THE ISOTROPIC PLANE

Prerequisites. Chapter 15, *The invariant derivation at a supersingular prime*: the moments $t(a,w)$, the functions F and Θ and the directions $e_\pm$ of Section 15.1, the formal group $\hat{E}$ and the ring $\mathcal{O}=\mathbb{Z}_p[\mathrm{i}]$ of Section 15.2, the function E_p, Problem 15.3.4 and Theorem 15.4.1, and Section 15.5. Quasi-periods of σ and Legendre's relation [Si2, §I.5]. Decomposition groups in cyclotomic fields. Rational functions and divisors on an abelian scheme over a discrete valuation ring, at the level of the statement that a rational function whose divisor avoids a point is regular there [BK, Lemma 2.13].

16.1. The isotropic plane

The function F does not gain by itself (Problem 15.5.3). Why should Θ along the directions $e_\pm=(1,\pm\zeta)$ do better? They are the eigenlines of an action of $\mathbb{Z}[\zeta]$ on $\mathbb{Z}[\mathrm{i}]^2$. Let

$$\rho(\zeta):=\begin{pmatrix}0&1\\ \mathrm{i}&0\end{pmatrix},$$

let σ_+ be the identity of $\mathbb{Q}(\zeta)$ and σ_- the automorphism $\zeta\mapsto-\zeta$, and let $H(Z,W):=Z_1\bar{W}_1+Z_2\bar{W}_2$.

Problem 16.1.1. ρ extends to a ring homomorphism $\mathbb{Z}[\zeta]\to M_2(\mathbb{Z}[\mathrm{i}])$, and $\rho(\bar{a})=\rho(a)^*$, the conjugate transpose.

Problem 16.1.2. $\rho(a)e_\pm=\sigma_\pm(a)e_\pm$, and $H(e_+,e_-)=0$.

For each prime $p\equiv3\pmod4$, fix an embedding $\mathbb{Q}(\zeta)\hookrightarrow\mathbb{Q}_p(\mathrm{i})$ extending the embedding of $\mathbb{Q}(\mathrm{i})$ given by $\mathcal{O}=\mathbb{Z}_p[\mathrm{i}]$, and use it for v_p and for reduction modulo p. Let σ_p be the nonidentity automorphism of $\mathbb{Q}_p(\mathrm{i})/\mathbb{Q}_p$.

Now let $p\equiv3\pmod8$. The Frobenius $\zeta\mapsto\zeta^3$ generates the decomposition group of p in $\mathbb{Q}(\zeta)$, with fixed field $\mathbb{Q}(\sqrt{-2})$, $\sqrt{-2}:=\zeta+\zeta^3$. Since $\mathbb{Z}[\sqrt{-2}]$ is a principal ideal domain, $p=x^2+2y^2$ for integers x, y.

Problem 16.1.3. After replacing y by $-y$ if necessary, $a:=x+y\sqrt{-2}$ lies in $p\mathcal{O}$, while $\bar{a}=x-y\sqrt{-2}$ is a unit of $\mathcal{O}$. Moreover $\sigma_-(a)=\bar{a}$.

Problem 16.1.4. If $p\equiv7\pmod8$, then $v_p(a)=v_p(\bar{a})$ for every $a\in\mathbb{Z}[\zeta]$.

On Gaussian coefficients σ_p agrees with complex conjugation. The local form $H_p(z,w):=z_1\sigma_p(w_1)+z_2\sigma_p(w_2)$ on $\mathcal{O}^2$ reduces to the hermitian form $h(z,w):=z_1w_1^p+z_2w_2^p$ on $\mathbb{F}_{p^2}^2$. Let $\bar{e}_\pm$ be the reductions of $e_\pm\in\mathcal{O}^2$. Write $\widetilde{\zeta}$ for the reduction of ζ modulo p.

Problem 16.1.5. $h(\bar{e}_+,\bar{e}_+)=h(\bar{e}_-,\bar{e}_-)=1+\widetilde{\zeta}^{p+1}$ and $h(\bar{e}_+,\bar{e}_-)=1-\widetilde{\zeta}^{p+1}$. So for $p\equiv3\pmod8$ both lines are isotropic and h pairs them, while for $p\equiv7\pmod8$ they are anisotropic and orthogonal.

Date: November 24, 2026.

