The generalized Riemann hypothesis for Dirichlet L-functions

27 November 2026 · Edition 930

Volume XI

Strict cohomology at exceptional weights

Abstract

We identify the twists at which two ordinary characters coincide. Bounds on conductors and the spacing of weights reduce the surviving cases to unit, regulator and class group calculations in the real cyclotomic tower and its quadratic extensions.

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

Contents

XI Strict cohomology at exceptional weights 1
54 Strict orders at varying coefficient primes . . . 3
54.1 The large-prime cohomology bound on the period fields . . . 3
54.2 Variation of the twist in the original weight space . . . 6
54.3 Distinct residual inertia characters at a coefficient prime . . . 9
54.4 The two moving ramified coefficient primes . . . 14
55 Colliding ordinary characters . . . 18
55.1 Frobenius at the two coincident inertia weights . . . 18
55.2 Ordinary cuspidal adjoints at the original weights . . . 22
55.3 Recovering the ordered local characters from Hecke traces . . . 26
55.4 The fiber of the split trace at repeated local characters . . . 30
55.5 Reducible traces when inertia is scalar on the descended plane . . . 35
55.6 Quadratic residual characters on one real subfield of the interval . . . 38
55.7 A ramified plane at an inert coefficient prime . . . 41
55.8 The conductor of the character used in descent . . . 44
55.9 Reducible traces for every pair of colliding weights . . . 46
55.10 Conductor bounds at the two colliding residues . . . 49
56 Exceptional weights in the cyclotomic tower . . . 51
56.1 Uniform exponent bounds for characters of growing order . . . 51
56.2 A single possible character orbit in a dyadic layer . . . 52
56.3 Spacing of the weights with large strict cohomology . . . 54
56.4 Full orders at weights outside the class group exceptions . . . 56
56.5 A finite class group determining the possible exceptional dyadic weight . . . 59
56.6 Full cohomology lengths at locally split weights . . . 61
56.7 Ideal classes at the primes testing the theta periods . . . 64
57 Units, regulators and relative class numbers . . . 66
57.1 Global units modulo the coefficient prime and the opposite root . . . 66
57.2 Norms of units at the exceptional dyadic weights . . . 68
57.3 A base unit test for all zero-residue weights . . . 70
57.4 Units supported at the coefficient prime and the real quadratic layer . . . 73
57.5 Two unit polynomials for the zero-residue strict groups . . . 76
57.6 Vanishing at zero-residue weights in the first three dyadic layers . . . 79
57.7 The two possible characters in the full real dyadic tower . . . 81
57.8 Relative regulators at the half-residue weights . . . 84

57.9 Relative class numbers in complex dyadic layers 88
57.10 Fixed characters at the limiting residue degree 91
57.11 Half-residue weights over a fixed abelian field of two-power degree 94
57.12 Descent at the zero residue over a fixed real cyclic field 97
57.13 Descent at varying Frobenius orders in the real dyadic tower 100
57.14 The relative class group at the half-residue weights 102
57.15 A single class number for the half-residue weights of the interval 105
57.16 Quantitative unit indices at split coefficient primes 107
57.17 One class group quotient for the sum at the half-residue weights 110
57.18 All weights at a good prime in one ordinary class group 112
57.19 Prime ideal generators at exact cyclotomic depth 115
58 References 118

54 Strict orders at varying coefficient primes

54.1 The large-prime cohomology bound on the period fields

Continue with $K = \mathbb{Q}(\sqrt{-s})$, E_x, the original weight and the unramified coefficient ring O of Section 44.10. Write $D = J/O$ and $S(\xi)$ for classes in $H^1(\mathbb{Q}, D(\xi))$ unramified at finite primes away from ℓ and zero at ℓ. Let $B = \bigoplus_j B_j$ consist of the finite sums of homogeneous elements in the completed marked solution ring. Here degree is the weight for conjugation by $\mathrm{diag}(a, 1, a^{-1})$. Rows and columns are numbered $0, 1, 2$.

Proposition 54.1 (The marked presentation on the chosen quadratic field)**.** *One has $B_0 = T$. When $S(\Psi^{-1}) \neq 0$, the augmented graded presentation of B satisfies the numerical and cotangent hypotheses of Proposition 41.4. Its negative weight-one cotangent quotient has length*

$$\mathrm{length}_O\, S(\Psi^{-1}) + \mathrm{length}_O\, S(\eta\Psi^{-1}),$$

where η is the quadratic character of K. The fixed subscheme consists of the split section $\operatorname{Spec} O$.

Proof. We check the dependence on the auxiliary quadratic character in Sections 32.4–32.8. The prime ℓ exceeds sN_*, $4t_* + 5$ and the class number of K throughout this range, for sufficiently large V. Both α and η are unramified there, $\Psi(c) = 1$, and $\eta(c) = -1$. Choose g_* in inertia at ℓ mapping to a generator of $\mathbf{F}_\ell^\times$ under the residual cyclotomic character. The three diagonal residual values are distinct. Thus the ordinary word cuts out the unique ordered inertia flag by Lemma 32.10. For $r \geq 2$ the dual twisted strictly upper triangular module has inertia exponents $1 - r$ and $1 - 2r$, both nonzero modulo $\ell - 1$. Theorem 32.11 gives the local chart. For $r = 1$ the proof of Theorem 32.15 uses the unramified quadratic algebra at ℓ. In the split case the two adjacent characters are separate unramified twists of the cyclotomic character. In the field case they form an induced module from the unramified quadratic extension. In each case the sum of the local degrees in Lemma 32.14 is two, saturation removes the valuation coordinates, and the outer obstruction vanishes by the residual exponent $1 - 2$. This gives the same local coordinate counts $(1, 2, 3, 4, 2)$ in weights $-2, -1, 0, 1, 2$.

Away from ℓ the inertia quotient has order prime to ℓ, including at s. In the relative cochain complex of Lemma 32.12 these places therefore contribute zero Euler characteristic. The action at infinity is minus reflected transpose as before. If a_j is the relative tangent dimension in weight j, the obstruction space has dimension $a_j + \mathbf{1}_{|j|\leq 1}$. Indeed the correction in degree three is dual to the global invariants of the dual twisted module. Inertia at ℓ excludes all weights except possibly $j = r = 1$. In that case the two characters are $\bar{\alpha}^{-1}$ and $\bar{\eta}\bar{\alpha}^{-1}$. The first is odd and the second is nontrivial on inertia at s, since $s \nmid N_*\ell$. This proves the asserted dimension by the Euler calculation in that lemma. The small-extension argument of Theorem 32.13 and the eight marking entries now give the following numbers.

j	-2	-1	0	1	2
variables	$a_{-2} + 1$	$a_{-1} + 2$	$a_0 + 3$	$a_1 + 4$	$a_2 + 2$
relations, at most	$a_{-2} + 1$	$a_{-1} + 3$	$a_0 + 3$	$a_1 + 3$	$a_2 + 1$.

Homogeneous generators and the ambient formal chart are obtained from the power series presentation by taking weight parts as in Lemma 32.17.

At a fixed lift all matrices on G_K are diagonal. The quotients of their three coordinate characters by their prescribed values reduce to one and are everywhere unramified. At ℓ this follows from the ordered flag and its distinct residual characters, and at the other primes it follows by the prime-to-ℓ inertia condition. Over an Artinian local test ring these quotients

therefore factor through both the class group of K and a finite ℓ-group. They are trivial since $\ell \nmid |\mathrm{Cl}(K)|$. The proof of Proposition 32.18 applied to all Artinian truncations identifies the fixed quotient with O. It also shows that the equations in degree zero span the integral degree-zero cotangent space.

For weight -1 the two lower adjacent directions split into the characters Ψ^{-1} and $\eta\Psi^{-1}$. The condition at c fixes the odd coboundary, and the adjacent marking at g_* fixes the other coboundary: its coefficient $(\Psi(g_*)+1)(\Psi(g_*)^{-1}-1)$ is a unit. The lower long entry has character $\eta\Psi^{-2}$; its coboundary is fixed at c. For either weight the ordinary local word forces a lower cocycle to be a local coboundary at ℓ: after removing its value at g_* by a local coboundary, the ordered flag is the standard flag and its lower entries vanish on inertia. The cocycle law and the unit difference on g_* then force it to vanish on the decomposition group. Conversely conjugating the split lift realizes each such local coboundary on the selected component. Away from ℓ averaging over the finite inertia quotient gives exactly the unramified condition. Applying this argument over O/ℓ^n for every n, as in Corollary 32.9 and Theorem 32.19, identifies the D-duals of the two negative cotangents with $S(\Psi^{-1}) \oplus S(\eta\Psi^{-1})$ and $S(\eta\Psi^{-2})$. The passage to D commutes with the strict conditions since the invariants at ℓ vanish and the invariants on each other inertia group are zero or divisible. Restriction to E_xK is injective on these groups by the prime-to-ℓ index. The finite characters become trivial there, and the strict groups of twists $r, 2r$ are finite by Theorem 25.1. Thus both negative cotangents are torsion, supplying rational spanning and the stated length.

Finally $Z = M(g_*) - M(cg_*^{-1}c) = \mathrm{diag}(z, 0, -z)$ with z a unit. Its square trace gives $2z^2$, so the specified square root z belongs to the closed trace ring by Hensel's lemma. Its spectral projectors are therefore polynomials in Z over T. The adjunction relation $M(ch^{-1}c) = J_3 M(h)^{\mathsf{T}} J_3$ puts each weight-zero entry monomial into products of directed cycles, as proved in Theorem 34.2. Inserting the projectors expresses each cycle as a trace. Closure gives $B_0 = T$. Moreover the entries of finitely many group generators generate B over T. Indeed their homogeneous differences from the split values topologically generate the completion. For any one weight, every monomial in those differences has a weight-zero factor times one of finitely many remainders by Lemma 32.17. Grouping each homogeneous series by its remainders gives the claimed algebraic generation. □

Lemma 54.2 (Multiplicity at a nonsplit trace)**.** *For each nonsplit geometric characteristic-zero character σ of T, put $k_0 = \overline{J}$ and $B^\sigma = B \otimes_{T,\sigma} k_0$. Then*

$$\dim_{k_0} B_0^\sigma = 1, \qquad \dim_{k_0} B_1^\sigma = \begin{cases} 1 & \text{at an irreducible trace,} \\ 0 & \text{at a line and an irreducible plane.} \end{cases}$$

These are also the dimensions obtained by localization in $T \otimes_O k_0$.

Proof. Corollary 44.43 makes the indicated local factor of $T \otimes_O k_0$ equal to k_0. Taking weights commutes with this scalar extension, so $B_0^\sigma = k_0$. Write $E^\sigma = E_M \otimes_{T,\sigma} k_0$ for the finite matrix algebra of Lemma 38.9. The universal group matrices have homogeneous entries, and therefore give a homomorphism $E^\sigma \to M_3(B^\sigma)$ preserving trace. Each of the three spectral projectors P_i of Z is the corresponding diagonal matrix unit in this map.

At an irreducible trace E^σ maps onto the full endomorphism algebra on its semisimple realization, by Burnside's theorem. Each P_i has trace one and is a rank-one projector there. In the eigenbasis of Z, choose two elements a, b mapping to opposite matrix units between the first and middle lines. Their order can be chosen so that $\mathrm{tr}(P_0 a P_1 b P_0) = 1$. In the universal matrices over B^σ this same trace is $a_{01}b_{10}$. These entries have degrees $1, -1$, respectively, since

elements of E^{σ} are scalar linear combinations of group matrices. Hence a_{01} is a unit of degree one, and multiplication by it identifies B_0^{σ} with B_1^{σ}.

At a line and an irreducible plane Lemma 40.9, applied first over a finite splitting field and then over k_0, gives $E^{\sigma} = k_0 \times M_2(k_0)$, with the group acting trivially on the first factor. Here the finite algebra calculation is essential: the proof uses the vanishing of extensions in both directions between the plane and the line. On the trivial factor $Z = 0$, so the middle projector $P_1 = 1 - Z^2/z^2$ is one there. Its total trace is one. On the plane it is an idempotent of trace zero in characteristic zero, hence zero. Thus P_1 is central in E^{σ}. Its image in $M_3(B^{\sigma})$ is the middle diagonal matrix unit, so every group matrix has all four adjacent entries zero in B^{σ}. The generation assertion of the proposition now shows that B^{σ} is generated in even degrees. This proves the assertion on the full odd piece, including its possible infinitesimal elements. □

Theorem 54.3 (The integral strict length for one character)**.** *Whenever $S(\Psi^{-1}) \neq 0$, with I, h as in Theorem 44.44, one has*

$$\operatorname{length}_O S(\Psi^{-1}) + \operatorname{length}_O S(\eta\Psi^{-1}) \;\le\; 2\operatorname{length}_O(I/hI).$$

In particular $\operatorname{length}_O S(\Psi^{-1})$ *is bounded by the right hand side for every character in the range.*

Proof. Proposition 54.1 supplies the presentation, the rational formal chart, and the two negative spanning conditions in Proposition 41.4. The fixed section is unique. Theorem 44.41 gives integral finiteness of B_0. The Frobenius difference h vanishes at the split character. At every nonsplit point it is nonzero by the archimedean estimate in Theorem 44.44. The characters nonzero on $B_{-2}B_2$ form a subset of the nonsplit points, since every nonzero-degree element has split value zero. At each of these characters the largest of the two local dimensions in Proposition 41.4 is one by the lemma. Applying that integral intersection inequality and enlarging the sum to all nonsplit points gives the bound by $2\sum_{\sigma\neq\text{split}} v_{\ell}(\sigma(h))$. The determinant formula in Theorem 44.44 identifies this sum without its factor two with the length of I/hI. □

Corollary 54.4 (All large coefficient primes on the original fields)**.** *For some constant C and every sufficiently distant polynomial-conductor interval of Section 6.6, one has, for all $V \le x \le V^{3/2}$,*

$$\mathcal{L}_{>}(x) = \sum_{\ell > P(x)} (\log \ell) \sum_{1 \le r < t(x)} \operatorname{length}_{\mathbb{Z}_{\ell}}\bigl(\mathcal{S}_{\ell,r}(E_x)^{c=(-1)^r}\bigr) \;\le\; 2\log D(V) \;\ll_{\psi,\varepsilon} V^{C}.$$

For any such ℓ prime to $D(V)$ all these complementary groups are zero. The large-prime summands $R_{\ell,r}$ of Section 6.6 satisfy the same total bound.

Proof. Since $\ell > [E_x : \mathbb{Q}]$, the character decomposition in Theorem 22.17 is integral after unramified coefficient extension. It gives the length at ℓ, r as the sum of $b_{\alpha} \operatorname{length}_O S(\Psi^{-1})$ over the complementary residue orbits. The conductor conditions in that theorem change none of the lengths here because the finite inertia has order prime to ℓ. Apply the theorem just proved to these scalar groups and sum the result using Theorem 44.44, which uses a single $D(V)$ for the interval. Its proof gives the same comparison at each individual ℓ with $v_{\ell}(D(V))$, proving the vanishing assertion. For $\ell > P(x)$, $R_{\ell,r}$ is a direct summand of the displayed complementary group by definition of the field average. This gives its bound. □

Since $V^{C} = o(\exp(x^{\varepsilon}/2))$ uniformly for $x \ge V$, the contribution from $\ell > P(x)$ fits the allowance in equation (L). For the odd primes at most $P(x)$, Proposition 6.11 leaves the quotients by the subgroup killed by ℓ^{b_0}. Section 6.6 also requires the integral comparison of projected theta periods over these same E_x.

54.2 Variation of the twist in the original weight space

Fix E_*, N_*, K, s, u and $D(V)$ as in Theorem 44.44. For this subsection allow any prime $\ell \geq 11$ such that

$$\ell \nmid suN_*[E_* : \mathbb{Q}]\,|\mathrm{Cl}(K)|.$$

Let $n = \ell - 1$. For each twist $r \geq 1$ let j be its representative in $\{0, \dots, n-1\}$. We consider $r = 1$, and also all r satisfying

$$2 \leq j \leq n-2, \qquad n/\gcd(n, j) > 4. \tag{$*$}$$

Write $\bar{\omega} = \bar{\kappa}_\ell|_{I_\ell}$. The significance of $(*)$ is that $\bar{\omega}^j$ has order greater than four and $j \not\equiv \pm 1 \bmod n$. The period fields and the test prime u are the same for the small and large coefficient primes.

Lemma 54.5 (The auxiliary ordinary ring at a residual weight)**.** *Let α be a character of E_x with $\alpha(c) = (-1)^r$. At $r = 1$ put $j = 1$. For each of the indicated j, α, there is a layer $L = KF_a^+$ of Proposition 36.15 for which every geometrically irreducible prime of the ordinary determinant ring with residual character $\bar{\alpha}\bar{\kappa}_\ell^j$ contains I_K. The weight map for any of the indicated positive twists congruent to j uses this same ring.*

Proof. We verify the input to the propagation argument of Theorem 44.39 with the exponent j. Only the residue of the exponent is used to specify the ordinary determinant and its finite inertia and diamond characters. The choice of a classical point to start the argument also needs an integral exponent of the specified parity. Here j itself has that parity since n is even.

The character α has order prime to ℓ and is unramified above it. At s the inertia character of K is nontrivial while α is unramified. Thus $K \cap E_* = \mathbb{Q}$, $\eta\alpha \neq 1$, and its conductor is $s\,\mathrm{cond}(\alpha)$. Take the auxiliary prime $w \equiv 1 \bmod sN_*\ell$ with ℓ a non-ℓ-th power modulo w by Lemma 37.3. In its Kummer argument $\ell \nmid sN_*$ gives valuation n for ℓ in the cyclotomic field. The other auxiliary prime may be chosen in the progression $-1 \bmod 8sN_*\ell$. The resulting L is disjoint from $E_*(\mu_\ell)$ as in Proposition 36.15: the only possible common ramification is at ℓ, with coprime ramification indices there. All designated finite places split in L/F_a^+ and inertia on G_L has residual cyclotomic image of order n. In particular one can choose the element of G_L acting as complex conjugation on $E_*(\mu_\ell)$, used in the relative duality arguments.

For the ordinary adjoint use weight $j+1$ in Lemma 36.16. Here $2 \leq j+1 < \ell - 1$, so the Bernoulli denominators through degree $j+1$ are prime to ℓ. Its auxiliary level $s\,\mathrm{cond}(\alpha)w$ is prime to ℓ. Therefore the Eisenstein congruence, free diamond action, and lifting of the indicated cuspidal character in that lemma apply. The order of $\bar{\omega}^j$ is greater than four also for $j = 1$. Thus the quadratic self-twist excluded in Theorem 36.17 is impossible. The resulting adjoint is absolutely irreducible on every open subgroup and ordinary with the required ordered residual characters. Its classical ordinary deformations and the full Hecke component of Theorem 37.36 use this seed. The ordinary flags are separated by inertia, and the exclusion of a cyclic permutation of three lines in Theorem 36.26 uses $(\bar{\omega}^j)^3 \neq 1$.

For the strict classes on the layer the two characters in Proposition 37.5 have inertia exponents $-ij$ and their Tate duals have exponents $1 + ij$, $i = 1, 2$. These four exponents are nonzero modulo n. For $1 + 2j$ this follows from parity, for $1 + j$ from $j \neq n - 1$, and for the other two from the order condition. The local contribution at w is still one, so the proof supplies both required strict classes. In Proposition 37.6 restriction to $LE_*(\mu_\ell)$ has prime-to-ℓ index over F_a^+ or L, since that index divides $2[E_* : \mathbb{Q}]n$. The bound h on class group generator numbers along the cyclotomic tower follows there from Ferrero–Washington. It may depend on ℓ, E_*, w. Theorem 37.8 then chooses a after h. The needed large real degree, local degrees

and intersection dimensions thus hold without any upper bound on the conductor in terms of ℓ.

For clarity, the two residual exclusions in the subsequent propagation have different origins. A hypothetically induced plane would acquire a quadratic self-twist, interchanging the two outer residual characters. This forces $(\bar{\omega}^j)^4 = 1$, by Lemma 44.9. A cyclic permutation of three lines in the absolutely irreducible case would give a cubic self-twist, forcing $(\bar{\omega}^j)^3 = 1$, as in the irreducible-curve argument of Section 42.2. Both are excluded. The residual projector constructions require the three eigenvalues to be distinct, and the matrix and sign projections require 2 and 3 to be units. The Taylor–Wiles primes for the separated curves are chosen after those curves, by the dual-space and Frobenius argument of Proposition 44.10. For the integral Hecke modules at these primes use the old-type coefficient lattices of Lemma 54.9. This includes the primes dividing the order of a local finite matrix group at the tame level. The ordinary level, rank and complete-intersection arguments apply to that field with those primes. The dimension bounds in Sections 44.5 and 44.6 use $d = [F_a^+ : \mathbb{Q}]$, the degrees at ℓ and h just obtained. With these inputs the marked-chart propagation and the connected lower fiber give Theorem 44.39 on the chosen layer.

Finally for $r \equiv j \bmod n$, the ordered residual characters agree on the whole group. On local units the change of exponent $r - j$ is trivial on the prime-to-ℓ part of the cyclotomic character, whose order divides n. On the principal units it defines an arithmetic specialization of the full weight algebra. The common cyclotomic normalization is independent of r. This proves the assertion about the ring. □

Proposition 54.6 (Specialization at the actual twist)**.** *At any $r = 1$ or r satisfying $(*)$, the fixed-weight ring T of the original quadratic field at exponent r is finite over O, with geometrically reduced generic fiber. Its nonsplit points have the two sorts of classical labels of Proposition 44.42 at the actual weight r.*

Proof. Use the upper ordinary problem from the lemma, while prescribing $\Psi = \alpha\kappa_\ell^r$ in the original problem. The inertia element g_* separates the three original characters since the order of $\bar{\omega}^r = \bar{\omega}^j$ exceeds four. The restriction-of-traces proof of Proposition 38.7 therefore gives a surjection onto T at the arithmetic weight of r: the polynomial projector identities and equality of matrix spans there divide only by residual unit differences. In characteristic ℓ the reducible trace argument of Theorem 40.7 applies. In the plane case its rational ordinary pseudorepresentation has odd determinant lifted by $\eta\Psi^{-2}$, de Rham at ℓ. Its reduction is nontrivial on I_ℓ because $(\bar{\omega}^j)^2 \neq 1$. Its local constituent lifting the trivial residual character is unramified after the prescribed twist. These are the hypotheses for the finiteness argument using Pan over $\mathbb{Q}$ in that theorem. The class-number argument for its one-dimensional summand uses $\ell \nmid |\mathrm{Cl}(K)|$. At a prime with irreducible trace the preceding lemma puts its restriction in Hecke support. The special-fiber argument of Theorem 44.41 now gives finiteness.

For $r > 1$ the residual Tate dual of the strictly upper triangular module has exponents $1 - j, 1 - 2j$ on inertia. Both are nonzero. The ordinary local chart is consequently formally smooth by the obstruction calculation of Theorem 32.11. At arithmetic weight $r \geq 2$ every successive positive difference of the three cyclotomic exponents is at least two. In constructing an extension of an earlier flag step by the next graded quotient, the Hom module from the quotient to the earlier step therefore has positive exponents and has no quotient with exponent one. Its Tate dual has zero invariants. The local Euler characteristic and the Bloch–Kato dimension formula make all such extensions of crystalline steps crystalline, as in Theorem 33.11. Density of integral evaluations in the smooth chart and the fixed Hodge-type crystalline quotient give that result on the whole chart. At $r = 1$ the unit part of the Kummer chart gives exactly

the first-twist calculation of Theorem 32.15. The finite matrix module and limit argument of Proposition 38.10 uses the fixed weight interval $[-r, r]$ for this triple. Liu's crystalline limit theorem permits any fixed finite interval for odd ℓ. [1, 2]

The ordinary control theorem on the upper layer applies to the dominant algebraic weight of r. The cuspidal descent in Proposition 44.42 uses the tame inertia type $\alpha, 1, \alpha^{-1}$ and the prime-to-three degree $[L : K]$. It gives the desired original level for irreducible points. For a line and a plane the odd descent and primitive form computation in Propositions 38.14 and 40.11 use distinct weights and the absence of a quadratic self-twist, guaranteed by the residual order greater than four. Thus the modular weight is $2r + 1$ and the level divides sN_*. The Selmer vanishing for the line–plane extensions uses Kato's off-center twist r of that same form, since $1 \le r \le 2r$ and $2r \ne 2r + 1$. The enormous-image proof at irreducible points uses the three distinct Hodge–Tate weights and excludes the cubic residual self-twist. Corollary 44.43 therefore computes these generic local rings at the shifted weight as well. [3, 4] □

Theorem 54.7 (Full lengths for the indicated residual twists)**.** *Sum over the primes specified at the beginning of this subsection and over $1 \le r < t(x)$ with $r = 1$ or $(*)$. Then throughout the same interval*

$$\sum_{\ell} \log \ell \sum_{r} \operatorname{length}_{\mathbb{Z}_\ell}(\mathcal{S}_{\ell,r}(E_x)^{c=(-1)^r}) \;\le\; 2 \log D(V).$$

The same estimate holds at one prime with the factors $\log \ell$ removed and the right side replaced by $2v_\ell(D(V))$.

Proof. For r satisfying $(*)$, the five dual twisted global matrix weights have exponents $1 - ar$, $a = 0, \pm 1, \pm 2$, on inertia. They are all nonzero modulo n: the two even multiples cannot equal the odd number one modulo even n, and $j \ne \pm 1$ accounts for the adjacent weights. For $r = 1$ the possible global invariants in weight one are again excluded by parity and ramification at s. The proof of Proposition 54.1 now gives the same numerical presentation. Strictness at ℓ uses the unit differences for $\bar{\omega}^{-j}$ and $\bar{\omega}^{-2j}$. Prime-to-ℓ restriction to $E_x K$ proves finiteness of the negative cotangents even when $r > \ell$. The fixed-point argument uses the stated class-number condition.

