariant is integral. The potential good reduction criterion gives a good integral Weierstrass equation with affine coordinates X, Y and coefficients a_i. We can also take all the finitely many torsion points used below to be rational. Write $b_2 = a_1^2 + 4a_2$. Completing the square in this equation gives a cubic with quadratic coefficient b_2 and leading coefficient 4. Removing the quadratic term gives

$$x = u^2 X + r, \qquad r = u^2 b_2/12, \qquad y = u^3(2Y + a_1 X + a_3)$$

for some u matching the specified differential. The two discriminants are units and their ratio is u^{12}, so u is a unit. Thus $dz = u^{-1} dX/(2Y + a_1 X + a_3)$ generates the invariant differentials over the local integer ring. Its dual derivation ∂ acts integrally on the structure sheaf. For the criterion see Silverman, *The Arithmetic of Elliptic Curves*, Proposition VII.5.5.

The section t_* misses the origin in every special fiber. For odd p this follows from injectivity of specialization on two-torsion. At 2 the two idempotents in $\mathcal{O}_K \otimes \mathbb{Z}_2 = \mathbb{Z}_2 \times \mathbb{Z}_2$ split the two-divisible group into two height-one factors, one connected in the special fiber and one étale, as proved in Lemma 65.24. The mark is the sum of the nonzero points from the two factors. Its image in the étale factor remains nonzero. In particular X is regular at its reduction. The identity $(\log \Theta_{t_*})''(z) = -u_\Lambda - x(z + t_*)$ of Theorem 65.5 shows that every logarithmic derivative at zero of order $i \geq 3$ is integral. Indeed ∂^{i-2} kills the constant r and preserves regularity of $u^2 X$ near the section.

It remains to estimate $u_\Lambda + x(t_*)$. At $p = 2, 3$ use the CM expression from the proof of Theorem 65.5. Substitution of the coordinate change, including its constant term, gives

$$u_\Lambda + x(t_*) = u^2 \left(X(t_*) - \frac{1}{2d_0} \sum_{0 \neq P \in C[\sqrt{-d_0}]} X(P) \right) + \frac{d_0 + 1}{2d_0}\, r.$$

All points in the sum have order prime to p and their affine coordinates are integral. Pairing $P, -P$ in this odd-order kernel makes the sum twice an integral element, since $X(P) = X(-P)$. The expression in parentheses is integral. At 2 the final coefficient is divisible by 4, whereas $v_{\mathfrak{p}}(r) \geq -2$. At 3 we have $v_{\mathfrak{p}}(r) \geq -1$, and if 3 splits then $-d_0 \equiv 1 \bmod 3$, so the coefficient is divisible by 3. For $p \geq 5$ the logarithmic derivative of order two has valuation at least $-\kappa_p$ by the CM computation in Theorem 65.5. The order-one logarithmic derivative is zero. In the integral Leibniz recurrence for $\Theta_{t_*}^{(n)}(0)$ in that theorem, each occurrence of the order-two derivative uses two of the n differentiations. This proves the bound, including $n = 0$ by the normalization at zero. □

67.7 Finite valuations of the CM splitting characters

The scalar in Theorem 83.19 contains the value of a unitary character at a uniformizer. For the splitting characters of a period square one can determine its valuations from the CM infinity type. This also specifies the coefficient primes at which the powers of the uniformizer in the finite determinant average can affect an integral period.

Proposition 67.13 (Valuations from the infinity type)**.** *Let E be a CM field, let Σ contain one complex embedding from each conjugate pair, and let ν be a unitary Hecke character of E whose archimedean component is $\prod_{\tau\in\Sigma}(z_\tau/|z_\tau|)^{m_\tau}$ with integral m_τ. Fix a finite prime $\mathfrak{p}$ of E above p and a local uniformizer π. Put $e_\mathfrak{p}=e(\mathfrak{p}/p)$ and $f_\mathfrak{p}=f(\mathfrak{p}/p)$. Then $u_\mathfrak{p}=\nu_\mathfrak{p}(\pi)$ is algebraic and every algebraic conjugate in $\mathbb{C}$ has absolute value one. For an extension v_λ to $\overline{\mathbb{Q}}$ of the valuation with $v_\lambda(\ell)=1$, it has valuation zero if $\ell\neq p$. At $\ell=p$, let $I_\tau=1$ if the prime on E induced by $v_\lambda\circ\tau$ is $\mathfrak{p}$, and zero otherwise. Then*

$$v_\lambda(u_\mathfrak{p})=-\frac{1}{2e_\mathfrak{p}}\sum_{\tau\in\Sigma}m_\tau(I_\tau-I_{\bar\tau}),\qquad |v_\lambda(u_\mathfrak{p})|\le\frac{f_\mathfrak{p}}{2}\max_{\tau\in\Sigma}|m_\tau|.$$

Proof. Take $h\ge1$ with $\mathfrak{p}^h=(y)$, using finiteness of the ideal class group. In the principal idele defined by y, the finite component is a unit at every place except $\mathfrak{p}$, where it is π^h times a unit. The values of a smooth character on the units are roots of unity and only finitely many local restrictions to units are nontrivial. Applying the character to this principal idele and squaring gives

$$u_\mathfrak{p}^{2h}=\zeta\prod_{\tau\in\Sigma}\left(\frac{\tau y}{\bar\tau y}\right)^{-m_\tau}$$

for a root of unity ζ. The right side is algebraic. Complex conjugation on the source CM field pairs τ with $\bar\tau$, and continues to pair them after any embedding of their images. Every algebraic conjugate of the right side therefore has absolute value one. At primes over $\ell\neq p$ every conjugate of y is a unit. At $\ell=p$ one has $v_\lambda(\tau y)=hI_\tau/e_\mathfrak{p}$. Taking valuations and dividing by $2h$ gives the formula. Among all embeddings of E, exactly $e_\mathfrak{p}f_\mathfrak{p}$ induce the prime $\mathfrak{p}$, since they correspond to the embeddings of $E_\mathfrak{p}$ in an algebraic closure of $\mathbb{Q}_p$. Bounding the sum by the total number of those embeddings proves the inequality. □

On E_x use $m=m_\alpha-m_\beta$ and the prime over v specified by the split chart. Its residue field has size q_v. Thus the determinant and Fourier scalars of Theorem 83.19 are units away from the residue characteristic of v, throughout each interval of Section 6.6.

68 Marked elliptic jets and their determinants

68.1 Joint row degrees on the even Frobenius cycles

Fix a good $p\ge5$, inert in K_d and unramified in E_x, and a definite edge with ranks $r\le s$ and partitions ν_τ of length at most r. Use the permutation $\pi=\sigma_p c_E$ on the embedding labels of Theorem 66.24. On each even cycle choose one alternating half. Let H be the union of the chosen halves, and L the union of their partners. Odd cycles belong to neither set. We give the operator a lower bound for every such choice and then maximize it.

For each $\mu\in L$ form the list indexed by triples $\iota=(h,l,j)$, where $h\in H,\ 1\le l\le r,\ j\ge1$ is odd and $\pi^j h=\mu$. The associated nonnegative integer is

$$D_\iota=d_{p^j}(\nu_{h,l},s),\qquad d_M(t,s)=\max\{0,\lceil(t-s(M-1))/M\rceil\}.$$

Only indices with p^j at most the maximum block degree need be used. Order this finite list decreasingly, writing its members as $D_{\mu,1},D_{\mu,2},\dots$. Set $\nu_{\mu,t}=0$ for $t>r$ and put

$$V_p(\nu;H)=\sum_{\mu\in L}\ \max_{0\le k\le\#\{\iota:\pi^j h=\mu\}}\ \sum_{t=1}^{k}(D_{\mu,t}-\nu_{\mu,t}),\qquad V_p(\nu)=\max_H V_p(\nu;H).$$

Both maxima include the zero contribution when the lists are empty. These integers use only the permutation and the partitions.

Lemma 68.1 (Simultaneous degrees of the exceptional coefficients)**.** *In a monomial of the exceptional factors in the low symbol at μ, let b_ι count occurrences of the direction indexed by ι. For any sublist I of size k,*

$$\sum_{\iota\in I} b_\iota \le \sum_{t=1}^{k} \nu_{\mu,t}.$$

Proof. After the high row substitution, the low symbol is $K_\mu(D+\sum_\iota y_\iota U_\iota)$, with a separate indeterminate for each direction before its scalar Taylor coefficient is restored. The matrices U_ι are outer products by Lemma 120.11. Treat the variables outside I as coefficients. The columns supplied by the perturbation from I lie in a space of dimension at most k, also after the right substitution and padding of the flag symbol. A determinant of height v has joint degree at most $\min(k,v)$ in these k variables by its multilinear expansion. Summing this bound over the diagram columns counts the boxes in its first k rows. Tableau products span the integral test lattice, so this proves the assertion for every test, as in Lemma 120.16. The statement holds before specializing any of the formal variables. □

Theorem 68.2 (The Weyl operator on independently oriented cycles)**.** *In the local integral frames of Theorem 66.24, the definite class operator sends its integral source Weyl lattice into $p^{V_p(\nu)}$ times its target Weyl lattice. For any fixed H, the summand at μ is at least $\sum_\iota [D_\iota-\nu_{\mu,1}]_+$ over its list.*

Proof. Fix the halves. Apply the operators in odd-cycle variables and then set those variables equal to zero. In the factorization of Theorem 66.24, blocks from different cycles and matrix entries are orthogonal. An odd block vacuum depends only on its own variables and its undivided derivatives at zero are integral by Theorem 65.15. Derivatives of the initial integral elliptic factor preserve integrality in the elliptic parameters. Hence the product rule leaves on the even cycles a sum of integral elliptic factors times the even block vacua. The coefficients of the odd Weyl symbols and their row parameters are integral. The argument of Lemma 120.11 now applies on each chosen half: after removing its exponential of exceptional linear terms in the low variables, all undivided low derivatives satisfy the elliptic factorial bound in the high variables. The Frobenius partner of h at exponent p^j is still $\pi^j h$ in its own cycle. No exceptional linear term joins two cycles.

On a high derivative monomial let $\alpha_{h,bl}$ be the order in row b of column l. The column sum over $1\le b\le s$ is $\nu_{h,l}$. Put

$$C_\iota = \sum_{b} \left\lfloor \alpha_{h,bl}/p^j \right\rfloor .$$

In an individual term, restoration of the exceptional scalar and extraction of high coefficients have valuation at least $\sum_\iota (C_\iota - b_\iota)$ after the undivided differentiation. Indeed the factorials pay $\sum_\iota C_\iota$ above the even-power factorial bound, and the coefficient g_{p^j} costs at most one more power of p per occurrence, by the proof of Theorem 120.12. Moreover $b_\iota \le C_\iota$: each occurrence consumes p^j powers of a single high variable in that column. Division with remainder gives $C_\iota \ge D_\iota$.

For a fixed μ, retain just the k indices with largest D_ι. The discarded differences $C_\iota - b_\iota$ are nonnegative. The lemma therefore bounds the retained sum below by $\sum_{t\le k}(D_{\mu,t}-\nu_{\mu,t})$. Maximize independently at each μ. Every coefficient in the independent row parameters satisfies the bound, so extracting the source generators and pairing with the integral dual output lattice proves the asserted inclusion for this H. The class operator is the same for each allowed H. The block factorizations used to prove the estimates all evaluate that operator in the fixed physical coordinates of Theorem 66.24. Taking the maximum is therefore valid.

Finally select the indices with $D_\iota > \nu_{\mu,1}$; the first k row lengths sum to at most $k\nu_{\mu,1}$. This gives the last assertion. □

Corollary 68.3 (The extra divisor on the projected signed columns)**.** *Use q_c independent signed columns on the projected small tests of Corollary 9.27; here q_c denotes their number. Let ν_{ij} be the physical partition tuple of column i at edge j. At all unramified $p \geq 5$ inert in K_d, extend U_p by zero when p is inert in K_q. In the centered upper bound of that corollary one can subtract the nonnegative quantity*

$$\mathcal{D}_u = \frac{2}{q_c} \sum_{\substack{p \geq 5 \text{ unramified in } E_x \\ p \text{ inert in } K_d}} \left(\sum_{i=1}^{q_c} \sum_{j=1}^{m} V_p(\nu_{ij}) - q_c U_p \right) \log p.$$

The sum is finite without a restriction on prime size.

Proof. In the signal signs, take $H = \Phi_0$. The last assertion of the theorem gives at least the row contribution of Theorem 120.12, and Lemma 141.11 bounds its sum over a word below by U_p. In the other signs, each V_p is nonnegative. For p larger than every block degree and every relevant word cutoff the summand is zero, by the definition of d_M.

All primes of this finite support miss the marked levels. Indeed every elementary test modification is at a rational prime split completely in E_x, as proved in Lemma 141.14. The simultaneous choice of bases in that lemma works on this enlarged finite set: at each prime it uses only that $p \geq 5$ is unramified in the period field and inert in K_d. Thus the translated elliptic products have prime-to-p shifts with integral coefficients and the class lattices match at every intermediate vertex. Each path in column i gains $\sum_j V_p(\nu_{ij})$ in valuation before the masses and external scalars. Conjugating a physical edge transports its partition tuple and its Frobenius cycles together. They have the same sorted lists and maximum because the field is abelian. Taking the signed sums, with the same common coset on consecutive edges, preserves the bound. Expansion of a minor adds the gains of its columns.

The two test lattices still have their original scalar, mass and projector costs, as in Theorem 141.15. The change back to the fixed product bases preserves the local-degree average by its phase calculation. The unramified inert primes outside the signal signs previously had zero local field and differential loss in Theorem 141.18. The terminal rescaling is a unit at all primes under consideration. Summing the two ideal inequalities in Theorem 141.9 thus contributes twice the indicated additional gains. Substitution in the centered identity of Theorem 9.26 gives the asserted subtraction, with the same ramified term. □

68.2 Elliptic theta derivatives at a split prime

Let $C = \mathbb{C}/\Lambda$ be the marked elliptic curve with complex multiplication by $\mathcal{O}_{K_d}$ used in Section 65.2. Write $x = \wp$, $y = \wp'$, $\omega = dx/y$ and $\partial = d/dz$. Let t be its nonzero two-torsion mark and $\Theta_t(0) = 1$ its even theta function in the Hermitian frame. Fix a prime $p \geq 5$ split in $K_d = \mathbb{Q}(\sqrt{-d_0})$, and a coefficient place with good integral Weierstrass model and nonvanishing reduction of ω. We may extend the coefficient field to contain the indicated torsion points. Write k for the algebraic closure of the residue field, and use the same notation for reduced functions when working on C_k. Put

$$q_0(z) = -u_\Lambda - x(z), \qquad q_t(z) = q_0(z + t).$$

Here $q_t = (\log \Theta_t)''$ in the complex uniformization.

Lemma 68.4 (A differential identity on the split reduction)**.** *There is a nonzero scalar $H_p \in k$, in the field of definition of the reduced curve and differential, such that*

$$\partial^p = H_p \partial, \qquad \partial^{p-1} q_t = H_p q_t$$

on the reduced elliptic curve. In the first equality the powers denote iterates on the rational function field.