We call e_- the *partner* of e_+. In terms of embeddings, $\sigma_- = c \circ \mathrm{Frob} \circ \sigma_+$, where c is complex conjugation and $\mathrm{Frob}(\zeta) = \zeta^p$; for $p \equiv 7 \pmod 8$, by contrast, $c \circ \mathrm{Frob} \circ \sigma_+ = \sigma_+$. The derivatives along e_+ will gain, and those along the partner e_- will pay for it.

16.2. Integrality on an eigenline

Let $P(s) := \Theta(se_+) = F(s)\,F(\zeta s)$. Since F is even, $\Theta(te_-) = P(t)$, and $t(n,0) = P^{(n)}(0)$. Write $P(s) = \hat{P}(\mathrm{sl}\, s)$ with $\hat{P} \in \mathbb{Q}[[X]]$. We show that $\hat{P}$ is p-integral for every prime $p \equiv 3 \pmod 8$, unlike F.

Let L be the period lattice of sl and η the quasi-period map of Λ. Since $\eta(\mathrm{i}\omega) = -\mathrm{i}\eta(\omega)$, Legendre's relation gives $\eta(\omega) = (\pi/\operatorname{vol}\Lambda)\,\bar{\omega}$, and with the law $\sigma(u+\omega) = \pm e^{\eta(\omega)(u+\omega/2)}\sigma(u)$ [Si2, §I.5],

$$F(u+\omega) = \exp\bigl(c\,\bar{\omega}u + \tfrac{c}{2}|\omega|^2\bigr)F(u), \qquad \omega \in \Lambda, \quad c := \frac{2\pi}{\operatorname{vol}\Lambda}.$$

Problem 16.2.1. For $\gamma \in L^2$, $\Theta(Z+\gamma) = \exp\bigl(cH(Z,\gamma) + \frac{c}{2}H(\gamma,\gamma)\bigr)\Theta(Z)$. For $a \in \mathbb{Z}[\zeta]$, $a \neq 0$, the function

$$F_a(Z) := \frac{\Theta(\rho(a)Z)}{\Theta(\rho(\bar{a})Z)}$$

is L^2-periodic with $F_a(0) = 1$. It descends to a rational function on $E \times E$ defined over $\mathbb{Q}(\mathrm{i})$.

Problem 16.2.2. On $\mathbb{C}/L = E(\mathbb{C})$, the zeros of F are the two points at infinity of $y^2 = 1 - X^4$, each with multiplicity two.

Let $\mathcal{A}$ be $E \times E$ over $\mathcal{O}$, an abelian scheme on which $\mathbb{Z}[\zeta]$ acts through ρ, and write $\hat{F}_a(X_1, X_2)$ for the expansion of F_a in $X_1 = \mathrm{sl}\, Z_1$, $X_2 = \mathrm{sl}\, Z_2$.

Problem 16.2.3. $\hat{F}_a \in \mathcal{O}[[X_1, X_2]]$.

Now let $p \equiv 3 \pmod 8$, and let a be as in Problem 16.1.3.

Problem 16.2.4. $\hat{P}([a]X) = \hat{F}_a(X, [\zeta]X)\,\hat{P}([\bar{a}]X)$.

Problem 16.2.5. The coefficients of $\hat{P}$ lie in $\mathbb{Z}_{(p)}$.

Problems 16.2.1–16.2.5 and Theorem 15.4.1 prove the following.

Theorem 16.2.1. *Let $p \equiv 3 \pmod 8$. Then $\hat{P} \in \mathbb{Z}_{(p)}[[X]]$, and $v_p(t(n,0)) = v_p(P^{(n)}(0)) \geq E_p(n)$ for every $n \geq 0$.*

The induction in Problem 16.2.5 is the argument Bannai and Kobayashi use for the Kronecker theta function at ordinary primes [BK, Prop. 2.14], where one element of the CM order serves for all coordinates at once. Here $\mathcal{A}$ is supersingular, but on the line $\mathbb{C}e_+$ the element a acts by a non-unit and $\bar{a}$ by a unit. At $p \equiv 7 \pmod 8$ there is no such element (Problem 16.1.4), and at $p = 7$ the conclusion fails.

Problem 16.2.6. $\hat{P}(X) = 1 - \frac{1}{70}X^8 + O(X^{12})$. So $\hat{P}$ is not 7-integral, and $t(8,0) = -576$.