The proposition gives the finite étale generic trace algebra at this weight. At a line and plane its specialized matrix algebra is the product of the scalar and full plane algebras by the vanishing of the extensions just proved and the opposite-matrix-unit calculation of Lemma 40.9. Thus the proof of Lemma 54.2 gives multiplicity one in the maximum over the two graded dimensions. The integral intersection inequality of Proposition 41.4 bounds the scalar strict length by twice the sum of the nonsplit Frobenius-difference valuations at u. The argument applies to every contributing scalar character.

For fixed r, ℓ the character decomposition is integral since $\ell \nmid [E_x : \mathbb{Q}]$. The local corrections at the conductor vanish for the same reason. For each ℓ, summing over the contributing characters and these r uses a sublist of the very factors defining $D(V)$ in Theorem 44.44, since those factors are indexed by the actual twists r. More explicitly, the diagonal value is $1 + u^r \alpha(u) + u^{-r} \alpha(u)^{-1}$ and the plane value is $1 + u^{-r} \alpha(u) a_u(f)$. The rank-three label has the corresponding archimedean weight and the same level bound as in that theorem. The test prime is different from ℓ, all denominator-clearing powers of u are units, and any unused factor has nonnegative valuation. Distinct labels for different points and the separate residue-character embeddings give the single-prime inequality. Multiplication by $\log \ell$ and summation prove the assertion. □

Corollary 54.8 (The residual twists at smaller coefficient primes)**.** *At each of the indicated $\ell \le P(x)$ and positive twists covered by the theorem, $R_{\ell,r} = 0$ on every sufficiently distant interval. For $r \ge 2$, a nonzero $R_{\ell,r}$ at one of these primes can therefore occur only if*

$$\ell - 1 \mid 2r, \quad \ell - 1 \mid 3r, \quad \ell - 1 \mid 4r, \quad \ell - 1 \mid r - 1, \quad \text{or} \quad \ell - 1 \mid r + 1.$$

In particular $\ell \le 4r + 1$ there, and at each such prime there are at most eight possible residue classes of twists.

Proof. The length of any one complementary group in the theorem is at most $2v_\ell(D(V)) \le 2 \log D(V)/\log 2$. This is $O_{\psi,\varepsilon}(V^C)$, uniformly on the interval. For $x \ge V$, $b_0 = \lfloor \exp(x^\varepsilon/8) \rfloor$ eventually exceeds this bound. A finite $\mathbb{Z}_\ell$-module of length at most b_0 is killed by ℓ^{b_0}, by its elementary divisors. This holds also for its direct summand $U_{\ell,r}$, proving the vanishing.

For the other twists the residue is $1, -1$, or its order in $\mathbb{Z}/n\mathbb{Z}$ divides one of $2, 3, 4$. These are precisely the indicated divisibility alternatives. There are at most $\varphi(1)+\varphi(2)+\varphi(3)+\varphi(4) = 6$ elements of orders at most four in a cyclic group. Adding the two unit residues gives eight. For $r \ge 2$ all the integers on the right of the divisibilities are positive and at most $4r$. This gives the prime bound. □

The exceptions on the prime side have a simple description on the period interval. The odd part of $[E_* : \mathbb{Q}]$ divides the fixed degree $[K_\psi : \mathbb{Q}]$, since the other extensions adjoined to it have two-power degree. Apart from the two moving primes q, d_0 in N_*, the excluded primes therefore come from a fixed finite set. Bounding their tails and the remaining residue classes is a further arithmetic requirement in Section 6.6.

54.3 Distinct residual inertia characters at a coefficient prime

Keep the primes ℓ, fields and test prime u of Section 54.2. Put $n = \ell - 1$. We shall require only $n \nmid 2r$ on the twist. Thus a separating inertia element g_* still exists even when the residual ratio of two adjacent ordinary characters is cyclotomic. For $r \ge 2$ we use the full ordinary inertia word at ℓ in the original marked matrix problem. At the actual twist $r = 1$ we keep the component of Theorem 32.15.

Lemma 54.9 (Integral coefficients for the prescribed tame types)**.** *On each layer L/F_a^+ of Proposition 36.15 constructed with the prime-to-ℓ conductor data above, the three ordinary modules needed for the changes of level at Q can be taken with coefficients in stable lattices in the old compact types. They are finite free over their respective weight and diamond group algebras, with the stated diamond coinvariants. Their characteristic-zero systems have the prescribed old inertia and zero monodromy.*

Proof. The numerical proof of Lemma 41.21 uses $\ell > N_*^{12}$ before averaging over a finite matrix group at an old place. A prime coprime to N_* can divide that group's order. For instance $13 \mid 3^3 - 1$. We give the integral construction at any prime in the present range. For each old compact type σ_v used in that lemma, enlarge the coefficient field J' to realize it. Its compact group acts through a finite quotient. The sum of the translates of any full lattice is an invariant full lattice. Take the tensor product W of their dual lattices. At an unramified place use the trivial lattice.

At the old places use the full maximal compact group and its action on W. An automorphic form is an equivariant function on the finite adelic double cosets with these coefficients. At a representative g its possible values are precisely the invariants in W under its arithmetic stabilizer Γ_g, with the ordinary algebraic coefficient included when present. These stabilizers

are finite. Their rational points are integral at every finite place for some lattice, and the real group is compact, so discreteness gives finiteness. They have order prime to ℓ. In fact an element of order ℓ would act faithfully on L^3, with a primitive ℓ-th root as an eigenvalue. Its degree over L is $\ell - 1 > 3$ by the disjointness of Proposition 36.15. Averaging over each Γ_g consequently gives free coefficient modules and commutes with reduction and extension of coefficients.

Consider any of the normal diamond covers at the coefficient places or at Q with finite ℓ-group quotient Δ. The stabilizer at the lower level maps trivially to Δ, since its order is prime to ℓ. Thus over each lower double coset the lifts are a free transitive Δ-set. Evaluation at one lift, followed by right translation to all the lifts, identifies its contribution with the regular module tensored with that lift's invariant lattice. This also gives the trace identification of coinvariants with the lower level. Dualizing gives the corresponding assertion for the dual modules. The argument works simultaneously for the independent normal covers. The finite diamonds of order prime to ℓ select their prescribed character by an integral idempotent.

For precision, the remaining change in the ordinary filtration is the inclusion between the levels with indices (b, b) and (b, c), $c \geq b$, at a coefficient place. The double-coset identity in Geraghty's Lemma 2.5.2 sends a form at the deeper level to the shallower level by a power of the positive diagonal operator. The coset representatives act only at the coefficient place, hence act trivially on W. Invertibility of that operator on the ordinary part gives the same control identity with these coefficients. The ordinary projector commutes with the diamonds and the trace maps. Its images in the finite free diamond modules are therefore projective, hence free over the local group rings. Compatible coinvariants give a common rank at every depth. Lifts of a basis at the residual level give a surjection from the free module of this rank over the completed group algebra by compact Nakayama. Modulo each open diamond kernel it is a surjection of equal-rank free modules, so an isomorphism. These kernels have zero intersection on the source. This proves freeness over the completed algebra, also with the diamonds at Q retained. Localization at the common residual Hecke system is a direct summand and preserves these conclusions. This is the double-coset proof of Geraghty's Lemma 2.2.6 and Proposition 2.5.3 with the old coefficient lattice carried through the maps. [5]

Over J', the equivariance condition at v selects $\mathrm{Hom}_{\mathrm{GL}_3(\mathfrak{o}_v)}(\sigma_v, \pi_v)$ in the local automorphic representation. The compact-type theorem in Lemma 41.21 therefore gives exactly its old inertial condition. In particular the ordinary vector of the initial adjoint occurs. The change-of-level operators and the integral identities at Q act by finite double cosets with identity component at the old places. Their convolution relations, and the classical tests of Proposition 41.22, apply to these modules. The determinant identities first checked at the dense classical weights then hold integrally, since the operators act on free modules over the weight ring. This supplies the integral modules used in the support argument of Lemma 54.5 even when the finite matrix group at an old conductor prime has order divisible by ℓ. □

Lemma 54.10 (A local presentation with the ordinary inertia word)**.** *Let $r \geq 2$, $n \nmid 2r$, and let W_1 be the residual module of the two upper adjacent matrix entries over $G_{\mathbb{Q}_\ell}$, with its polarized action. Put $e = \dim_k H^2(\mathbb{Q}_\ell, W_1)$. The full framed local ordinary ring admits a presentation with*

$$(1,\, 2,\, 3,\, 4 + e,\, 2)$$

variables of weights $(-2, -1, 0, 1, 2)$ and at most e relations, all of weight one. In the full original marked global presentation this adds e to the variable count and to the relation allowance at weight one in Proposition 54.1.

Proof. The three distinct residual eigenvalues of g_* give the unique ordinary flag by Lemma 32.10. Use its lower unitriangular coordinates and put it in standard position. These are three free coordinates of weights $-2, -1, -1$. The diagonal characters on inertia are fixed. The diagonal variation is determined by its unramified Frobenius value in the signed diagonal group, hence is formally smooth in three coordinates of weight zero. Work relative to this diagonal ring. The remaining matrices are upper unitriangular corrections. At the residual diagonal their Lie module is $W_1 \oplus W_2$, with W_2 the upper long entry. On the Tate dual of W_2, inertia has exponent $1 - 2r$. It is nonzero modulo the even integer n, so $H^2(\mathbb{Q}_\ell, W_2) = 0$ by local duality.

With the diagonal held fixed the framed first-order lifts on each weight form $Z^1(\mathbb{Q}_\ell, W_i)$. The local Euler characteristic gives $\dim Z^1 = 2 \dim W_i + \dim H^2$, after adding the coboundary dimension $\dim W_i - \dim H^0$ to $\dim H^1$. Thus the two further variable counts are $4 + e$ and two. For a small coefficient extension with square-zero kernel J' annihilated by the maximal ideal, fix the lifted diagonal and lift the upper entries as continuous cochains. Their multiplication defect is a two-cocycle in $(W_1 \oplus W_2) \otimes_k J'$. Changing the entry lifts changes it by a coboundary, and subtracting a correcting cochain gives a lift exactly when its class vanishes. Keeping the diagonal fixed preserves the required inertia characters.

Choose a power series presentation over the diagonal ring using the computed relative tangent basis, with kernel J_0 and power series maximal ideal $\mathfrak{m}$. The usual small-extension argument in Theorem 32.13 injects the dual of $J_0/\mathfrak{m}J_0$ into this obstruction space. Indeed a functional killing its component of the universal obstruction allows the corresponding pushed-out extension to lift. The relative variables can then only change by square-zero elements. Every relation has zero relative linear term at the residual point, so these changes cannot alter its value in that kernel. The functional must therefore vanish on every relation. One may take sufficiently high Artinian truncations as in that theorem. This construction is equivariant under the diagonal torus. Taking the weight parts of lifts of a basis, followed by Nakayama's lemma, gives at most e generating relations, all of weight one.

In the relative global calculation of Lemma 32.12 the local lift at ℓ is given. Its ring need not be smooth for that calculation: the obstruction is the defect of a global lift with that specified local restriction. The possible dual invariants in degree three have inertia exponents $1 - ar$ with $a = 0, \pm 1, \pm 2$. Only $a = \pm 1$ could contribute, and then $r \equiv \pm 1 \bmod n$ is odd. The residual characters of the corresponding dual pair, after cancellation of the cyclotomic factor, are $\bar{\alpha}^{\pm 1}$ and $\bar{\eta}\bar{\alpha}^{\pm 1}$. The first is odd and the second ramifies at s, so neither has global invariants. The relative counts and the eight marks in Theorem 32.13 therefore apply as before. Adding the local presentation gives the asserted global counts. In the notation of Corollary 32.20 this replaces R' by $R' + e$, which is allowed in Proposition 41.4. □

Proposition 54.11 (Crystallinity of modules for the ordinary matrix algebra)**.** *Let $r \geq 2$. Write T for the original trace ring with the full ordinary word and E_M for the T-span of the group matrices on G_K. Let $T \to D'$ be a continuous specialization to a finite local algebra over a finite extension of $\mathbb{Q}_\ell$ with integral residue point. Every finite $E_M \otimes_T D'$-module, as a coefficient-field representation, is crystalline at all places of K above ℓ.*

Proof. As in Lemma 38.9, E_M is a finite T-module by finiteness of the Cayley–Hamilton algebra. Its action and the action of the Galois group on any such module are continuous. Fix a place above ℓ. Inside E_M use the polynomial projectors e_0, e_1, e_2 of the local inertia element g_* and the three fixed eigenvalues. They lie in E_M, even if D' has nilpotents. For each local group element g the following identities hold in the original matrix algebra:

$$e_i M(g) e_j = 0 \quad (i > j), \qquad e_i M(g) e_i = \xi_i(g) e_i, \quad \xi_i(g) = t(e_i M(g)).$$

Indeed the eigenlines of g_*, in their ordinary order, split the ordinary filtration. Each initial sum of these lines is stable under the local group by uniqueness of the flag. On each successive quotient the group acts by the corresponding diagonal character, which gives both identities in this eigenbasis. At a conjugate place use the reflected dual flag in its ordinary order. The characters ξ_i take values in T, and restrict on inertia to $\kappa_\ell^{r}, 1, \kappa_\ell^{-r}$, respectively.

On a finite module U over the specialized algebra, the partial sums of $e_i U$ are therefore stable. Each successive quotient, after removing its indicated scalar Tate twist, is an unramified finite-dimensional representation, including any unramified Jordan blocks. Such a representation is crystalline of weight zero. Suppose an initial part U' of the filtration is crystalline, and Q' is the next quotient. For $V' = \mathrm{Hom}(Q', U')$, all the cyclotomic exponents are at least r. This module is crystalline, and $H^0(K_v, (V')^\vee(1)) = 0$, since a trivial subrepresentation would have weight zero and its weights are at most $1 - r < 0$ in this exponent convention. The Bloch–Kato dimension formula gives $\dim H^1_f(K_v, V') = \dim H^0(K_v, V') + [K_v : \mathbb{Q}_\ell] \dim V'$; all its exponents are positive. The local Euler characteristic and local duality give the same dimension for $H^1(K_v, V')$. Every extension of Q' by U' is consequently crystalline. Induction proves the result. In particular this computation applies to the trace realization, its dual-number lifts, and extensions between two distinct simple constituents of the finite algebra. [6] □

Lemma 54.12 (An ordinary flag excludes a transitive permutation of lines)**.** *Consider the normalized plane or the normalized irreducible three-dimensional representation in the curve arguments of Lemmas 44.9 and 44.13, or at the classical points in the corresponding arguments. Suppose the residual inertia character $\bar{\Psi}$ has order greater than two. If the local ordinary characters have pairwise ratios of infinite order on a common inertia subgroup, the global group cannot permute transitively a decomposition of the representation into lines.*

Proof. In a stable lattice the subgroup $\ker \bar{\Psi}$ has pro-ℓ image, because its reduction is unipotent after a triangular residual change of basis. A permutation action on two or three lines is continuous: the stabilizers of the lines have closed finite index. Its order is prime to ℓ, so this action factors through the cyclic image of $\bar{\Psi}$. In the transitive case the permutation group has order b, where b is the dimension two or three. Giving its generator a primitive b-th root of unity as value defines a character δ. In a basis of the lines numbered in cyclic order, conjugation by the diagonal with successive powers of that root gives the self-twist by δ or its inverse.

On the specified compact inertia subgroup choose an element whose local diagonal ratios all have nontrivial sixth powers. Each ratio to the sixth power has infinite image. Its kernel has Haar measure zero since it has arbitrarily many disjoint translates of equal measure. A finite union of these kernels therefore omits an element. The sixth power of the chosen matrix fixes every global line and has distinct eigenvalues. The lines of the decomposition are exactly its eigenlines. Every step of the ordinary flag, being stable under this matrix, is spanned by a subset of them. A permutation preserving every step of a complete coordinate flag fixes each line individually. The local decomposition group thus acts trivially on the lines, so δ is trivial there.

The reduction $\bar{\delta}$ still has order b. For the plane it must interchange the two global residual characters $\bar{\Psi}, \bar{\Psi}^{-1}$, forcing $\bar{\delta} = \bar{\Psi}^2$ or $\bar{\Psi}^{-2}$. For the triple, the orbit of the trivial character under multiplication has three elements and is the residual triple, so $\bar{\delta} = \bar{\Psi}$ or $\bar{\Psi}^{-1}$. Each conclusion is nontrivial on the local inertia group under the stated order hypothesis. This contradicts local triviality of δ. □

Theorem 54.13 (The length bound at every twist with distinct inertia)**.** *For every x in the same sufficiently distant interval,*

$$\sum_{\substack{\ell\geq 11 \text{ prime}\\ \ell\nmid suN_*[E_*:\mathbb{Q}]|\mathrm{Cl}(K)|}} (\log \ell) \sum_{\substack{1\leq r<t(x)\\ \ell-1\nmid 2r}} \mathrm{length}_{\mathbb{Z}_\ell}\big(\mathcal{S}_{\ell,r}(E_x)^{c=(-1)^r}\big) \;\leq\; 2\log D(V).$$

For each one of these primes the inner sum is at most $2v_\ell(D(V))$.

Proof. First obtain the upper-field Hecke support at the residue $j \in \{1,\dots,n-1\}$ of r. The hypothesis $n \nmid 2j$ ensures that $\bar\omega^j, 1, \bar\omega^{-j}$ are distinct at every coefficient place of the layer. In Lemma 54.5 there are three issues when the stronger restrictions on j are removed.

First, for $j = n-1$ the starting Eisenstein series in the seed argument has weight $k = j+1 = \ell-1$. Put $\chi = \eta\alpha$ and let D_0 be its primitive conductor. In the expansion of

$$B_{k,\chi} = D_0^{k-1}\sum_{a=1}^{D_0} \chi(a)B_k(a/D_0)$$

the only Bernoulli number through degree k whose denominator can contain ℓ is B_k. Its coefficient $D_0^{k-1}\sum_a \chi(a)$ is zero because χ ramifies at s. All remaining terms are integral at ℓ, and $2k$ is a unit. Thus the constant term is integral, which supplies the required congruence at this weight in Lemma 36.16. The ordinary unit root and the prescribed tame characters follow as in that lemma.

Second, the Tate dual of $\bar\Psi^{-1}\eta$ can have trivial inertia at ℓ when $j = n-1$. Its global character then equals $\bar\alpha\bar\eta$, nontrivial at s. For $\bar\Psi^{-2}\eta$ the dual inertia exponent $1+2j$ is odd and nonzero modulo n. The two original characters are nontrivial at ℓ, by $n \nmid 2j$. These are the global invariant vanishings and the zero local H^0 at ℓ entering the strict-class Euler count in Proposition 37.5. Its two strict classes on the auxiliary layer are therefore available.

Third, use Lemma 54.12 in place of the order-three and order-four exclusions in the argument of Lemma 54.5. For a separated curve in residue characteristic the ratios on inertia in the cyclotomic kernel reduce to one. Each nontrivial such ratio has infinite image since the principal units of a Laurent series field in characteristic ℓ have no torsion. The initial curve of the auxiliary ordinary family has the same property by its chosen principal-unit direction. At classical specializations with distinct ordinary exponents, on an open subgroup of inertia the ratios are nonzero powers of the cyclotomic character in the parallel-weight cases. More generally, distinct labeled weights give infinite character ratios, since finite characters have weight zero at every embedding. For the plane its local flag is obtained by intersecting the full stable flag with the plane and discarding repeated steps. Thus in each use of these exclusions the lemma applies. A scalar action on an open subgroup is excluded already by the same infinite ratios. The original two-dimensional seed with residual characters $1, \bar\eta\bar\Psi$ also has no quadratic self-twist, since a swap would force $(\bar\omega^j)^2 = 1$. This verifies the upper-field propagation, including at order three or four on inertia. The lower-root dimension estimates and the local degree of the auxiliary layer are unchanged in the argument of Lemma 54.5.

We specialize at the actual weight r. The trace minors and ordered diagonal characters in Proposition 54.6 require just the three distinct residual inertia eigenvalues. At the reducible special-fiber points, Pan's ordinary finiteness argument uses the nontriviality of $\bar\Psi^{-2}$ on inertia, which is precisely $n \nmid 2r$. Thus finiteness of the entire original trace ring follows from the two-quotient argument in Theorem 44.41. For $r \geq 2$ Proposition 54.11 gives crystallinity for all the modules used in the generic-fiber arguments. The old inertia is finite of prime-to-ℓ order by the original tame condition. Hence the descent and the level calculation of Proposition 44.42 give exactly the same lists at r. In the non-CM and enormous-image arguments for the plane

and for an irreducible original point, the corresponding local ordinary exponents are distinct, so Lemma 54.12 again excludes the permutation case. The adjoint Selmer vanishings and the two extension vanishings used in Lemma 40.9 therefore apply. In particular the generic trace algebra is étale and the graded multiplicities are those of Lemma 54.2. At $r = 1$ these conclusions already follow from Proposition 54.6.

For $r \geq 2$ the local presentation of Lemma 54.10 has exactly the allowed surplus of variables over relations in each weight. The identification of the two negative cotangents in Proposition 54.1 remains valid for the full ordinary word. Indeed a negative root class, after its local coboundary adjustment at g_*, has standard ordered flag and zero lower entries on inertia. Conversely any local coboundary is a conjugate of the ordinary split lift. The unramified and marked conditions away from this place, the fixed section and the trace description of B_0 follow from the same identities. In particular the two negative cotangents are torsion. Apply Proposition 41.4 with the Frobenius difference at u. For $r = 1$ apply Theorem 54.3 with the local chart already checked in Proposition 54.6 and Theorem 54.7. The sum of the valuations over nonsplit points in all the resulting bounds is at most $v_\ell(D(V))$ for each prime: the labels use the actual α, r, their multiplicities are one, and u is a unit there. The character descent and summation of Theorem 54.7 prove both assertions. □

Corollary 54.14 (The two remaining inertia residues)**.** *At primes $\ell \leq P(x)$ satisfying the prime conditions of the theorem, the remaining $R_{\ell,r}$ in Section 6.6 can be nonzero only for*

$$r \equiv 0 \quad or \quad r \equiv (\ell - 1)/2 \pmod{\ell - 1}.$$

At these twists the summand for the trivial character of E_x, when it has the complementary sign, is zero.

Proof. The high-power truncation kills each group bounded by the theorem, since $2v_\ell(D(V)) < b_0$ uniformly for sufficiently large V, as in Corollary 54.8. Precisely the two displayed residues satisfy $\ell - 1 \mid 2r$. The trivial character has the specified sign only for even r. Its strict summand descends integrally to $\mathbb{Q}$ since $\ell \nmid [E_x : \mathbb{Q}]$. At this even twist its dual is the ℓ-primary part of $K_{2r}(\mathbb{Z})$, which vanishes under this divisibility by Proposition 20.6. □

54.4 The two moving ramified coefficient primes

Fix the polynomial-conductor family of Theorem 19.15. Write $\ell = q$ or $\ell = d_0$, $n = \ell - 1$, and let τ be the quadratic Dirichlet character of $\mathbb{Q}(\sqrt{-\ell})$. We keep the same split test prime u, the same quadratic field $K = \mathbb{Q}(\sqrt{-s})$, and the integer $D(V)$ of Theorem 44.44. The finite character of an ordinary Galois representation can now be ramified at the coefficient prime itself. On both outer lines its finite inertia character then equals τ.

Lemma 54.15 (An unramified character giving the same residual problem)**.** *Let α be a character of E_x of sign $(-1)^r$, with $1 \leq r < t(x)$. There are $b \in \{0, 1\}$ and a character α_0 of conductor prime to ℓ such that $\alpha = \alpha_0 \tau^b$. Put $j = r + bn/2$. Then*

$$\bar{\alpha}\, \bar{\kappa}_\ell^r = \bar{\alpha}_0\, \bar{\kappa}_\ell^j, \qquad \alpha_0(c) = (-1)^j.$$

There is an auxiliary layer $L = KF_a^+$ on which all the geometrically irreducible primes of the corresponding ordinary determinant ring contain the Hecke kernel. The finite ordinary diamonds on this ring agree with those prescribed by $\alpha\kappa_\ell^r$.

Proof. The construction of Theorem 19.15 gives $q, d_0 > H^{401W}$, $V^2 \leq H^{K_0}$ and $W > K_0 + 2$. Hence $\ell - 1 > 8t_* + 8$ for sufficiently large H, since $t_* \leq H^{401(3K_0/4)}$. The primes s, u, the class

number of K, and the odd prime divisors of $[E_* : \mathbb{Q}]$ are fixed. Thus ℓ divides none of them. In E_* the only factor ramified at ℓ is $\mathbb{Q}(\sqrt{-\ell})$. Indeed all other factors in the displayed field of Theorem 19.15 have conductor prime to ℓ. Their compositum is disjoint from this ramified quadratic field, by looking at inertia. Take b according to the restriction of α to this order-two inertia group. Then α_0 factors through the other factors, whose compositum we denote by E°. Write $N^\circ = N_*/\ell$. Since the level in that theorem contains each moving prime exactly once, the conductor of E° divides N°.