Proof. The p-th power of a derivation is a derivation by the binomial formula. Invariant vector fields on an elliptic curve form a line, so invariance of ∂^p gives H_p over the field of definition. For the moment it may be zero. Set $\Xi(f) = \partial^{p-1} f - H_p f$. Its derivative vanishes and $\Xi(\partial g) = 0$ for every rational function g. The kernel of ∂ on $k(C)$ is $k(C)^p$. Indeed x is a separating coordinate and $1, x, \dots, x^{p-1}$ are a basis over $k(C)^p$, as in Lemma 66.12. Differentiating in this basis proves the assertion. Consequently $\Xi(q_0)$ is a p-th power. Its only possible pole is the origin, of order at most $p+1$, since x has a double pole and the vector field is regular. A p-th root would have at most a simple pole there. Riemann–Roch in genus one makes that root constant.

We determine the constant using the original complex multiplication. Take $\alpha = \sqrt{-d_0}$. In characteristic zero put

$$B(z) = \frac{1}{\alpha} \sum_{0 \neq P \in C[\alpha]} \frac{y(z) - y(P)}{2(x(z) - x(P))}.$$

The zeta addition formula gives derivative $x(z) - x(z+P)$ for each fraction in the sum. The isogeny identity of Section 65.2 reads $\sum_{P \in C[\alpha]} x(z+P) = \alpha^2 x(\alpha z) + c_\alpha$, where $c_\alpha = \sum_{P \neq 0} x(P)$ and $u_\Lambda = c_\alpha / (\alpha(\alpha - \bar{\alpha}))$. Thus

$$\partial B(z) = \alpha q_0(\alpha z) - \bar{\alpha} q_0(z).$$

This is an identity of rational functions with good reduction at the chosen place. In fact $p \nmid 2 d_0$, every nonzero kernel point specializes away from the origin, and all denominators $x - x(P)$ are nonzero rational functions on the special fiber. The CM isogeny has degree prime to p and extends on the good model. These facts also give integrality of u_Λ.

Write a, a' for the reductions of $\alpha, \bar{\alpha}$. They are distinct elements of $\mathbb{F}_p^\times$ by splitting. The pullback of ω by $[\alpha]$ is $a\omega$. It follows that $\Xi(af \circ [\alpha]) = a(\Xi f) \circ [\alpha]$, since $a^p = a$. Apply Ξ to the differential identity for B. Its left side vanishes and its right side is $(a - a')\Xi(q_0)$, since $\Xi(q_0)$ is constant. Thus $\Xi(q_0) = 0$. Translation by t commutes with ∂ and gives the second identity of the lemma.

Finally, if $H_p = 0$, this argument would give $\partial^{p-1} x = 0$. The function-field computation in the proof of Lemma 66.12 shows that for a smooth cubic in characteristic $p \geq 5$, $\partial^p = 0$ implies $\partial^{p-1} x \neq 0$. In that computation nilpotence would otherwise make both dx/y and $x\,dx/y$ exact; their two missing coefficients in the Legendre model cannot vanish together. This portion of the argument uses only the smooth cubic and nilpotence. We conclude $H_p \neq 0$. □

Theorem 68.5 (All derivatives of a marked torsion translate at a split prime)**.** *Let $F = U_w \Theta_t$, where w has order prime to p modulo Λ, and put $J_n(F) = F^{(n)}(0)$ in the marked frame. The undivided derivatives are integral at the chosen place and satisfy, in its residue field,*

$$J_{n+p}(F) = H_p J_{n+1}(F) \qquad (n \geq 0).$$

This includes a translate vanishing at the origin. In particular, for $n \geq 1$ write $n = b(p-1) + r$, $1 \leq r \leq p-1$. Then $J_n(F) = H_p^b J_r(F)$ in that field.

Proof. Use the ring of undivided derivative sequences from Theorem 66.13. Its multiplication uses binomial coefficients and its derivation D shifts a sequence by one place. The reference logarithmic derivative $l = (\log \Theta_t)'$ vanishes at zero and satisfies $Dl = q_t$. Its higher entries are integral since q_t is regular at the reduced origin and the invariant vector field is integral. From $D\Theta_t = l\Theta_t$ and $\Theta_t(0) = 1$ all entries of the reference theta are integral by induction. Theorem 65.6 also gives integrality of $R_w = F/\Theta_t$ in an elliptic formal parameter, including when its constant term vanishes.

Reduce these sequences. By the lemma, $D(D^{p-1}l - H_p l) = 0$. A sequence killed by the shift is constant. Its constant term here is zero, since l is odd and $p-1$ is even. Also l^p is constant by the derivation rule and is zero at the origin. Repeated differentiation gives

$$D^p\Theta_t = (D^{p-1}l + l^p)\Theta_t = H_p D\Theta_t.$$

For the first equality, the product rule gives one contribution per partition of p labeled positions, with a block of size i contributing $D^{i-1}l$. Cyclic permutation kills all orbits of size p in the residue field. The only invariant partitions are the single block and the singletons, since the blocks must then be the cosets of a subgroup of $\mathbb{Z}/p$.

On the completed elliptic local ring in characteristic p, $\partial^p = H_p\partial$ as well. The two continuous derivations agree on the local parameter and on constants, hence on power series. Taking all further invariant derivatives of the integral germ R_w consequently gives $D^p R_w = H_p D R_w$ as sequences. Now D^p is a derivation in the reduced sequence ring. The product $R_w\Theta_t$ satisfies the same identity. Reading entry n proves the recurrence, and iteration gives the formula for arbitrary positive orders. □

Corollary 68.6 (Finite matrix evaluation for the prescribed period)**.** *Fix the fields, signed data and projected tests of Theorem 143.5. Choose a good split prime as above at which their scalar normalizations, changes of frame and finite coefficients are integral and which is prime to the orders of the torsion shifts. Every entry of the period matrix at the original tests can be reduced by the following finite rule. Use the elliptic product expansion of Proposition 122.13. For a product coordinate with derivative variable Z, reduce its differential symbol in*

$$k[Z]/(Z^p - H_p Z).$$

On its basis $1, Z, \dots, Z^{p-1}$ use the first p derivatives of the indicated translate. Take tensor products over all the coordinates, with the corresponding reduced differentials on conjugated edges. Sum with the original signed coefficients and the shared coupling index. A nonzero minor of the resulting matrix proves independence of those columns in characteristic zero.

Proof. The theorem states that the derivative functional on a monomial kills every multiple of $Z^p - H_p Z$. The ordinary chain rule first expresses a matrix differential as a polynomial in the commuting product-coordinate derivatives. On each tensor product section these act on different factors independently. Thus the calculation gives exactly the reduction of every original entry, by the linear terminal and path formulas. The integers b_i^{per} of Lemma 141.26 are units at these split primes, so the same rule applies to the divided columns. Determinants commute with reduction.

For any finite set of such data, a single rational prime may be taken split completely in their common normal coefficient field and their period fields, outside all the finite exclusions, by Chebotarev's theorem. Moreover, the characteristic-zero ranks are preserved at all but finitely many of these primes. To see this, in each positive-rank matrix fix one nonzero minor of its rank and exclude the primes dividing its numerator or denominator. All larger minors are already zero. This last existence assertion gives no lower bound on the ranks. A lower bound for the family in Section 6.6 requires a surviving minor for its actual signed tests. □

68.3 Simultaneous interpolation on the marked elliptic curve

At a good split prime p, Theorem 68.5 reduces the derivatives on each elliptic coordinate of an actual period to orders $0, \dots, p-1$. We determine which such values can be prescribed simultaneously at a finite set B of torsion shifts of order prime to p. Throughout this section B is nonempty. Use the same mark, differential and good model, extending the coefficient valuation ring to contain the finitely many data below, and take ranks over the algebraic closure k of its residue field.

Fix $M \geq 2$ prime to p. Let $\mathcal{L} = \mathcal{O}_C([t])$, with its section of divisor $[t]$, rigidified to have value one at the origin in the marked fiber. On the elliptic curve itself use the line bundle $\mathcal{L}_M = [M]^*\mathcal{L}$. In the analytic coordinate v, write

$$s_a(v) = (U_a\Theta_t)(Mv), \qquad a \in C[M].$$

Choose lifts of the torsion points consistently in all appearances of this formula. Its meaning on the algebraic line bundle is $s_a = s_0 R_a(Mv)$, where $R_a = (U_a\Theta_t)/\Theta_t$.

Lemma 68.7 (A basis after reduction)**.** *The M^2 sections s_a are integral on the good model of $\mathcal{L}_M$, and their reductions are a basis of $H^0(C_k, \mathcal{L}_{M,k})$.*

Proof. Theorem 65.6 makes $R_a(Mv)$ a rational function over a finite extension, with horizontal divisor $[M]^*([t-a]-[t])$. Its possible vertical divisor is an integer multiple of the special fiber, which is geometrically integral. At the origin its leading coefficient in a local parameter is a unit. To recall the reason, the M-th power of R_a is a constant times a rational function with divisor $M([t-a]-[t])$. After giving the function vertical order zero, the product of its translates by $0, a, \dots, (M-1)a$ is a unit constant. The corresponding product for R_a is a unit multiplier of the original theta. Hence the first constant is a unit. Near the origin the rational function is a unit times the M-th power of a parameter if $a = t$, and a unit otherwise. Distinct prime-to-p torsion specializes distinctly. Taking the chosen M-th root preserves the unit leading coefficient, also after pullback by $[M]$, whose tangent is a unit. Thus there is no vertical contribution. Multiplication by s_0 leaves the effective divisor $[M]^*[t-a]$ and gives a nonzero section after reduction.

Translation by $b \in C[M]$ is a deck transformation of $[M]$. It fixes s_0 with the pullback action. On the ratio s_a/s_0 it acts by the commutator of a with the period Mb. In lattice coordinates this is $\exp(\pm 2\pi i\, e(Mb, a))$, where e is the unimodular alternating form of the polarization and the sign is fixed by the convention for U. As a varies modulo the period lattice these characters are distinct. In fact a vector pairing integrally with every period is itself a period. All character values have order dividing M; they reduce injectively on the roots of unity of that order. The character eigenspaces on the special fiber are therefore distinct and the nonzero sections are independent. Their number is the dimension, since $\deg \mathcal{L}_M = M^2$ and Riemann–Roch on a genus-one curve gives this dimension for a line bundle of positive degree. □

Theorem 68.8 (The exact rank of the simultaneous derivative table)**.** *Consider the matrix with columns $a \in C[M]$ and rows (b, r), $b \in B$, $0 \leq r < p$, whose entry is*

$$J_r(U_b U_a \Theta_t) \pmod{\mathfrak{p}}.$$

Its rank is $\min(M^2, p|B|)$. The operator U_b is the fixed outer translation in each row. The result includes rows on which an individual translate vanishes at the origin.

Proof. For each chosen lift of b take the point $v_b = b/M$ on the cover, so $[M]v_b = b$. These points have order prime to p, and their reductions are distinct because their images are distinct.

At v_b use a local trivialization of $\mathcal{L}_M$ by some s_c with $c \in C[M]$, $c + b \neq t$. Such a c exists since $M \geq 2$. The horizontal divisor above shows s_c is a unit in this trivialization. On a neighborhood of zero we have

$$\frac{(U_b U_a \Theta_t)(z)}{(U_b U_c \Theta_t)(z)} = (s_a/s_c)(v_b + z/M).$$

The common translation factor cancels before any differentiation. The denominator on the left has unit value at zero and has integral undivided derivatives. Indeed $U_b U_c$ is U_{b+c} times a root of unity, and $b + c \neq t$. The local calculation in the lemma and Theorem 68.5 give the claims.

Multiplication by the germ of this denominator acts triangularly on the list of the first p undivided derivatives with unit diagonal. Comparison with coefficients in an algebraic parameter at v_b is triangular as well. In order r the leading coefficient is $r!$ times the r-th power of the nonzero tangent conversion, including M^{-1}. All are units for $0 \leq r < p$. Thus reduction gives an invertible row change, independent of a, from these p entries to restriction of the section to the length-p subscheme supported at v_b. This argument uses only finite jets of the marked frame.

By the lemma the matrix therefore has the rank of restriction of all sections of $\mathcal{L}_{M,k}$ to $p\sum_{b\in B}[v_b]$. Its kernel is the space of sections of $\mathcal{L}_{M,k}(-p\sum_b[v_b])$. That bundle has degree $M^2 - p|B|$, which cannot equal zero since $p \nmid M$. Its dimension is its degree when positive, and zero when negative, by Riemann–Roch or the degree of the zero divisor. Subtracting from M^2 gives the formula. □

Corollary 68.9 (One choice of additional translates for an entire edge)**.** *Use an elliptic product presentation of an edge of the signed column as in Proposition 122.13. In coordinate l, let B_l include every distinct original shift in that presentation and suppose their orders are prime to p. Fix one prime $P_0 \neq p$ and put $b_* = \max_l |B_l|$. One may take M a power of P_0 with*

$$\sqrt{pb_*} < M \leq P_0\sqrt{pb_*}.$$

There is one linear combination of the additional product translates $\bigotimes_l U_{a_l}\Theta_{t,l}$, $a_l \in C_l[M]$, giving any prescribed residue table of derivatives of coordinate orders $0, \dots, p-1$ at all shift tuples $(b_l)_l$. The coefficients can be integral at the testing place. All the original translations are applied outside the added translations.

Proof. Take the least power strictly above $\sqrt{pb_*}$. The theorem gives full row rank in each coordinate. Its tensor product is onto the space of arrays on $\prod_l (B_l \times \{0, \dots, p-1\})$, since elementary tensors span and each factor map is onto. At each coordinate a maximal nonzero minor is a unit before reduction. Solving on those columns, or lifting a residue solution, gives the asserted integral coefficients after a finite extension if needed. A single product input constructed with those coefficients serves every original shift tuple simultaneously. Theorem 68.5 determines its higher orders from the prescribed table. □

In particular there is full local freedom in these low derivatives when the product input can be varied at this auxiliary torsion order. For the period at the specified input, the coefficients of the additional translates are fixed, with only the original vacuum present. Proving independence there still requires the signed path sum to survive evaluation on that particular table.

68.4 Positive derivatives of a fixed signed theta section

Retain the elliptic curve, differential, two-torsion mark t and split prime from Theorem 68.5. Fix $M \geq 2$ prime to p, write $d = M^2$, and suppose $p > 2d + 2$. Use the sections $s_a(v) =$

$(U_a\Theta_t)(Mv)$ of $\mathcal{L}_M = [M]^*\mathcal{O}([t])$ from Lemma 68.7. Write k for the algebraic closure of the residue field. The next argument works with the given coefficients of a signed sum at a single prescribed shift. In particular it will also apply when its value at that shift is zero.

Lemma 68.10 (The second logarithmic derivative on the torsion cover)**.** *Let S be a nonzero section of $\mathcal{L}_{M,k}$. There is a rational function Q_S on the special fiber whose poles are precisely the distinct zeros of S, each of order two. On the open set where $s_c \neq 0$ its formula, with $h = S/s_c$, is*

$$Q_S(v) = M^2 q_t(Mv + c) + \partial_v\Big(\frac{\partial_v h}{h}\Big), \qquad q_t(z) = -u_\Lambda - x(z + t).$$

In particular $Q_S \neq 0$ and its pole divisor has degree at most $2d$.