16.3. The cross term

Theorem 16.2.1 accounts for the derivatives along each axis. What remains is a factor equal to 1 on both axes. Throughout, $p \equiv 3 \pmod 8$, $X_1 = \operatorname{sl} s$, $X_2 = \operatorname{sl} t$, and $P_n := P^{(n)}(0)$.

Problem 16.3.1. $J(s,t) := \partial_s \partial_t \log \Theta(se_+ + te_-) = 2\operatorname{sl}^2(s+t) - 2\mathrm{i}\,\operatorname{sl}^2\big(\zeta(s-t)\big)$, and $J \in \mathcal{O}[[X_1, X_2]]$.

Let $M(s,t) := \int_0^s \int_0^t J$, and $M_{\alpha\beta} := \partial_s^\alpha \partial_t^\beta M(0,0)$.

Problem 16.3.2. $\Theta(se_+ + te_-) = P(s)\,P(t)\,e^{M(s,t)}$. The numbers $M_{\alpha\beta}$ vanish unless $\alpha, \beta \geq 1$, and then $M_{\alpha\beta} \in p^{E_p(\alpha-1)}\mathcal{O}$.

Problem 16.3.3. Let S and T be disjoint sets with a and w elements, respectively. Then

$$t(a,w) = \sum P_{|S_0|}\,P_{|T_0|} \prod_{B \in \pi} M_{|B\cap S|,|B\cap T|},$$

the sum over subsets $S_0 \subseteq S$, $T_0 \subseteq T$, and partitions π of $(S \smallsetminus S_0) \sqcup (T \smallsetminus T_0)$ into blocks each meeting both S and T.

Problem 16.3.4. Each term in Problem 16.3.3 has at most w blocks and valuation at least $\lfloor a/p \rfloor - w$.

Thus $v_p(t(a,w)) \geq \lfloor a/p \rfloor - w$. The *type* of a term in Problem 16.3.3 consists of $a_0 = |S_0|$, $w_0 = |T_0|$, and the numbers $m_{\alpha\beta}$ of blocks with $|B \cap S| = \alpha$ and $|B \cap T| = \beta$.

Problem 16.3.5. For every type $(a_0, w_0, (m_{\alpha\beta}))$ occurring in Problem 16.3.3, the number of terms of that type is $N \cdot a!/\big(a_0! \prod_{\alpha,\beta} (\alpha!)^{m_{\alpha\beta}}\big)$ for some positive integer N.

Problem 16.3.6. Let $\alpha_1, \ldots, \alpha_k$ be positive integers and a_0 a nonnegative integer such that $a_0 + \sum_{b=1}^k \alpha_b = a$. Let $n_i := \#\{b : p^i \mid \alpha_b\}$. Then

$$v_p\Big(\frac{a!}{a_0!\,\alpha_1! \cdots \alpha_k!}\Big) + E_p(a_0) + \sum_{b=1}^k E_p(\alpha_b - 1) \;\geq\; \sum_{\substack{i \geq 1 \\ i \text{ odd}}} \Big(\Big\lfloor \frac{a}{p^i} \Big\rfloor - n_i\Big)_+,$$

where $x_+ := \max(x, 0)$.

Problems 16.3.2–16.3.6, Theorem 16.2.1 and the symmetry $t(a,w) = t(w,a)$ of Problem 15.1.5 give the following theorem.

Theorem 16.3.1. *Let $p \equiv 3 \pmod 8$. For all integers $a, w \geq 0$,*

$$v_p\big(t(a,w)\big) \;\geq\; \max\Bigg(\sum_{\substack{i \geq 1 \\ i \text{ odd}}} \Big(\Big\lfloor \frac{a}{p^i} \Big\rfloor - w\Big)_+,\; \sum_{\substack{i \geq 1 \\ i \text{ odd}}} \Big(\Big\lfloor \frac{w}{p^i} \Big\rfloor - a\Big)_+ \Bigg).$$

In the table of Section 15.1 the bound is an equality whenever it is positive. It is not always sharp: $t(11,1) = -2^9 \cdot 3^6$, while the bound at $p = 3$ is 2.