Both moving primes are $3 \bmod 4$. The unique quadratic subfield of $\mathbb{Q}(\mu_\ell)$ is therefore $\mathbb{Q}(\sqrt{-\ell})$, and $\bar{\tau} = \bar{\kappa}_\ell^{n/2}$ on $G_\mathbb{Q}$. Its value at complex conjugation is -1 and $n/2$ is odd. This proves the two identities. For $b = 0$ the size inequality gives $j = 1$ or $2 \le j \le n-2$ with $n/\gcd(n, j) > 4$. For $b = 1$ the latter alternative always holds. In fact $hj \equiv hr$ or $n/2 + hr \bmod n$ for $1 \le h \le 4$, and $0 < hr < n/2$. Neither residue is zero.

Apply the construction in Lemma 54.5 to $\alpha_0, j, E^\circ, N^\circ$. Its proof uses the conductor divisibility, $\ell \nmid sN^\circ[E^\circ : \mathbb{Q}]$, the specified parity, and the ramification of η at s. They hold because $E^\circ \subset E_*$ and $\ell \nmid N^\circ$. In particular L is disjoint from $E^\circ(\mu_\ell)$, which already contains E_*. The auxiliary congruences include splitting at ℓ in L/F_a^+, and the cyclotomic inertia image on G_L still has order n. The class-rank bound and the choice of the depth use the field $LE^\circ(\mu_\ell)$. The old types away from ℓ are the same for α_0 and α, because τ is unramified there. Use the integral modules of Lemma 54.9 for those types. The Hecke support conclusion of Lemma 54.5 follows.

On the prime-to-ℓ part of the local units, finite character values of order prime to ℓ are determined by their reductions. Thus the residual identity gives equality of the prescribed finite diamonds of the two ordered triples, including after restriction to L. On principal units τ is trivial, and the actual exponent r specifies the arithmetic specialization of the variable weight ring. The residual equality holds on whole decomposition groups, so it also gives the same order of the residual diagonal characters there. □

Proposition 54.16 (The local ordinary modules of quadratic type)**.** *Suppose $b = 1$. Use the full ordered ordinary word in the marked problem, with inertia characters $\tau\kappa_\ell^r, 1, \tau\kappa_\ell^{-r}$. The framed local ring over O is smooth with coordinate counts $1, 2, 3, 4, 2$ in weights $-2, -1, 0, 1, 2$. At each $v \mid \ell$ of K, every finite module of the specialized matrix algebra of Proposition 54.11 becomes crystalline over $K_v' = K_v(\sqrt{-\ell})$. Extensions of such modules have the Bloch–Kato finite local condition whenever the extension itself is a module for that algebra.*

Proof. The separating element exists by the lemma. On the two adjacent upper entries the residual Tate-dual inertia exponent is $1 - j$, and on the long upper entry it is $1 - 2j$. Both are nonzero modulo n. Hence the obstruction group for lifting the upper entries with a given unramified diagonal variation is zero by local duality. The flag and diagonal are smooth in the three lower and three diagonal coordinates, respectively. The cocycle calculation of Lemma 54.10 gives four adjacent and two long upper variables. It uses only the residual actions and works also when the actual exponent is one.

The ordered projectors of the separating element give the filtration on every finite matrix module exactly as in Proposition 54.11. On a graded piece the group acts by the prescribed inertial character times an unramified representation, which can have unipotent Frobenius. This piece is de Rham over K_v and crystalline over K_v'. We prove the latter statement for successive extensions by induction. Let A be an initial part already crystalline over K_v' and B the next graded piece. The module $V' = \mathrm{Hom}(B, A)$ is de Rham over K_v by descent of de Rham periods, and every cyclotomic exponent on it is strictly positive.

We claim $H^0(K_v, (V')^\vee(1)) = 0$. For exponents greater than one this follows from the nonzero Hodge–Tate weights on the corresponding graded part of the dual twist. An exponent equal to one requires $r = 1$ and two adjacent steps. The corresponding finite inertia character of the dual twist is τ, even with the unramified coefficient blocks. Inertia of K_v, which is unramified over $\mathbb{Q}_\ell$, contains an element acting there by -1. Thus this graded part also has zero invariants. An invariant in a filtered space with zero invariants on all graded pieces is zero, proving the claim.

The Bloch–Kato dimension formula for de Rham coefficients gives $\dim H^1_f = \dim H^0 + [K_v : \mathbb{Q}_\ell] \dim V'$, since all exponents of V' are positive. The local Euler characteristic and the claim give the same value for $\dim H^1$. Thus the extension class restricts to $H^1_f(K'_v, V')$ by functoriality. Its end terms are crystalline there, so its middle term is crystalline there as well. This proves the induction, including the first twist. For an arbitrary short exact sequence of finite matrix modules its restriction to K'_v now splits after tensoring with B_{cris}. Indeed the crystalline period spaces give an exact sequence of vector spaces over the maximal unramified period field, which admits a linear splitting. Extension to B_{cris} gives an equivariant splitting. The class in the B_{cris}-cohomology of the Hom module over K_v is therefore zero by restriction and corestriction, whose composite multiplies by two. This is the finite local condition over K_v. [6] □

Proposition 54.17 (The original trace ring at a moving prime)**.** *For each α, r above, the fixed-weight trace ring T is finite over O with geometrically reduced generic fiber. Its nonsplit geometric traces occur with the original level and weight in the lists defining $D(V)$.*

Proof. For $b = 0$, the original problem can be imposed with E°, N°. In the constructions of Propositions 54.1 and 54.6 the inertia kernel away from the coefficient prime is the kernel of the prescribed character together with the quadratic sign. At the coefficient prime it is the ordinary condition alone that is imposed. Thus replacing N_* by N° here gives precisely the required trace calculation. The resulting levels divide the original ones. We treat $b = 1$ in detail.

Restrict the original integral matrices to G_L. The projector calculation of Proposition 38.7 recovers each diagonal character from a trace. Lemma 54.15 puts these in the same ordered weight component. On inertia away from ℓ, α and α_0 agree, so restriction factors through the prescribed ramification quotient. Put $G = G_K$, $H = G_L$, and take a separating inertia element in H. Its spectral projectors e_i belong to the restricted matrix span. For $g \in G$, normality puts $M(g)e_iM(g)^{-1}$ there as well. Its (k, i)-block is $e_kM(g)e_i$ multiplied by $\mathrm{tr}(e_iM(g)^{-1})$, a unit since its residue is a diagonal character value. This proves equality of the two matrix spans over T by summing the blocks. Thus all trace-minor ideals on G are extended from H by multilinearity. In particular the four-by-four minors generate the original augmentation ideal by Proposition 38.2. That proposition uses the separated ordered diagonal and the splitting of all allowed character lifts by the class-number condition. In this application each ordered character divided by its split value is unramified at ℓ, because their prescribed inertia characters agree there, and at the other places by the prime-to-ℓ inertia condition. Its residual value is one and $\ell \nmid |\mathrm{Cl}(K)|$, as required. The closed restricted trace ring then equals T by Theorem 38.6, giving the surjection of Proposition 38.7 at the actual weight.

At an irreducible special-fiber trace the restriction is therefore in Hecke support. For a reducible trace the special-fiber descent in Theorem 40.7 uses the distinct residual eigenlines and the class number of K prime to ℓ. On the plane the twist by $\bar{\Psi}^{-1}$ makes one ordinary inertia character trivial. The determinant lift $\eta\Psi^{-2}$ is odd and de Rham, and its inertia reduction is nontrivial since $n \nmid 2r$. Thus the ordinary pseudodeformation finiteness theorem used there

applies with the ramification set dividing $sN^{\circ}\ell$. These two cases give finiteness of T by the special-fiber argument in Theorem 44.41. [7]

At an irreducible characteristic-zero point the upper ordinary specialization is classical. In Geraghty's control theorem the weight consists of a dominant algebraic part and a finite diagonal character. Here the first is the weight belonging to r, and on local units the second has components $\tau, 1, \tau$, restricted by the local norm on the upper field. Their product with the algebraic character has exactly the prescribed tame diamonds. Lemma 2.6.4 of that theorem thus places the specialization on the finite-level classical module, with any nilpotent kernel of the specialization map killed by evaluation in a field. The old type coefficients commute with this control map by Lemma 54.9. The restricted representation is irreducible, so the transfer is cuspidal. The degree $[L : K]$ is prime to three. The determinant-one cyclic descent, including its uniqueness, is that of Proposition 44.42. The determinant on K is indeed one since the product of the three prescribed inertia characters is one at every finite place and $\ell \nmid |\mathrm{Cl}(K)|$. [5, 8]

At $v \mid \ell$ the local parameter of the descent has zero monodromy by Proposition 54.16. On its ordinary filtration the inertial types of the graded pieces are $\tau, 1, \tau$. Exactness of the potentially semistable period functor and semisimplicity of finite inertia in characteristic zero give this same inertial type on the Frobenius-semisimplified Weil–Deligne parameter. Frobenius preserves each inertia eigenspace. After semisimplification it can be diagonalized on each, giving three Weil characters trivial on principal local units. Local–global compatibility at the coefficient prime applies since the rank is odd and the weight is regular. This places the local component in the same principal level as at any finite place of exponent one in the argument of Theorem 36.18. At the other finite places that argument applies verbatim. The weight at infinity is determined by r. Thus the rank-three label is at level N_{*}. [9, 10]

At a line and a plane the line is trivial by uniqueness of the middle residual character and the class-number argument of Theorem 38.11. The symmetric plane adjunction gives its odd extension W over $\mathbb{Q}$, of determinant η, as in Proposition 38.14. It is de Rham with weights $r, -r$, since this is true upon finite local extension. Its modularity and the non-CM assertion follow there by Pan's theorem and the order of the residual inertia character, which exceeds four. The form for $W\kappa_{\ell}^{r}\alpha^{-1}$ has weight $2r + 1$ and nebentypus $\eta\alpha^{-2}$. Twisting its plane parameters at ℓ by α^{-1} removes τ from both inertia characters. Monodromy is zero. Since $K_v/\mathbb{Q}_{\ell}$ is unramified, the Weil inertia group for the rational parameter is the same. The primitive level is consequently the conductor of $\eta\alpha^{-2}$, as in Proposition 40.11. At u the trace formula $1 + u^{-r}\alpha(u)a_u(f)$ uses the actual α. [7, 11]

Finally, all extensions of simple modules and dual-number lifts arising from the marked algebra satisfy the finite local condition by Proposition 54.16. Away from ℓ their prescribed inertia is finite of order prime to ℓ. For a split triple the decreasing extension groups vanish after restriction to KE_x by the negative-twist argument of Theorem 38.15. For a plane the off-diagonal groups vanish by Kato's theorem over the same quadratic K for the modular form attached to $W\kappa_{\ell}^{r}$, at the twist r. Its restriction after the dual and twist is the indicated plane. These are the vanishings giving the product matrix algebra at the plane in Lemma 40.9. At an irreducible trace the ordinary exponents are distinct and its residual inertia order exceeds four. The enormous-image argument of Lemma 40.1 and the polarized adjoint Selmer vanishing of Newton and Thorne therefore apply. The same adjoint vanishing for the non-CM modular plane gives its trace rigidity. The tangent argument of Corollary 44.43 now makes every geometric generic local ring a field. [3, 4] □

Theorem 54.18 (Full length at both moving coefficient primes)**.** *For sufficiently distant*

intervals and every $V \le x \le V^{3/2}$, at each $\ell \in \{q, d_0\}$ one has

$$\sum_{1 \le r < t(x)} \operatorname{length}_{\mathbb{Z}_\ell}\big(\mathcal{S}_{\ell,r}(E_x)^{c=(-1)^r}\big) \;\le\; 2v_\ell(D(V)).$$

Consequently $R_{\ell,r} = 0$ at both moving primes for every twist on the interval.

Proof. For $b = 1$ the local chart has the same five weight counts as in Proposition 54.1. For the relative global presentation, none of the dual inertia exponents $1, 1 \pm j, 1 \pm 2j$ is zero, since $j = n/2 + r$ and $0 < 4r < n/2$. The away Euler terms and the polarization at infinity are unchanged. The fixed section and the negative cotangent modules use the actual Ψ in that proposition. Its proof uses the units $\bar{\Psi}(g_*)^{\pm 1} - 1$ and $\bar{\Psi}(g_*)^{\pm 2} - 1$, the diagonal projectors, and prime-to-ℓ inertia away from ℓ. Each holds here. At the coefficient place the local lower-root coboundary is equivalent to the strict local condition, by subtracting its value at the separating element and using the ordinary flag. Restriction to KE_x still has index prime to ℓ and proves finiteness of the negative cotangents. For $b = 0$ use the same presentation at $r \ge 2$, and the first-twist chart of Theorem 32.15 at $r = 1$, with the reduced tame modulus N°.

The proposition and the calculation at its plane points give the multiplicities of Lemma 54.2 in both cases. Apply Proposition 41.4 and sum the resulting valuations at u. The lists in Theorem 44.44 are indexed by the original (α, r). Distinct trace characters for that pair give distinct labels, since the embedded label determines all good traces and these determine the trace character. The factors clearing denominators are powers of $u \ne \ell$. Summing over the residue conjugates and the twists thus uses at most $v_\ell(D(V))$, with the factor two in the length bound. The scalar character descent of Theorem 22.17 is exact also at these ramified primes since $\ell \nmid [E_x : \mathbb{Q}]$. In particular local restriction and corestriction at ℓ are injective in the required direction because the local degree is a unit. This proves the displayed inequality. The moving primes are at most $N_* \ll V^C$, hence eventually at most $P(x)$. Since $2v_\ell(D(V)) \ll V^C < b_0$, truncation kills all their remaining summands. □

Corollary 54.19 (Support of the remaining odd-prime tails)**.** *There is a finite set of primes depending only on the fixed data such that, outside it, a nonzero $R_{\ell,r}$ with $\ell \le P(x)$ requires $\ell - 1 \mid 2r$. In particular $\ell \le 2r + 1$. Above $P(x)$ the total complementary length with weights $\log \ell$ is $O_{\psi,\varepsilon}(V^C)$ as in Corollary 54.4.*

Proof. Include the primes below eleven and the prime factors of $su\,2F[K_\psi : \mathbb{Q}]\,|\mathrm{Cl}(K)|$ in the finite set. Outside it, the only prime divisors of $N_*[E_* : \mathbb{Q}]$ are q, d_0. The theorem treats both, and Corollary 54.14 treats the other primes with $\ell - 1 \nmid 2r$. Divisibility by the positive integer $\ell - 1$ gives the last inequality for any remaining positive twist. □

55 Colliding ordinary characters

55.1 Frobenius at the two coincident inertia weights

Keep the interval and the fields of Theorem 19.15. Write $K = \mathbb{Q}(\sqrt{-s})$, write η_K for its quadratic character, and take a prime $\ell \ge 11$ prime to $2suN_*[E_* : \mathbb{Q}]\,|\mathrm{Cl}(K)|$, with u as in Theorem 44.44. Let α be a character of E_x with $\alpha(c) = (-1)^r$, where $2 \le r < t(x)$ and $\ell - 1 \mid 2r$. Set $\Psi = \alpha\kappa_\ell^r$ and let O be an unramified coefficient DVR containing the values of α, with residue field k. The two outer characters of the rank-three diagonal $(\Psi, 1, \Psi^{-1})$ coincide on residual inertia at ℓ. For a substantial part of this family the ordered flags and the reducible traces can still be determined at ℓ.

Lemma 55.1 (A separating element on every auxiliary layer)**.** *Suppose $\alpha(\ell)^4 \neq 1$. Fix a place above ℓ in an algebraic closure of $\mathbb{Q}$. There is an element h in its decomposition group which belongs to G_K and to every $G_{KF_a^+}$ in Proposition 36.15 for the fixed auxiliary primes. It has $\kappa_\ell(h) = 1$, and $b = \bar{\Psi}(h)$, 1, b^{-1} are pairwise distinct. For a fixed ℓ one choice works for every indicated α, r, x. Conjugate elements have the same three values.*

Proof. The local cyclotomic extension of $\mathbb{Q}_\ell$ is totally ramified. Multiply an arithmetic Frobenius lift by an inertia element to obtain a lift ϕ with $\kappa_\ell(\phi) = 1$. Take $h = \phi^{2\ell}$. The cyclotomic factor F_a of F_a^+ is fixed already by ϕ. On the other factors, the unramified local degree divides 2ℓ. Indeed the two quadratic factors are unramified at ℓ and the factor of prime conductor w has degree ℓ. This also shows that h fixes K. We have $b = \bar{\alpha}(\ell)^{2\ell}$. Reduction preserves the order of $\alpha(\ell)$, which is prime to ℓ. Thus $b^2 \neq 1$ is equivalent to $\alpha(\ell)^4 \neq 1$. All characters used here are global abelian characters, which proves the last assertion. □

Use the marked matrix problem on G_K of Section 32.4 with its symmetric adjunction and the same inertia kernels away from ℓ. Use h for the element in the adjacent-entry mark of Corollary 32.9. At places above ℓ prescribe a flag stable under the full decomposition group. Its ordered inertia characters are $\Psi, 1, \Psi^{-1}$ and its residual graded characters on the full local group are $\bar{\Psi}, 1, \bar{\Psi}^{-1}$. At a conjugate place use the dual flag in the reversed order. Write M for the matrices on G_K. The adjunction in the marked coordinates is $M(cg^{-1}c) = J_3 M(g)^{\mathsf{T}} J_3$, where J_3 is the anti-diagonal permutation matrix. We describe the local conditions before passing to traces.

Proposition 55.2 (Integral flags and the strict lower entries)**.** *Under the hypothesis of Lemma 55.1, the ordered local condition is given by closed matrix equations over O. On its solutions the flag is unique. For a square-zero deformation supported in one lower matrix entry at the split diagonal, these equations hold exactly when the local extension class is zero. This assertion holds over every finite length O-module of coefficients.*

Proof. Work first over a complete Noetherian local O-algebra with residue field k. Index the three rows by $0, 1, 2$. The characteristic polynomial of $M(h)$ has three distinct residual roots. Hensel's lemma gives roots λ_i with the prescribed reductions. Their differences are units, and Cayley–Hamilton gives three mutually orthogonal projectors

$$e_i = \prod_{j \neq i} \frac{M(h) - \lambda_j I}{\lambda_i - \lambda_j}, \qquad \sum_{i=0}^{2} e_i = I.$$

Each has free image of rank one, by reduction and Nakayama's lemma. The roots lie already in the completed algebra of characteristic-polynomial coefficients. An ordered stable flag, if it exists, is split by these projectors. Its first line and first plane must be the first eigensummand and the sum of the first two, since the residual ranks prescribe which summands occur. It follows that the equations are

$$\begin{aligned} e_i M(g) e_j &= 0 && (i > j,\ g \in G_{K_v}),\\ e_i M(\tau) e_i &= \Psi(\tau)^{1-i} e_i && (\tau \in I_v,\ 0 \leq i \leq 2). \end{aligned}$$

Conversely these equations give the indicated stable flag and inertia action. The construction uses only units as denominators, commutes with change of coefficients, and gives a closed ideal in the universal complete local ring.

For a lower entry use a square-zero ideal N and write its matrix as $(1 + z(g)E_{ij})d_3(g)$, $i > j$, with d_3 the split diagonal. Its character ratio θ_{ij} satisfies $\theta_{ij}(h) - 1 \in O^\times$ by the

lemma. Conjugate by a unique matrix $1 + yE_{ij}$, $y \in N$, to make $z(h) = 0$. Conjugation adds a coboundary and gives the standard projectors at h. The first row of equations now forces $z(g) = 0$ on the entire local group. A local coboundary conversely gives a conjugate of the split flag. This works with $O \oplus N$ for every such N; the normalization divides by the displayed unit. For a class defined over $\mathbb{Q}_\ell$, restriction to K_v also detects zero, since corestriction composed with restriction is multiplication by $[K_v : \mathbb{Q}_\ell] \in \{1, 2\}$. □

Let T^{ord} denote the completed trace algebra of this fixed-weight problem. More explicitly, take the image of the universal determinant ring for G_K, unramified outside the given finite set, in the framed marked matrix ring with the displayed local equations. Since $2, 3 \in O^\times$, the coefficients of characteristic polynomials are polynomials in traces of powers. Denote the group trace by t. For $m \geq 1$ let I_m be generated by $\det(t(g_i h_j))_{1 \leq i,j \leq m}$, $g_i, h_j \in G_K$.

Theorem 55.3 (Finiteness on the reducible locus at coincident inertia weights)**.** *If $\alpha(\ell)^4 \neq 1$, then T^{ord}/I_m is a finite O-module for $6 \leq m \leq 9$. At any geometric field point its semisimple representation is reducible exactly when I_m vanishes there. For every continuous local map from the quotient to $k'[[z]]$ with k'/k finite, all group traces belong to k'.*

Proof. The determinant ring is complete Noetherian, and its universal Cayley–Hamilton algebra is finite over it. Here the required finiteness of residual first cohomology follows by restriction to a finite extension killing the residual representation. For the trivial residual module one may also adjoin μ_ℓ; Kummer theory then gives a bound from the finite ℓ-torsion of the class group and the finitely generated group of units outside the given finite set. Inflation–restriction adds only finite groups. The determinant and Cayley–Hamilton finiteness theorems therefore apply just as in Lemma 38.9. The trace ring, as an image of a compact complete ring with finite residue field, is a complete Noetherian quotient. The span of the universal group matrices over it is finite by the same Cayley–Hamilton theorem. [12]

Let $T^{\mathrm{ord}} \to k'[[z]]$ be a continuous local map with k'/k finite. Take the semisimple representation of its determinant over an algebraic closure of $k'((z))$. It factors through the specialized matrix algebra. Indeed each matrix relation gives zero trace after multiplication by every group matrix. In a semisimple realization these matrices span the product of full matrix algebras on its distinct constituents, and the trace pairing on each factor is the usual pairing times its multiplicity. All these multiplicities are units since $\ell > 3$. The pairing is thus nondegenerate. The realization is defined over a finite extension of $k'((z))$, since the algebra through which it factors is finite dimensional. It is continuous there by finiteness of the integral matrix algebra, and its compact image preserves a lattice. Its semisimplified reduction on such a lattice is $\bar{\Psi} \oplus 1 \oplus \bar{\Psi}^{-1}$. The projectors and both local matrix identities in the proposition descend to this realization.

If the representation is a sum of lines, match each character with its reduction at the element h. At every place above ℓ the prescribed inertia character on that line in equal characteristic is exactly its residual one. In fact the three idempotents label the three local constituents, and the distinct reductions at h determine the label, also at a conjugate place. Away from ℓ the prescribed inertia quotient has order prime to ℓ. Dividing the character by the constant lift of its residual character therefore yields an everywhere unramified character into principal units. Such a character factors through the class group of the imaginary quadratic field K; its image is trivial since $\ell \nmid |\mathrm{Cl}(K)|$. Thus every line is constant. The same argument applied to the determinant shows that the determinant of the entire realization is one: its inertia product at ℓ and its residual character are both trivial.

In the other reducible case write the representation as a line λ and an absolutely irreducible plane P. By conjugate duality the unique line has $\lambda^c = \lambda^{-1}$. Each possible reduction extends

to $G_{\mathbb{Q}}$; the two outer characters have square different from one at h. Hence $\bar{\lambda} = 1$. The ordinary projectors assign this line the middle inertia character, including when inertia alone has three equal reductions. The unramified character argument just given shows $\lambda = 1$, so that $\det P = 1$.

We recall the odd descent of this plane to make the use of Pan's theorem precise. The adjunction descends to the semisimple group span: its kernel there is the radical of the trace pairing, which adjunction preserves. It fixes the plane factor, the unique simple factor of dimension four. On it the adjunction is adjoint to a symmetric or an alternating form, because an involution of a matrix algebra fixing scalars is transpose followed by an inner automorphism. The alternating possibility is excluded by the integral identity $2XYX = t(XY)X$ for skew matrices in this rank-three symmetric adjunction, proved in Proposition 38.14. Skew elements in the quotient lift by taking half the difference with the adjoint, and their line component is zero. For alternating adjunction the traceless matrices $X = \operatorname{diag}(1, -1)$ and $Y = E_{12} + E_{21}$ are skew, whereas $XYX = -Y$ and $\operatorname{tr}(XY) = 0$.

Write S for the symmetric form on the plane and J_0 for its alternating determinant form. Then $S^{-1}J_0$ intertwines P with its conjugate by c: the adjunction sends $P(g)$ to $P(cg^{-1}c)$, and $\det P(g) = 1$. This intertwiner is invertible with trace zero. After a finite scalar extension rescale it to square one. Assigning it to c extends P to W on $G_{\mathbb{Q}}$ with $\det W = \bar{\eta}_K$. In a stable lattice the residual semisimplification is a sum of two characters. An irreducible residual plane would restrict semisimply to the normal subgroup G_K, since the translates of a simple subspace span it. Its two distinct restricted characters extend to $G_{\mathbb{Q}}$, so their two isotypic lines would each be stable under c, a contradiction. Twisting W by $\bar{\eta}_K$ if necessary, its two residual characters are therefore $\bar{\Psi}, \bar{\eta}_K\bar{\Psi}^{-1}$.

On G_{K_v} the first local flag line lies in P: its eigenvalue at h has reduction $b \neq 1$. This line is preserved by ϕ, because ϕ commutes with h and the two eigenvalues of $W(h)$ are distinct. Together G_{K_v} and ϕ generate $G_{\mathbb{Q}_\ell}$; the quotient is unramified of degree one or two. Thus $W\bar{\Psi}^{-1}$ has reducible local trace. On its first line inertia acts trivially, since $I_{K_v} = I_{\mathbb{Q}_\ell}$. Its residual character on that line is one: among the two global residual characters after twisting, only one takes the value one at h.