Proof. The open sets in the statement cover the curve. The zero divisor of s_c is $[M]^*[t-c]$; two different c's have disjoint zero divisors. On an overlap the ratio $s_{c'}/s_c$ is a unit. In characteristic zero its second logarithmic derivative is the difference $M^2(q_t(Mv+c')-q_t(Mv+c))$. Indeed the linear exponential in each Hermitian translate has zero second logarithmic derivative. Both sides are rational functions and can be reduced on the overlap: the indicated sections, the functions q_t, and the invariant vector field are integral there. The quotient rule now gives agreement of the two formulas for any reduced section S.

The first summand is regular wherever $s_c \neq 0$, because its only possible poles there would have $Mv + c = -t = t$. At a zero P of S of multiplicity j, write $h = w^j u$ for a local parameter w and a unit u. The coefficient of w^{-2} in the second summand equals $-j(\partial_v w(P))^2$. It is nonzero since the invariant vector field never vanishes and $1 \leq j \leq d < p$. Away from these zeros h is a unit in a suitable chart and both terms are regular. The zero divisor of S has degree $d > 0$; there is a pole and there are at most d distinct poles. □

Theorem 68.11 (Positive derivatives detect every fixed signed section)**.** *Let b be any fixed torsion shift of order prime to p. Over k the matrix with columns $a \in C[M]$, rows $1 \leq r \leq 2d+2$, and entries*

$$J_r(U_b U_a \Theta_t)$$

has column rank d. The same holds upon replacing every r independently by $r + m_r(p-1)$, with m_r a nonnegative integer. In particular the positive orders in any $p-1$ consecutive positive integers suffice.

Proof. Take a nonzero vector $(u_a)_a$ of residue coefficients and set $S = \sum_a u_a s_a$. The torsion basis makes $S \neq 0$. Write F_b for the marked derivative sequence $\sum_a u_a J_\bullet(U_b U_a \Theta_t)$ and $P = b/M$ for the chosen point of the cover. Let $R = 2d + 2$. Through degree R use the ordinary truncated series with coefficient $F_b^{(r)}(0)/r!$ in degree r; all these factorials are units. To relate this frame to the algebraic curve, take $s_c(P) \neq 0$. The quotient formula in the proof of Theorem 68.8 expresses the series as the product of $U_b U_c \Theta_t$ and $(S/s_c)(P + z/M)$ through every degree under consideration. The first factor has unit constant term and the map from a local parameter at P to z has unit tangent. These comparisons use only the indicated finite Taylor coefficients and commute with reduction.

If $S(P) = 0$ with multiplicity j, then $1 \leq j \leq d$. The coefficient of z^j in this product is nonzero, so its j-th derivative is nonzero. If $S(P) \neq 0$, suppose that all the derivatives of orders $1, \dots, R$ vanish. The truncated series is then a nonzero constant through degree R. Its second logarithmic derivative is zero through degree $R-2$: differentiate twice, using the quotient rule and the inverse of the unit series. By the product formula just given and the definition of Q_S, this is the series of $M^{-2}Q_S(P + z/M)$ through that degree. Hence Q_S has order at least

$R-1=2d+1$ at P. A nonzero rational function on a smooth projective curve has zero and pole divisors of equal degree. The lemma gives the contradiction. Thus no nonzero coefficient vector is in the kernel. By Theorem 68.5, each indicated row replacement multiplies that row by the unit $H_p^{m_r}$. A block of $p-1$ positive integers contains one positive representative of each residue class modulo $p-1$. □

Corollary 68.12 (The span of the derivatives at one product shift)**.** *In each coordinate l of an elliptic product fix a torsion level $M_l \geq 2$, a mark t_l and a shift b_l, with torsion orders prime to the common good split prime p. Suppose $p > 2\max_l M_l^2 + 2$. Let $v_{\boldsymbol{a}}$ be any fixed array of vectors in a finite dimensional k-space, indexed by $\boldsymbol{a} \in \prod_l C_l[M_l]$. The vectors*

$$\sum_{\boldsymbol{a}} v_{\boldsymbol{a}} \prod_l J_{r_l}(U_{b_l} U_{a_l} \Theta_{t_l}), \qquad 1 \leq r_l \leq 2M_l^2 + 2,$$

span exactly the span of the $v_{\boldsymbol{a}}$. Each coordinate admits the same replacements of positive orders as in the theorem.

Proof. In each coordinate the rows in the theorem span the full dual of the space indexed by $C_l[M_l]$. Their tensor products span the full dual on the product index set. Applying to this dual the linear map sending a coordinate functional to the associated $v_{\boldsymbol{a}}$ gives the two asserted spans. □

Corollary 68.13 (Ranks of the positive-derivative Hankel matrices)**.** *For a nonzero scalar coefficient vector in the theorem write $m_n = \sum_a u_a J_n(U_b U_a \Theta_t)$ for $n \geq 0$, and let $H = H_p$. There are unique coefficients $w_z \in k$, indexed by $z^p = Hz$, with $m_n = \sum_z w_z z^n$ for all $n \geq 0$ (using $z^0 = 1$). At least one w_z with $z \neq 0$ is nonzero. For every integer $A \geq 1$,*

$$\operatorname{rank}(m_{A+i+j})_{0 \leq i,j \leq p-2} = |\{z \neq 0 : w_z \neq 0\}|.$$

If H and all m_n belong to $\mathbb{F}_p$, this rank is at least the multiplicative order of H in $\mathbb{F}_p^{\times}$.

Proof. The recurrence in Theorem 68.5 defines the moment functional $Z^n \mapsto m_n$ on $k[Z]/(Z^p - HZ)$. Since $H \neq 0$, the polynomial has p distinct roots. Evaluation at them identifies the quotient with k^p, giving the weights and their uniqueness. If their support were contained in zero, every positive derivative would vanish, contrary to the theorem. On the $p-1$ nonzero roots the square matrix $(z^i)_{0 \leq i \leq p-2, z \neq 0}$ is invertible. Multiplying it by the diagonal matrix with entries $w_z z^A$ and then by its transpose gives the displayed Hankel matrix, proving the rank. Over $\mathbb{F}_p$, uniqueness gives $w_{z^p} = w_z^p$. Each nonzero root has Frobenius orbit of length exactly the multiplicative order of H, since $z^p = Hz$. □

For the signed columns in Theorem 143.5, any torsion sums on a given product with the same derivative symbol can be grouped into an array as in the corollary, retaining all repeated indices in its coefficients. Its mixed derivatives detect this entire array at the fixed shift. The designated Weyl projections prescribe linear combinations of the derivatives. A lower bound on their images still needs information about which linear combinations the projected period supplies.

68.5 Common split primes for signed theta derivatives

At a split prime, a differential symbol multiplies the weights in Corollary 68.13 by its values at the roots of $Z^p - H_p Z$. To use this for a prescribed symbol, we need many roots carrying weight on the same reduction. We will choose a single prime for any given finite list of the marked curves and torsion data. The coefficients within a signed sum on their product can depend on all its torsion indices jointly.

Lemma 68.14 (The recurrence scalar and the Frobenius trace)**.** *Let the marked model in Lemma 68.4 reduce over $\mathbb{F}_p$, with $y^2 = f(x) = 4x^3 - g_2x - g_3$ and $\omega = dx/y$. Write $a_p = p + 1 - \#C(\mathbb{F}_p)$. Then*

$$H_p = [x^{p-1}]\, f(x)^{(p-1)/2} = a_p \pmod p.$$

Proof. Write $K = \mathbb{F}_p(C)$ and $L = K^p$, so $1, x, \dots, x^{p-1}$ is an L-basis of K. The L-linear operator $\partial = y\, d/dx$ has characteristic polynomial $T^p - H_pT$. Indeed it is annihilated by this separable polynomial by Lemma 68.4, and has rank $p-1$. Adjoin its eigenvalues to L. This is a separable extension and its compositum with the purely inseparable field K is their tensor product, hence is a field. There is a nonzero eigenvalue λ, with eigenvector u. The nonzero elements $1, u, \dots, u^{p-1}$ have distinct eigenvalues $0, \lambda, \dots, (p-1)\lambda$ by the derivation rule. They exhaust the dimension and prove the polynomial formula.

For a field element g let $\ell(g)$ be its coefficient on x^{p-1} in the displayed basis. The adjugate of d/dx maps g to the constant $-\ell(g)$. Its only nonzero cofactor comes from the entries $1, \dots, p-1$ on the superdiagonal, whose product is -1, with positive cofactor sign. Multiplication by y has determinant y^p, the norm in the purely inseparable extension of degree p. Its adjugate is therefore y^p times multiplication by $1/y$. Taking the adjugates in reverse order gives $\operatorname{tr}\operatorname{adj}(\partial) = -y^p\ell(1/y)$; here the trace of $g \mapsto L_0(g)\,1$ is $L_0(1)$ for any L-linear functional L_0. This trace is the coefficient of T in the characteristic polynomial, as p is odd. Since $1/y = f(x)^{(p-1)/2}/y^p$ and $3(p-1)/2 < 2p-1$, the only monomial of that numerator contributing to x^{p-1} in the field basis has degree $p-1$. This proves the first equality.

There are $1 + f(u)^{(p-1)/2}$ points above $x = u$ modulo p, including at a root of f. Add the point at infinity. The sum of u^j over $u \in \mathbb{F}_p$ is zero modulo p except for positive multiples of $p-1$, where it is -1. The degree of $f^{(p-1)/2}$ is less than $2(p-1)$, giving the asserted congruence for a_p. □

Theorem 68.15 (Simultaneously long orbits at a split prime)**.** *Fix finitely many marked CM elliptic curves as above, with any finite sets of algebraic coefficients and torsion translates used in their theta functions. Take a finite Galois number field J containing their CM fields, the data, the fields of the algebraic translation ratios and scalar normalizations, all their five-torsion points, and the fifth roots of unity. Fix $0 < \delta < 1/4$. For all sufficiently large X, among the rational primes $p \in [X, 2X]$ splitting completely in J, all but $O(X^{1-2\delta})$ satisfy*

$$\operatorname{ord}_{\mathbb{F}_p^\times}(H_p) > X^{1/4-\delta}$$

for every indicated curve at every place over p. The implied constant is absolute. In particular there are such primes in each sufficiently distant interval $[X, 2X]$ for the fixed data.

Proof. Take X above the finitely many bad primes and the torsion orders. At each completely split prime the residue field is $\mathbb{F}_p$, the group of rational points contains the full five-torsion, and $p \equiv 1 \bmod 5$. Consequently $a_p \equiv 2 \bmod 5$, excluding $0, 1, -1$. Also $|a_p| \le 2\sqrt{p}$ by Hasse's inequality. Recall its degree argument: for the p-power Frobenius T, the quadratic form on elliptic endomorphisms given by isogeny degree yields $\deg([m] - [n]T) = m^2 - a_pmn + pn^2$. Its cross term follows from $\deg(1 - T) = \#C(\mathbb{F}_p)$, since $1 - T$ is separable. Nonnegativity for integral m, n, and density of the ratios m/n in $\mathbb{R}$, give the bound.

Put $B = \lfloor X^{1/4-\delta} \rfloor$. For each integer a with $2 \le |a| \le 2\sqrt{2X}$ form the nonzero integer $N_a = \prod_{j=1}^{B}(a^j - 1)$. Its absolute logarithm $\log|N_a|$ is $O(B^2 \log X)$, by summing $\log(2|a|^j)$. Thus at most $O(B^2)$ distinct primes at least X divide it. Summing over the possible integers a gives $O(\sqrt{X}B^2)$ primes in total. Outside this single exceptional set, each possible Frobenius trace a_p has multiplicative order greater than B modulo p; for X large it is nonzero modulo

p. The lemma identifies its residue with H_p. The Chebotarev density theorem for the identity conjugacy class in $\mathrm{Gal}(J/\mathbb{Q})$ gives $(1+o_J(1))X/([J:\mathbb{Q}]\log X)$ completely split primes in $[X,2X]$ [9, §1A]. This exceeds the exceptional count for all sufficiently large X. □

Lemma 68.16 (The number of nonzero weights after scalar extension)**.** *Fix a curve at one of these primes, with the data of Theorem 68.11 defined over the common degree-one residue field, and $p>2M^2+2$. Write $d=M^2$ and $h=\mathrm{ord}_{\mathbb{F}_p^\times}(H_p)$. For* every *nonzero coefficient vector $u\in k^d$, the weight vector $W(u)=(w_z)_{z\neq 0,\ z^p=H_pz}$ of its positive derivatives has at least $\lceil h/d\rceil$ nonzero entries.*

Proof. The map W is linear and injective by Corollary 68.13 and Theorem 68.11. The derivative sequences of the individual basis translates are defined over $\mathbb{F}_p$. In fact the reference derivatives follow by differentiating $Dl=q_t,\ D\Theta_t=l\Theta_t$ from the marked values $l(0)=0,\Theta_t(0)=1$. The translates are obtained by their algebraic ratios and the scalar multipliers, all defined in J. Thus coefficient Frobenius $F:u\mapsto u^{(p)}$ sends the support of $W(u)$ to its permutation $z\mapsto z^p$, by uniqueness of the weights and conjugation of all the moments.

The span of $u,Fu,F^2u,\dots$ is generated by its first $j\le d$ vectors. Once a power lies in the span of its predecessors, that span is stable under the semilinear automorphism F, since its image has the same dimension. The union of the supports of W on this span therefore consists of entire Frobenius orbits, all of length h. It is nonempty by injectivity. It is already the union for the first j vectors, each with the same support size as $W(u)$. Hence $h\le j|\operatorname{supp}W(u)|$, as claimed. □

Corollary 68.17 (Bounded-degree symbols on a fixed signed tensor)**.** *On a product of the indicated curves let $F=\sum_{\boldsymbol a}u_{\boldsymbol a}\bigotimes_l U_{b_l}U_{a_l}\Theta_{t_l}$, where $a_l\in C_l[M_l]$, each b_l is fixed, and the coefficient array has nonzero reduction. Take a common prime as in the theorem with $p>2\max_l M_l^2+2$. Put $\Delta_l=\lceil\mathrm{ord}(H_{p,l})/M_l^2\rceil$. Let $P\in k[Z_1,\dots,Z_g]$ be nonzero of coordinate degrees $e_l<\Delta_l$. For each multi-index $\boldsymbol A$ with positive entries, the square matrix on $\boldsymbol i,\boldsymbol j\in\{0,\dots,p-2\}^g$ whose entry is the reduced mixed derivative*

$$J_{\boldsymbol A+\boldsymbol i+\boldsymbol j}(P(\partial)F)$$

has rank at least $\prod_l(\Delta_l-e_l)$. For fixed characteristic-zero data, a single prime can be chosen to give this nonvanishing for all nonzero reductions of symbols of any prescribed bounded coordinate degrees.

Proof. In coordinate l let $\mathcal{W}_l$ be the image of the map W in the lemma, viewed as functions on the $p-1$ nonzero roots. The weight function G on the product of these sets belongs to $\bigotimes_l\mathcal{W}_l$, and is nonzero since the tensor product of the injective maps W is injective. A polynomial in the derivatives multiplies it pointwise by P. Roots with some zero coordinate make no contribution to the displayed matrix since each A_l is positive.

We count the indices at which $PG\neq 0$. In one variable the lemma supplies at least Δ_1 points where $G\neq 0$; the polynomial can lose at most e_1. For the induction choose one value of the last variable for which the slice of G is nonzero. It belongs to the tensor product of the preceding spaces. Select any nonzero coefficient of P regarded as a polynomial in the last variable. Apply the induction hypothesis to this coefficient and the chosen slice. At least $\prod_{l<g}(\Delta_l-e_l)$ choices of the preceding coordinates give nonzero values for both. Over each such choice, the last fiber of G is a nonzero member of $\mathcal{W}_g$, and the last-variable polynomial is nonzero. The one-variable bound gives at least Δ_g-e_g points in that fiber. This proves the product bound.