Exercise. Let $M = s^p t/p$ and let $w \geq 0$ be an integer. Show that $\partial_s^{pw} \partial_t^w e^M(0,0) = (pw)!/p^w$, with valuation $v_p(w!)$. Deduce that this valuation is 0 for $0 \leq w < p$. Show also that for every $G \in \mathcal{O}[[X_1, X_2]]$, with $X_1 = \operatorname{sl} s$ and $X_2 = \operatorname{sl} t$, the valuation of $\partial_s^{pw} \partial_t^w G(0,0)$ is at least w.

16.4. Questions

Theorem 16.3.1 does not extend to $p \equiv 7 \pmod 8$: it fails at $p = 7$ (Problem 16.2.6). What fails is the choice of directions: $e_\pm$ are global eigenlines of $\mathbb{Z}[\zeta]$, and they are isotropic modulo p only for $p \equiv 3 \pmod 8$ (Problem 16.1.5). For every prime $p \equiv 3 \pmod 4$, the local form H_p on $\mathcal{O}^2$ admits a basis f, f' with $H_p(f, f) = H_p(f', f') = 0$ and $H_p(f, f') = 1$. If $p \equiv 7 \pmod 8$, neither line $\mathbb{Q}_p(\mathrm{i})e_\pm$ contains a nonzero isotropic vector. Theorem 16.3.1 concerns the two global eigenlines.

Let A be an abelian variety with complex multiplication by the ring of integers of a CM field K, with CM type Φ, and let Θ be a normalized theta function on its universal cover. Fix a prime p and an embedding $\jmath : \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$, so that $\jmath \circ \phi$ determines a prime of K above p. The eigenlines $\mathbb{C}e_\phi$ ($\phi \in \Phi$) replace $e_\pm$; the case above is $K = \mathbb{Q}(\zeta)$, $\Phi = \{\sigma_+, \sigma_-\}$. The argument of Section 16.2 on $\mathbb{C}e_\phi$ needs an element a of the CM order with $\phi(a)$ a non-unit and $\phi(\bar{a})$ a unit, and such an element exists exactly when complex conjugation does not fix the prime of K determined by ϕ. In the first sum of Theorem 16.3.1, the subtracted order is w, the order along e_-. For $p \equiv 3 \pmod 8$, this is the partner direction at every odd level i, since $c \circ \mathrm{Frob}^i \circ \sigma_+ = \sigma_-$. For a general CM type, suppose p is unramified in the normal closure of K, and let Frob be the arithmetic Frobenius at the chosen prime of that closure. At a level i with $\mathrm{Frob}^i \circ \phi \notin \Phi$, is the order subtracted from the order along e_ϕ the order along $e_{c \circ \mathrm{Frob}^i \circ \phi}$?

Among the odd supersingular primes for E, the choice of a global CM element in Problem 16.1.3 fails exactly for $p \equiv 7 \pmod 8$. What derivative estimates hold in local hyperbolic coordinates at these primes? Let A_5 be the Jacobian of $y^2 = x^5 - 1$, with CM by $\mathbb{Q}(\zeta_5)$. Among odd primes $p \neq 5$, the supersingular primes for A_5 are exactly those with $p \not\equiv 1 \pmod 5$, by the Shimura–Taniyama formula for the slopes of a Jacobian with complex multiplication [LMPT]. At these primes complex conjugation is in the decomposition group of every prime above p, so there is no element of the CM order separating a prime from its conjugate. For this Jacobian at such a prime, what choices of normalized theta function, eigenline direction and formal parameter from an integral model give a restriction with p-integral coefficients? What valuation bound then holds for the derivatives in that direction at the origin?

Which step this chapter serves. This chapter gives a two-variable model for the partner terms in the divisibility estimate of the proof. Theorem 17.5.1 of Chapter 17, *Pairings on a formal group of height two*, bounds the valuation of jets along products of minors for series in the prescribed normal form and at the prescribed scale. Write $r_e(\tau)$ for the partner of the infinite place τ at level e, as defined there. Among the columns of height less than the number of rows, let a_τ count the columns of height one at τ, and let a'_τ count the other columns there. In the positive-level sum for the predicted divisibility, the summand at τ and e contains the positive part $\left(a_\tau/p^e - a_{r_e(\tau)} - a'_{r_e(\tau)}\right)_+$. The sum runs over all infinite places and over odd positive e if p is inert in $\mathbb{Q}(\sqrt{-d})$, or all positive e if $p = d$. Its weight is 1 if p is inert and $1/2$ if $p = d$. The order w along e_- in the first sum of Theorem 16.3.1 plays the analogous role. Theorem 17.5.1 assumes that the prime p does not split in $\mathbb{Q}(\sqrt{-d})$, with no separate congruence condition on p modulo 8. Theorems 16.2.1 and 16.3.1 give the estimates for the workbook moments.