Apply Pan's Theorem 5.1.2(1) to $F = \mathbb{Q}$ with determinant $\chi = \eta_K\Psi^{-2}$. It is odd, unramified outside the stated finite set and de Rham at ℓ. Its reduction extends to $G_{\mathbb{Q}}$ and is nontrivial on $G_{\mathbb{Q}_\ell}$, since $\bar{\chi}(h) = b^{-2} \neq 1$. These are the hypotheses of Section 5.1.1 of that paper. The ordinary pseudodeformation ring is finite over $O[[1 + \ell\mathbb{Z}_\ell]]$; this last algebra acts by the local character reducing to one. That character is unramified here, so the action factors through the augmentation. Applying this to the trace of $W\bar{\Psi}^{-1}$ over the coefficient valuation ring shows that its image is a finite domain in characteristic ℓ, hence a finite field. If necessary enlarge the constant residue field in this application. Restoring the finite-valued twist and the line shows that the original traces are algebraic over k'. Inside $k'[[z]]$ such elements are constant. [7]

It remains to pass from curves to the entire quotient. At a geometric field point the semisimple group span has dimension nine in the irreducible case and at most five in the reducible case. By the nondegenerate trace pairing, in the irreducible case one can successively choose m independent group matrices and then m independent pairings with other group matrices. This gives a nonzero m-minor. In the reducible case every such minor vanishes. If the special fiber of T^{ord}/I_m had positive dimension, it would have a one-dimensional complete local domain quotient by a prime. The normalization of this curve is a complete equal-characteristic DVR with finite residue extension, hence is $k'[[z]]$. Here one uses the standard normalization theorem for complete local domains, also obtained by finite Noether normalization over $k[[z_0]]$. The induced trace has reducible generic representation by the minor test. Its traces are constant by

the preceding argument, and topologically generate the curve algebra over k, contradicting its dimension. The special fiber is therefore Artinian and has finite k-dimension. In the complete quotient a power of the maximal ideal then lies in ℓ times the ring. Its ℓ-adic and maximal-ideal topologies agree, so lifts of a basis of the special fiber generate the quotient over O, by successive approximation. □

Corollary 55.4 (The characters for which this Frobenius test fails)**.** *Write $E_x = BC_J$, $B = K_\psi(\sqrt{-q}, \sqrt{-d_0})$, and put $o = \mathrm{ord}(\psi)$. Define*

$$c_0 = v_2(4\,\mathrm{lcm}(o,2)), \qquad t_\ell = v_2(\ell^2-1) - 3.$$

Every α with $\alpha(\ell)^4 = 1$ factors through $BC_{\min(J,t_\ell+c_0)}$. There are at most $4o\,2^{\min(J,t_\ell+c_0)}$ such characters, without imposing a parity. In the range $r \le x^{\varepsilon/128}$, if $2^{t_\ell+c_0} \le 2^{\lfloor(\varepsilon/128)\log_2 x\rfloor}$, every character contributing to the complementary field summand $U_{\ell,r}$ in Section 6.6 passes the Frobenius test of the theorem.

Proof. Every character of BC_J can be expressed as $\beta\delta$, with β a character of B and δ a character of C_J. Indeed its Galois group is a subgroup of the product of the two finite abelian groups, and characters with values in all roots of unity extend from a subgroup. This last fact follows by adjoining one generator at a time and taking a root of the prescribed value of its first power in the old subgroup. The exponent of $\mathrm{Gal}(B/\mathbb{Q})$ divides $\mathrm{lcm}(o,2)$. Thus $\alpha(\ell)^4 = 1$ implies that the order of $\delta(\ell)$ divides 2^{c_0}.

The class of 5 generates $(\mathbb{Z}/2^{J+2}\mathbb{Z})^\times/\{\pm1\}$ of order 2^J. Indeed $v_2(5^{2^a}-1) = a+2$ for $a \ge 0$, by successive squaring. Choose the sign of ℓ so that $u_\ell = \pm\ell$ is 1 mod 4. Then $v_2(u_\ell - 1) = t_\ell + 2$, since the other factor of ℓ^2-1 has valuation one. The subgroups generated by 5^{2^a} are precisely the images of $1 + 2^{a+2}\mathbb{Z}_2$, by their orders. For a character δ of order 2^j, $j \le J$, this gives $\mathrm{ord}(\delta(\ell)) = 2^{\max(0,j-t_\ell)}$. Consequently $j \le t_\ell + c_0$, proving the factorization. The two factors of the resulting field have degrees at most $4o$ and $2^{\min(J,t_\ell+c_0)}$, respectively, which proves the count. Under the last inequality the character factors through L_x of Section 6.6. The average of $\mathrm{Gal}(E_x/L_x)$ is the identity on that character; its complementary projector is zero. □

Theorem 55.3 controls the reducible part of the fixed-weight trace algebra. To bound the strict length at these weights one still needs control of the irreducible components and an upper bound for the integral intersection lengths at the split section.

55.2 Ordinary cuspidal adjoints at the original weights

We construct an ordinary cuspidal form for each of the original characters and weights, including those for which all three residual Frobenius eigenvalues at ℓ agree. A second prime in the nebentypus rules out quadratic self-twists. Both auxiliary primes can be chosen with polynomial size on the period interval.

Keep $K = \mathbb{Q}(\sqrt{-s})$, E_x, E_*, N_*, t_* and L_* from Sections 46.1 and 55.1. In particular $s \equiv 3 \bmod 4$ is prime and $s \nmid 2N_*$. Here we allow every $5 \le \ell \le L_*$ prime to $2sN_*$, including primes dividing $[E_* : \mathbb{Q}]$. Fix a geometric character α of E_x, of sign $(-1)^r$, and $2 \le r < t(x)$. Set $\chi = \eta_K\alpha$, of primitive conductor $D = s\,\mathrm{cond}(\alpha)$, and $\Psi = \alpha\kappa_\ell^r$. In the proof, coefficients are enlarged as needed at the chosen place over ℓ.

Lemma 55.5 (Integrality of the Eisenstein constant term at every weight)**.** *Let λ be any nontrivial Dirichlet character of conductor d prime to ℓ. Then $B_{k,\lambda}/k$ is integral at every place over ℓ for every integer $k \ge 1$.*

Proof. For the Bernoulli polynomial $B_k(X)$, set $P_k(X) = (B_k(X) - B_k(0))/k$. The identity $B_k(X+1) - B_k(X) = kX^{k-1}$ gives $P_k(m) = \sum_{j=0}^{m-1} j^{k-1}$ for each $m \geq 1$; for $k = 1$ every summand is one. Also $P_k(0) = 0$. The polynomial is continuous on $\mathbb{Z}_\ell$, the nonnegative integers are dense there, and $\mathbb{Z}_\ell$ is closed. Thus $P_k(\mathbb{Z}_\ell) \subseteq \mathbb{Z}_\ell$. Since $\sum_{a=1}^{d} \lambda(a) = 0$, the generalized Bernoulli formula becomes

$$B_{k,\lambda}/k = d^{k-1} \sum_{a=1}^{d} \lambda(a) P_k(a/d).$$

Each argument a/d lies in $\mathbb{Z}_\ell$; all character values are algebraic integers. This proves the assertion also when ℓ divides k or the order of λ. □

For each ℓ choose primes w_1, w_2 such that

$$w_1 \equiv 1 \bmod 8sN_*\ell, \qquad w_2 \equiv 1 \bmod 8N_*\ell, \qquad \eta_K(w_2) = -1.$$

The last condition specifies a nonsquare residue modulo s. The Chinese remainder theorem gives a unit residue class for w_2, distinct from that for w_1. Linnik's least-prime theorem bounds each chosen prime by an absolute constant times $(8sN_*\ell)^{C_1}$, for an absolute C_1. They are independent of x, r, α on this interval for the fixed ℓ. Choose a character ϑ_i of order ℓ and conductor w_i for each $i = 1, 2$.

Proposition 55.6 (An ordinary newform with two auxiliary characters)**.** *There is a normalized ℓ-ordinary cuspidal newform f of weight $r+1$, exact level Dw_1w_2, and nebentypus $\chi\vartheta_1\vartheta_2$. At a place over ℓ its residual Galois semisimplification is $1 \oplus \bar{\chi}\,\bar{\kappa}_\ell^{r}$.*

Proof. Put $k = r + 1 \geq 3$ and $M = Dw_1w_2$. The Eisenstein series $E_k(1, \chi)$ has the required parity. Its constant term is $-B_{k,\chi}/(2k)$, integral by the lemma since χ ramifies at s. Its other coefficients are $\sum_{j|n} \chi(j) j^{k-1}$. Good reduction at ℓ and the expansion principle give integrality at all cusps, as in Lemma 36.16. Explicitly a vertical pole on a component, after clearing its order, would give a nonzero reduction on that component with zero expansion at a cusp above infinity. One may check this on a full prime-to-ℓ level, with the conjugate expansions at lifts of infinity on its components. [13, 14]

Write $E = E_k(1, \chi)$ and reduce $E(z) - E(w_1 z)$ at level Dw_1. It is cuspidal. At a cusp with primitive column $(b, c)^{\mathsf{T}}$, put $h_1 = \gcd(c, w_1)$. For $E(w_1 z)$ the column on level D is $(w_1 b/h_1, c/h_1)^{\mathsf{T}}$ and the constant term acquires a factor $(h_1/w_1)^k$ by the slash formula. The two columns agree modulo D since $w_1 \equiv 1 \bmod D$. Their completions to determinant-one matrices therefore differ modulo D by a translation at the cusp, which preserves the constant term. The remaining factor reduces to one. Pull back this cusp form to level M. Its first Fourier coefficient is one; it remains an eigenvector for all good Hecke operators, including T_ℓ with eigenvalue one modulo the maximal ideal.

Here the desired characteristic-zero character can have an ℓ-part already at D. Write the diamond group $(\mathbb{Z}/M\mathbb{Z})^\times = P \times H$ with P its ℓ-Sylow subgroup. The P-action on $X_1(M)$ is free on geometric fibers. A stabilizer in the smooth elliptic locus comes from an automorphism of order divisible only by two or three. At a cusp its order divides $2n$ for an n-gon with $n \mid M$. Neither allows an element of order ℓ. Thus $X_1(M)$ is a finite étale P-torsor over its quotient. On that quotient descend the weight k cusp line with the character of P prescribed by $\chi\vartheta_1\vartheta_2$, using the inverse character for the equivariance on the line. The corresponding twist reduces to the trivial line, since all ℓ-power roots of unity reduce to one. On H the projector for the prescribed character is integral, and agrees on reduction with the character of the cusp form.

On the special fiber the dual of the first cohomology of this descended cusp line is the space of sections of ω^{2-k} by Serre duality and Kodaira–Spencer; the cusp divisor cancels the divisor in the canonical line. It vanishes because ω has positive degree and $k > 2$. Cohomology and base change consequently lift the residual section to the prescribed character. The finite algebra of good Hecke operators acts faithfully on the torsion-free integral cusp space. Its residual eigencharacter has a minimal prime below its maximal ideal in characteristic zero, since a uniformizer is a nonzero divisor. Simultaneous triangularization in characteristic zero gives a cuspidal eigensystem there with the required reduction. The character $\chi\vartheta_1\vartheta_2$ is primitive of conductor M, so the normalized newform has exact level M. Its eigenvalue at ℓ is a unit. Its good Frobenius polynomials, reduction and Chebotarev give the asserted residual semisimplification. [13, 15, 16, 17] □

Theorem 55.7 (Cuspidal adjoints for all the indicated original characters)**.** *The Galois representation W_f of every newform supplied by the proposition has Zariski-dense projective image in* PGL_2*. For each ℓ and each depth a there is an auxiliary CM field L, the same for all x, r, α on the interval, such that $U = \mathrm{Ad}^0(W_f)|_{G_L}$ is absolutely irreducible on every open subgroup and is cuspidal automorphic in the normalization of Theorem 36.17. At places away from ℓ its inertia characters are $\alpha, 1, \alpha^{-1}$, with zero monodromy. At places above ℓ it is ordinary crystalline with ordered inertial characters $\kappa_\ell^r, 1, \kappa_\ell^{-r}$ and ordered residual local characters $\bar\Psi, 1, \bar\Psi^{-1}$.*

Proof. Suppose W_f has a nontrivial quadratic self-twist δ. Reduction preserves the order of δ. Multiplication by $\bar\delta$ must interchange the two residual characters, which are distinct since χ ramifies quadratically at s. It follows that $\bar\delta = \bar\chi\,\bar\kappa_\ell^r$. This character is unramified at w_2 and takes value -1 on its arithmetic Frobenius: $w_2 \equiv 1 \bmod N_*\ell$ and $\eta_K(w_2) = -1$. The same is true of δ. On the other hand, $\dim W_f^{I_{w_2}} = 1$. Indeed the local conductor exponent is exactly one by conductor compatibility for a newform; the determinant ramifies, so the codimension of inertia invariants is at least one, and it plus the nonnegative Swan conductor equals one. An intertwiner for δ must preserve this inertia-fixed line, and Frobenius preserves it too. On the line the intertwiner and Frobenius act by nonzero scalars. The proposed intertwining relation would make their product equal its negative. This proves that the self-twist is impossible. [18]

The characteristic-zero representation W_f is absolutely irreducible and has distinct Hodge–Tate weights. Its projective image is infinite, since a scalar representation on an open subgroup has equal weights. A proper connected positive-dimensional subgroup of PGL_2 is solvable and triangularizable. If it has a nontrivial unipotent radical, its unique fixed line would be preserved by the full image. The remaining possibility is a torus. Its normalizer then permutes its two lines, transitively by irreducibility, yielding a quadratic self-twist by conjugation with the diagonal matrix with entries $1, -1$. This too was excluded. The projective image is therefore Zariski dense, as is that of every open subgroup by connectedness. The adjoint representation is irreducible there because its invariant subspaces are ideals of $\mathfrak{sl}_2$.

Choose a prime $v \equiv -1 \bmod 8sN_*\ell$, distinct from w_1, w_2. Let F_i be the real field of degree ℓ of conductor w_i, and F_a the real degree-ℓ^a field in $\mathbb{Q}(\mu_{\ell^{a+1}})$. Set

$$F = \mathbb{Q}(\sqrt{sv})F_1F_2F_a, \qquad L = KF.$$

These fields depend only on the interval, ℓ, a, and the choices of the three auxiliary primes. They have the splitting at $sN_*\ell$ used in Proposition 36.15 since $-v$ is a square at these places. The field L kills $\eta_K, \vartheta_1, \vartheta_2$. At an old ramified prime of W_f, the conductor exponents of W_f and its determinant agree: both are the exponent of the primitive nebentypus conductor. Each term of the Artin conductor bounds the corresponding term for the determinant. Equality forces a one-dimensional space of inertia invariants. In the Weil–Deligne representation the

two finite inertia characters are therefore the trivial and the ramified determinant characters. The nilpotent monodromy commuting with these distinct characters is zero. This applies also at both new primes; at other good primes inertia is trivial. Restricting the two characters to G_L and taking their ratios proves the claimed inertia description.

At ℓ the ordinary crystalline representation of the newform has unramified quotient with unit Frobenius root reducing to one; the subcharacter follows from its determinant. On G_L their ratio has inertia κ_ℓ^r and reduction $\bar{\Psi}$. On $\mathfrak{sl}_2$ the strictly upper triangular line and upper triangular plane give the asserted ordinary flag, whether or not its residual characters coincide. The Gelbart–Jacquet adjoint transfer of f is cuspidal, since a quadratic automorphic self-twist would give one on W_f by the good Frobenius polynomials. The transfer has central character one and is self-dual. Along a tower of cyclic extensions to L the degrees are two and ℓ. Loss of cuspidality at one such step would give a self-twist of that prime order by cyclic base change; the equality of central characters forces this order to divide three. Thus cuspidality persists. The archimedean parameters are regular for $r > 0$, and at good primes the Satake parameters are the two Frobenius ratios and one. These give the same Tate normalization as in Theorem 36.17. [19, 11, 20, 8] □

Corollary 55.8 (Fixed-weight rigidity at the constructed points)**.** *At U on L/F, the polarized characteristic-zero ordinary deformation problem of Section 36.8 has zero tangent space with the inertial weights and the old inertia type fixed. Its completed local ring with all weights varying is the formal weight ring of dimension $3[F:\mathbb{Q}]$ over the coefficient field.*

Proof. The closure of the image of the commutator of G_L under the projective action is PGL_2, since the original image is dense and this algebraic group equals its derived group. Thus the image on the cyclotomic kernel is already dense. In the adjoint action its span is the full matrix algebra by irreducibility. For any nonzero endomorphism X, the open set $\mathrm{tr}(gX) \neq 0$ therefore meets the open set of elements with three distinct eigenvalues. Some eigenprojector pairs nontrivially with X. This verifies the enormous-image hypothesis in Newton and Thorne's Theorem A as in Proposition 36.20. The polarized regular algebraic cuspidal representation just constructed supplies its automorphic hypothesis, giving vanishing of the polarized adjoint Bloch–Kato Selmer group. [4]

For clarity, at every chosen place above ℓ the base representation is crystalline and the positive root exponents are $r, r, 2r$, all at least two. On the dual strictly upper triangular module twisted by one all exponents are negative. Thus its local H^2 vanishes by Tate duality, and the fixed-inertia tangent lies in the finite local condition by Lemma 36.19. Away from ℓ the imposed inertia image is finite and averaging is available in characteristic zero. The local excess of the fixed-weight tangent dimension over the invariant dimension is $3[F_w:\mathbb{Q}_\ell]$ at $w \mid \ell$, zero at other finite places, and -3 at each real place. Their sum is zero. The two global invariant spaces in Poitou–Tate vanish as in Proposition 36.20: the commutant on the cyclotomic kernel consists of scalars, complex conjugation negates the scalar Lie algebra, and the Tate twist has infinite cyclotomic image. Hence both fixed-weight Selmer and dual Selmer groups vanish. The small-extension argument of Theorem 36.21 then gives a unique global lift for each lift of the weights, up to strict conjugacy. Its local ordinary argument uses distinct inertia eigenvalues in characteristic zero, where the infinite cyclotomic powers already separate them. The formal characters of the principal local units have the asserted $3[F:\mathbb{Q}]$ independent parameters. □

Theorem 55.9 (A simultaneous congruence bound for these adjoints)**.** *On the original interval there is a rational prime p split in K and a positive integer $D_{\mathrm{ad}}(V)$, with $p + \log D_{\mathrm{ad}}(V) \ll_{\psi,\varepsilon} V^C$, such that all the constructed forms satisfy*

$$0 < v_\ell\Big(\mathrm{tr}\,\mathrm{Ad}^0(W_f)(\mathrm{Frob}_p) - \big(1 + \alpha(p)p^r + \alpha(p)^{-1}p^{-r}\big)\Big) \le v_\ell(D_{\mathrm{ad}}(V)).$$

Here $v_\ell(\ell) = 1$ and the place is the one giving the congruence in Proposition 55.6.

Proof. Put $M_\ell = sN_*w_1w_2$. All these integers and the number of eligible primes are $O_{\psi,\varepsilon}(V^{C_2})$ by the least-prime bound and the polynomial bounds for N_*, L_*. Choose a power 2^j strictly above $16, L_*$ and every M_ℓ, taking the least such power. The least prime $p \equiv 1 \bmod 2^j s$ is polynomially bounded by the same theorem. It exceeds these quantities, splits in K, and is a good prime different from every ℓ under consideration.

For each ℓ and $2 \le r \le t_*$ let $\mathcal{F}_{\ell,r}$ be all normalized newforms of weight $r+1$ and level dividing M_ℓ, with all their coefficient embeddings. Take each distinct normalized eigenform once, so the list is stable under rational Galois conjugation. It has size $O((r+1)M_\ell^3)$: the forms are independent in the classical space at principal level M_ℓ by multiplicity one at good primes. The valence formula bounds the dimension there by $1 + (r+1)[\mathrm{SL}_2(\mathbb{Z}) : \Gamma(M_\ell)]/12$, and the index is at most M_ℓ^3. Equivalently one may use the degree of the Hodge line and the degree bound on the number of sections of a line bundle on a curve.

For such a form let ϵ_f be its nebentypus. Its adjoint trace is $u_f = a_p(f)^2/(\epsilon_f(p)p^r) - 1$, so $p^r u_f$ is an algebraic integer. Deligne's theorem gives absolute value $p^{r/2}$ to each of the two Frobenius roots at every complex embedding. Their ratios have modulus one, giving $|u_f| \le 3$. For every $\zeta^{[E_*:\mathbb{Q}]} = 1$ put

$$b(f,\zeta) = p^r\,(u_f - 1 - \zeta p^r - \zeta^{-1}p^{-r}).$$

It is an algebraic integer. Its magnitude is positive, since $p^r - 1 - p^{-r} > 3$, and is at most $7p^{2r}$. The absolute value of the product of these integers over all listed ℓ, r, f, ζ is a positive rational integer by Galois invariance; use one for an empty product. The degree $[E_* : \mathbb{Q}]$, t_*, p, all levels and the numbers of factors are polynomial in V. The logarithm of each magnitude is at most $2r\log p + \log 7$, which proves the claimed estimate for this product.

For the actual form the list contains $b(f, \alpha(p))$. All other integral factors have nonnegative valuation there; p^r is a unit at ℓ. Finally $\eta_K(p) = 1$. Taking the adjoint of the residual semisimplification in the proposition shows that this particular trace difference reduces to zero. This proves both bounds. □

These congruences concern actual points obtained from the constructed forms. An upper bound for the full strict cohomology also requires a comparison of its integral length with congruences on all the components that carry it. The comparison with the integral projected theta period remains required on the same interval.

55.3 Recovering the ordered local characters from Hecke traces

At a prime where the three residual inertia characters agree, the integral Hecke trace algebra need not separate the three ordinary quotients. At the original positive weight their inertia characters in characteristic zero do separate them. We compute an explicit integer that controls the discrepancy on the whole specialization, including its torsion.

Lemma 55.10 (Three ordered roots over a trace domain)**.** *Let B be a domain, let $s_1, s_2, s_3 \in B$ have nonzero pairwise differences, and let $t_0, t_1, t_2 \in B$. Use the three equations $\sum_i s_i^j u_i = t_j$ for $0 \le j \le 2$ to define $u_i \in \operatorname{Frac} B$. Suppose they are the roots with multiplicity of a monic cubic over B with invertible constant coefficient. Set $\delta_i = \prod_{j\neq i}(s_i - s_j)$ and $C = B[u_1, u_2, u_3]$. Then all u_i are units of C. It is generated as a B-module by*

$$u_1^i u_2^j, \qquad 0 \le i \le 2, \quad 0 \le j \le 1, \qquad \delta_1^2\delta_2 C \subset B.$$

Proof. For $\{i,j,k\} = \{1,2,3\}$, subtract $(s_j + s_k)t_1$ from $t_2 + s_j s_k t_0$. Only $\delta_i u_i$ remains. The determinant of the three equations is a Vandermonde product and is nonzero in the fraction field. The monic cubic reduces all powers of u_1 to degrees at most two; division by $X - u_1$ gives a monic quadratic for u_2 over $B[u_1]$. The remaining root is $t_0 - u_1 - u_2$. These facts give the six generators, without requiring their independence. Each becomes integral in B after multiplication by $\delta_1^2\delta_2$, by the first identity. The product of the three roots is a unit of B, so their inverses already belong to C. □

For the newform of Proposition 55.6 use the same fields F, L of Theorem 55.7, at a chosen depth a. Let $d = [F : \mathbb{Q}]$, let g_ℓ be the number of places of F above ℓ, and choose one place of L above each of them. The completions at a chosen pair coincide. Write Λ for the full three-character ordinary weight algebra over a sufficiently large coefficient DVR O, with the prime-to-ℓ diamonds of the adjoint fixed. The local unit groups have no ℓ-power torsion: their ramification indices at ℓ are ℓ^a, while $\mathbb{Q}_\ell(\mu_\ell)$ is totally ramified of degree $\ell - 1$. Consequently Λ is a power series ring in $3d$ variables. Use the cyclotomic normalization of the traces in which the constructed point is $U = \mathrm{Ad}^0(W_f)|_{G_L}$.

Proposition 55.11 (Interpolation of Frobenius on the ordered quotients)**.** *There is an ordinary good Hecke domain B through this point, finite over and containing Λ, with continuous group traces $t(g) \in B$ on G_L. On any such full component through the point one can adjoin all the ordered local characters at ℓ within* $\operatorname{Frac} B$*, obtaining a finite algebra B^{ord}. It has at most 6^{g_ℓ} module generators over B. For each $w \mid \ell$ choose an element σ_w of inertia whose cyclotomic value is $(1+\ell)^{\ell^a}$. Let $s_{wi} \in \Lambda$ be the three ordered weight character values there, let $\delta_{wi} = \prod_{j \neq i}(s_{wi} - s_{wj})$, and put*

$$H = \prod_{w \mid \ell} \delta_{w1}^2 \delta_{w2} \in \Lambda. \qquad H B^{\mathrm{ord}} \subset B.$$

Proof. We specify the Hecke algebra in use. The group is the definite unitary group of rank three over F, quasi-split at the finite places. The extension L/F is unramified there. At a prime dividing $sN_*\ell$ this follows from the local splitting supplied by $-v$ being a square in the construction of F; at other primes it follows by base change from $K/\mathbb{Q}$. Labesse's descent to this group, in the form used in Proposition 36.23, applies to the regular algebraic conjugate self-dual cuspidal representation of Theorem 55.7. At ℓ it has an ordinary refinement, since the two Frobenius slopes of the newform are $0, r$ and the adjoint has their ordered differences. Take a tame level carrying this descent; one can take it sufficiently small at an additional split place. The dual ordinary module is finite free over Λ, and the control theorem identifies its regular algebraic specializations with the corresponding classical ordinary spaces. This is the definite ordinary control theorem used in Proposition 36.23. Its construction and level control are independent of distinctions between residual inertia characters. [5]

Form the commutative subalgebra of its endomorphisms generated over Λ by good split Hecke operators. It is finite and torsion-free over Λ. Localize at the residual system of the adjoint and quotient by a minimal prime through the adjoint in characteristic zero. The resulting domain B contains Λ, since its nonzero elements act as nonzero divisors before passage to the minimal prime. Dominant algebraic weights with sufficiently large successive gaps and the specified finite diamonds are Zariski dense: on small logarithmic neighborhoods one can vary every labeled integral exponent through an arithmetic progression, and the matrix of the local embeddings has full rank. Increasing successive exponents to retain the gaps leaves a dense set in each variable. Points above these weights outside any proper closed subset are dense in B. Indeed a nonzero element of the finite domain generates an ideal meeting Λ nontrivially,

by its minimal polynomial over the fraction field and clearing denominators. Every such point occurs in the specialized ordinary space, by faithful support and Nakayama’s lemma.