The matrix in the assertion is a tensor product of invertible Vandermonde evaluation matrices on its left, their transposes on its right, and between them the diagonal with entries

$P(\boldsymbol{z})G(\boldsymbol{z})\prod_l z_l^{A_l}$. This follows by expanding the moments in each coordinate. Its rank is precisely the number just bounded. For fixed data the theorem allows every Δ_l to exceed the prescribed degrees at one prime. A minor nonzero in the residue field is also nonzero in characteristic zero for any integral lifts of the data. □

The further differentiations in the matrix run through a box of positive orders. In the period of Theorem 143.5 the final projection fixes its own linear functional on the derivatives. The rank bound proves survival under further differentiations of a fixed symbol. Application to that final functional requires showing which of these evaluations it retains.

68.6 Integral elementary divisors of the theta derivative table

We determine the integral image of all the input translates at a single auxiliary level, with the output shifts and orders fixed in advance. This gives the factorial cost in the marked differential even when the highest order exceeds the residue characteristic. Work over the integers O of a finite coefficient extension at a prime $p \geq 5$. Use a good Weierstrass model of the marked CM curve from Section 68.2, with $\omega = dx/y$ an integral generator and $p \nmid 2d_0$. We allow either splitting behavior of p in the CM field. Fix $M \geq 2$ prime to p and a finite nonempty set B of distinct shifts of order prime to p. For each $b \in B$ fix a lift, the point $P_b = b/M$ on the cover, and an integer $n_b \geq 1$. Take O large enough to contain these data and their translation factors. Put

$$d = M^2, \qquad n = \sum_{b\in B} n_b, \qquad D = \sum_{b\in B} n_b[P_b], \qquad P_* = Mt - \sum_{b\in B} n_b P_b \quad \text{in } C.$$

The n-by-d matrix E has column $a \in C[M]$ and row (b, j), $0 \leq j < n_b$, with entry $J_j(U_bU_a\Theta_t)$. The original shifts act on the outside of the input.

Lemma 68.18 (Factorials in the marked local frame)**.** *At each P_b use a local parameter w_b of the smooth integral curve, vanishing on the section P_b, and trivialize $\mathcal{L}_M = [M]^*\mathcal{O}([t])$ by s_c with $b + c \neq t$. Let B_0 map coefficients in the s_a to their ordinary Taylor coefficients in w_b through degree $n_b - 1$ at every P_b. There is a block diagonal matrix $L \in \mathrm{GL}_n(O)$, lower triangular in each block, such that*

$$E = L\ \mathrm{diag}_{(b,j)}(j!)\, B_0.$$

Proof. The proof of Lemma 68.7 gives an integral basis $s_a(v) = (U_a\Theta_t)(Mv)$ after reduction also at the present primes. Indeed its ingredients are the unit leading term of a prime-to-p torsion ratio, the distinct deck characters on $C[M]$, and Riemann–Roch. All three apply at good reduction when $p \nmid M$. At P_b the section s_c is a unit because its zero divisor is $[M]^*[t-c]$ and distinct prime-to-p torsion sections stay distinct.

Write $G_b(z) = (U_bU_c\Theta_t)(z)$. Its value at zero is a unit and its undivided derivatives are integral. For the latter assertion, $q_t = -u_\Lambda - x(z+t)$ is regular at the origin over O because t is a nonzero section of order two and the CM formula in Lemma 68.4 for u_Λ has unit denominator at $p \nmid 2d_0$. Integrating the identities $Dl = q_t$, $D\Theta_t = l\Theta_t$ as undivided derivative sequences from $l(0) = 0, \Theta_t(0) = 1$ preserves integrality by the Leibniz rule. The ratio for the prime-to-p translate is integral in an algebraic parameter at the origin, as proved in Theorem 65.6, and its constant term here is a unit. Composition of the two translations adds a root of unity.

For a section with local representative $h = S/s_c$, its marked derivatives are those of $G_b(z)h(P_b + z/M)$, by the quotient formula in Theorem 68.8. On the cover let $D_b = M^{-1}\partial_v$, so $D_b^j w_b(P_b)$ is integral in every positive order and $D_b w_b(P_b)$ is a unit. For the term w_b^j in h, each undivided derivative of order r of $G_b w_b^j$ at the point is divisible by $j!$. In the repeated product rule assign the r labeled derivatives to G_b and to the j ordered copies of w_b. A term

survives only if every copy of w_b receives a derivative. Permuting these copies acts freely on the assignments that survive and preserves their value. Each orbit thus contributes $j!$ times an integral element. For $r < j$ there is no such assignment, and for $r = j$ the quotient by $j!$ is $G_b(0)(D_b w_b(P_b))^j$, a unit. The case $j = 0$ uses the single empty family of copies and the same diagonal formula. Truncation of h is legitimate since an order r derivative depends only on its first $r + 1$ coefficients. This gives the claimed matrices L directly. □

Theorem 68.19 (The integral image at and above the interpolation degree)**.** *Suppose $d \ge n$. If $d > n$, or if $d = n$ and $P_* \neq 0$, then*

$$\operatorname{coker}_O E \simeq \bigoplus_{b \in B,\, 0 \le j < n_b} O/(j!).$$

If $d = n$ and $P_* = 0$, choose a row $m = (b_*, n_{b_*} - 1)$ with $n_{b_*} = \max_b n_b$. In this case

$$\operatorname{coker}_O E \simeq O \;\oplus \bigoplus_{(b,j) \neq m,\; 0 \le j < n_b} O/(j!).$$

Proof. The matrix B_0 reduces to restriction of all sections of $\mathcal{L}_M$ to the divisor D on the special fiber, in the chosen Taylor bases. Its kernel over that field is $H^0(\mathcal{L}_M(-D))$. When $d > n$ this has dimension $d - n$ by Riemann–Roch, so restriction is onto. If $d = n$ the class of $\mathcal{L}_M(-D)$ in $\operatorname{Pic}^0(C) = C$ is P_*. In fact the zeros of s_0 are $v_0 + C[M]$ for $Mv_0 = t$, and their group sum is $M^2 v_0 = Mt$. The sum of $C[M]$ is zero by pairing inverses and, for even M, summing the four two-torsion points. Subtracting D gives the formula, on either fiber. All the points involved have order prime to p, so $P_* \neq 0$ remains nonzero on reduction. A nontrivial degree-zero bundle has no section. Thus B_0 is surjective over the residue field in this case as well. In both cases some n-row square minor is a unit over O. The lemma now gives the first cokernel.

Suppose $d = n$ and $P_* = 0$. Over the fraction field the bundle $\mathcal{L}_M(-D)$ is trivial. Choose a section S_* of $\mathcal{L}_M$ with divisor D, multiplying by a scalar to make its coordinates in the s_a integral with some coordinate a unit. It is nonzero on reduction by the basis lemma. In the local frames above, $S_*/s_c = w_b^{n_b} u_b(w_b)$ with $u_b(0)$ a unit. Indeed the lower coefficients vanish in characteristic zero, and the reduction already has zeros of total multiplicity at least $n = d$ at the distinct reductions. Each therefore has exactly the prescribed multiplicity.

On a tuple $(h_b \bmod w_b^{n_b})_b$ define the integral linear form

$$R((h_b)_b) = \sum_b \operatorname{res}_{P_b} \frac{h_b\, \omega}{w_b^{n_b} u_b(w_b)}.$$

The indicated coefficient of $w_b^{-1} dw_b$ depends only on the given jet. The coefficient of the last Taylor entry at each b is a unit since both $u_b(0)$ and the coefficient of dw_b in ω are units. For $h_b = S/s_c$ the differentials in this sum come from $(S/S_*)\omega$. It has no poles elsewhere, so its residues sum to zero. The image of B_0 lies in $\ker R$. Over the residue field its rank is $d - 1$ by the one-dimensional kernel computed from the trivial degree-zero bundle. Since R is primitive and splits off one coordinate, $\ker R$ reduces onto the residue kernel of its reduction. Nakayama's lemma gives $\operatorname{im} B_0 = \ker R$ over O.

Write $R(h) = \sum_i R_i h_i$ and $w_i = j!$ for row $i = (b, j)$. Eliminate coordinate m using the unit R_m. After applying $\operatorname{diag}(w_i)$, the other rows on the free coordinates of this kernel are diagonal with entries w_i, and the last row has entries $-w_m R_i / R_m$. Each w_i divides w_m by the choice of m. Integral row additions therefore clear the entire last row. Multiplying by L does not change the cokernel. This proves the second formula. □

Corollary 68.20 (Determinantal ideals after a fixed signed projection)**.** *Use finitely many coordinates l in the first case of the theorem. Let A be any specified integral linear map from the array of their derivative values to a free target, incorporating the desired signs and projections. Write $E_{\otimes} = \bigotimes_l E_l$, $L_{\otimes} = \bigotimes_l L_l$, and $w_i = \prod_l j_l!$ for the row $i = ((b_l, j_l))_l$. If I_s denotes the ideal generated by all minors of size s, then*

$$I_s(AE_{\otimes}) = \sum_{|T|=s} \left(\prod_{i \in T} w_i \right) I_s((AL_{\otimes})_{*,T}).$$

The sum uses subsets of the row index set of the derivative array. One common input level can ensure the strict inequality $M^2 > \sum_b n_{l,b}$ in every coordinate. Given a prime P_0 distinct from the coefficient primes under study, take the least power $M \geq 2$ of P_0 greater than $\sqrt{\max_l \sum_b n_{l,b}}$.

Proof. The tensor product of the surjective Taylor maps $B_{0,l}$ has an integral right inverse, by tensoring choices of right inverses for the free targets. Appending this surjection to a matrix leaves every determinantal ideal equal, by Cauchy–Binet first for the product and then for its product with the right inverse. In the resulting matrix $AL_{\otimes} \operatorname{diag}(w_i)$ each minor using column set T acquires exactly the product displayed. This proves the formula, including vanishing ideals. The stated power gives $M^2 > \sum_b n_{l,b}$ directly. □

For a product slot in the signed period, the formula applies when its fixed class actions are expressed by these outer shifts and the fixed linear map on the resulting jets. It computes the ideal over all columns of the common input level. Determining which minors survive on the prescribed input columns, including the original vacuum $a = 0$, remains part of the integral period comparison of Section 6.6.

68.7 The archimedean determinant of the same elliptic jets

Fix a complex embedding of the marked model in Theorem 68.19. Write $C = \mathbb{C}/\Lambda$, $c = \pi/\operatorname{area}(\Lambda)$, and use the metric $\|f(v)\| = \exp(-c|v|^2/2)|f(v)|$ in degree one. Let h be an odd theta section with simple zero at zero, in the same Hermitian frame. Normalize its positive scalar so that $g(v) = \|h(v)\|$ satisfies $\int_C \log g(v)\, dv = 0$, using Haar probability. The phase of h can be chosen freely. Its sole logarithmic singularity is integrable. Put $\gamma = \lim_{v \to 0} g(v)/|v| = |h'(0)| > 0$. Thus g is the multiplicative Arakelov Green function with one argument zero. Write $\Theta_t(0) = 1$ for the even marked theta section of divisor $[t]$, $M \geq 2$, $d = M^2$, and order the sections $s_a(v) = (U_a\Theta_t)(Mv)$, $a \in C[M]$. Here and below a point in a holomorphic formula comes with a chosen lift. Norms on the torus do not require lifts.

Lemma 68.21 (Distribution over torsion)**.** *For every integer $m \geq 2$,*

$$\prod_{a \in C[m]} g(v + a) = g(mv), \qquad \prod_{a \in C[m] \setminus \{0\}} g(a) = m.$$

In particular the sum of $\log g(a)$ over the points of exact order m is $\Lambda(m)$, the von Mangoldt function. Also $\|\Theta_t(v)\| = g(v - t)/g(t)$.

Proof. Away from its zero the logarithm of the theta norm is the log absolute value of a holomorphic nonvanishing function minus $c|v|^2/2$. Hence the two sides of the first identity have logarithms with the same Laplacian and matching simple zeros. Their log difference extends harmonically across those zeros. It is constant on the compact torus and has mean zero because translation and multiplication by m preserve Haar probability. Letting $v \to 0$ gives the second assertion by the definition of γ. These are the elliptic projection and torsion

product formulas [10, Thm. 3.2, Cor. 4.5]. Partition the nonzero m-torsion by exact order and apply Möbius inversion to $\log m = \sum_{e\mid m} \Lambda(e)$, with order one omitted. For the last assertion the two norms have the same curvature and divisor. Their ratio is constant by the same harmonic argument. Evaluation at zero and $g(-t) = g(t)$ fix it. □

Theorem 68.22 (The alternating determinant in the marked frame)**.** *There is a constant ξ of absolute value one, independent of $v_1, \dots, v_d$, such that*

$$\det\bigl(s_a(v_i)\bigr)_{i,a} = \xi\, \frac{M^{d/2}}{g(t)^d}\, (U_{-Mt}h)\biggl(\sum_{i=1}^{d} v_i\biggr) \prod_{i<j} h(v_j - v_i).$$

The constant is determined, including its phase, by evaluation at any ordered fiber $v_0 + C[M]$ for which $dv_0 \neq Mt$ on C.

Proof. First take distinct points v_i on the torus. Their evaluation matrix is singular exactly when a nonzero section of $\mathcal{L}_M = [M]^*\mathcal{O}([t])$ vanishes at all of them. The s_a form a basis in characteristic zero by the deck character calculation of Lemma 68.7. The degree of $\mathcal{L}_M$ is d and its divisor class has group sum Mt, as in Theorem 68.19. Thus singularity for distinct points is equivalent to $\sum_i v_i = Mt$ on C.

Consider the norm of the determinant, using the pullback degree-d metric in every row. Fix all but v_i in general position. As a section in v_i, it vanishes at the other $d-1$ points by equality of rows in the same fiber, and at $Mt - \sum_{j\neq i} v_j$ by the divisor criterion. For general fixed points these are d distinct zeros. The section is nonzero for other v_i, so each zero is simple. The product

$$g\biggl(\sum_i v_i - Mt\biggr) \prod_{i<j} g(v_j - v_i)$$

has these same zeros and curvature in v_i. The logarithm of the ratio of norms is harmonic across the zeros and constant in this variable. This argument applies to every variable. Equivalently the ratio on the locus of nonzero evaluations is locally constant on the generic open set. It has a single value there, since the complement of finitely many proper analytic divisors in a connected complex torus product is connected (a path can be displaced locally away from real codimension two). Continuity gives the same norm identity at every tuple.

To evaluate its constant use a fiber $v_0 + C[M]$ as in the statement. All the row fibers are canonically identified by pullback from Mv_0. In these identifications column a is its value at v_0 times a character of $C[M]$, and the d characters are distinct. The Fourier matrix has determinant of modulus $d^{d/2}$, since its product with its adjoint is dI. The product of the norms at v_0 equals

$$g(t)^{-d} \prod_{a\in C[M]} g(Mv_0 + a - t) = g(t)^{-d} g(dv_0 - Mt)$$

by the lemma and the unitary translation formula. The group sum over the fiber is dv_0. The product over its unordered pairs of g of their differences is $M^{d/2}$. Indeed its square counts each nonzero difference exactly d times and $g(-a) = g(a)$. The lemma supplies the product over the nonzero differences. Dividing gives the asserted constant in norm, since $d^{d/2}/M^{d/2} = M^{d/2}$.