In the Lean formalization. Theorem 17.5.1 is the valuation form of `Parameters.norm_jet_minorProd_le_of_has` in `grh/src/New/Derivatives/Divisibility/Count.lean` of the Lean proof [GL]. Its predicted divisibility is `predictedDivisibility` in the same file. The positive partner levels are `positivePartnerExponents` in `grh/src/Lib/CM/FormalGroup/PrimeNotation.lean`, and the partner map is `Parameters.partner` in `grh/src/New/Derivatives/FormalGroup/ThetaProducts.lean`

Hints

§16.1.

16.1.1: $\rho(\zeta)^2 = \mathrm{i}$, and $\rho(\zeta)$ is unitary.

16.1.3: $a\bar{a} = p$, and $\mathcal{O}$ is a discrete valuation ring with uniformizer p. For $p = 3$, take $x = 1$ and test the two signs of $y = \pm 1$ in the chosen embedding.

16.1.4: The Frobenius automorphism of $\mathcal{O}$ preserves v_p and maps ζ to ζ^p.

16.1.5: Compare the actions of σ_p and of complex conjugation on ζ.

§16.2.

16.2.1: $\rho(a)$ preserves L^2 because $\mathrm{i}L = L$, and $\rho(a)^*\rho(a) = \rho(a\bar{a}) = \rho(\bar{a})^*\rho(\bar{a})$. For the field of definition, compare the Taylor expansion at the origin with its transforms under automorphisms of $\mathbb{C}$ over $\mathbb{Q}(\mathrm{i})$.

16.2.2: $F = \sigma^2/\mathrm{sl}^2$ by Problem 15.1.1.

16.2.3: Use Problem 16.2.2 to locate the horizontal components of the divisor near the origin of the special fiber. How can the value $F_a(0)$ determine the remaining vertical multiplicity?

16.2.4: Evaluate $\Theta(\rho(a)Z) = F_a(Z)\Theta(\rho(\bar{a})Z)$ at $Z = se_+$, using Problems 16.1.2 and 15.2.4.

16.2.5: Induction on the degree, comparing coefficients of X^n in Problem 16.2.4.

§16.3.

16.3.1: Problem 15.5.1. Then $\mathrm{sl}(s+t) = X_1 \oplus X_2$ and $\mathrm{sl}(\zeta(s-t)) = [\zeta](X_1 \ominus X_2)$.

16.3.2: Restrict $\log\Theta$ to the two axes. For the bound, express $M_{\alpha\beta}$ through derivatives of J, and use Theorem 15.4.1.

16.3.3: Expand $e^M = \sum_k M^k/k!$ and distribute the $a+w$ labelled derivatives.

16.3.4: Each block meets T. Keep only the first level of each E_p.

16.3.5: Choose the T-parts first; after that the blocks are distinguishable.

16.3.6: Apply Legendre's formula level by level, and use $\lfloor \alpha/p^i \rfloor - \lfloor (\alpha - 1)/p^i \rfloor \in \{0, 1\}$. Each level contributes a nonnegative amount.

References

[BK] K. Bannai and S. Kobayashi, *Algebraic theta functions and the p-adic interpolation of Eisenstein–Kronecker numbers*, Duke Math. J. **153** (2010), 229–295; arXiv:math/0610163. Numbering as in the arXiv version.

[GL] L. Sernau, *GRH for Dirichlet L-functions, in Lean 4*, a shorter rewriting of the Lean proof, text by Claude, `https://github.com/lsernau/grh-lean`, commit `72fead1`, readable edition `grh/`.

[LMPT] W. Li, E. Mantovan, R. Pries and Y. Tang, *Newton polygons of cyclic covers of the projective line branched at three points*, arXiv:1805.04598.

[Si2] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Grad. Texts in Math. 151, Springer, 1994.