At these classical points the good Hecke generators give the normalized Galois traces. To obtain $t(g)$ for arbitrary g, approximate the conjugacy class of g by good split Frobenius classes using Chebotarev. For each finite list of classical points one can approximate the traces there to arbitrary coefficient precision by continuity of the classical representations. The compact Hecke algebra has closed image in the product of their valuation rings. This gives the trace tuple in the algebra; the density just proved makes it unique in B. The compact image is homeomorphic to the algebra with its maximal-ideal topology, which also gives continuity. Newton’s identities supply the characteristic coefficients since $3! \in O^{\times}$. This is the trace construction of Proposition 36.23.

The only ramified factor at ℓ in the construction of L is the degree-ℓ^{a} cyclotomic layer. All other factors are unramified locally. Total ramification of the cyclotomic extension therefore allows the indicated σ_w in inertia. At the adjoint its ordered values are $(x_\ell, 1, x_\ell^{-1})$ with $x_\ell = (1+\ell)^{\ell^{a} r}$. They are distinct in characteristic zero; every Vandermonde factor is consequently nonzero in B.

Choose an arithmetic Frobenius lift ϕ_w. In the lemma take $t_j = t(\phi_w \sigma_w^{j})$. On the dense regular classical points where the weight values are distinct, the ordinary Galois filtration has the three ordered inertia characters of the weight, with the fixed common normalization. This is local ordinary compatibility in Proposition 41.22. We can restrict the tests to the open set on which a nine-by-nine trace minor nonzero at the adjoint is nonzero; their transfer is then cuspidal, by the rank of the semisimple group span. At each test point the trace of $\phi_w \sigma_w^{j}$ is the sum of the three products on the flag quotients, regardless of off-diagonal entries. The three solutions u_{wi} over $\operatorname{Frac} B$ therefore agree with the correctly ordered values at ϕ_w. Their elementary symmetric functions agree with the characteristic coefficients of ϕ_w on this dense open set, and hence in the field. The constant coefficient is a unit of B, by reduction at the residual system. This proves every hypothesis of the lemma without dividing by a residual eigenvalue difference.

Adjoin these three values at every w. Products of the local module generators generate the resulting algebra, and multiplication by H carries each of them into B. It remains to see that these values give the full characters. Local reciprocity identifies the abelian local group with the product of its compact units and a procyclic factor generated by the image of a Frobenius lift, after making the corresponding choice of splitting. The values on inertia are given by the weights. On the procyclic factor there is a continuous character sending its generator to u_{wi}: the unit group of a finite complete local algebra with finite residue field is profinite. The resulting characters agree with the classical ones on the dense test set, proving the assertion for every local group element. □

Theorem 55.12 (Integral loss on the entire original weight specialization)**.** *Specialize $\Lambda \to O$ to the original three inertia weights $\kappa_\ell^{r}, 1, \kappa_\ell^{-r}$. The kernel and cokernel of*

$$B \otimes_{\Lambda} O \longrightarrow B^{\mathrm{ord}} \otimes_{\Lambda} O$$

are annihilated by $\ell^{6 g_\ell (1 + a + v_\ell(r))}$, with $v_\ell(\ell) = 1$. The same bound holds after any further scalar extension from O, including every finite precision. One has $g_\ell \le 2\ell^{2}$. In particular at $a = 0$ the annihilating exponent is polynomial in V, uniformly for all the characters and twists in Section 55.2.

Proof. Write $i : B \to B^{\mathrm{ord}}$ for the inclusion. Multiplication by H is a B-linear map $j : B^{\mathrm{ord}} \to B$ by the proposition. Both ij and ji are multiplication by H. The two identities persist under

every scalar extension, so its image annihilates the kernel and cokernel even when the extension is not flat.

At the prescribed weights the three specialized differences are, up to sign, $x_\ell - 1, 1 - x_\ell^{-1}$ and $x_\ell - x_\ell^{-1}$. The factors x_ℓ and $x_\ell + 1$ are units. All differences have valuation $1 + a + v_\ell(r)$. Indeed raising a principal unit to an exponent prime to ℓ preserves the valuation of its difference from one. Raising it to the ℓ-th power increases that valuation by one for these rational principal units, by the binomial theorem and $\ell > 2$. Each δ_{wi} has two such factors, so the specialized H is the stated power of ℓ times a unit. Finally $[F : \mathbb{Q}] \le 2\ell^{a+2}$, and F has ramification index ℓ^a at ℓ. The local degrees sum to $[F : \mathbb{Q}]$, giving $g_\ell \le 2\ell^2$. At depth zero use $\ell \le L_*$, $r \le t_*$, both polynomially bounded on the interval, to obtain the assertion. □

Corollary 55.13 (The ordinary component through the adjoint)**.** *Suppose additionally that $\ell \ge 11$ is prime to $[E_* : \mathbb{Q}]$. Use the stable compact type at the old places of Lemma 54.9, with hyperspecial level at the other places away from ℓ. Let R be the polarized ordinary determinant ring over L/F with three labeled full local characters, the old inertia kernels of U, and freely varying ordered weights as in Section 37.9. At the characteristic-zero point of U, R has a unique irreducible component. Its integral domain is B^{ord} for any minimal good Hecke component B through that point with these types. Its local ring at the point is regular of dimension $3d$.*

Proof. The old conductor places are split in L/F. The adjoint has inertia type $\alpha \oplus 1 \oplus \alpha^{-1}$ there and zero monodromy. The compact types and their stable coefficient lattices consequently include it. For ordinary control with these coefficients the arithmetic stabilizers have order prime to ℓ: an element of order ℓ in $\mathrm{GL}_3(L)$ would have a primitive ℓ-th root as eigenvalue, of degree $\ell - 1 > 3$ over L. Here $L \cap \mathbb{Q}(\mu_\ell) = \mathbb{Q}$ since ramification at ℓ in L has ℓ-power index. The double-coset and lattice proof of Lemma 54.9 applies, and the old compact type gives precisely this inertia and zero monodromy at the cuspidal classical test points. At every other finite place away from ℓ the descent and the test representation are unramified.

The determinant and local characters on B^{ord} give a surjection $R \to B^{\mathrm{ord}}$. To check its equations, one may invert H, where $B^{\mathrm{ord}}[1/H] = B[1/H]$. At the dense cuspidal classical tests the polarized trace identities and the identities for every prescribed tame inertia kernel hold, by local compatibility. For the local ordinary word, each $M(g_i) - \xi_i(g_i) I$ carries the i-th flag step to the preceding step. The product in step order therefore vanishes, also after multiplication and taking the trace against any group element. The associated local characteristic polynomial identities hold as well. All these are equalities in the domain B^{ord} by density. Surjectivity follows because R supplies the weights, all the good Hecke coefficients, and precisely the u_{wi} adjoined above.

The augmentation at the adjoint extends to B^{ord} with the same characteristic-zero residue field J, since the ordered Frobenius values there are those of U and are integral units in a sufficiently large O. The domain B^{ord} is integral and finite over the normal domain Λ. The prime of this weight in $\Lambda[1/\ell]$ has height $3d$, since its completion has the translated weight variables as a regular set of parameters. Going down and incomparability give the same height for the adjoint prime of B^{ord}.

At the corresponding prime of R its tangent space over J injects into the $3d$-dimensional space of weight tangents. Here one uses the characteristic-zero argument of Lemma 37.35, with the following checks at coincident residual weights. A determinant over the dual numbers lifting the absolutely irreducible U is given by a representation unique up to strict conjugacy, by Chenevier's theorem. The nonsingular trace pairing makes the tame kernel identities actual matrix identities and does the same for the ordinary word. The eigenvalues of σ_w are distinct in J, and their differences are units over the dual numbers over J. In its eigenbasis, put σ_w

in every position of the word except the i-th. The factors on the left are units on rows of index at least i, those on the right on columns of index at most i. This forces triangularity in the prescribed order with diagonal ξ_i, and recovers those labeled characters from the matrices. Conjugate duality for this absolutely irreducible determinant gives the polarized lift over F, by the symmetric pairing argument of the same lemma. Continuity follows by recovering matrix coordinates from the traces against a fixed basis of nine group matrices. Corollary 55.8 gives the asserted injection. The hypotheses concern this one adjoint, for which its automorphic realization was proved above.

The local ring of R now has a quotient of dimension $3d$ and embedding dimension at most $3d$. It is regular, hence a domain. The prime kernel of the local surjection is zero, since a positive-height prime would lower the dimension. Its contraction is the unique minimal prime of R contained in the adjoint prime. The original surjection identifies the quotient by that contraction with B^{ord}. □

This identifies the component passing through the chosen automorphic point even when all three residual local characters coincide. It remains to determine which further components meet the split section carrying the strict classes and to bound their total integral intersection there.

55.4 The fiber of the split trace at repeated local characters

At the weight and on the auxiliary field L/F of Theorem 55.7, consider the split determinant with diagonal $\Psi, 1, \Psi^{-1}$, restricted to G_L. It has the prescribed polarization, tame inertia and ordered inertia weights. We use the cyclotomic normalization of that theorem. Restoring the common twist multiplies the factors of the ordinary word below by units and carries each local characteristic polynomial to its twist. We keep one place of L over each $w \mid \ell$ of F. Write G_w, I_w for its local group and inertia. The coefficient ring O is the ring of integers of a finite extension of $\mathbb{Q}_\ell$ containing all the diagonal values, with residue field k and uniformizer ϖ. Here $\ell \geq 5$ and $\ell \nmid 2sN_*$.

The source defines an ordinary pair by a global determinant, three local characters $\xi_{w,i}$ with prescribed reductions and torsion values, and the equations

$$t(h(g_1 - \xi_{w,1}(g_1))(g_2 - \xi_{w,2}(g_2))(g_3 - \xi_{w,3}(g_3))) = 0. \tag{55.1}$$

Here $g_i \in G_w$, $h \in G_L$, group elements are read in the group algebra, and t is extended linearly. See `Development/AutomorphicArithmetic/AutomorphicVarieties/WeilGroupCharacters/UniversalOrdinaryDeterminantRing.lean`, line 94 and lines 127–147 there. The source's residual data in this definition have three distinct *global* characters. Their restrictions to G_w can coincide. For an actual stable flag with ordered line quotients the characteristic polynomial on G_w also satisfies

$$\mathrm{char}_D(g; X) = \prod_{i=1}^{3} (X - \xi_{w,i}(g)) \qquad (g \in G_w). \tag{55.2}$$

Indeed in an adapted basis the matrix is triangular, also over a local ring with nilpotents. We compute the effect of this additional identity. The quotients considered below keep the given local weights at every place.

Theorem 55.14 (The complete fiber of the ordinary word equations)**.** *Fix the global determinant to be the constant residual split determinant over k, after any extension of its coefficient algebra. At each w partition $\{1,2,3\}$ by equality of the three residual characters on the* full

G_w. *Denote the partition by* $\mathcal{B}_w$. *In the problem defined by* (55.1)*, the complete ring for the remaining local characters is*

$$k[[z_{wi} : w \mid \ell,\ 1 \le i \le 3]]\Big/\Big(\prod_{i\in B} z_{wi} : w \mid \ell,\ B \in \mathcal{B}_w\Big).$$

It is reduced and equidimensional of dimension $\sum_{w|\ell}(3 - |\mathcal{B}_w|)$. *There are* $\prod_{w,B} |B|$ *minimal primes.*

Proof. Write β_i for the residual diagonal characters at one place and choose an arithmetic Frobenius lift ϕ. A lift of β_i to a complete Noetherian local k-algebra with residue field k and fixed inertia equals $\beta_i(g)(1 + z_i)^{n(g)}$. Here $n(g)$ is the image in the pro-ℓ quotient $\mathbb{Z}_\ell$ of the unramified Galois group, normalized by $n(\phi) = 1$. Indeed $1 + \mathfrak{m}$ in each Artinian quotient is a finite ℓ-group, and passage to the limit gives precisely the continuous powers of $1 + z_i$. An unramified variation kills the torsion in the local abelianization, since its unramified pro-ℓ quotient is torsion-free. These parameters therefore respect the specified torsion values.

With the global determinant fixed, its trace of the product in (55.1) can be computed on the split diagonal. On a line of local character β the product acts by $P_\beta = \prod_i(\beta(g_i) - \xi_i(g_i))$. Taking the testing element h in the local group gives the sum of $|B|\beta(h)P_\beta$ over the distinct characters β, where $B = \{i : \beta_i = \beta\}$. Their joint image is a finite abelian group of order prime to ℓ. Multiplication by $\beta(h)^{-1}$ and averaging over representatives of that image selects $|B|P_\beta$. The factor $|B|$ is invertible in k. Thus the equations are equivalent to the vanishing of every P_β. Conversely this vanishing kills every diagonal entry and therefore every test with global h.

For $i \in B$ the ideal of differences $\beta(g) - \xi_i(g)$ is (z_i), by evaluation at ϕ. For $i \notin B$ it is the unit ideal, by evaluation at a group element on which the residual characters differ. The g_i vary independently, so the ideal of the products is exactly $(\prod_{i\in B} z_i)$. The only remaining data of the pair are the characters at the chosen places, hence the independent sets of equations give the asserted ring. The ideal just found is the intersection of the coordinate ideals obtained by choosing one variable from each block. Indeed a monomial avoiding at least one variable in every block fails to belong to the coordinate ideal generated by those avoided variables. Membership in these monomial ideals is coefficientwise for power series. All the coordinate ideals in the intersection are incomparable primes of the same height, one for each indicated choice. This gives all the claims. □

Proposition 55.15 (A triple local coincidence on the common intervals)**.** *On every sufficiently distant interval of Theorem 19.15 there are a single allowed* ℓ*, an even character* α *of all* E_x *and a single twist* r *in the required range such that the residual global diagonal has three distinct characters on* G_L*, while at every* $w \mid \ell$ *all three are trivial. This holds at every auxiliary depth* a*. The constant-trace fiber of* (55.1) *then has dimension* $2g_\ell$*, where* $g_\ell = \#\{w \mid \ell \text{ in } F\}$.

Proof. Fix four distinct primes congruent to one modulo 32 and prime to the conductor of the fixed ψ. Such primes exist by Dirichlet's theorem. Only q, d_0, s can remove further primes from this list under the condition $\ell \nmid 2sN_*$, by the conductor in Theorem 19.15. Select a remaining prime. On sufficiently large intervals all four primes are below L_*, and all their predecessors $\ell - 1$ are below $t(x)$. The dyadic layer C_J then contains $\mathbb{Q}(\zeta_{32})^+$, since J grows uniformly with x. Take a faithful character of this real cyclic field of degree eight and set $r = \ell - 1$. Its value at ℓ is one, so its restriction to $G_{\mathbb{Q}_\ell}$ is trivial. The residual cyclotomic factor to the power r is trivial everywhere. These facts give the assertion at the local places.

The field L is the compositum of two quadratic fields and abelian extensions of ℓ-power degree. The 2-primary part of its Galois group has exponent at most two. Its intersection with the cyclic field of degree eight therefore has degree at most two. Reduction at the odd prime

ℓ preserves the order of the eighth roots of unity. It follows that $\bar{\Psi}|_{G_L}$ has order at least four, which makes the global triple distinct. The dimension is now given by Theorem 55.14. For example one can vary a single unramified label freely in $k[[z]]$ and keep the two others and the global determinant constant. □

Theorem 55.16 (The finite fiber imposed by local characteristic polynomials)**.** *In the fiber of Theorem 55.14, impose* (55.2) *for every w and g. The resulting ring is the tensor product over k, over all blocks $B \in \mathcal{B}_w$, of*

$$k[z_{wi} : i \in B]/(e_1(z_B), \dots, e_{|B|}(z_B)),$$

where e_j is the elementary symmetric polynomial of degree j. It has length $\prod_{w,B} |B|!$. The dimension of its cotangent space is $\sum_w (3 - |\mathcal{B}_w|)$.

Proof. At a place let Δ be the joint residual character image. The map $G_w \to \Delta \times \mathbb{Z}_\ell$ given by the residual characters and n is onto. Indeed take powers of a lift of any $\delta \in \Delta$ with exponents congruent to one modulo $|\Delta|$ and tending to zero in $\mathbb{Z}_\ell$. Its images tend to $(\delta, 0)$ in the compact image. Surjectivity onto $\mathbb{Z}_\ell$ gives the other factor after multiplication by such elements.

For every positive integer j, take local elements with images (δ, j) and compare their traces. Orthogonality on Δ gives for each block of size m

$$\sum_{i \in B} (1 + z_i)^j = m.$$

At $j = 1, \dots, m$ successive expansion gives zero for the power sums of z_i of degrees $1, \dots, m$. Newton's identities and $\ell > m$ give $e_1 = \cdots = e_m = 0$. Conversely these identities imply $z_i^m = 0$, since $\prod_{i \in B}(X - z_i) = X^m$ and each z_i is a root. All positive power sums vanish by Newton's identities in degrees below m and this nilpotence thereafter. Expansion gives the displayed equality for all nonnegative integer exponents and then for all $n \in \mathbb{Z}_\ell$ by continuity. Thus the local traces agree at every element, including its second and third powers, which gives the full characteristic polynomial by Newton's identities. The product equation from the ordinary word is already $e_m = 0$ in each block.

The block ring represents ordered factorizations of X^m into monic linear factors. Adjoin the first root of X^m, divide by its monic linear factor, and adjoin a root of the remaining monic polynomial. Continuing gives free extensions of ranks $m, m-1, \dots, 1$. The resulting ring represents the same factorizations, so its dimension is $m!$. All variables are nilpotent and the only linear equation is $\sum_{i \in B} z_i = 0$. Tensoring the block algebras proves the formula for both invariants. The product is already complete because it is Artinian and local. □

Corollary 55.17 (The integral contribution of ordered labels)**.** *At the original inertia weight over O, let C be the ordinary determinant algebra with* (55.2) *imposed, or any closed quotient through the split section. Only the determinant and the three ordered characters at each chosen place are recorded. Let B be the closed O-subalgebra of C generated by all global traces. Write J_B, J_C for the augmentation ideals at the split section, put $b = 1 + a + v_\ell(r)$, and normalize $v_\ell(\ell) = 1$. The map*

$$J_B/J_B^2 \longrightarrow J_C/J_C^2$$

has cokernel of O-length at most

$$2\, v_\varpi(\ell)\, b \sum_{w \mid \ell} (3 - |\mathcal{B}_w|).$$

Its kernel is killed by $\ell^{12 g_\ell b}$. These assertions apply to the image of the determinant and its ordered characters in any family of actual local flags through the split section, including families

over rings with nilpotents. At depth zero the sum of the displayed upper bounds, divided by $v_\varpi(\ell)$ and weighted by $\log \ell$, over the indicated primes, twists and characters of any E_x, is polynomially bounded in V throughout the common interval.

Proof. Let $u_{wi} = \xi_{w,i}(\phi_w)$ for an arithmetic Frobenius lift. The algebra C is topologically generated over B by these values. Indeed the determinant is determined by traces when 3! is a unit, and all inertia characters are fixed. Every unramified character is determined continuously by Frobenius. Equivalently one may use a presentation of the determinant and character rings with these generators before imposing the equations. The coefficient ring and the completed deformation rings here are compact with finite residue field. The finite spans of monomials over the closed ring B used below are therefore closed.

Take σ_w as in Proposition 55.11. Its inertia weights s_i are $x, 1, x^{-1}$ with $x = (1+\ell)^{\ell^a r}$. The trace coefficient of (55.2) at $\phi_w \sigma_w^j$ gives $t(\phi_w\sigma_w^j) = \sum_i u_{wi} s_i^j$. For $\{i,j,k\} = \{1,2,3\}$, multiplication by the coefficients of $(X-s_j)(X-s_k)$ and summation give $(s_i-s_j)(s_i-s_k)u_{wi} \in B$. Each difference has valuation b, by the binomial calculation of Theorem 55.12. Thus $\ell^{2b}u_{wi} \in B$ without any condition on the components of C.

By (55.2) at ϕ_w, the three u_{wi} are the roots of a split monic cubic over B with unit constant coefficient. One can eliminate the third using their sum, reduce powers of the first using the cubic and those of the second using the remaining quadratic. This holds over arbitrary commutative rings by monic division. The resulting six monomials at each place have total degree at most three. Inverses of the roots are already in this algebra by the unit product. Taking products over the places gives C as the finite span of these monomials and gives $\ell^{6g_\ell b}C \subset B$. If $y \in J_B \cap J_C^2$, multiplication by $\ell^{12g_\ell b}$ multiplies both factors in each product from J_C^2 by $\ell^{6g_\ell b}$. Each factor then lies in J_B, proving the kernel assertion.

The cokernel is generated over O by the classes of $u_{wi} - u_{wi}^0$, where the superscript denotes augmentation. The interpolation calculation kills each class by ℓ^{2b}. Modulo ϖ, this cokernel is the cotangent space of $C/(\varpi, J_BC)$ at its residue point. In fact its presentation is $J_C/(J_C^2 + J_BC + \varpi J_C)$, since modulo J_C^2 a coefficient in C acts on J_B by augmentation. The ring in this fiber is a quotient of the ring in Theorem 55.16. It fixes every trace to its residual split value, hence fixes the determinant as well. The dimension of its cotangent space is at most the number in that theorem. Nakayama's lemma and the annihilator give the length bound. Finally $g_\ell \le 2\ell^2$; at depth zero $b \le 1 + \log_\ell t_*$. There are at most $n_* = [E_* : \mathbb{Q}]$ characters on each field, at most t_* twists and at most L_* primes, all polynomially bounded in V. This proves the uniform assertion. □

Theorem 55.18 (Elementary divisors at the original split trace)**.** *Keep the global determinant equal to the original split determinant over O, for any α, r, ℓ, a in this subsection. Choose ϕ_w of cyclotomic value one. Let y_w be the ℓ-power part of the root of unity $\alpha(\phi_w)$, set $x = (1+\ell)^{\ell^a r}$, and put*

$$h_w = \min\{v_\varpi(x-1), v_\varpi(y_w - 1)\}, \qquad v_\varpi(0) = +\infty.$$

In the fixed-weight algebra satisfying (55.1) and (55.2), the cotangent module of this fiber at the split section is

$$\bigoplus_{w\mid\ell} \bigoplus_{B\in\mathcal{B}_w} \bigoplus_{j=1}^{|B|-1} O/\varpi^{jh_w}O.$$

For any quotient through the split section this gives the sharper bound $\sum_{w,B} \binom{|B|}{2} h_w$ for the cokernel length in Corollary 55.17. For the actual family of Proposition 55.15 the displayed cotangent module is

$$\bigoplus_{w\mid\ell} (O/\ell^{a+1}O \;\oplus\; O/\ell^{2(a+1)}O).$$

Proof. Work one place at a time. Write $\lambda = \Psi|_{G_w}$, τ for the Teichmüller lift of its reduction, and $d = \lambda/\tau$. The local field is an unramified extension of the completion of the degree-ℓ^a cyclotomic layer. The cyclotomic extension above it is totally ramified. Consequently the prescribed ϕ_w exists by multiplying a Frobenius lift by inertia. On inertia the principal-unit image of d is topologically generated by x, and $d(\phi_w) = y_w$. Indeed α is unramified and the image of the principal cyclotomic character is $(1+\ell)^{\ell^a\mathbb{Z}_\ell}$. In particular $d(g) \equiv 1 \bmod \varpi^{h_w}$ for every g.

Use the exponents $e_i = 1, 0, -1$. Write the i-th local character as $\lambda^{e_i}(1+z_i)^n$, with n the unramified coordinate used above. Modulo quadratic terms its variation is $\lambda(g)^{e_i} n(g) z_i$. The image of (τ, d, n) is the direct product of $\operatorname{im}\tau$ with the image of (d, n). In fact the first group has finite prime-to-ℓ order and the second is pro-ℓ. Powers congruent to one modulo the first order and to zero modulo arbitrarily large powers of ℓ isolate the first group in the compact image. Complementary multiplication isolates the second. We can therefore average the linearized trace relations over $\operatorname{im}\tau$ using its character idempotents over O. This separates precisely the stated blocks. For a block B the relations are the rows

$$n(g)\big(d(g)^{e_i}\big)_{i\in B}$$

acting on its generators z_i. Comparing traces at the second and third powers of each local element gives all characteristic coefficients, as 3! is invertible.