The marked translation satisfies $\|U_w h(v)\| = g(v + w)$. Moreover

$$\biggl|\sum_i v_i\biggr|^2 + \sum_{i<j} |v_j - v_i|^2 = d \sum_i |v_i|^2.$$

Thus the Gaussian metric factors on the two holomorphic sides agree exactly on the universal cover. Their holomorphic quotient has constant absolute value wherever defined. The open

mapping theorem makes it constant on a nonempty open set, and the identity theorem gives the asserted formula everywhere, also at repeated points. A nonsingular fiber fixes ξ. □

Corollary 68.23 (The absolute determinant for prescribed multiplicities)**.** *Take pairwise distinct outer shifts b and integers $n_b \geq 1$ with $\sum_b n_b = d$. Use $P_b = b/M$ and the matrix E of Theorem 68.19, and put $u = \sum_b \binom{n_b}{2}$. Its exact determinant norm is*

$$|\det E| = \frac{M^{d/2}}{g(t)^d} \left(\frac{\gamma}{M}\right)^u \left(\prod_b \prod_{j=0}^{n_b-1} j!\right) g\Big(\sum_b n_b P_b - Mt\Big) \times \prod_{b<b'} g(P_{b'} - P_b)^{n_b n_{b'}}.$$

Any ordering of the shifts gives the same product. In particular the very same group sum governs vanishing at the complex embedding and the exceptional relation in the integral theorem.

Proof. In each cluster indexed by b, replace P_b by the n_b points $P_b + \epsilon t_j$ for distinct fixed complex numbers t_j. Use the Hermitian translation at P_b as a holomorphic local frame with unit norm at that point. In this frame the representative of s_a at w is $(U_b U_a \Theta_t)(Mw)$, by the explicit translation formula with metric parameter dc on the cover. Expand each row in ϵt_j. Alternation forces distinct powers within each cluster. Dividing the determinant by the product within each cluster of $\epsilon(t_j - t_i)$, then passing to the limit, gives the determinant with consecutive Taylor-coefficient rows. The coefficient of order j is $M^j J_j(U_b U_a \Theta_t)/j!$. This limiting identity also holds if its determinant is zero. The additional metric factors in the local frames tend to one. On the product of norms in the theorem each internal pair contributes γ after division, all other factors tending to the displayed values. The number of internal pairs, and the sum of all the row orders, both equal u. This gives the formula with all factorials. □

Corollary 68.24 (Fixed signed rows and selected torsion columns)**.** *Let $A \subset C[M]$ have size $s \geq 1$. Choose s fixed linear functionals L_i on the s_a, each given by a finite signed linear combination of marked derivative evaluations at prescribed shifts, with arbitrary orders. Every minor $\det(L_i(s_a))_{1\leq i\leq s,\, a\in A}$ is obtained by applying an explicit product of row functionals to the single holomorphic product in the theorem, including its one common phase. This uses the prescribed evaluations, with no further derivative orders in those rows.*

Proof. For a row of order j at $b = MP_b$, apply in its own variable the functional

$$f \longmapsto M^{-j} \, \frac{d^j}{dw^j} \left(e^{-dcw\overline{P_b} - dc|P_b|^2/2} f(P_b + w)\right)\Big|_{w=0}.$$

The local translation identity just proved gives the desired J_j. Extend linearly with the specified signs. For $s = d$ apply these functionals in independent variables to the determinant identity and use its multilinearity.

For $s < d$ select a nonsingular fiber $v_0 + C[M]$. Identify its row fibers by the pullback action and choose one common frame, writing λ_z for evaluation there at $v_0 + z$. Set $s_a^0 = \lambda_0(s_a) \neq 0$, and let χ_a be its actual deck character, so $\lambda_z(s_a) = \chi_a(z) s_a^0$. For each $a' \notin A$ append the evaluation row

$$\frac{1}{d\, s_{a'}^0} \sum_{z \in C[M]} \chi_{a'}(z)^{-1} \lambda_z.$$

Character orthogonality makes this row one at a' and zero on all other columns. Order these appended rows and permute the full columns with the associated determinant sign. Expansion along the appended rows leaves the requested minor. Each λ_z in the holomorphic frame is a

scalar times point evaluation, determined by the common pullback identification (equivalently normalize it so that $\lambda_z(s_0) = \lambda_0(s_0)$). This specifies all the functionals occurring on the product. □

The formulas give the finite and archimedean sizes of a whole elliptic interpolation determinant in the same normalization. They also retain the cancellations in prescribed rows of one elliptic slot. For the full period, different slots are coupled by the class sum and the final projections in Theorem 143.5. An upper estimate and the required rank for that coupled determinant on the interval of Section 6.6 remain to be proved.

68.8 The rational norm of the marked elliptic determinant

We now sum the archimedean identity of Corollary 68.23 over the embeddings of the actual coefficient field. Write K for the imaginary quadratic field, assume complex multiplication by its full ring of integers $\mathcal{O}_K$, and use the same marked differential $\omega = dx/y$. For a proper nonzero ideal $\mathfrak{a}$ put

$$\Phi_K(\mathfrak{a}) = |(\mathcal{O}_K/\mathfrak{a})^\times|,$$
$$\Lambda_K(\mathfrak{a}) = \begin{cases} \log N\mathfrak{q}, & \mathfrak{a} = \mathfrak{q}^e, \quad \mathfrak{q} \text{ prime}, \ e \geq 1, \\ 0, & \text{otherwise}, \end{cases} \qquad b_K(\mathfrak{a}) = \frac{\Lambda_K(\mathfrak{a})}{2\Phi_K(\mathfrak{a})}.$$

For a nonzero torsion point P, abbreviate $b_K(\operatorname{Ann}_{\mathcal{O}_K} P)$ to $b_K(P)$.

Lemma 68.25 (The Green function in the original differential)**.** *At every complex embedding the coefficient γ of Lemma 68.21 satisfies $\gamma^{12} = |g_2^3 - 27g_3^2|$ in the Weierstrass equation $y^2 = 4x^3 - g_2x - g_3$ with $dz = dx/y$. In particular $\gamma = 1$ on the discriminant-one model of Proposition 65.21.*

Proof. Let t_1, t_2, t_3 be the nonzero two-torsion points and put $e_i = x(t_i)$. The elliptic function $x - e_i$ has divisor $2[t_i] - 2[0]$ and leading coefficient one at its double pole in the coordinate z. Cancellation of zeros, poles and curvatures makes the logarithm of the ratio between $|x(v) - e_i|$ and $g(v - t_i)^2/g(v)^2$ constant off their divisors and harmonic across them. Comparison at zero gives

$$|x(v) - e_i| = \frac{\gamma^2}{g(t_i)^2} \frac{g(v - t_i)^2}{g(v)^2}.$$

Evaluate at t_j for $i \neq j$, using $t_j - t_i = t_k$ at the third index. Multiplication over the three unordered pairs gives $\prod_{i<j} |e_i - e_j| = \gamma^6/(\prod_i g(t_i))^2 = \gamma^6/4$ by Lemma 68.21 at $m = 2$. The cubic discriminant identity is $g_2^3 - 27g_3^2 = 16 \prod_{i<j}(e_i - e_j)^2$. Taking absolute values proves the claim. □

Lemma 68.26 (The arithmetic mean of a torsion Green value)**.** *Let $P \neq 0$ be a torsion point on C. Take a number field J containing K over which the curve, its CM action and P are defined. If g_σ denotes the normalized function of Lemma 68.21 on C^σ, then*

$$\frac{1}{[J : \mathbb{Q}]} \sum_{\sigma : J \hookrightarrow \mathbb{C}} \log g_\sigma(P^\sigma) = b_K(P).$$

Proof. For each ideal class take its complex torus $C_I = \mathbb{C}/I$, and for each integral ideal $\mathfrak{a}$ use the quotient isogeny $f : C_I \longrightarrow C_{\mathfrak{a}^{-1}I}$. Its kernel is $C_I[\mathfrak{a}]$ of order $N\mathfrak{a}$. Use any nonzero complex coordinates on the source and target. The product of $g_{C_I}(v + Q)$ over the kernel equals $g_{C_{\mathfrak{a}^{-1}I}}(f(v))$. In fact the isogeny pulls back probability area on the target to $N\mathfrak{a}$ times

probability area on the source, so the logarithms have equal Laplacian off their matching simple zeros. Their log difference is harmonic on the torus and has mean zero, just as in Lemma 68.21.

For a torus $C_L = \mathbb{C}/L$ put $h(C_L) = \log(\gamma_{C_L}\sqrt{\operatorname{area}(L)})$; this depends only on its complex isomorphism class since scaling a lattice scales the derivative and the square root of the area inversely. Let v tend to zero in the product identity. The tangent factor satisfies $|f'(0)|^2 \operatorname{area}(I) = N\mathfrak{a}\,\operatorname{area}(\mathfrak{a}^{-1}I)$ in compatible coordinates. It follows that

$$\sum_{0\neq Q\in C_I[\mathfrak{a}]} \log g_{C_I}(Q) = \tfrac{1}{2}\log N\mathfrak{a} + h(C_{\mathfrak{a}^{-1}I}) - h(C_I).$$

Average over all ideal classes. The last two terms cancel since multiplication by $\mathfrak{a}^{-1}$ permutes the classes. Partition the sum on the left by exact annihilator. Unique factorization of ideals gives $\log N\mathfrak{a} = \sum_{\mathfrak{b}\mid\mathfrak{a}} \Lambda_K(\mathfrak{b})$, with the unit ideal contributing zero. Möbius inversion therefore makes the class average of the sum over exact annihilator $\mathfrak{a}$ equal to $\frac{1}{2}\Lambda_K(\mathfrak{a})$.

For the passage to embeddings we use the main theorem of complex multiplication for elliptic curves in its reciprocity form [1, Part II]. For the CM type given by the chosen embedding of K, the finite ideles act on the completed ideal lattice and its torsion by multiplication, up to simultaneous isomorphism of the marked pair. Reciprocity identifies these isomorphism classes with the Galois orbit over K. The ideal part reaches every lattice class. At a fixed class, the integral idele units map onto $(\mathcal{O}_K/\mathfrak{a})^{\times}$ by local reduction. The module $\mathfrak{a}^{-1}I/I$ is free of rank one over $\mathcal{O}_K/\mathfrak{a}$, as is seen separately at each prime power and then by the Chinese remainder theorem. Thus the unit group acts transitively on its $\Phi_K(\mathfrak{a})$ generators, exactly the points of the stipulated annihilator. Passing to isomorphism classes at each lattice identifies the action of $\mathcal{O}_K^{\times}$. Every generator has the same stabilizer, consisting of units congruent to one modulo $\mathfrak{a}$, and g is invariant under these isomorphisms by its normalization. Consequently the uniform class and generator average just computed is the uniform average on the Galois orbit. Embeddings of J extending the chosen embedding of K give equal multiplicities on that orbit, by passing to a normal closure. The other embedding uses $\overline{\mathfrak{a}}$, for which b_K has the same value. Division by the number of generators proves the asserted mean. □

Theorem 68.27 (The rational norm of the complete elliptic jet determinant)**.** *Use the square matrix E of Corollary 68.23 with the original discriminant-one differential. Assume $P_* = Mt - \sum_b n_b P_b \neq 0$. Take a coefficient field J containing all the points, the CM action, the algebraic translation data and the entries of E. With $u = \sum_b \binom{n_b}{2}$, one has*

$$\frac{\log|N_{J/\mathbb{Q}}\det E|}{[J:\mathbb{Q}]} = (d/2-u)\log M + \sum_b \sum_{j=0}^{n_b-1} \log(j!) - d\,b_K(t) + b_K(P_*) + \sum_{b<b'} n_b n_{b'}\, b_K(P_b - P_{b'}).$$

For a general good algebraic scaling of the differential add $\frac{u}{12[J:\mathbb{Q}]}\log|N_{J/\mathbb{Q}}(g_2^3 - 27g_3^2)|$ to the right. If $P_* = 0$ the determinant itself is zero.

Proof. We first justify using the same marked table after each embedding. Phases have to be compatible in a determinant. On the M-cover, write $s_a/s_0 = R_a(Mv)$. Theorem 65.6 shows as germs at zero that $\sigma(R_a(Mv))$ is a single root of unity ϵ_a times the transported torsion ratio for a^{σ}. Here the origin parameter is taken with respect to the transported differential. Both ratios on the cover are rational functions, so this equality holds globally. For each b choose c with $b + c \neq t$. The ratio of the two row germs for a, c is $(s_a/s_c)(P_b + z/M)$. After transport it is the corresponding ratio multiplied by ϵ_a/ϵ_c, choosing the lift of b^{σ} to be M times the

chosen lift of P_b^{σ}. The denominator germ $U_bU_c\Theta_t$ is itself a root of unity times $U_{b+c}\Theta_t$, whose algebraic transport has a single phase in every derivative order by the same theorem. Thus the matrix after embedding differs from the analytically transported matrix by unit phases on its columns and on each row block, as well as a possible permutation of columns. Their determinant absolute values agree.

Take logarithms of the formula of Corollary 68.23. Distinct b's give distinct P_b's, t is nonzero, and the assumed condition makes every factor nonzero. Average each term over the embeddings. Lemma 68.26 applies individually to t, P_* and all the differences, on the same field J. Additivity of the logarithm needs no independence between these points. Lemma 68.25 evaluates the remaining tangent factor, also for the alternate scaling. The singular case follows at once from the complex formula. □

Corollary 68.28 (Prime-by-prime mean content and the total pair contribution)**.** *For a rational prime p define $b_{K,p}(P) = 0$ unless $\mathrm{Ann}(P) = \mathfrak{p}^e$ for a prime $\mathfrak{p} \mid p$ and $e \ge 1$. In this case put $b_{K,p}(P) = f(\mathfrak{p}/p)/(2\Phi_K(\mathfrak{p}^e))$. On the discriminant-one model with $\det E \neq 0$, the exact mean of its valuations v_λ, normalized by $v_\lambda(p) = 1$, is*

$$\begin{aligned}\frac{1}{[J:\mathbb{Q}]}\sum_{\lambda\mid p}[J_\lambda:\mathbb{Q}_p]\,v_\lambda(\det E) = (d/2-u)v_p(M) + \sum_b \sum_{j=0}^{n_b-1} v_p(j!)\\ - d\,b_{K,p}(t) + b_{K,p}(P_*)\\ + \sum_{b<b'} n_b n_{b'}\, b_{K,p}(P_b - P_{b'}).\end{aligned}$$

Furthermore, if the differences $P_b - P_{b'}$ belong to $C[\mathfrak{m}]$, with integral nonzero ideal $\mathfrak{m}$, and $n_{\max} = \max_b n_b$, then

$$0 \;\le\; \sum_{b<b'} n_b n_{b'} b_K(P_b - P_{b'}) \;\le\; \tfrac{1}{4} d\, n_{\max} \log N\mathfrak{m}.$$

Equality on the right holds for a full coset of $C[\mathfrak{m}]$ with equal multiplicities.