There are three available values of $d(g)$, all with $n(g)$ a unit, whose pairwise differences have valuation exactly h_w. When $v_\varpi(x-1) \le v_\varpi(y_w - 1)$ use $y_w, y_w x, y_w x^2$, obtained with $n = 1$ by varying inertia. Otherwise use y_w, y_w^2, y_w^3, obtained on the first three powers of ϕ_w. Here $1, 2, 3$ are units, and the difference between two consecutive powers has the same valuation as the difference two powers apart, since the sum of a principal unit and one is a unit.

A singleton block has a unit row entry and contributes zero. A block of size two occurs when $\bar\lambda$ has order two, and its exponents are $1, -1$. Multiplying each row by the unit $d(g)$ gives the two columns $d(g)^2, 1$, with row factor $n(g)$. Every two-row minor is divisible by ϖ^{h_w}, and two of the displayed values attain that valuation since their sum is a unit. Its nonunit elementary divisor is therefore ϖ^{h_w}. For a block of size three the same unit scaling gives the columns $d(g)^2, d(g), 1$. Every two-row minor has valuation at least h_w and every three-row determinant at least $3h_w$, by the Vandermonde product and the row factors. The displayed choices attain both minima. The entries generate the unit ideal. Smith normal form now gives the three valuations $0, h_w, 2h_w$. These minor computations apply to the whole span of the rows, since it is a submodule of a finite free module over a DVR and its minor ideals are generated by the minors of the generating rows.

It remains to check the ordinary word at first order. On the i-th split global line the i-th factor has zero constant term, so only its own variation can contribute. This variation is a multiple of z_i. Each other index in its block supplies a factor divisible by ϖ^{h_w}, because the Teichmüller characters agree and the remaining values are congruent to one modulo that power. Thus the linear term is a multiple of $\varpi^{(|B|-1)h_w} z_i$, already zero by the elementary divisors. The global polarization and tame equations hold on the fixed determinant. Local torsion values are fixed by inertia. The independent places therefore give the direct sum asserted.

Quotienting the original deformation algebra through its split section gives a quotient on the fibers with all traces fixed to their split values. Their augmentation cotangent modules are the respective cokernels in the corollary, by the same ideal computation over O. This gives the length bound. In Proposition 55.15 each place has one block, $y_w = 1$ and $r = \ell - 1$, giving $h_w = (a+1)v_\varpi(\ell)$ as claimed. □

These calculations concern a specific cost in passing from global traces to local character labels. In particular the positive-dimensional fiber of the word equations cannot supply a finiteness argument at the split trace for these characters. Recovering the total strict cohomology length requires control of the global trace relations that detect extensions. The signed period on the prescribed analytic row in Section 6.6 remains to be compared with the integral arithmetic period on each E_x.

55.5 Reducible traces when inertia is scalar on the descended plane

Fix one of the common intervals of Theorem 19.15. Use the same auxiliary quadratic field $K = \mathbb{Q}(\sqrt{-s})$, characters α of E_x, sign condition, and twists $2 \le r < t(x)$ as in Section 55.2. Take $5 \le \ell \le L_*$ prime to $2sN_*$ and suppose $\ell - 1 \mid 2r$. Put $\Psi = \alpha\kappa_\ell^r$. Bars denote reduction in the residue field k of a coefficient ring O containing the character values. We use Pan's two ordinary finiteness theorems over $\mathbb{Q}$. Passing from the plane over K to a representation over $\mathbb{Q}$ requires checking its inertia before either theorem can be applied.

Lemma 55.19 (A stable local line in the descended plane)**.** *Let V be a continuous two-dimensional representation of $G_{\mathbb{Q}_\ell}$ over a finite extension of $k((z))$. Suppose every inertia element has both eigenvalues one. After a finite extension of coefficients V has a $G_{\mathbb{Q}_\ell}$-stable line. The characters ξ_1, ξ_2 on the line and quotient are unramified. For any global representation extending V its trace satisfies*

$$\operatorname{tr}\big((V(\sigma) - \xi_1(\sigma)I)(V(\tau) - \xi_2(\tau)I)M\big) = 0$$

for all local σ, τ and any matrix M of the global representation.

Proof. If inertia has a nonidentity element u, choose a basis in which $u = I + E_{12}$. For every other inertia matrix A, both uA and A have trace two, which gives $A_{21} = 0$. The diagonal entries of A are then both one. Consequently the common inertia fixed space is the first line, unique because $u \neq I$. Normality of inertia makes this line stable under the decomposition group. If inertia is trivial, choose an eigenline of an arithmetic Frobenius lift after splitting its characteristic polynomial. The unramified quotient is procyclic and the stabilizer of a line is closed, so this line also suffices. In both cases inertia acts trivially on the two quotients. The second matrix difference in the formula maps into the line, and the first kills the line. This proves the identity, including after any multiplication and trace. □

Consider lifts on G_K of the split residual diagonal $(\bar{\Psi}, 1, \bar{\Psi}^{-1})$, unramified outside a finite set containing the primes over $2sN_*\ell$. Use the symmetric adjunction in a fixed basis from Proposition 38.14. Thus the matrix of $cg^{-1}c$ is the adjoint of the matrix of g for the fixed invertible symmetric antidiagonal form, with the common cyclotomic twist removed. Here c is a complex conjugation. Away from ℓ impose finite inertia image by fixing inertia kernels contained in the kernels of the split type, of finite index in the local inertia groups. For instance one may use the kernels of α on inertia there. At each $v \mid \ell$ impose only

$$\operatorname{char}_{M(\sigma)}(X) = (X - \Psi(\sigma))(X - 1)(X - \Psi(\sigma)^{-1}) \qquad (\sigma \in I_v).$$

These are closed equations in the framed matrix deformation ring and hold on all actual flags of the original weights. Let T be the closed O-algebra of traces of the resulting universal matrices. Further matrix markings or flag conditions give trace images which are quotients of T. Let $I_m \subset T$ be generated by the size-m minors of $(t(g_i h_j))$, where $g_i, h_j \in G_K$.

Theorem 55.20 (Finiteness of the entire reducible trace quotient)**.** *Suppose $\bar{\Psi}|_{G_K}$ has order greater than two or is trivial. For $6 \le m \le 9$, T/I_m is a finite O-module. Its geometric field points are exactly the points of T with reducible semisimple representation. In particular this holds for every globally distinct residual triple on G_K in the stated range, regardless of the values of $\alpha(\ell)$ or $\eta_K(\ell)$.*

Proof. The framed ring is a quotient of the usual complete matrix deformation ring unramified outside the indicated set. Finiteness of residual first cohomology follows by Kummer theory, as in Theorem 55.3. The complete determinant ring is therefore Noetherian and its Cayley–Hamilton algebra is module finite. Its image in the framed ring is T, since 3! is a unit and the determinant coefficients are recovered from traces. The image is closed by compactness. The span of group matrices is finite as a T-module by the same Cayley–Hamilton theorem. [12]

At a geometric field point the semisimple group span is a product of matrix algebras acting on the distinct simple constituents. Its trace pairing is nondegenerate since it is the ordinary matrix trace pairing on each factor times a multiplicity between one and three. The span has dimension nine in the absolutely irreducible case and at most five otherwise. Group elements span it in both variables of the pairing, which proves the minor assertion. A semisimple realization factors through the specialized integral matrix span. Indeed an identity of group matrices has trace zero against all group matrices and therefore acts as zero on the semisimple realization, by the nondegeneracy just proved. The adjunction also passes to this semisimple span since its trace radical is preserved.

It suffices to test a continuous map from T/I_m to $k'[[z]]$ with k'/k finite. Over a finite extension of its fraction field take the semisimple realization just described. Its continuity and the existence of a stable lattice follow from the finite integral matrix span as in Theorem 55.3. Its residual semisimplification is the prescribed diagonal. Character values in residue fields are read as constants in the equal-characteristic coefficient DVR, enlarged when needed.

Each one-dimensional constituent is the constant lift of its reduction. In fact for any $\sigma \in I_v$, $v \mid \ell$, its value is one of the three constant roots of the displayed inertia polynomial in characteristic ℓ, hence is determined by its reduction. At other places inertia has finite image. A finite-order unit in an equal-characteristic DVR with finite residue field is its constant residual lift: the principal units are pro-ℓ and have no nontrivial ℓ-power torsion, by the power identity in characteristic ℓ. The character divided by its constant residual lift is consequently everywhere unramified. The class group of K is finite, so its image in these principal units is trivial. The same reasoning for the determinant gives determinant one, since its inertia at ℓ and its reduction are trivial. This treats a sum of three lines.

In the remaining case there is a unique line constituent λ and an absolutely irreducible plane P. Polarization gives $\lambda^c = \lambda^{-1}$. Every possible residual character on this line extends to $G_{\mathbb{Q}}$, hence is fixed by c on G_K. The order hypothesis forces $\bar{\lambda} = 1$: for order greater than two neither outer character squares to one, and in the trivial case all three are one. The preceding argument gives $\lambda = 1$ and $\det P = 1$. In particular the residual semisimplification of the plane on G_K consists of $\bar{\Psi}, \bar{\Psi}^{-1}$ with their multiplicities.

We give the odd descent explicitly. The adjunction fixes the plane factor in the semisimple span. On a full matrix algebra over a splitting field an involution fixing scalars is adjoint to a symmetric or alternating form, by composing it with transpose and using innerness of a matrix algebra automorphism. Proposition 38.14 gives the polynomial identity $2XYX = t(XY)X$ for skew elements of the original rank-three symmetric matrix algebra. Skew elements in its semisimple quotient lift by antisymmetrization, since two is invertible. The identity rules out alternating adjunction on the plane: in such a basis $X = \operatorname{diag}(1,-1)$ and $Y = E_{12} + E_{21}$ are skew, but $XYX = -Y$ and $\operatorname{tr}(XY) = 0$. Both elements have zero line component here.

Let S be the resulting symmetric form matrix on the plane and J its standard alternating form, preserved by P because the determinant is one. The adjunction identity gives $P(cgc) = S^{-1}P(g)^{-\mathsf{T}}S$. The matrix $S^{-1}J$ therefore intertwines P with its conjugate by c. It is invertible with trace zero, so after a finite scalar extension it can be rescaled to square one, with determinant -1. Let c act by this matrix. This extends P to a continuous representation W of $G_{\mathbb{Q}}$ of determinant η_K.

After taking a stable lattice, every irreducible constituent of its residual semisimplification restricts semisimply to G_K: the translates of a simple submodule for the normal subgroup span a semisimple module invariant under $G_{\mathbb{Q}}$. When the two restricted characters are distinct they already extend to $G_{\mathbb{Q}}$, so both isotypic lines in a purported irreducible residual plane would be stable. When they are equal, twisting off their global extension would give an irreducible residual plane of a group of order two, also impossible. Thus the residual characters on $G_{\mathbb{Q}}$ are $\bar{\Psi}, \bar{\eta}_K\bar{\Psi}^{-1}$, after twisting W by η_K if necessary, using its determinant to fix their product. In the repeated case the restrictions are trivial and the determinant gives the pair $1, \bar{\eta}_K$.

Now set $V = W\bar{\Psi}^{-1}$, using the global constant lift of $\bar{\Psi}$ in characteristic ℓ. Since $K/\mathbb{Q}$ is unramified at ℓ, its local inertia is the same as that over $\mathbb{Q}_\ell$. The characteristic polynomial on the plane there is the prescribed polynomial with the line factor $X - 1$ removed. Its two roots are $\bar{\Psi}(\sigma), \bar{\Psi}(\sigma)^{-1}$. They agree for every inertia element by $\ell - 1 \mid 2r$ and $\ell \nmid N_*$. This proves the unipotent inertia hypothesis of Lemma 55.19 for V. It gives two unramified local characters and a stable line over a finite extension. The compact image preserves a lattice, whose intersection with the line is saturated. Thus both characters take values in the coefficient DVR.

Apply Pan's finiteness theorems to the rational field with fixed determinant $\chi = \eta_K\Psi^{-2}$. This character is odd, unramified outside a finite set, and de Rham at ℓ, being a finite character times a cyclotomic power. The residual trace of V is $1 + \bar{\chi}$. If $\bar{\chi}|_{G_{\mathbb{Q}_\ell}} \neq 1$, the local trace is the sum of two characters with the prescribed distinct reductions. Pan's Theorem 5.1.2(1) applies to its ordinary pseudodeformation. If $\bar{\chi}|_{G_{\mathbb{Q}_\ell}} = 1$, mark the actual stable line of the lemma. Its character reduces to one, the quotient character is the determinant divided by that character, and the matrix identity of the lemma is exactly the ordered trace identity in Pan's Definition 5.3.2. These verify the additional hypotheses for his Theorem 6.1.2(1). In either case the applicable ring is finite over $O[[1+\ell\mathbb{Z}_\ell]]$, after finite coefficient extension if needed. Its weight character is unramified on our curve, since both local characters are unramified. The map to the equal-characteristic coefficient DVR therefore kills the weight augmentation ideal and ϖ. The image is a finite field. Undoing the constant twist, adjoining the trivial line and restricting to G_K proves that all original traces in $k'[[z]]$ are constant. [7]

If the special fiber of T/I_m had positive dimension, a one-dimensional complete local domain quotient and its normalization would give just such a curve with nonconstant trace. Indeed the normalization is a complete DVR finite over $k[[z_0]]$ by complete Noether normalization, and the traces topologically generate the quotient. Thus the special fiber is Artinian. A power of the maximal ideal lies in $\varpi(T/I_m)$; completeness and lifting a basis of the special fiber show that T/I_m is a finite O-module, including its torsion. □

Corollary 55.21 (Integral finiteness with the characters of a flag)**.** *In the range of the theorem, adjoin to the trace image of any of these fixed-weight symmetric matrix problems the three ordered local characters of an actual flag at each chosen place over ℓ. More generally one may adjoin such labels with the local characteristic-polynomial identities (55.2). The quotient of the resulting determinant and character algebra by I_m is finite over O for $6 \leq m \leq 9$. The conclusion includes the characters and twists of Proposition 55.15 on the same period intervals.*

Proof. All inertia values are fixed and each local unramified quotient is procyclic. Therefore only the ordered Frobenius values must be adjoined. Their local cubic has coefficients in the trace image and invertible constant coefficient. Successive monic division gives at most six module generators per place, as in Corollary 55.17, with no assumption on the differences of its roots. This finite span is compact and contains the continuous character values, so it also contains their closed algebra. Reducing by I_m leaves a finite module over a quotient of T/I_m. The order-eight character of the cited proposition retains order at least four on G_L, hence also on G_K. Its twist obeys the collision congruence. All hypotheses therefore hold for that same character and field choice. □

Finiteness here controls the reducible part of the trace problem at a fixed weight. An interval bound for the entire strict group still requires a quantitative bound on the integral extension classes, including their intersections with the irreducible locus. The period comparison in Section 6.6 uses those same E_x.

55.6 Quadratic residual characters on one real subfield of the interval

Keep the symmetric rank-three trace algebra T, the ideals I_m, the imaginary quadratic field $K = \mathbb{Q}(\sqrt{-s})$ and the finite inertia conditions of Section 55.5. Take the same interval with largest period field E_* and conductor divisor N_*. We treat the case in which the two outer residual characters agree globally and are nontrivial. When $\ell - 1 \mid r$, they can be removed over a subfield of E_* selected before x or ℓ is chosen. A trace identity brings the conclusion back to G_K.

Lemma 55.22 (Integral traces over a quotient of exponent two)**.** *Let $\rho : G \to \mathrm{GL}_3(A)$, where A is a commutative ring in which 6 is invertible. Let Γ be normal with G/Γ of exponent dividing two. For $g \in G$, denote the elementary characteristic coefficients of $\rho(g^2)$ by s_1, s_2, s_3, in order. Then $t = \operatorname{tr}\rho(g)$ satisfies*

$$\left((t^2 - s_1)^2 - 4s_2\right)^2 - 64 s_3 t^2 = 0.$$

All three coefficients s_i belong to the $\mathbb{Z}[1/6]$-algebra generated by traces on Γ. In particular, on a curve over a finite field, constancy of the restricted traces implies constancy of every trace. If B is the closed restricted trace algebra and is finite over a complete coefficient DVR O with finite residue field, a Hausdorff trace algebra topologically generated over B by d further traces is generated by at most 8^d elements as a B-module.

Proof. Write t, b, δ for the three elementary coefficients of $\rho(g)$. The elementary symmetric polynomials of the three squared roots give $s_1 = t^2 - 2b$, $s_2 = b^2 - 2\delta t$ and $s_3 = \delta^2$. These are polynomial identities of matrices over any commutative ring. Indeed they hold for the universal matrix over its characteristic-zero rational function field by triangularization over a splitting field, hence as identities in the integral polynomial ring in the entries. Substitution and squaring give the formula. Newton's identities express s_1, s_2, s_3 by traces of $\rho(g^2), \rho(g^4), \rho(g^6)$ with denominators dividing six. All three group elements belong to Γ.

In an equal-characteristic complete DVR with finite residue field, an element algebraic over a finite constant field is a constant. Indeed it belongs to a finite field and satisfies $X^q = X$ for a power q of the characteristic. Reduction is injective on these roots since two roots with the same residue have a difference of positive valuation equal to its qth power. The unique lifts of the residue field inside the coefficient DVR give those constants. Apply this to the monic equation for t. Finally powers of each additional trace reduce to powers of degree at most seven by its monic equation. The span of the resulting 8^d monomials is compact as the image of a

finite power of B. It is closed and contains the algebraic generators and all their polynomial combinations. It contains their closure. □

Define $H \subset E_*$ as the compositum of the real quadratic subfields of E_*, taking $H = \mathbb{Q}$ if the list is empty. Put $L = KH$ and write η for the quadratic character of L/H.

Proposition 55.23 (Odd descent after the residual character is killed)**.** *The field H is abelian and totally real, of degree at most 16, and is unramified at every $\ell \nmid N_*$. Suppose $5 \le \ell \le L_*$, $\ell \nmid 2sN_*$ and $\ell - 1 \mid r$. Let $\Psi = \alpha\kappa_\ell^r$ with the sign and field of Section 55.2. Suppose $\bar{\Psi}|_{G_K}$ has order at most two. For every equal-characteristic DVR curve of the reducible trace quotient in Section 55.5, all traces on G_L are constant.*

Proof. The group of $E_*/\mathbb{Q}$ embeds into a product of four cyclic groups by the description of E_* in Theorem 41.17. A subgroup of such a product has at most four generators. Projection onto one cyclic factor supplies a cyclic image. A lift of a generator, together with generators for the kernel obtained by induction, generates the subgroup. Its group of quadratic characters therefore has order at most 2^4. The even quadratic characters cut out H, giving all the asserted field properties. Since K is imaginary quadratic, $H \cap K = \mathbb{Q}$, and $\mathrm{Gal}(L/K)$ is elementary abelian of exponent at most two.

The character $\bar{\Psi}$ equals $\bar{\alpha}$ on $G_{\mathbb{Q}}$ by the congruence on r. It is even by the sign condition. Consequently its fixed field is totally real, is contained in E_x, and meets K in $\mathbb{Q}$. Restricting it to G_K preserves its order. It follows that $\bar{\Psi}|_{G_L} = 1$. In particular, the three residual characters are all trivial on G_L.

Take a semisimple realization on the curve, passing to a finite extension of the coefficient fraction field as in Theorem 55.20. The representation over G_K is reducible and has a stable lattice. Its restriction to G_L is semisimple over a splitting field. Indeed the translates of any simple G_L-submodule in a simple G_K-summand span that entire summand by normality and irreducibility. A sum of simple submodules is semisimple. Thus the restricted representation consists of three lines or of a line and an absolutely irreducible plane.

Every one-dimensional constituent on G_L is trivial. To see its reduction, filter a stable lattice by intersection with a composition series on the generic fiber. The successive lattice quotients are torsion free. Reduction of this filtration preserves the composition factors with multiplicity; the residual semisimplification restricted from G_K has only trivial constituents. The line thus reduces to one, and it has finite inertia image away from ℓ. At primes over ℓ each inertia matrix has characteristic polynomial $(X-1)^3$ in characteristic ℓ, by the original inertia equations. Its character is therefore one on this inertia. A finite-order principal unit in the coefficient DVR equals one, since the units congruent to one are pro-ℓ and are torsion free in characteristic ℓ. At the other primes this proves the same triviality. The remaining character factors through the finite class group of L by global class field theory and is again a principal unit, so is trivial. The same argument gives trivial determinant on G_L. This settles the sum of three lines.

Write P_0 for the plane in the remaining case. It has determinant one. Choose a complex conjugation c_0 in G_H. It acts nontrivially on K and $G_H = G_L \rtimes \langle c_0 \rangle$. We may use the original conjugation of the marked symmetric problem for c_0, since every complex conjugation fixes the totally real field H. The adjunction preserves the simple plane factor, the unique factor of matrix size two. On this factor it is adjoint to a symmetric form. For clarity, the polynomial identity of Proposition 38.14 on skew elements passes to the span of G_L and its semisimple image by antisymmetrizing lifts. Alternating adjunction on the plane would make both $X = \mathrm{diag}(1,-1)$ and $Y = E_{12} + E_{21}$ skew. With their line components zero the identity would say $2XYX = \mathrm{tr}(XY)X$, whereas $XYX = -Y$ and $\mathrm{tr}(XY) = 0$.

Let S be the matrix of this symmetric form and J_2 the alternating matrix with upper-right entry one. Polarization gives $P_0(c_0gc_0) = S^{-1}P_0(g)^{-\mathsf{T}}S$; determinant one gives $P_0(g)^{-\mathsf{T}} = J_2P_0(g)J_2^{-1}$. The intertwiner $S^{-1}J_2$ is invertible of trace zero. After scaling over a finite extension it squares to the identity and has determinant -1. Using it as the value at c_0 extends the plane to a continuous representation W of G_H with determinant η. The sum of a G_L-stable lattice and its translate by c_0 is a G_H-stable lattice. On each irreducible residual constituent the restriction to the normal subgroup G_L is semisimple by the translate argument above. The residual semisimplification on G_L is trivial, so these constituents factor through the order-two quotient. The determinant then gives residual trace $1 + \bar{\eta}$.

For every $v \mid \ell$ of H, the extension L/H is unramified there because $K/\mathbb{Q}$ is unramified at ℓ. Thus W has unipotent inertia at v. If there is a nonidentity unipotent, choose a basis in which it is $I + E_{12}$. The trace of its product with any inertia matrix equals the trace of that matrix. Hence the lower-left entry of every inertia matrix is zero. All inertia matrices fix the first line pointwise, and their common fixed line is unique and stable under the decomposition group. If inertia is trivial choose an eigenline of a Frobenius lift after a finite extension. These arguments give a stable line and two unramified local characters simultaneously at all $v \mid \ell$. The induced lattice on the line is saturated.

We apply the finiteness assertions of Pan with base field H and fixed characteristic-zero determinant $\eta = \eta_K|_{G_H}$, using the finite set of primes containing the ramification of the representation and all primes above ℓ. The determinant extends from $\mathbb{Q}$, is finite order and de Rham at ℓ, and is odd at every real place of H. The coefficient prime is unramified in this abelian totally real field. All places $v \mid \ell$ have the same local alternative for $\bar{\eta}$ because they are conjugate over $\mathbb{Q}$ and η is the restriction of a rational character. If their local character is nontrivial, the local trace is the sum of characters with distinct reductions, one trivial, and Theorem 5.1.2(1) of Pan applies. If they are all trivial, mark the local stable lines just constructed. For local elements σ, τ, the matrix $W(\tau) - \xi_2(\tau)I$ maps into the line with character ξ_1, where ξ_2 is the quotient character. Left multiplication by $W(\sigma) - \xi_1(\sigma)I$ kills this image. Taking the trace after any further matrix multiplication gives the ordered identity in Pan's Definition 5.3.2. His Theorem 6.1.2(1) therefore applies in this case. Both theorems give a ring finite over the product weight algebra, the completed tensor product over O of the completed group algebras of the pro-ℓ unit groups at $v \mid \ell$. All weight characters on the curve are trivial on those units by local reciprocity and unramifiedness. The map into the coefficient DVR kills the augmentation ideal of the weight algebra and the coefficient uniformizer. Its image is a finite domain over the residue field, hence a field of constants. This proves constancy of the traces of W, and restriction to G_L and addition of the trivial line prove the proposition. [7] □

Theorem 55.24 (The reducible trace quotient at twists divisible by $\ell - 1$)**.** *At every x of the same interval and every original character of sign $(-1)^r$, let $5 \le \ell \le L_*$ be prime to $2sN_*$. If $2 \le r < t(x)$ and $\ell - 1 \mid r$, the full reducible quotient T/I_m, $6 \le m \le 9$, is finite over O. This includes the scheme structure at the split trace and the case of repeated global residual characters. The corresponding quotient with the local characters of genuine flags adjoined is also finite over O.*

Proof. If $\bar{\Psi}|_{G_K}$ has order greater than two, Theorem 55.20 applies directly. In the remaining cases the proposition makes every restricted trace constant on each equal-characteristic curve through the split trace. Apply Lemma 55.22 with $G = G_K$ and $\Gamma = G_L$. Each original trace is constant. The rank characterization of I_m in the proof of Theorem 55.20 uses only dimensions of semisimple matrix spans, so those are exactly the curves that must be considered here.

If the complete Noetherian local special fiber had positive dimension, divide it by a prime of dimension one and normalize. This gives a complete DVR finite over a power series ring in one variable over a finite field. The map from the special fiber to this DVR has one-dimensional image, whereas every trace in the image is constant. The traces topologically generate and the coefficient residue field is finite, a contradiction. The special fiber is therefore Artinian. A power of the maximal ideal of T/I_m is contained in $\varpi(T/I_m)$; lifting a basis modulo ϖ and iterating the expansion proves module finiteness by completeness. This step retains nilpotent elements and coefficient torsion. For a genuine flag each local Frobenius character value is a root of the local characteristic polynomial. Successive monic division bounds the rank of the ordered-root algebra by six per place, with fixed inertia values, as in Corollary 55.21. This proves the last assertion. □

The field H works for the whole interval. The theorem proves finiteness at these weights. The bound in Section 6.6 requires a bound on the lengths of strict extension classes as the field, twist and coefficient prime vary, including their contributions on irreducible components.

55.7 A ramified plane at an inert coefficient prime

We return to the second congruence for coincident weights in Section 55.5. Suppose $\ell - 1 \mid 2r$ and $\ell - 1 \nmid r$, with $\ell \geq 5$ prime to $2sN_*$. Write $\omega = \bar{\kappa}_\ell$ and suppose the even character $\beta = \bar{\alpha}\omega^r$ has order two. Its restriction to inertia at ℓ is nontrivial. Indeed $r \equiv (\ell-1)/2 \bmod (\ell-1)$, α is unramified there and the local cyclotomic character maps inertia onto $\mathbb{F}_\ell^\times$. We shall impose $\eta_K(\ell) = -1$, so that K has a unique prime over ℓ.

Lemma 55.25 (The full decomposition group of the plane)**.** *Let P_0 be the absolutely irreducible plane in a reducible semisimple representation on an equal-characteristic curve of the symmetric trace problem. Suppose that its line constituent has residual character $\beta|_{G_K}$. At the unique place $w \mid \ell$ of K one has, after a finite coefficient extension,*

$$P_0|_{G_{K_w}} = 1 \oplus \beta|_{G_{K_w}} \quad \textit{up to isomorphism.}$$

Proof. The line is its constant residual lift. At ℓ, every inertia value is a root of the prescribed characteristic polynomial and all roots are constants in characteristic ℓ. At other places the inertia image is finite. After division by the residual character, the resulting principal-unit character factors through the finite class group, as in Theorem 55.20. The same argument gives determinant one for the entire representation. The plane thus has determinant $\beta|_{G_K}$ and residual semisimplification $1 \oplus \beta|_{G_K}$.

Write c_0 for the complex conjugation in the symmetric adjunction. The adjunction on the plane is symmetric by the skew-matrix argument in Proposition 55.23. With form matrix S and standard alternating matrix J_2, put $B = S^{-1}J_2$. The two-dimensional alternating identity gives

$$P_0(c_0 g c_0) = \beta(g)\, B P_0(g) B^{-1} \qquad (g \in G_K).$$

Consequently for any $h \in G_{\mathbb{Q}} \setminus G_K$, conjugation by h on the group arguments gives a representation isomorphic to βP_0. Changing c_0 to $h = g_0 c_0$ merely changes the intertwiner to $P_0(g_0)B$.

In a fixed rational decomposition group at ℓ, let D be G_{K_w} and I its inertia. The extension is unramified quadratic, so I is also the rational inertia group. Choose h in this rational decomposition group outside D. It belongs to the nontrivial global coset, normalizes D, I, and preserves $I_0 = \ker(\beta|_I)$. Every element of I_0 acts unipotently on the plane. If there is a nonidentity such element, the trace-two calculation in Lemma 55.19 gives a unique line fixed

by all of I_0. It is stable under I, with character either 1 or $\beta|_I$, since I/I_0 has order two. Conjugating the arguments by h preserves this character. Twisting by β changes it to the other character. The two representations of I would therefore be isomorphic with different characters on their unique I_0-fixed lines, a contradiction. Hence $P_0(I_0) = 1$.

The nontrivial coset of I/I_0 has distinct eigenvalues $1, -1$ on the plane by the original inertia polynomial after dividing out the line. The two eigenspaces are stable under D, which acts trivially on this order-two quotient. Thus $P_0|_D = \xi \oplus \beta\xi^{-1}$ with ξ unramified. Conjugation by h fixes ξ, as D/I lies in the abelian unramified quotient of the rational decomposition group. It fixes β as well. In βP_0 the unique unramified constituent is ξ^{-1}. The isomorphism on D gives $\xi^2 = 1$. Its reduction is the trivial constituent of $1 \oplus \beta|_D$, since the latter's other constituent ramifies on inertia. To see this directly on a stable lattice, the idempotents $(1 \pm P_0(i))/2$ for $i \in I \setminus I_0$ split it integrally. A quadratic character reducing to one in odd characteristic is trivial. This proves the formula on all of D. □

Lemma 55.26 (A finite twist of the polarized plane)**.** *There is a finite-order character θ of G_K with values of two-power order in a finite extension of the constant field such that $\theta^{c_0}/\theta = \beta|_{G_K}$. For the plane of Lemma 55.25, θP_0 extends to an odd representation W of $G_{\mathbb{Q}}$. Its residual representation is absolutely irreducible, is induced from θ over K, and has projective fixed field KH_β, where H_β is the real quadratic field cut out by β.*

Proof. Use the finite idèle class quotient $A = \mathbb{A}_{K,f}^{\times}/K^{\times}$. It is profinite. Indeed the valuations map it onto the finite ideal class group with open kernel $\widehat{\mathcal{O}}_K^{\times}/\mathcal{O}_K^{\times}$. The latter is profinite since an imaginary quadratic field has finite units. The diagonal $K^{\times}$ is closed in the finite idèles, since in each open fiber of the valuation map its intersection consists of the generators of a single fractional ideal and hence is finite. This gives the Hausdorff quotient used here. By class field theory, finite characters of A are characters of G_K. Restriction of β to G_K corresponds to $\beta \circ N_{K/\mathbb{Q}}$ on the idèles.

The c_0-fixed subgroup of A is the image of the rational finite idèles. To see this, if x represents a fixed class, $\overline{x}/x = b \in K^{\times}$ has norm one. Hilbert's Theorem 90 gives $b = \overline{y}/y$ for $y \in K^{\times}$. The idèle x/y is fixed in each conjugate system of local fields, hence is rational. On these fixed classes $\beta \circ N_{K/\mathbb{Q}}$ is trivial, since the norm of a rational idèle is its square. On the closed subgroup $D_0 = (c_0 - 1)A$ the rule

$$\overline{x}/x \longmapsto \beta(N_{K/\mathbb{Q}}x)$$

therefore defines a character. It is continuous since the continuous surjection from compact A to Hausdorff D_0 is a quotient map. Take an open subgroup U of A whose intersection with D_0 is in its kernel. Its character on the image of D_0 in A/U extends to the finite abelian group A/U with values of two-power order. For example, extend one cyclic quotient generator at a time. If its order modulo the previous subgroup is e, prescribe a value whose eth power is the value already assigned to its eth power. Every such root can be chosen in the group of all two-power roots of unity in $\overline{\mathbb{F}}_\ell$, since raising to any positive integer is surjective on that group. This gives θ and its asserted conjugation law.

The identity of Lemma 55.25 now says that $(\theta P_0)^{c_0}$ is conjugate to θP_0 by B. The matrix $B = S^{-1}J_2$ has trace zero and is invertible. Rescale it over a finite extension to have square one and determinant -1, and let c_0 act by this matrix. The semidirect product $G_{\mathbb{Q}} = G_K \rtimes \langle c_0 \rangle$ gives W, continuous and odd. Summing a G_K-stable lattice and its translate by c_0 supplies a stable lattice.

The two residual characters on G_K are $\theta, \theta\beta$. They are distinct and c_0 exchanges them. A reducible residual representation on $G_{\mathbb{Q}}$ would have two character factors, each with c_0-

invariant restriction to G_K. This proves absolute residual irreducibility. Its restriction to the normal subgroup is semisimple by the translate argument of Proposition 55.23. A vector on the θ-line and its translate by c_0 exhibit the induced representation. On G_K its projective kernel is $\ker\beta\cap G_K$, and each element outside G_K interchanges the two lines. This proves the field assertion. □

Theorem 55.27 (Finiteness at the ramified collision for inert primes)**.** *At every x on the original interval suppose $5\le\ell\le L_*$, $\ell\nmid 2sN_*$, $\eta_K(\ell)=-1$, $2\le r<t(x)$, $\ell-1\mid 2r$ and $\ell-1\nmid r$. Assume $\bar\alpha\neq 1$ and $\beta=\bar\alpha\omega^r$ has order two. Then T/I_m is a finite O-module for $6\le m\le 9$, also after adjoining the local characters of genuine flags. The auxiliary quadratic field K and the period fields are the ones fixed on the interval.*

Proof. It suffices to prove constancy on each equal-characteristic curve, by the special-fiber argument of Theorem 55.24. Each line constituent is its constant residual lift by the first paragraph of Lemma 55.25. If the representation is a sum of lines this proves the claim.

Suppose first that there is an irreducible plane and the line constituent is trivial. The plane has determinant one and the symmetric adjunction descends it to $G_{\mathbb{Q}}$ with odd determinant η_K, by the explicit intertwiner in Theorem 55.20. Twist the descended plane by the global constant β. Its determinant is still η_K and its residual characters are $1,\eta_K$. Indeed its residual constituents restrict semisimply to G_K where both factors are now trivial; each consequently factors through the order-two quotient. Inertia at ℓ is unipotent after this twist, since the two roots left on the plane before twisting were both β. Lemma 55.19 gives unramified local characters, with distinct reductions because $\eta_K(\ell)=-1$. Pan's Theorem 5.1.2(1) over $\mathbb{Q}$ gives finiteness over the ordinary weight algebra. The weight acts by augmentation on this curve, so its trace image is constant, as required. [7]

It remains to treat the line $\beta|_{G_K}$. Use W of Lemma 55.26. Its residual image has two-power order in the induced basis. We verify absolute irreducibility after restriction to $G_{\mathbb{Q}(\zeta_\ell)}$. The field KH_β is biquadratic. The fields K and its third quadratic subfield both ramify at s, since H_β is unramified there. Moreover $\bar\alpha=\beta\omega^{-r}$ is a nontrivial quadratic character of conductor prime to ℓs. It must ramify at some finite prime dividing N_*, since $\mathbb{Q}$ has no nontrivial everywhere finite-unramified quadratic extension. At that prime ω^r is unramified, so H_β ramifies there too. Thus none of the three quadratic fields is contained in $\mathbb{Q}(\zeta_\ell)$. Their compositum meets $\mathbb{Q}(\zeta_\ell)$ in $\mathbb{Q}$. The projective image of the restricted residual group is consequently still the full group of order four. It contains the nontrivial diagonal ratio and an element exchanging that diagonal element's two eigenlines. No line is stable under their lifts.

This restricted residual image is adequate. Indeed its order is prime to ℓ, so averaging kills its positive-degree cohomology, including with adjoint coefficients. Its invariant trace-zero endomorphism space vanishes by absolute irreducibility and $\ell\neq 2$. All group elements are semisimple. Their span over an algebraic closure is the full matrix algebra by absolute irreducibility, verifying the semisimple spanning condition for adequacy.

Choose a finite set of primes away from ℓ containing the other ramified primes of W, including any ramification of θ. The inertia group at ℓ equals the inertia group in K_w. By Lemma 55.25 its matrices in W have the two characters $\theta,\theta\beta$ and split over the fraction field. If an inertia element has trivial residual matrix, both constant character values are one, so the matrix itself is the identity. Hence the extension cut out by W over the residual fixed field is unramified above ℓ. This is the local condition in the unramified deformation ring of Allen and Calegari, which allows the residual representation itself to ramify at ℓ.

Apply their Theorem 1 over the totally real field $\mathbb{Q}$, with the residual field enlarged to contain the matrix entries. The representation is two-dimensional and odd, the prime is odd,

and adequacy over $\mathbb{Q}(\zeta_\ell)$ was just verified. Their unramified deformation ring, allowing the specified finite set away from ℓ, is finite over the Witt vectors of its residue field. After choosing an integral basis, W on our curve gives a specialization of that ring. Since the curve has characteristic ℓ, the image is contained in a finite field of constants. In particular its traces are constant. Restricting to G_K, undoing the constant twist and adjoining the constant line recovers the traces originally under consideration. This proves the assertion on curves. Completeness gives the integral finiteness, and the ordered roots of the local Frobenius polynomial give the assertion on flags as in Theorem 55.24. [21] □

The conductor hypothesis is used to keep all three quadratic subfields of the projective residual field outside $\mathbb{Q}(\zeta_\ell)$. Estimating the strict cohomology lengths on the entire interval still requires quantitative control on the corresponding integral deformation rings and their irreducible components.

55.8 The conductor of the character used in descent

The deformation argument in Theorem 55.27 uses a finite character θ of G_K. Its construction there leaves its conductor unspecified. We determine which primes are needed and bound the degree of the residual field. Throughout this subsection $K = \mathbb{Q}(\sqrt{-s})$ is the field of Proposition 36.3, c is its nontrivial automorphism and $\mathfrak{s} = (\sqrt{-s})$ is the prime above s. Write h_K for the ordinary class number.

Proposition 55.28 (The obstruction at the discriminant prime)**.** *Let M be a positive integer prime to s, and let β be an even quadratic Dirichlet character of conductor dividing M. Write β_K for its restriction to G_K, and put $\delta = 0$ if $\beta(s) = 1$ and $\delta = 1$ if $\beta(s) = -1$. There exists a finite character θ of two-power order satisfying*

$$\theta^c/\theta = \beta_K, \qquad \mathfrak{f}_\theta \mid \mathfrak{f} = (M)\mathfrak{s}^\delta.$$

A solution of conductor dividing (M) exists exactly when $\beta(s) = 1$. The character values can be taken in a finite extension of any field of odd positive characteristic.

Proof. Let $A = \mathrm{Cl}_{\mathfrak{f}}(K)$ be the group of fractional ideals prime to $\mathfrak{f}$ modulo the ideals (b) with $b \equiv 1 \bmod \mathfrak{f}$. The congruence is in the localizations at the primes dividing $\mathfrak{f}$. By the norm compatibility of Artin reciprocity, β_K acts on an ideal $\mathfrak{a}$ by $\beta(N_{K/\mathbb{Q}}\mathfrak{a})$. The value on a positive rational number prime to M is taken by reducing its numerator and denominator modulo M. This rule factors through A, since the norm of a generator congruent to one modulo (M) is one modulo M. We use reciprocity and the ray class exact sequence in their usual finite-modulus form. [22]

We prove that β_K is trivial on the classes fixed by c. Let $\mathfrak{a}$ represent such a class. Then $\bar{\mathfrak{a}}/\mathfrak{a} = (b)$ with $b \equiv 1 \bmod \mathfrak{f}$. Taking ideal norms gives $b\bar{b} = 1$, since the field norm is positive. Choose $y \in K^\times$ with $b = \bar{y}/y$ by Hilbert's Theorem 90. At a split prime $p \mid M$, the two valuations of y agree since b is a unit. An inert $p \mid M$ has one valuation, and every prime over M has ramification index one. We can therefore make y a unit at every prime over M by multiplying by a rational number with the prescribed valuations at the primes dividing M. If $\delta = 1$, write locally at $\mathfrak{s}$ $y = (\sqrt{-s})^j u$ with u a unit. Conjugation acts trivially on the residue field. Thus $\bar{y}/y \equiv (-1)^j \bmod \mathfrak{s}$. As s is odd and $b \equiv 1 \bmod \mathfrak{s}$, j is even. Multiplication by $s^{-j/2}$ makes y a unit at $\mathfrak{s}$ also. Rational rescalings preserve $\bar{y}/y$.

The residue of y modulo (M) is now a unit fixed by c. It lies in the image of $(\mathbb{Z}/M\mathbb{Z})^\times$. Indeed, $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}(1 + \sqrt{-s})/2$, and the difference between the second basis element and its conjugate is $\sqrt{-s}$, a unit modulo (M). Comparing the two coefficients forces the second

coefficient of a fixed residue to vanish modulo M. This applies to y by clearing denominators prime to M. Hence $y\bar{y}$ is a square unit modulo M, and $\beta(N(y)) = 1$.

The ideal $\mathfrak{b} = \mathfrak{a}/(y)$ is fixed by conjugation. Its split prime factors occur with equal conjugate exponents. Each inert prime has square norm. Hence its norm is a rational square times a power of s. When $\delta = 1$, this last exponent vanishes because $\mathfrak{b}$ is prime to $\mathfrak{s}$. When $\delta = 0$, $\beta(s) = 1$. It follows that $\beta_K(\mathfrak{a}) = 1$.

On the subgroup $D = \{\bar{a}/a : a \in A\}$ the rule $\bar{a}/a \mapsto \beta_K(a)$ is therefore a well-defined homomorphism. Extend it to A one cyclic quotient generator at a time. For a generator of order d modulo the current subgroup, its value must have d-th power equal to a prescribed two-power root of unity. Such a root exists among the two-power roots of unity in the algebraic closure of any field of odd characteristic. The resulting character of the finite group A has precisely the required quotient under c. Class field theory gives $\mathfrak{f}_\theta \mid \mathfrak{f}$.

For necessity, work in the ray group of (M) alone. The ideal $\mathfrak{s}$ is prime to (M) and fixed by conjugation. Every quotient θ^c/θ on this group takes value one on its class. The value of β_K there is $\beta(N\mathfrak{s}) = \beta(s)$. This proves the equivalence. □

Theorem 55.29 (Ramification and degree on the period interval)**.** *Under the hypotheses of Theorem 55.27, put $M = N_*\ell$. For the character just constructed, let $\bar{W} = \operatorname{Ind}_{G_K}^{G_{\mathbb{Q}}} \theta$ and let $F_{\bar{W}}$ be the fixed field of its kernel. Its Artin conductor $C(\bar{W})$ and field degree satisfy*

$$C(\bar{W}) \mid s^{1+\delta} M^2, \qquad [F_{\bar{W}} : \mathbb{Q}] \le 2h_K (s-1)^\delta M^2.$$

The exponents of s and ℓ in $C(\bar{W})$ are exactly $1+\delta$ and 2, respectively. On inertia over ℓ the character θ has exact order $2^{1+v_2(\ell-1)}$.

Proof. The character $\bar{\alpha}$ has conductor dividing N_* and ω^r is quadratic of conductor ℓ. Thus M is a multiple of the conductor of β and $v_\ell(M) = 1$. Use Proposition 55.28. The ray class field $K_{\mathfrak{f}}$ is stable under c because its defining modulus is stable. Both θ and θ^c factor through $\mathrm{Gal}(K_{\mathfrak{f}}/K)$. The restriction of $\bar{W}$ to G_K is their direct sum, so $F_{\bar{W}} \subset K_{\mathfrak{f}}$. The ray class exact sequence bounds its degree by

$$2|\mathrm{Cl}_{\mathfrak{f}}(K)| \le 2h_K |(\mathcal{O}_K/\mathfrak{f})^\times| \le 2h_K M^2 (s-1)^\delta.$$

Here $|\mathcal{O}_K/(M)| = M^2$, and the residue field of $\mathfrak{s}$ has s elements.

We compute the conductor using the finite complex lifts of the two-power roots of unity. The kernel on every subgroup is the same in the induced bases in both characteristics, and the inertia characters may be computed with either realization. At a split prime $p \mid M$, the local representation is the sum of the two characters at the primes over p. Each conductor exponent is at most $v_p(M)$. At an inert $p \mid M$ the quadratic base change is unramified. Its inertia and higher ramification groups agree with those over $\mathbb{Q}_p$. On these groups $\bar{W}$ again restricts to two characters, both of conductor exponent at most $v_p(M)$. In either case their exponents add, giving at most $2v_p(M)$. Every prime outside sM is unramified.

At ℓ, inertia for θ factors by local reciprocity through $\mathbb{F}_{\ell^2}^\times$. For a generator u of this group, c sends u to u^ℓ, and its norm generates $\mathbb{F}_\ell^\times$. The restriction of β to rational local units is the nontrivial quadratic character there. Consequently

$$\theta(u)^{\ell-1} = (\theta^c/\theta)(u) = -1.$$

For a root of unity of two-power order this equation fixes its order to be $2^{1+v_2(\ell-1)}$. Both inertial summands are nontrivial and tame, giving conductor exponent two.

At s the inertia image is tame since s is odd and the induced image is a two-group. If $\delta = 0$, inertia over $K_{\mathfrak{s}}$ acts trivially. Rational inertia maps onto the quadratic quotient and exchanges the induced lines. Its nontrivial image is an involution with eigenvalues $1, -1$, so the fixed subspace has dimension one. If $\delta = 1$, θ must ramify at $\mathfrak{s}$, by necessity in Proposition 55.28. Its inertia character factors through $\mathbb{F}_s^\times$, on which conjugation acts trivially. Some element of inertia over $K_{\mathfrak{s}}$ acts on both lines by the same nontrivial scalar. The fixed subspace has dimension zero. In the tame case the conductor exponent is the codimension of the fixed subspace, proving the asserted exponent at s. □

Corollary 55.30 (One ray field for all points of the interval)**.** *For each eligible $\ell \le L_*$ both $C(\bar{W})$ and $[F_{\bar{W}} : \mathbb{Q}]$ are bounded by a fixed power of V, uniformly in $x \in [V, V^{3/2}]$, r and α. There is also one explicitly bounded auxiliary field containing these residual fields for all the eligible primes together.*

Proof. The prime s and its field are fixed by Proposition 36.3. The estimates there and in Lemma 46.1 bound N_* and L_* by fixed powers of V. Apply Theorem 55.29. For the simultaneous assertion take the set $\mathcal{L}$ of all primes $5 \le \ell \le L_*$ inert in K and prime to $2sN_*$. Put $P = \prod_{\ell \in \mathcal{L}} \ell$, using $P = 1$ for the empty set. Every modulus used above divides $\mathfrak{F} = (N_*P)\mathfrak{s}$. Functoriality of ray class fields embeds all $F_{\bar{W}}$ in $K_{\mathfrak{F}}$. Since $P \le \max(2, L_*)^{L_*}$, the same ray class estimate gives

$$\log[K_{\mathfrak{F}} : \mathbb{Q}] \le \log\bigl(2h_K(s-1)\bigr) + 2\log N_* + 2L_* \log\max(2, L_*).$$

All these constructions use the N_* of the original interval and the character $\bar{\alpha}$ of the actual E_x. □

The bounds control the residual representations entering the deformation argument. The length of a strict cohomology group also depends on how far its classes lift through powers of ℓ. Bounding those lifts and comparing the integral projected theta periods over E_x remain necessary for Section 6.6.

55.9 Reducible traces for every pair of colliding weights

There are two ways that the residual characters on the plane behave at a coefficient prime. At a split prime its decomposition group preserves a line. At an inert prime the two characters on inertia are exchanged after descent to $\mathbb{Q}$, and the entire local trace is prescribed. We use these facts to treat the remaining reducible quotients of Section 55.5.

Lemma 55.31 (Local characters after quadratic descent)**.** *Suppose $5 \le \ell \le L_*$, $\ell \nmid 2sN_*$, $\ell - 1 \mid 2r$, and $\ell - 1 \nmid r$. Suppose the even character $\beta = \bar{\alpha}\omega^r$ is quadratic. On an equal-characteristic curve of the reducible trace quotient, let P be the absolutely irreducible plane accompanying the line β_K. Choose θ by Proposition 55.28 with $M = N_*\ell$. There is an odd extension W of θP to $G_{\mathbb{Q}}$, with absolutely irreducible residual representation $\operatorname{Ind}_{G_K}^{G_{\mathbb{Q}}} \theta$.*

If ℓ splits in K, $W|_{G_{\mathbb{Q}_\ell}}$ has a stable line. The characters on the line and the quotient are trivial on principal units under local reciprocity. If ℓ is inert, then, for the unique $w \mid \ell$,

$$W|_{G_{\mathbb{Q}_\ell}} \simeq \operatorname{Ind}_{G_{K_w}}^{G_{\mathbb{Q}_\ell}} (\theta|_{G_{K_w}}).$$

In particular every trace on this rational decomposition group is a constant in the coefficient DVR.

Proof. The character and determinant argument in Theorem 55.20 gives the line β_K and $\det P = \beta_K$. The residual characters of P are $1, \beta_K$. They are distinct because β_K ramifies over ℓ. With the symmetric plane form S and alternating matrix J_2, put $B = S^{-1}J_2$. Polarization gives $P(cgc) = \beta_K(g)BP(g)B^{-1}$ for a complex conjugation c. Together with $\theta^c/\theta = \beta_K$, this makes B an intertwiner for θP and its conjugate. The trace of B is zero and B is invertible. Scaling it over a finite coefficient extension to square one makes it an involution of determinant -1. Giving c this action defines W. The sum of a stable lattice over K and its translate by c is a stable lattice over $\mathbb{Q}$. The two distinct residual characters θ, θ^c on G_K are exchanged by c. A residual stable line over an algebraic closure would restrict to a character fixed by c, which is impossible. The restriction of this irreducible residual representation to the index-two subgroup is semisimple because the translates of a simple submodule span the representation. Taking a nonzero vector on the θ-line and its translate by c gives the induced residual representation.

First suppose ℓ splits. Identify $D = G_{\mathbb{Q}_\ell}$ with the decomposition group at one of the two primes in K. Let I denote inertia and let $I_0 = \ker(\beta|_I)$. The characteristic polynomial for $P(i)$ has roots $1, \beta(i)$ for every $i \in I$. Every element of I_0 thus acts unipotently. If some $g \in I_0$ acts nontrivially, write $P(g) = 1 + E_{12}$ in a basis. For every $h \in I_0$, the equality $\operatorname{tr} P(gh) = \operatorname{tr} P(h) = 2$ forces $P(h)_{21} = 0$. The common fixed space is exactly the first line. Normality of I_0 in D preserves that line. If $P(I_0) = 1$, the inertia image has order two with distinct eigenvalues. The decomposition group acts trivially on the quotient I/I_0, so both eigenlines are stable. On any of the lines obtained this way the inertia character and its quotient factor through I/I_0. Twisting by the finite two-power character θ preserves triviality of both characters on wild inertia. The principal units correspond to the image of wild inertia under local reciprocity. Intersect the stable line with the integral lattice. The intersection is saturated, so both characters are integral.