Proof. Every term in the rational norm formula is a finite rational linear combination of logarithms of rational primes. The coefficient of $\log p$ in $b_K(P)$ is $b_{K,p}(P)$. The logarithm on the left has coefficient $v_p(N_{J/\mathbb{Q}}\det E)/[J:\mathbb{Q}]$, equal to the displayed local mean by the norm formula. These coefficients are unique, since clearing denominators in a rational relation among logarithms of distinct primes gives an integer factorization of one. This includes primes dividing M or the shift orders.

For fixed b the differences with $b' \neq b$ are distinct. For any nonunit ideal $\mathfrak{a} \mid \mathfrak{m}$ at most $\Phi_K(\mathfrak{a})$ of them have that exact annihilator. Multiplying by $b_K(\mathfrak{a})$ and summing over the divisors of $\mathfrak{m}$ gives at most $\frac{1}{2}\log N\mathfrak{m}$. Bound each $n_{b'}$ by $n_{\max}$, multiply by n_b, sum using $\sum_b n_b = d$, and divide by two to pass to unordered pairs. All terms are nonnegative. A full coset with equal multiplicities attains every counting bound. □

These are arithmetic norm and valuation identities for the same elliptic block over the period field and any larger coefficient field. They use only its listed torsion points, their multiplicities and the original differential. The signed sums over several edges and the prescribed projection in the GRH argument have a different determinant. Their interaction and the uniform cohomology estimate of Section 6.6 remain to be established.

68.9 Green energy and signed elliptic determinants

The absolute norm of a single determinant is given by Theorem 68.27. In a sum of determinants the largest summand can depend on the embedding. We first bound the product over point differences uniformly over configurations at each embedding.

Theorem 68.29 (Weighted elliptic Green energy)**.** *Let g be the multiplicative Green function of Lemma 68.21 on a complex torus of area A in its chosen coordinate. Put*

$$\widehat{\gamma} = \sqrt{A}\,\lim_{v\to 0} g(v)/|v|, \qquad L_C = \log\pi + 1 + \gamma_{\mathrm{E}} - 2\log\widehat{\gamma},$$

where γ_{E} is Euler's constant. At distinct points z_i take positive real weights w_i, with $N = \sum_i w_i$ and $B = \sum_i w_i^2$. Then

$$\sum_{i<j} w_i w_j \log g(z_i - z_j) \le \frac{B}{4}\bigl(\log(N^2/B) + L_C\bigr), \qquad \sup_{z\in C} \log g(z) \le \tfrac{1}{2}(\log 2 + L_C).$$

Proof. Rescale the coordinate by $A^{-1/2}$, so that the lattice Λ now has covolume one. The function $G = \log g$ has mean zero and $G(z) = \log|z| + \log\widehat{\gamma} + o(1)$ at zero. In this coordinate its distributional Laplacian is $2\pi(\delta_0 - 1)$. Indeed the logarithm of a holomorphic simple zero contributes $2\pi\delta_0$, and the log of the metric contributes the Laplacian of $-\pi|z|^2/2$. For $t > 0$ let $G_t = H_t * G$, with the periodic heat kernel

$$H_t(z) = \frac{1}{4\pi t}\sum_{\lambda\in\Lambda} e^{-|z+\lambda|^2/(4t)}.$$

The kernel has integral one by unfolding the lattice sum. The Fourier coefficient of G_t at a nonzero dual vector ξ is $-e^{-4\pi^2 t|\xi|^2}/(2\pi|\xi|^2)$, by applying the Laplacian to the Fourier character $e^{2\pi i\langle\xi,z\rangle}$. The constant coefficient is zero. The series is absolutely convergent. Each nonconstant term of $\sum_{i,j} w_i w_j G_t(z_i - z_j)$ is this negative coefficient times the squared modulus of a sum of characters. The double sum is therefore nonpositive.

We have $\partial_t G_t = 2\pi(H_t - 1)$. At $z \neq 0$, integration from time zero and $H_t \ge 0$ give $G(z) \le G_t(z) + 2\pi t$. At zero the contribution of the central Gaussian to the heat average of $\log|z|$ is $\frac{1}{2}\log(4t) - \frac{1}{2}\gamma_{\mathrm{E}}$. This follows by the radial substitution $r^2/(4t) = y$ and $\int_0^\infty e^{-y}\log y\,dy = -\gamma_{\mathrm{E}}$. For the small-time limit one may restrict to a disk about zero smaller than half the shortest period. The heat mass outside the disk decays exponentially, also against the integrable periodic logarithmic singularity. Inside the disk the continuous remainder tends in heat average to $\log\widehat{\gamma}$. Integrating the displayed time derivative from this limit gives

$$G_t(0) = \tfrac{1}{2}\log(4t) - \tfrac{1}{2}\gamma_{\mathrm{E}} + \log\widehat{\gamma} - 2\pi t + 2\pi\int_0^t \frac{1}{4\pi s}\sum_{0\neq\lambda\in\Lambda} e^{-|\lambda|^2/(4s)}\,ds.$$

The integral is nonnegative. If E is the pair sum in the theorem, the nonpositive double sum and the off-diagonal inequality give $2E \le -BG_t(0) + 2\pi t(N^2 - B)$. Substitute the lower bound for $G_t(0)$ and take $t = B/(4\pi N^2)$. This proves the first assertion. Two points with unit weights give the second at every nonzero difference. At zero g vanishes. □

For the following results use the discriminant-one model with CM by $\mathcal{O}_K$. Write $d_0 = |\operatorname{disc} K|$, $D_{\xi_{d_0}} = L'(1,\xi_{d_0})/L(1,\xi_{d_0})$, and set

$$L_K = 1 + \log\left(\frac{\sqrt{d_0}}{2\pi}\right) + D_{\xi_{d_0}}.$$

Use $\mathbb{E}_\sigma$ for the uniform mean over all complex embeddings of the common coefficient field J of Theorem 68.27. Lemma 68.25 gives $\widehat{\gamma}_\sigma = \sqrt{A_\sigma}$, and Theorem 65.22 gives $\mathbb{E}_\sigma L_{C^\sigma} = L_K$.

Theorem 68.30 (A signed sum with prescribed row multiplicities). *Fix $M \ge 2$, $d = M^2$, the nonzero mark t, and positive multiplicities $n_1, \dots, n_m$ of sum d. Let $u = \sum_i \binom{n_i}{2}$, $B = \sum_i n_i^2$. Form any finite list of the complete marked matrices of Corollary 68.23. Use these multiplicities in each matrix and any distinct torsion shifts within that matrix. For $Z = \sum_\lambda c_\lambda \det E_\lambda \neq 0$, $c_\lambda \in J$,*

$$\mathbb{E}_\sigma \log|\sigma Z| \le \mathbb{E}_\sigma \log \sum_\lambda |\sigma c_\lambda| + (d/2 - u)\log M + \sum_i \sum_{j=0}^{n_i - 1} \log(j!) - d\, b_K(t) + \tfrac{B}{4}\big(\log(d^2/B) + L_K\big) + \tfrac{1}{2}(\log 2 + L_K).$$

Proof. At each embedding apply the confluent formula to all the transported matrices. The transport preserves their absolute determinants by the row and column phase calculation in Theorem 68.27. The tangent factor is one before the factor M^{-u}. The weighted energy bound with $z_i = P_i = b_i/M$, $w_i = n_i$ bounds the log of the pair product. The supremum bound controls the remaining factor at $\sum n_i P_i - Mt$. Both bounds hold simultaneously for every tuple of the given shape. A singular summand contributes zero. The triangle inequality now bounds $|\sigma Z|$ by $\sum |\sigma c_\lambda|$ times the common upper bound. Take logarithms and average. Lemma 68.26 gives $\mathbb{E}_\sigma \log g_\sigma(t^\sigma) = b_K(t)$. □

Corollary 68.31 (Arbitrary derivative orders on the complete input basis). *Keep the same CM curve, mark, and input columns $a \in C[M]$. Choose nonnegative orders $j_1, \dots, j_d$. In summand λ let row i be the order-j_i derivative at zero of $U_{b_{\lambda i}} U_a \Theta_t$ in column a, with any torsion shifts $b_{\lambda i}$, including repetitions. Denote the resulting matrix by F_λ. Define $C(0) = 1$ and $C(j) = j!(e/j)^{j/2}$ for $j \ge 1$. If $Z = \sum_\lambda c_\lambda \det F_\lambda \neq 0$, then*

$$\mathbb{E}_\sigma \log|\sigma Z| \le \mathbb{E}_\sigma \log \sum_\lambda |\sigma c_\lambda| + \tfrac{d}{2}\log M - d\, b_K(t) + \tfrac{d}{4}(\log d + L_K) + \tfrac{1}{2}(\log 2 + L_K) + \sum_i \log C(j_i) + \tfrac{1}{2}\Big(\sum_i j_i\Big)\Big(D_{\xi_{d_0}} - \gamma_{\mathrm{E}} - \log(2\pi/\sqrt{d_0})\Big).$$

Proof. Use a different complex displacement z_i in each physical row before differentiating, and put $c = \pi/A_\sigma$. The determinant of these holomorphic rows has its weight $\exp(-c\sum_i |z_i|^2/2)$ in the translated frame. Its metric norm equals the norm of the undifferentiated alternant at the d points $(b_{\lambda i} + z_i)/M$ on the cover. Indeed its metric is the pullback metric, and translating each row is an isometry with a scalar common to all its columns. Apply Theorem 68.22 and the energy bound with d unit weights. The determinant vanishes at collisions, so the bound extends to the entire polydisk. Its weighted norm is at most

$$M^{d/2} g_\sigma(t^\sigma)^{-d} \exp\Big\{\tfrac{d}{4}(\log d + L_{C^\sigma}) + \tfrac{1}{2}(\log 2 + L_{C^\sigma})\Big\}.$$

For $j_i > 0$ use the Cauchy circle $|z_i| = \sqrt{j_i/c}$; for $j_i = 0$ evaluate at zero. Removing the Gaussian and applying the derivative formula on these circles multiplies the bound by $\prod_i C(j_i) c^{j_i/2}$. Differentiating once in each independent row variable to its specified order gives the claimed determinant by multilinearity. The transport proof of Theorem 68.27 applies to the whole row germ and hence to every chosen order. Apply the triangle inequality and average as before, using Theorem 65.22 for $\mathbb{E}_\sigma \log c$. □

68.10 Theta derivatives at ordinary primary torsion

Let $C = \mathbb{C}/\Lambda$ carry the marked model of Theorem 65.5. Write O for its origin, t for its nonzero point of order two, $x = \wp$, $y = \wp'$, and $\partial = d/dz$ for the vector field dual to dx/y. Fix a

good split prime $p \geq 5$ prime to the CM discriminant, a place λ above it, and a valuation $v(p) = 1$. Work over finite extensions at that place as required and denote reduction in the algebraic closure k of the residue field by a bar. The special fiber C_k is ordinary. For example, the nonzero scalar in $\partial^p = H_p \partial$ of Lemma 68.4 is the Hasse invariant in this differential. Put $J_n(F) = F^{(n)}(0)$, without factorials.

Lemma 68.32 (An additive character of the ordinary torsion)**.** *The differential determines an injective homomorphism $\lambda_C : C_k[p](k) \longrightarrow (k, +)$ with the following description. In characteristic zero put*

$$Z(P) = \zeta(z) - u_\Lambda z - (\pi/A)\bar{z}, \qquad P = [z] \neq O.$$

This is independent of the representative z. Let P be torsion and $m' p^\nu P = O$, with $p \nmid m'$ and $\nu \geq 1$. If $\bar{P} \neq O$, then $p^\nu Z(P)$ is integral and

$$\overline{p^\nu Z(P)} = -\frac{1}{\overline{m'}}\, \lambda_C([m' p^{\nu-1}]\bar{P}).$$

Proof. We give the integral group in which multiplication computes this residue. Enlarge the local ring to contain $C[2]$. For $d \in C[2]$, take an affine-line coordinate s_d over the open set on which $P + d \neq O$. Set $h_0 = 0$ and

$$h_d(P) = \frac{y(P)}{2(x(P) - x(d))} \quad (d \neq O).$$

Glue the coordinates by $s_d - s_e = h_d - h_e$. The only possible poles of h_d lie at d and O. At O every h_d for $d \neq O$ has principal part $-1/T$ in $T = -2x/y$. Distinct points of order two remain distinct in the residue field. Thus all the transition functions are regular on their overlaps over the integer ring. This gives a smooth additive torsor $\pi : G \to C$.

For inputs above P, Q, take coordinates with $P + d, Q + e, P + Q + d + e \neq O$ and add by

$$s_{d+e}(\text{sum}) = s_d(\text{first}) + s_e(\text{second}) + B(P + d, Q + e), \qquad B(U, V) = \frac{y(U) - y(V)}{2(x(U) - x(V))}.$$

Such charts cover each geometric fiber. One shift is excluded when choosing d and at most two when choosing e. On this open set the chord is regular. Near $U = V$ its other expression has numerator $4(x(U)^2 + x(U)x(V) + x(V)^2) - g_2$ and denominator $2(y(U) + y(V))$. The only common exceptional case on the diagonal has $U + V = O$, already excluded. The zeta addition formula reads $Z(U + V) = Z(U) + Z(V) + B(U, V)$. Oddness gives $Z(d) = 0$ at a nonzero point of order two. Thus the complex points have coordinates $s_d = Z(P + d) + a$; the law adds the two constants a. This proves compatibility and the group identities on the generic fiber, and hence on the integral charts by density. Inversion is given by $(P, s_d) \mapsto (-P, -s_d)$. The identity over O has $s_d = 0$ for $d \neq O$, and the kernel is the additive group. The section of abstract complex groups with $a = 0$ supplies the unique torsion lift of each torsion point: multiplication by a nonzero integer is bijective on the characteristic-zero kernel. In particular these lifts at torsion points are algebraic, by the same uniqueness applied over $\overline{\mathbb{Q}}$.

The reduced torsor admits no regular section. A section in the chart $d = 0$ would give a rational function f regular off O. For $d \neq O$ its coordinate $f + h_d$ must be regular at O. Hence f would have precisely one simple pole. Riemann–Roch in genus one excludes such a function.

On the special fiber $[p]_G$ kills the additive kernel and so descends to a homomorphism $f : C_k \to G_k$. One can construct it by applying $[p]_G$ to any local section of the torsor. The differential of $[p]_G$ is zero and π is smooth, so $df = 0$. It follows that $f = s \circ F$, where $F : C_k \to C_k^{(p)}$ is relative Frobenius. Indeed the pullbacks of rational coordinates through f lie in $k(C_k)^p$, the kernel of the invariant derivation. On regular local rings of the smooth curve a

rational p-th power regular at a point has a regular root there. This also proves regularity of s; the homomorphism identity follows after pullback by F. The equality $\pi f = [p]_{C_k}$ gives $\pi s = V$, with $V : C_k^{(p)} \to C_k$ the Verschiebung. On an ordinary elliptic curve V is a separable isogeny of degree p. If s killed its kernel, it would descend through V: the translates by the kernel are precisely the fibers of this finite étale quotient. The descended map would be a regular section of π, which the pole calculation rules out. Consequently s is injective on the cyclic kernel. Now F sends $C_k[p](k)$ bijectively onto $\ker V(k)$. Taking sF on those points gives the asserted λ_C in the additive coordinate over O.

Finally choose an integral point Q_0 of G above P with $s_0 = 0$, possible since $\bar{P} \neq O$. Its torsion lift has coordinate $Z(P)$. Subtracting the two points gives this scalar in the kernel. Multiplication by $m'p^\nu$ gives $p^\nu Z(P) = -[m'p^\nu]_G Q_0/m'$ in that kernel. The numerator on the right is integral and its reduction is $f([m'p^{\nu-1}]\bar{P})$, as claimed. □

Theorem 68.33 (Leading residues at every prescribed derivative order)**.** *Let $M = p^\nu m_0$, $\nu \geq 1$, $p \nmid m_0$, and $M[w] = O$. Put $P = t + [w]$. Take $m' = 2m_0$ and set*

$$L_\nu(w) = -\frac{\lambda_C([m'p^{\nu-1}]\bar{P})}{\overline{m'}}.$$

This value depends additively on $\overline{[w]}$ and is independent of the prime-to-p multiple used to kill the prime-to-p parts of t and $[w]$. For $F_w = U_w\Theta_t$ and all $n \geq 0$,

$$p^{\nu n} J_n(F_w) \text{ is integral}, \qquad \overline{p^{\nu n} J_n(F_w)} = \overline{J_0(F_w)}\, L_\nu(w)^n, \qquad 0^0 = 1.$$

If the p-primary part of $\overline{[w]}$ has order p^ν, then $v(J_n(F_w)) = -\nu n$ for every $n \geq 0$.

Proof. Multiplication by m' removes the prime-to-p part. On the remaining p-torsion after multiplication by $p^{\nu-1}$, the scalar $\overline{m'}$ is invertible. This proves independence and additivity. In particular L_ν is nonzero precisely when the indicated primary part has full order.

The value J_0 is integral and is a unit if $\bar{P} \neq O$. To see this even when $p \mid M$, write $(F_w/\Theta_t)^M = ch$ as in Theorem 65.6, where h has horizontal divisor $M([t - [w]] - [t])$ and vertical order zero on the good model. The product of its M translates by $[w]$ is a constant of valuation zero, giving $v(c) = 0$. The pole section t misses O; the potential zero section $t - [w] = -P$ misses O in the reduction when $\bar{P} \neq O$. Evaluate at O and use $\Theta_t(0) = 1$.

When $P \neq O$, the logarithmic derivatives b_j of F_w at zero satisfy

$$b_1 = Z(P), \qquad b_2 = -u_\Lambda - x(P), \qquad b_j = -\partial^{j-2} x(P) \quad (j \geq 3).$$

Indeed F_w is proportional to the Hermitian translate of $e^{-u_\Lambda z^2/2}\sigma(z)$ by a lift of P, so the translation exponential contributes exactly the antiholomorphic term in b_1. The formula for u_Λ in Theorem 65.5 gives integrality here. If $\bar{P} \neq O$, then b_j is integral for $j \geq 2$, and Lemma 68.32 gives the residue of $p^\nu b_1$.

Suppose next that $\bar{P} = O$ but $P \neq O$. The point is in the formal group, with $0 < v(T(P)) \leq 1/(p-1)$. For the upper bound, the strict formal logarithm obtained by integrating the unit differential has form $T + \sum_{j \geq 2} a_j T^j/j$ with integral a_j. For $v(T) > 1/(p-1)$ the first term has strictly smallest valuation, since $v_p(j) \leq (j-1)/(p-1)$; the series converges and is additive there by its formal identity. This neighborhood is stable under the integral group law. Hence it contains no nonzero torsion. In the chart $d \neq O$ the torsion lift has coordinate $Z(P) + h_d(P)$. The integral lift with $s_d = 0$ in the same argument as in the lemma gives $\overline{p^\nu(Z(P) + h_d(P))} = \lambda_C(O) = 0$. The Laurent series of h_d has integral coefficients and pole order one at O. Thus $p^\nu h_d(P)$ is in the maximal ideal. Also $T^j \partial^{j-2} x$ is integral in the formal

coordinate for $j \geq 2$, as ∂ is an integral unit times d/dT. It follows that $p^{\nu j} b_j$ is in the maximal ideal for every $j \geq 1$.

For either case $P \neq O$, apply the integer polynomial identity for $J_n(F_w)/J_0(F_w)$ in the b_j. Every monomial has weight n with b_j of weight j, and the sole monomial in b_1 alone is b_1^n, with coefficient one. This follows by differentiating $F_w' = F_w(\log F_w)'$ repeatedly. After multiplication by $p^{\nu n}$, all terms with $j \geq 2$ vanish in the residue field. If $P = O$ in characteristic zero, $[w] = t$, $J_0 = 0$, and all the derivatives are integral by Theorem 65.6 at this prime-to-p translate. This covers the remaining case. At full primary order $\bar{P} \neq O$ and both factors in the residue formula are nonzero, giving the claimed valuation. □

Corollary 68.34 (Leading reduction of a signed homogeneous test)**.** *In a fixed basis write one of the signed columns of Theorem 143.10 as*

$$Y_i = \sum_{a,\alpha} v_{i,a,\alpha} \prod_h J_{\alpha_h}(F_{a_h}), \qquad |\alpha| = k_i.$$

Use the actual shifts (with their chosen lifts) and a common annihilator M as above. Choose a scalar $c_i \neq 0$ making all $c_i v_{i,a,\alpha}$ integral at the given place. Put $P_{i,a}(X) = \sum_\alpha c_i v_{i,a,\alpha} X^\alpha$. The integral column $c_i p^{\nu k_i} Y_i$ has reduction

$$\sum_a \Big(\prod_h \overline{J_0(F_{a_h})} \Big) \overline{P_{i,a}}((L_\nu(a_h))_h).$$

On conjugate factors use the corresponding transported differential and reduction. If a square minor of these reduced columns is nonzero, the corresponding minor of the Y_i has valuation $-\sum_i (v(c_i) + \nu k_i)$, with the sum over its columns.

Proof. Distribute $p^{\nu k_i}$ over the individual derivatives using homogeneity. Apply Theorem 68.33 factor by factor and sum in the residue field. Taking a determinant commutes with reduction. A nonzero residue gives valuation zero before undoing the column scalings. □

The formula keeps the finite character coefficients and the original projection. To use it in Section 6.6 one needs a nonzero minor, or control of the higher terms if the displayed residue vanishes.

68.11 Division functions for normalized theta translates

Keep the marked elliptic curve, the lattice, and the normalization $\Theta_t(0) = 1$ of Theorem 65.5. The exact scalar in a torsion translation matters when several translations are added. We recover it by using the evenness of Θ_t on two opposite points of a division cover. This is the symmetric translation construction in the algebraic theory of theta functions; see K. Bannai and S. Kobayashi, *Algebraic theta functions and p-adic interpolation of Eisenstein–Kronecker numbers*.

Theorem 68.35 (A rational expression with its translation scalar)**.** *Fix $w \in M^{-1}\Lambda$, $M \geq 1$. Put $N = 2M$, $b = [w/2] \in C[N]$, and $d = [w/(2N)] \in C[N^2]$. Choose a rational function r_b on C with divisor $[N]^*([t-b] - [t])$. It can be chosen over any characteristic-zero field containing the marked model and the point b. For the fixed complex lift w there is an identity of meromorphic functions*

$$\frac{U_w \Theta_t(z)}{\Theta_t(z)} = \frac{r_b(d + [z/N])}{r_b(-d - [z/N])}.$$

In particular the marked model, u_Λ, and $C[N^2]$ generate a field containing every derivative of every such translate, with the relative scalars of different translates.

Proof. The divisor has degree zero. Under $\mathrm{Pic}^0(C) = C$ its class is $-Nb = O$ since multiplication by N is its own dual. Its principality over the field of definition follows by base change for global sections of a line bundle: the space of functions with the required divisor inequality has dimension one after extension to an algebraic closure, hence already over the base. Equality of divisors follows from degree zero.

Write $b_0 = w/2$ for the complex lift and $R(z) = U_{b_0}\Theta_t(z)/\Theta_t(z)$. The transformation rule under a period λ is

$$R(z+\lambda) = \exp(2\pi i E(\lambda, b_0))R(z), \qquad E(v_1, v_2) = \mathrm{Im}(\bar{v}_1 v_2)/A.$$

Indeed division of the two theta multipliers cancels their signs and leaves the exponent $(\pi/A)(\bar{\lambda}b_0 - \lambda\bar{b}_0)$. Thus $R(Nv)$ is periodic with the divisor defining r_b. It equals $c\, r_b([v])$ for some nonzero constant c. By evenness of Θ_t and the two translation exponentials, $R(-z-b_0)R(z) = 1$. Also $R(z+b_0)R(z) = U_w\Theta_t(z)/\Theta_t(z)$ by multiplication of the collinear translation factors. Substitution gives the displayed quotient, where c cancels. This computation is valid as an identity of meromorphic functions, including a common zero or pole in its right side.

For derivatives, expand at d and $-d$ by translation on the algebraic curve and use the parameter $T = -2x/y$ at O. The power series $T(z/N)$ is defined over the model field: integrate dx/y, which has leading term dT, then invert the series and substitute z/N. Division in the Laurent series field handles any common vanishing orders. The resulting quotient is holomorphic at zero because $\Theta_t(0) = 1$. The derivatives of Θ_t are in the marked model field with u_Λ by the recurrence of Theorem 65.5. This proves all field assertions with the specified lift. □

We choose the convention

$$e_N([s_0], [q_0]) = \exp(2\pi i N E(s_0, q_0)), \qquad Ns_0, Nq_0 \in \Lambda,$$

for the Weil pairing. It is perfect and alternating. Its values are algebraic N-th roots of unity. The multiplier calculation in the proof also identifies it without a choice of a primitive root.

Corollary 68.36 (Field automorphisms of a fixed translate)**.** *Let B contain the marked model, u_Λ, and $C[N]$. For $\sigma \in \mathrm{Gal}(B(C[N^2])/B)$ and $j \geq 0$,*

$$\sigma\big(J_j(U_w\Theta_t)\big) = e_N(\sigma d - d, b)^2 J_j(U_w\Theta_t).$$

Proof. Take r_b over B. For $s = [s_0] \in C[N]$, the equality $R(Nv) = c\, r_b([v])$ and the multiplier for the period Ns_0 give $r_b(v+s) = e_N(s,b)r_b(v)$. Now $\sigma d - d \in C[N]$. In the rational expression of Theorem 68.35, the numerator and denominator move by opposite points. The ratio therefore acquires the square of this pairing. All base coefficients of the germ of Θ_t are fixed. Differentiating proves the assertion also at a zero. The scalar is a character of σ, since the difference $\sigma d - d$ is additive in σ when its values are fixed by the group. □

Theorem 68.37 (Galois decomposition at the prescribed tests)**.** *Consider any chosen exterior product $\Xi = Y_1 \wedge \cdots \wedge Y_s$ of the prescribed columns in Theorem 143.10. Choose a coordinate basis for their common space and a field B containing the entries of the finite coefficient vectors in that basis, the model data just used, and $C[N]$ for every elliptic factor. Take M to kill all shifts and $N = 2M$. Let H be any subgroup of the Galois group over B of the compositum of the N^2-division fields of those curves.*

In the full multilinear expansion of Ξ, assign a character to a term by multiplying the characters of Corollary 68.36 over all its translated factors. Write Ξ_χ for the sum of the terms

assigned to χ, over the original signed coefficients. Then

$$\Xi_\chi = \frac{1}{|H|}\sum_{\sigma\in H}\chi(\sigma)^{-1}\sigma\Xi, \qquad \Xi\neq 0 \iff \Xi_\chi\neq 0 \text{ for some } \chi.$$

For any embedding into $\mathbb{C}$ and any fixed Hermitian norm on the exterior space,

$$\frac{1}{|H|}\sum_{\sigma\in H}\|\sigma\Xi\|^2 = \sum_{\chi}\|\Xi_\chi\|^2.$$

At a finite place with valuation v, for any one minor z and the corresponding coordinates z_χ, put $m_H = \min_{\sigma\in H} v(\sigma z)$. If $z\neq 0$, then

$$m_H - v(|H|) \;\le\; \min_{\chi} v(z_\chi) \;\le\; m_H.$$

Proof. Relative to the lower field the action on $C[N^2]$ is contained in the matrices $1+ND$ modulo N^2. They commute, including when N is composite. This holds on each factor, so H is finite abelian. The lower field contains the roots of unity occurring in the characters, by the Weil pairing on its rational N-torsion. Since each scalar derivative transforms by its stated character and each finite coefficient is fixed in the chosen basis, every term of the expansion is an eigenvector. Complex or algebraic character orthogonality gives the projector formula, the equivalence, and, on expanding a squared norm, the sum of squares. For the finite-place bounds use the nonarchimedean triangle inequality first on each projector, then on $\sigma z = \sum_\chi \chi(\sigma) z_\chi$. All character values are units there. □

The group in this theorem acts on algebraic numbers at the given tests. The decomposition preserves each coupled class index in the period. Terms carrying the same character still enter a single signed sum. The theorem gives a determinant criterion even if only a proper subgroup of the division group acts on the coefficients.

68.12 Independence of prescribed derivatives at split primes

Let $p^\nu \| M$, $\nu \ge 1$, for a good split prime $p \ge 5$. Write $N = 2M$. Fix an embedding into $\mathbb{C}$, let ι be complex conjugation, and fix a place $\mathfrak{P}$ of $\overline{\mathbb{Q}}$ above p. Consider a finite list of the marked CM curves with the same imaginary quadratic field K. Let $B/\mathbb{Q}$ be a finite Galois extension containing K, their marked models and differentials, the constants u_Λ, and the fields of definition of their CM actions. Assume each curve has good reduction at the places above p and $p \nmid e(B_{\mathfrak{P}}/\mathbb{Q}_p)$. Denote by B_0 the compositum of B, the maximal rational abelian extension $\mathbb{Q}^{\mathrm{ab}}$, and the fields of the N-torsion of all the curves. Allowing the abelian extension here keeps finite characters of arbitrarily large conductor fixed.

These conditions on B allow the discriminant-one models of the manuscript at every split $p \ge 5$ prime to the CM discriminant. Indeed for full CM by $\mathcal{O}_K$ the classical theorem of complex multiplication places j in the Hilbert class field of K. That field is Galois over $\mathbb{Q}$ and unramified at such p. Adjoin μ_6 and all the conjugates of the roots in

$$g_2^3 = j/1728, \qquad 27g_3^2 = g_2^3 - 1.$$

The degrees above the Hilbert class field have only 2 and 3 as prime divisors. Good reduction follows from the unit discriminant. The full two-torsion is unramified at these good primes. Each CM endomorphism descends over the resulting field: Galois conjugation preserving its tangent multiplier preserves the endomorphism, since the tangent representation of CM in characteristic zero is faithful. The expression in (65.5) for u_Λ uses a Galois-stable kernel and

hence already belongs to the same field. Taking all marked conjugates gives the required Galois field. This choice does not require tame ramification for the subsequent rational abelian coefficients adjoined in B_0.

Lemma 68.38 (Opposite inertia actions)**.** *For each $t_0 \in \mathbb{Z}/p^\nu\mathbb{Z}$ there is an automorphism h of $\overline{\mathbb{Q}}$ fixing B_0. It is trivial on the prime-to-p torsion of every curve on the list. On each $C[p^{2\nu}]$ its actions on the connected and the étale CM lines at $\mathfrak{P}$, respectively, are $u = 1 + p^\nu t_0$ and u^{-1} modulo $p^{2\nu}$.*

Proof. The CM idempotents in $\mathcal{O}_K \otimes \mathbb{Z}_p = \mathbb{Z}_p \times \mathbb{Z}_p$ split the p-divisible group of a good ordinary curve into two height-one groups. They extend over the good model since the CM endomorphisms do. The summand acting on the tangent line is connected in the special fiber, and the summand with zero tangent space is étale. At the conjugate place the two idempotents are interchanged, as their tangent multipliers come from the two embeddings at p. Inertia over B fixes the étale torsion. Its scalar action on the other rank-one Tate module is the p-adic cyclotomic character, by the determinant identity from the Weil pairing. Inertia also fixes prime-to-p torsion by smooth good reduction.

Absolute inertia at $\mathfrak{P}$ maps onto $(\mathbb{Z}/p^{2\nu}\mathbb{Z})^\times$ under the cyclotomic character because the corresponding local cyclotomic extension is totally ramified. Intersecting inertia with the absolute Galois group of B cuts its index by $e(B_{\mathfrak{P}}/\mathbb{Q}_p)$, prime to p. Consequently the image of this intersection contains the whole p-Sylow subgroup. Choose g in it with cyclotomic value u at this level. The element $g' = \iota g \iota^{-1}$ lies in inertia at the conjugate place, fixes B by normality, and has the same cyclotomic value. Thus $h = g(g')^{-1}$ acts in the stated way on both lines, fixes the prime-to-p torsion, and fixes $C[N]$ since $u \equiv 1 \bmod p^\nu$. It is a commutator, so it fixes $\mathbb{Q}^{\mathrm{ab}}$. The same g works on every curve. □

On each curve use a basis (E_2, F_2) of the two lines at level $p^{2\nu}$, connected first. Take it so that at level p^ν the basis $(E_1, F_1) = ([p^\nu]E_2, [p^\nu]F_2)$ has Weil pairing a fixed primitive root ζ_{p^ν}, with the sign convention of Corollary 68.36. For $a = [w]$ write x_a, y_a for the coordinates of its p-primary part in this lower basis.

Theorem 68.39 (The character of a prescribed derivative)**.** *For h of Lemma 68.38 the exact action on every M-torsion translate, including its choice of lift, is*

$$h\big(J_j(U_w\Theta_t)\big) = \zeta_{p^\nu}^{\,t_0 x_a y_a} J_j(U_w\Theta_t) \qquad (j \ge 0).$$

In a product of derivatives the label in the exponent is $\sum_a x_a y_a$, counted with multiplicity. At several distinct good split primes satisfying the same hypotheses the labels can be separated simultaneously over B_0.

Proof. Use $d = [w/(2N)]$ and $b = [w/2] = [N]d$ of Theorem 68.35. Write the p-part of d as $XE_2 + YF_2$. With $N' = N/p^\nu$ we have

$$(h-1)d = t_0 X E_1 - t_0 Y F_1, \qquad b_p = N'(XE_1 + YF_1), \qquad (x_a, y_a) = 2N'(X, Y) \pmod{p^\nu}.$$

Here h fixes every other primary part, and $(1 + p^\nu t_0)^{-1} = 1 - p^\nu t_0 \bmod p^{2\nu}$. Distinct primary parts pair trivially. On $C[p^\nu]$ the pairing e_N is $e_{p^\nu}^{N'}$, as follows directly from the alternating form defining it. Hence

$$e_N((h-1)d, b)^2 = \zeta_{p^\nu}^{\,4t_0(N')^2XY} = \zeta_{p^\nu}^{\,t_0 x_a y_a}.$$

Corollary 68.36 proves the derivative formula. Characters multiply on products. Each of the automorphisms constructed for another prime acts trivially on all the prime-to-that-prime

torsion. Thus their restrictions commute on the common division field and the independent choices of t_0 give the direct product of label characters there. □

Corollary 68.40 (Independent derivatives of arbitrarily prescribed orders)**.** *For one of the curves choose p^ν shifts w_u with p-parts $(u,1)$, one for every $u \in \mathbb{Z}/p^\nu\mathbb{Z}$. Their prime-to-$p$ components killed by M, their lifts, and their derivative orders $j_u \geq 0$ can be chosen independently. Then the p^ν numbers $J_{j_u}(U_{w_u}\Theta_t)$ are linearly independent over B_0. More generally, in a signed period with coefficient vectors over B_0, a component with an isolated nonzero term having a specified tuple of labels cannot be cancelled by terms with a different tuple.*

For a pure terminal frequency of Lemma 141.20, supported on one CM half in a locally integral CM product basis, its label at the terminal prime is zero.

Proof. At $\mathfrak{P}$ the y-coordinate specializes injectively on the étale line. Thus $(u,1)$ specializes with full primary order. Every stated derivative is nonzero by Theorem 68.33. Applying the powers of an automorphism for $t_0 = 1$ to a relation over B_0 gives the Fourier matrix $(\zeta_{p^\nu}^{vu})_{v,u}$ on the summands. Its inverse extracts each summand, proving independence. The same character projector proves the assertion on isolated terms. At the terminal place a pure frequency is in the dual position component. In each scalar factor one of its split coordinates is therefore zero. This gives the last claim and explains why these terminal frequencies alone furnish no distinct labels. □

68.13 Cyclic terminal Fourier projections on an elliptic curve

Let Λ be a scaled fractional ideal of $\mathcal{O}_K$ in the marked elliptic model, and let $p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$ be a good split prime $p \geq 5$. Take the frequency subgroup $\mathfrak{p}^{-1}\Lambda/\Lambda$. Choose a positive basis ω_1, ω_2 of Λ such that $w = 2\omega_1/p$ generates this subgroup and $\omega_1 \in \bar{\mathfrak{p}}^{\,2}\Lambda$. The proof below shows that this choice is possible for any prescribed nonzero generator modulo Λ. The factor two gives $pw \in 2\Lambda$. For $k \in \mathbb{F}_p$, $\zeta_p = \exp(2\pi i/p)$, put

$$S_k(z) = \frac{1}{p}\sum_{j=0}^{p-1} \zeta_p^{-kj} U_{jw}\Theta_t(z).$$

Lemma 68.41 (The elliptic curve and the scalar of the Fourier sum)**.** *Put $\Gamma = \mathbb{Z}\omega_1 + \mathbb{Z}p\omega_2$ and $\Lambda' = \mathbb{Z}(\omega_1/p) + \mathbb{Z}p\omega_2$. They are $\bar{\mathfrak{p}}\Lambda$ and $\mathfrak{p}^{-1}\bar{\mathfrak{p}}\Lambda$, respectively. On $\mathbb{C}/\Lambda'$ there is a nonzero two-torsion mark t' such that $S_0 = c\Theta'_{t'}$, where $\Theta'_{t'}(0) = 1$ and $c = S_0(0) \neq 0$. For each k choose $\lambda_k \in \Lambda$ satisfying $\exp(2\pi i E(\lambda_k, w)) = \zeta_p^{-k}$. Then $S_k = \epsilon_t(\lambda_k)^{-1}U_{\lambda_k}S_0$, with ϵ_t the original period sign. For $k \neq 0$ the class of λ_k has exact order p in the $\bar{\mathfrak{p}}$-torsion of $\mathbb{C}/\Lambda'$. In the common variable z there are differences e and e' between distinct Weierstrass two-torsion x-coordinates on the original and the new curve such that*

$$c^4 = p^{-2}\, e'/e.$$

Proof. The subgroup of Λ with $E(\gamma, w)$ integral is Γ, by the displayed basis. It is also $\bar{\mathfrak{p}}\Lambda$: the adjoint of a CM scalar for the alternating form is its complex conjugate, and this ideal lattice has index p and annihilates the frequency under the pairing. Adjoining w to Γ gives Λ'. The extra congruence in the choice of the basis is possible with the prescribed generator. Indeed one can lift its half at the first prime modulo p^2, take zero at the other, and lift the resulting primitive pair modulo p^2 to a unimodular integral basis. Elementary matrices generate $\mathrm{SL}_2(\mathbb{Z}/p^2\mathbb{Z})$ by elimination at a unit entry. With this choice w belongs to the claimed fractional ideal, and the two superlattices of Γ have the same index p. In particular $\Lambda \cap \Lambda' = \Gamma$, and Λ/Γ is the stated opposite CM line.

All $U_{jw}\Theta_t$ are sections on the common cover by Γ. The operator U_λ for $\lambda \in \Lambda$ acts there on the j-th section as $\epsilon_t(\lambda)\exp(2\pi i j E(\lambda, w))$, by the multiplier in Theorem 68.35. This gives the asserted formula for S_k. Also $U_w S_0 = S_0$ because $U_{pw}\Theta_t = \Theta_t$. Thus S_0 has the principal polarization on Λ', which has the same area as Λ. It is even. It is nonzero since the p terms in its sum have distinct eigencharacters under Λ/Γ. Its unique zero in this degree-one line is simple, fixed by negation and away from zero by evenness. This gives t'. The quotient by the marked Hermitian theta with the same divisor has periodic absolute value, since its remaining period multipliers are unitary. It is constant by Liouville's theorem.

To compute that constant put $\tau = \omega_2/\omega_1$, $s = z/\omega_1$, and $A = \operatorname{Im}(\bar{\omega}_1\omega_2)$. For the even half-characteristic (a, b) of the original mark write

$$\vartheta_{a,b}(s,\tau) = \sum_{n\in\mathbb{Z}} \exp\{\pi i(n+a)^2\tau + 2\pi i(n+a)(s+b)\}.$$

The normalized Hermitian theta is this function divided by its value at zero and multiplied by $\exp(\pi\bar{\omega}_1 z^2/(2A\omega_1))$. This follows from the period multipliers of the series on ω_1, ω_2; it has the given even characteristic and value one. Translation along $2j\omega_1/p$ translates the argument of the series by $2j/p$ with the same exterior Gaussian at z. The average over j retains precisely $n + a = p(m + a)$, since p is odd. Consequently

$$c = \frac{\vartheta_{a,pb}(0, p^2\tau)}{\vartheta_{a,b}(0,\tau)}.$$

The Jacobi identities identify the fourth power of each even theta constant with the square of its first full period divided by π^2, times a difference of the Weierstrass roots. These are the half-period formulas in NIST, Weierstrass functions and theta functions, §23.6(i), together with $\vartheta_3^4 = \vartheta_2^4 + \vartheta_4^4$. Reducing a half-characteristic modulo integers introduces only a sign here. The two first full periods are ω_1 and ω_1/p, proving the identity in the common differential. □

Theorem 68.42 (Integral derivatives of a complete cyclic projection)**.** *Use the choice of generator to precision p^2 made in Lemma 68.41. Let b_0 lift any prime-to-p torsion point of $\mathbb{C}/\Gamma$. At a place over p where the original differential is a good invariant differential, use $v(p) = 1$. If the original frequency line $C[\mathfrak{p}]$ is connected in the reduction, then*

$$v(c) = 0, \qquad v\big(J_n(U_{b_0}S_k)\big) = 0 \quad (k \neq 0,\ n \geq 0), \qquad v\big(J_n(U_{b_0}S_0)\big) \geq n.$$

At the other orientation $v(c) = -1$, and every k, n satisfies $v(J_n(U_{b_0}S_k)) \geq -1 - n$.

Proof. The two isogenies

$$C_\Gamma = \mathbb{C}/\Gamma \ \longrightarrow\ C = \mathbb{C}/\Lambda, \qquad C_\Gamma \ \longrightarrow\ C' = \mathbb{C}/\Lambda'$$

have degree p and respective kernels the $\bar{\mathfrak{p}}$-line and the $\mathfrak{p}$-line. One can start algebraically with the quotient by a CM torsion subgroup and its dual; the maps and the differential pulled back from C are defined over a number field. The curves have good models after finite extension since they have CM and integral j. For invariant differentials of good models the pullback multiplier of an isogeny with étale reduction is a unit. For these degree-p isogenies with connected kernel the dual has étale kernel, so the two multipliers have valuations one and zero by their composition $[p]$.

Write $\alpha\, dz$ for a good invariant differential of C', where dz denotes the common analytic variable. At the connected frequency orientation the isogeny to C is étale and the one to C' has connected kernel. Since dz on C is good, $v(\alpha) = 1$. At the other orientation the roles

are reversed and $v(\alpha) = -1$. Choose a discriminant-one model of C'; its differential has this same valuation relative to dz. In the normalized coordinate $z' = \alpha z$, every difference between distinct two-torsion roots is a unit, because the discriminant is a unit and $p \geq 5$. Returning to z multiplies the root differences by α^2. The lemma therefore gives $4v(c) = -2 + 2v(\alpha)$.

The section $U_{b_0} S_k$ is c times the translate of the normalized theta on C' by $b_0 + \lambda_k$, up to a root of unity from the period sign and the translation law. All the translations are rational in the common real period lattice, so the composition phases are indeed roots of unity. Passing to z' multiplies its n-th derivative in the original variable by the factor α^n relative to the derivative in z'. The equality of the Hermitian translations under this variable change follows from $\operatorname{area}(\alpha\Lambda') = |\alpha|^2 A$. At the connected frequency orientation and $k \neq 0$, the point $[\lambda_k]$ on C' has full étale order p. The added prime-to-p shift preserves this order. By Theorem 68.33, the derivative in z' has valuation $-n$. At $k = 0$ it is integral by Theorem 65.6. In the opposite orientation the only primary shift is connected on C', so Theorem 66.35 gives integrality in z' in every order. Combining these facts with the two values of $v(\alpha)$ and $v(c)$ proves the assertions. □

69 References

[1] J. S. Milne, *Complex Multiplication*, version 0.10, 2020, Part II. Arithmetic theory of CM abelian varieties.

[2] J. H. Silverman, *The Arithmetic of Elliptic Curves*, second edition, Springer, 2009, Chapters IV and VII. Formal groups and reduction.

[3] D. Mumford, *Abelian Varieties*, Oxford University Press, 1970, §17, p. 163. See also J. S. Milne, *Abelian Varieties*, Remark 7.3.

[4] NIST, *Digital Library of Mathematical Functions*, Chapter 20. Quasiperiodicity, definitions and zeros and Product formulas.

[5] J. Thorner and A. Zaman, *An explicit bound for the least prime ideal in the Chebotarev density theorem*, Algebra Number Theory **11** (2017), 1135–1197. Theorem 1.2.

[6] C.-L. Chai and F. Oort, *Moduli of abelian varieties and p-divisible groups*, Clay Math. Proc. **8** (2009), 439–536. Duality theorem for abelian schemes, Section 10.

[7] W. T. Gan, *Automorphic forms and the theta correspondence*, Arizona Winter School lectures. Lecture notes.

[8] S. S. Kudla, *Notes on the local theta correspondence*, European School of Group Theory, 1996. Chapter III, Section 6, pp. 53–54.

[9] J. Thorner and A. Zaman, *A unified and improved Chebotarev density theorem*, Algebra Number Theory **13** (2019). Theorem 1.4 and Theorem 3.1.

[10] R. de Jong, *On the Arakelov theory of elliptic curves*, Enseign. Math. (2) **51** (2005), 179–201. Theorem 3.2 and Corollary 4.5.