If ℓ is inert, Lemma 55.25 gives $P|_{G_{K_w}} = 1 \oplus \beta$. Consequently W has the two characters $\theta, \theta\beta$ on G_{K_w}, which are already distinct on inertia. An element h outside G_{K_w} in $G_{\mathbb{Q}_\ell}$ interchanges the two lines, since its conjugation sends θ to $\theta\beta$. In the basis $v, W(h)v$ with v on the θ-line, G_{K_w} acts diagonally and $W(h)^2 v = \theta(h^2)v$. These are precisely the matrices of the stated induction. Every element outside G_{K_w} has trace zero, and the two characters inside it are constant. This proves the assertion. □

Theorem 55.32 (Finiteness of the reducible quotient at every collision)**.** *For every $x \in [V, V^{3/2}]$ on the original intervals, take any of the characters of E_x of sign $(-1)^r$. Suppose*

$$5 \le \ell \le L_*, \qquad \ell \nmid 2sN_*, \qquad 2 \le r < t(x), \qquad \ell - 1 \mid 2r.$$

For each $6 \le m \le 9$, the entire reducible trace quotient T/I_m of Section 55.5 is finite as an $\mathcal{O}$-module. This holds also after adjoining the local characters of actual ordinary flags.

Proof. If $\ell - 1 \mid r$, apply Theorem 55.24. Let $\ell - 1 \nmid r$. The character $\beta = \bar{\alpha}\omega^r$ is even and has order two on inertia at ℓ. Its fixed field is totally real, hence disjoint from the imaginary quadratic K. Its order on G_K equals its global order. If that order exceeds two, apply Theorem 55.20. It remains to treat a quadratic β, allowing $\bar{\alpha} = 1$.

Take a semisimple realization over the fraction field of a complete DVR finite over $k[[z]]$, enlarging that field to split the constituents as in that theorem. Every line constituent is its constant residual lift. This settles a sum of three lines. For a line and an absolutely irreducible plane the line must be 1 or β_K. If it is 1, odd descent of the determinant-one plane gives a rational representation with determinant η_K. Twist by β. Its residual semisimplification restricts trivially to G_K, so has characters $1, \eta_K$, by its determinant. Its local inertia is unipotent, since

the two inertial roots before twisting both equal β. Lemma 55.19 supplies a stable line and unramified characters. With fixed odd determinant η_K the ordinary pseudodeformation theorem of Pan applies over $\mathbb{Q}$. Use his Theorem 5.1.2(1) if η_K is nontrivial at ℓ, and Theorem 6.1.2(1) with the actual line if η_K is locally trivial. The weight evaluates at augmentation, so its finite algebra has constant image on the curve. This gives constant traces on the plane after undoing the twist. [7]

For the line β_K, take W from Lemma 55.31. We use two finiteness results of Zhang over $\mathbb{Q}$, stated in Appendix A of the cited preprint. We give the relevant local and global hypotheses here. Choose the finite set Σ to include ℓ and every finite prime ramifying in W. The residual representation $\bar{W}$ of $G_{\mathbb{Q},\Sigma}$ is continuous, odd and absolutely irreducible. Enlarge the finite residue field to contain its entries. The determinant of W is constant on G_K, where it is $\theta^2\beta_K$, and on the second coset it is determined by $\det W(c) = -1$. Consequently it is the constant residual determinant on the whole group. For the characteristic-zero fixed-determinant deformation problem we may take the determinant of a regular modular lift of $\bar{W}$ as in Zhang, enlarging Σ to include its ramification. Such a lift is supplied by Serre’s modularity theorem in the form used there. On an equal-characteristic curve every lift of the fixed determinant reduces to this same constant character. Thus W in an integral basis is a point of the specified deformation problem.

At a split prime let ξ_1, ξ_2 be the actual characters on the integral line and the quotient from the lemma. Their reductions are distinct on inertia. For $\sigma, \tau \in G_{\mathbb{Q}_\ell}$ we have

$$\operatorname{tr} W = \xi_1 + \xi_2 \ \text{ on } G_{\mathbb{Q}_\ell}, \qquad (W(\sigma) - \xi_1(\sigma) I)(W(\tau) - \xi_2(\tau) I) = 0.$$

The factor on the right maps into the stable line, which the left factor kills. These are exactly the equations defining the ordinary deformation ring with the specified residual subcharacter. Zhang’s Theorem A.3.1 makes this ring finite over $O[[1 + \ell\mathbb{Z}_\ell]]$, with weight given by ξ_1 on principal units. The lemma makes this weight trivial. Modulo the coefficient uniformizer and the weight augmentation ideal the ring is a finite-dimensional algebra over a finite field. Its image in the coefficient DVR is a finite domain and hence a field of constants. [23]

At an inert prime apply Zhang’s Proposition A.1.4. It says that the global fixed-determinant deformation ring for $\bar{W}$, allowing the finite set Σ, is finite over the local fixed-determinant pseudodeformation ring at ℓ. By the lemma the local trace equals its residual trace on the full rational decomposition group, including Frobenius elements outside G_{K_w}. In dimension two with 2 invertible, trace and fixed determinant determine the local pseudorepresentation. Its map to the curve therefore factors through the residue field. Finiteness again forces every global trace to be constant. For $\bar{\alpha} \neq 1$ this conclusion also follows from the separate argument in Theorem 55.27. [23]

In both cases restrict W back to G_K, divide out the constant twist and adjoin the constant line character. Every trace of the original representation is constant on every equal-characteristic curve of T/I_m. A positive-dimensional special fiber would have a one-dimensional complete domain quotient and a finite DVR normalization on which the traces generate a positive-dimensional image. Thus the special fiber is Artinian. Lifting a basis and using completeness gives finiteness over O, including nilpotents and torsion. The flag assertion follows from Corollary 55.21 because the ordered Frobenius values are successively integral by monic division and their inertia values are prescribed. □

The theorem applies at all the stated coefficient primes on the original interval. Its proof gives finiteness at each weight. The sum in Proposition 6.11 requires a quantitative bound on integral lengths, including contributions where reducible and irreducible components meet.

55.10 Conductor bounds at the two colliding residues

Let $E = E_x$ be the period field at a point of the interval of Section 6.6, and let N_* be the conductor modulus for that interval. Write $\ell \geq 5$ for a prime. Let α be a character of $E/\mathbb{Q}$ of order d and primitive conductor C, where $\ell \nmid dC$. Take $1 \leq r < t(x)$ with $\alpha(c) = (-1)^r$. We treat the two residues $r \equiv 0, (\ell-1)/2 \bmod \ell - 1$ in Corollary 54.14. The scalar strict group $S(\alpha, r)$ and its subgroup $S^{N_*}(\alpha, r)$ are defined in Section 22.13. The former uses divisible coefficients, zero localization at ℓ, and unramified classes at every other finite prime.

Put $O = \mathbb{Z}_\ell[\alpha]$, let J be its fraction field, and write $k = O/\ell O$. Since d is prime to ℓ, O is unramified and reduction is faithful on $\alpha(G_\mathbb{Q})$. Write $\theta = \alpha^{-1}\kappa_\ell^{-r}$, $D = (J/O)(\theta)$, and $\tau = \bar{\alpha}^{-1}\omega_\ell^{-r}$, where ω_ℓ is the reduction of the cyclotomic character. Let L be the fixed field of $\ker \tau$ and let $\Delta = \mathrm{Gal}(L/\mathbb{Q})$. This is a cyclic group of order m prime to ℓ. The parity condition makes L totally real. When $m > 1$, put $f = \mathrm{ord}_m(\ell)$.

Lemma 55.33 (A class number divisor at a nonsplit coefficient prime)**.** *Suppose that τ is nontrivial on a decomposition group at ℓ. If $S(\alpha, r) \neq 0$, then*

$$\ell^f \;\mid\; \left|\mathrm{Cl}(L)/\langle [\lambda] : \lambda \mid \ell \rangle\right|.$$

Proof. Every continuous cocycle with values in D has finite image by compactness. A nonzero element of the strict group therefore has a multiple of order ℓ. Both $D^{G_\mathbb{Q}}$ and $D^{G_{\mathbb{Q}_\ell}}$ are zero since some local element acts by a scalar whose difference from one is a unit. The exact sequence for multiplication by ℓ on D now lifts the element of order ℓ uniquely to a class with values in $k(\tau) = D[\ell]$. Its localization at ℓ is zero with these finite coefficients by the same exact sequence locally.

On G_L a cocycle of this finite class is a homomorphism u. It is nonzero, since inflation from Δ has zero source by averaging over m. Away from ℓ, the divisible cocycle on inertia is a coboundary. On inertia intersected with G_L, $\kappa_\ell = 1$ and $\bar{\alpha} = 1$, so also $\alpha = 1$. There the coboundary is zero and hence so is u. At every place over ℓ the finite cocycle itself is locally a coboundary, so u is zero on the whole decomposition group over L. Global class field theory thus factors u through the class group in the statement. At real places an odd-order quotient kills complex conjugation, so the ordinary class group suffices.

For $g \in G_\mathbb{Q}$ and $h \in G_L$, the cocycle formula gives $u(ghg^{-1}) = \tau(g)u(h)$. Its nonzero image in the additive group of k is consequently stable under the field generated by the m-th roots in $\tau(G_\mathbb{Q})$ over $\mathbf{F}_\ell$. This field has degree f, since a primitive m-th root lies in $\mathbf{F}_{\ell^a}$ exactly when $m \mid \ell^a - 1$. The image has order a positive power of ℓ^f, proving the divisibility. □

Theorem 55.34 (A conductor test at a colliding residue)**.** *At $r \equiv (\ell-1)/2 \bmod \ell - 1$, set $e = 2$ and $m = \mathrm{lcm}(d, 2)$. At $r \equiv 0 \bmod \ell - 1$, suppose $\alpha(\ell) \neq 1$ and set $e = 1$, $m = d$. In either case put*

$$Y = \max\left\{1, \frac{m!}{m^m}\, C^{(m-1)/2}\ell^{m(1-1/e)/2}\right\}.$$

If $\ell^f > Y(1 + \log Y)^{m-1}$, then $S(\alpha, r) = 0$. At the zero residue $\ell \nmid |\mathrm{Cl}(L)|$ also suffices, and there L is the field cut out by α.

Proof. At the half residue the residual cyclotomic factor is the quadratic character of conductor ℓ. The Chinese remainder theorem allows the arguments of this character and of α to vary independently modulo ℓ and C. Thus their product has image of order $\mathrm{lcm}(d, 2)$, and the inertia group at ℓ has order two. At the zero residue the cyclotomic factor is trivial, and $\alpha(\ell) \neq 1$ gives nontrivial decomposition group at ℓ. These observations verify the local hypothesis of Lemma 55.33 in both cases.

The characters of L are the powers of the finite character τ, after lifting its values to roots of unity. Their prime-to-ℓ conductors divide C, and the trivial one has conductor one. Exactly $m(1-1/e)$ of the characters are nontrivial on inertia at ℓ, all of conductor exponent one there. The conductor–discriminant formula gives

$$|\operatorname{disc} L| \le C^{m-1}\ell^{m(1-1/e)}.$$

Minkowski's ideal class bound for a totally real field supplies an integral ideal of norm at most Y in each class. The number of ideals of norm n is at most $d_m(n)$, the number of ordered positive factorizations of n into m factors. Indeed at a rational prime the Euler factor for each prime above it is coefficientwise at most $(1-X)^{-1}$, and there are at most m such primes. After fixing the first $m-1$ factors, the number of choices for the last one is at most Y divided by their product. Enlarging the first $m-1$ sums to $[1,Y]$ and bounding the harmonic sum by $1+\log Y$ proves

$$|\operatorname{Cl}(L)| \le Y(1+\log Y)^{m-1}.$$

Each stated condition is now incompatible with the divisibility from the lemma. □

Corollary 55.35 (Quadratic and prime-order characters on the period intervals)**.** *At the half residue every quadratic α of the specified parity has $S(\alpha,r)=0$ if*

$$\ell > 4N_*(1+\log(2N_*))^2.$$

More generally fix $m=\operatorname{lcm}(d,2)$ and suppose $\operatorname{ord}_m(\ell) > m/4$. There is an effective constant K_m such that $\ell > K_m(2N_*)^{4m}$ gives the same conclusion for every such α, r, x. For an odd prime order d this includes all $\ell \equiv 1 \bmod 4$ which are primitive roots modulo d and satisfy this bound. For cubic characters these primes are $\ell \equiv 5 \bmod 12$. Whenever $\ell \nmid [E_x:\mathbb{Q}]$, the indicated summands have length zero in the original period-field cohomology.

Proof. For $d=2$ we have $m=2$, $f=1$. A nontrivial quadratic character has $C \ge 3$, so $Y=\sqrt{C\ell}/2>1$. With $H=1+\log(2C)$, at the real value $\ell_0=4CH^2$ the ratio $Y(1+\log Y)/\ell_0$ equals $(1+\log C+\log H)/(4H)<1$. Here $1+\log C<H$ and $\log H<H$. As a function of $\ell \ge \ell_0$ the ratio decreases, since it is a positive constant times $(1+\log Y)/Y$. Apply the theorem and use $C \le N_*$.

For general $m \ge 2$, let B_m be the maximum of $(1+z)^{m-1}\exp(-z/(2m))$ for $z \ge 0$. This is an effectively computable finite number. The ideal count is at most

$$B_m Y^{\,1+1/(2m)} \;\le\; B_m N_*^{\,m/2}\ell^{\,m/4+1/8},$$

because $Y \le N_*^{(m-1)/2}\ell^{m/4}$ and $(m-1)(1+1/(2m)) < m$. The integer $f > m/4$ satisfies $f \ge m/4+1/4$. Thus $K_m = B_m^8$ suffices. If d is an odd prime, $m=2d$ and a primitive root $\ell \bmod d$ has $f=d-1>d/2$. Such a character is even, and $\ell \equiv 1 \bmod 4$ makes the half residue even. When $d=3$ the extra congruence is $\ell \equiv 2 \bmod 3$.

The bounds use the common modulus N_*, so they hold simultaneously on the prescribed interval for all positive twists in the stated residue. Vanishing of S implies vanishing of its subgroup S^{N_*}. The character length identity of Theorem 22.17 identifies the stated zero terms when the field degree is prime to ℓ. □

The zero residue with $\alpha(\ell)=1$ has a different local condition. At the half residue the estimates above still leave coefficient primes below the conductor bound and characters for which the residue degree is small. These terms occur in the weighted sum of Section 6.6.

56 Exceptional weights in the cyclotomic tower

56.1 Uniform exponent bounds for characters of growing order

Keep $\alpha, C, \ell, r, L, m, f$ from Section 55.10. The bounds here use the primitive conductor C of the individual character. In particular, conductor factors belonging to a different character of E_x do not enter the estimate.

Lemma 56.1 (The class number divisor at higher levels)**.** *Suppose τ is nontrivial on a decomposition group at ℓ. For $1 \le a \le 1 + v_\ell(r)$, an element of order ℓ^a in $S(\alpha, r)$ implies*

$$\ell^{af} \mid |\mathrm{Cl}(L)/\langle [\lambda] : \lambda \mid \ell \rangle| .$$

Proof. Let $\widetilde{\tau}$ be the lift of τ to a character of order m with values in $O^\times$. For an ℓ-adic unit, the quotient by the root of unity lifting its residue is in $1 + \ell\mathbb{Z}_\ell$ when the unit is in $\mathbb{Z}_\ell^\times$. By the binomial theorem an ℓ-th power increases the congruence depth in this subgroup by at least one. Applying this to the cyclotomic character gives $\theta \bmod \ell^a = \widetilde{\tau} \bmod \ell^a$ through the stated depth. In particular G_L acts trivially on $D[\ell^a]$.

The global and local invariants of D at $\mathbb{Q}$ and $\mathbb{Q}_\ell$ vanish by the unit difference in the proof of Lemma 55.33. The finite lift of an element of order ℓ^a is unique and is locally zero at ℓ. Restriction to G_L is injective on its global finite cohomology group by averaging over Δ. Hence the restricted homomorphism has exact additive order ℓ^a. As in that lemma it kills all inertia away from ℓ and all decomposition groups over ℓ. Away from ℓ this uses that $\theta = 1$ on inertia intersected with G_L even for the divisible coefficients.

Identify the target with $O/\ell^a O$. A value of exact order ℓ^a is represented by a unit in O. By equivariance, its multiples by $\mathbb{Z}_\ell[\widetilde{\tau}(\Delta)]$ lie in the image. This ring is the ring of integers of the unramified extension of degree f. Indeed a primitive m-th root modulo ℓ generates the field of ℓ^f elements, and the roots of $X^m - 1$ lift uniquely. The ring modulo ℓ^a has cardinality ℓ^{af}, and multiplication by the unit value embeds it in the image. This proves the divisibility. □

Theorem 56.2 (Conductor thresholds independent of the character order)**.** *Let $1 \le a \le 1 + v_\ell(r)$. Either of the following conditions implies $\ell^{a-1} S(\alpha, r) = 0$.*

1. *At $r \equiv (\ell - 1)/2 \bmod \ell - 1$, one has $af \ge m/2$ and $\ell > 4096 C^4$.*
2. *At $r \equiv 0 \bmod \ell - 1$, one has $\alpha(\ell) \ne 1$, $af \ge m/4$, and $\ell > 256 C^{8/3}$.*

For $\ell \le P(x)$ prime to $[E_x : \mathbb{Q}]$, each indicated character component contributes zero to $R_{\ell,r}$ on sufficiently distant original intervals.

Proof. Let $e = 2$ at the half residue and $e = 1$ at the zero residue. Use the discriminant bound of Theorem 55.34 and Minkowski's theorem. Every class has an integral representative of norm at most $Y_0 = C^{(m-1)/2} \ell^{m(1-1/e)/2}$. For every integral ideal with norm at most Y_0, its contribution to $Y_0^{4/3} \zeta_L(4/3)$ is at least one. The Euler factor comparison with m copies of the rational zeta function gives $\zeta_L(4/3) \le \zeta(4/3)^m \le 4^m$, using $1 + \int_1^\infty u^{-4/3}\, du = 4$. Consequently

$$|\mathrm{Cl}(L)|^{1/m} \le 4 C^{2/3} \ell^{2(1-1/e)/3}.$$

In the first case the right hand side is less than $\ell^{1/2}$; in the second it is less than $\ell^{1/4}$. In each case $|\mathrm{Cl}(L)| < \ell^{af}$. The local hypotheses of Lemma 56.1 hold by Theorem 55.34. Any element of order at least ℓ^a in an ℓ-primary torsion group has a multiple of order precisely ℓ^a. The lemma therefore proves the exponent bound, including vanishing when $a = 1$.

For the application, $a-1 \le v_\ell(r) \le \log_2 t(x)$. This is smaller than $b_0(x) = \lfloor \exp(x^\varepsilon/8) \rfloor$ for all sufficiently large x, since $t(x) = \lfloor x^{401} \rfloor$. The bound passes to S^{N_*}. At primes prime to the field degree, descent after unramified extension of coefficients identifies these scalar groups with the character components of the strict group over E_x. This is the prime-to-degree decomposition used in Theorem 22.17 and in Lemma 24.8. The quotient by the subgroup killed by ℓ^{b_0} therefore has zero component there. □

Corollary 56.3 (Half and zero residues in the growing real dyadic tower)**.** *In Section 6.6 let l be the least integer with $2^l \ge x^{2+8\varepsilon}$, and take a faithful character α of $C_l = \mathbb{Q}(\zeta_{2^{l+2}})^+$, inflated to E_x. For every sufficiently large x on the stated intervals and every prime $\ell \equiv 5 \bmod 8$ in $[x^{16}, 2x^{16}]$ the following hold for $1 \le r < t(x)$.*

1. *If $\ell - 1 \mid r$, then $S(\alpha, r) = 0$.*
2. *If $r \equiv (\ell-1)/2 \bmod \ell - 1$ and $\ell \mid r$, then $\ell S(\alpha, r) = 0$.*

Both sets of twists occur on each interval and these components give zero in the truncated cohomology $R_{\ell,r}$.

Proof. The character has order $m = 2^l$ and conductor $C = 2^{l+2}$: faithfulness prevents descent to the preceding dyadic level. Thus $C < 8x^{2+8\varepsilon}$. Since $0 < \varepsilon < 1/52$, both conductor thresholds in Theorem 56.2 are below x^{16} for large x. For $\ell \equiv 5 \bmod 8$ one has $v_2(\ell - 1) = 2$, and for every $j \ge 0$, $v_2(\ell^{2^j} - 1) = j + 2$. Indeed each successive squaring introduces a factor $\ell^{2^j} + 1$ of valuation one. Odd powers preserve the valuation. It follows that $\mathrm{ord}_{2^l}(\ell) = 2^{l-2} = m/4$ for $l \ge 3$. The class of ℓ modulo 2^{l+2} differs from both 1 and -1 already modulo eight. Its Frobenius in C_l is nontrivial, so $\alpha(\ell) \ne 1$.

Take $a = 1$ at the zero residue and $a = 2$ at the half residue with $\ell \mid r$. The ramification and parity conditions hold since C is a power of two, α is even and $(\ell-1)/2$ is even. The odd part of the degree of E_x divides $[K_\psi : \mathbb{Q}]$, independently of x, and $2x^{16} < P(x)$ for large x. This verifies the remaining hypotheses.

The prime number theorem for the fixed progression 5 mod 8 gives primes throughout the indicated dyadic range for large x. For each such prime the two types occur already at $r = \ell - 1$ and $r = \ell(\ell-1)/2$, respectively, which are positive and less than $t(x)$. Both exceed $x^{\varepsilon/128}$ and ℓ exceeds the fixed primes in Π. Hence the field average $J_{\ell,r}$ from Section 6.6 is zero at these examples. Their elimination follows from the scalar cohomology bounds themselves. □

56.2 A single possible character orbit in a dyadic layer

Fix a character α as in Section 55.10. Choose one of the two residues there, with $\alpha(\ell) \ne 1$ in the zero residue. For a twist r in that residue of the required parity, write $\tau = \bar{\alpha}^{-1}\omega_\ell^{-r}$ as before. The field L cut out by τ depends only on the residue, α and ℓ. Let H be the ℓ-primary subgroup of $\mathrm{Cl}(L)/\langle [\lambda] : \lambda \mid \ell \rangle$. Its $\Delta = \mathrm{Gal}(L/\mathbb{Q})$-action will keep track of the characters simultaneously.

Lemma 56.4 (Faithful characters of the same residual field)**.** *As β ranges over the generators of the cyclic character group $\langle \alpha \rangle$, its residual twists in this residue range bijectively over all faithful characters of Δ. The correspondence commutes with raising character values to the ℓ-th power. Their coefficient rings are all isomorphic to the ring of integers of the unramified extension of $\mathbb{Q}_\ell$ of degree $f = \mathrm{ord}_m(\ell)$, where $m = |\Delta|$.*

Proof. In the zero residue $m = d = \mathrm{ord}(\alpha)$ and the correspondence sends α^u to τ^u for every u prime to d. In the half residue the cyclotomic factor has order two. If d is even, every u prime

to d is odd. If d is odd, each unit modulo d has exactly one odd lift modulo $2d$. Thus in both cases the units $u \bmod m$, $m = \operatorname{lcm}(2, d)$, give all generators once and preserve the quadratic factor when raising τ to the u-th power. Also ℓ is odd, which gives equivariance. The groups of d-th and m-th roots generate the same coefficient ring since adjoining a sign does not enlarge it. Its residue degree is f by lifting roots of unity of order prime to ℓ. The hypotheses exclude $m = 1$. □

For each orbit $\mathcal{O}$ of the faithful residual characters under the ℓ-th power map, choose a representative $\beta_{\mathcal{O}}$ on E_x by the lemma. Write O for its coefficient ring, using an embedding for each choice. The module length in the next formula is the length over this ring. Twists need only have the same residue and parity.

Theorem 56.5 (A simultaneous class group bound for different twists)**.** *For each $\mathcal{O}$ choose a positive twist $r_{\mathcal{O}}$ in the fixed residue and a depth $1 \le a_{\mathcal{O}} \le 1 + v_\ell(r_{\mathcal{O}})$. Then*

$$f \sum_{\mathcal{O}} \operatorname{length}_O(S(\beta_{\mathcal{O}}, r_{\mathcal{O}})[\ell^{a_{\mathcal{O}}}]) \;\le\; v_\ell(|H|).$$

In fact the finite group in each summand is dual, at this depth, to the $\mathcal{O}$-component of H.

Proof. Fix an orbit and its β, r, a. Let $A = (O/\ell^a)(\widetilde{\tau}_\beta)$, where $\widetilde{\tau}_\beta$ lifts the residual twist to roots of order prime to ℓ. The congruence in Lemma 56.1 identifies A with the ℓ^a-torsion of the divisible coefficient module. The unit difference at ℓ gives its unique finite global lift for every strict class at this depth. Restriction to G_L identifies $H^1(\mathbb{Q}, A)$ with $\operatorname{Hom}(G_L, A)^\Delta$, using continuous homomorphisms. Indeed the first and second cohomology of Δ vanish by averaging, and G_L acts trivially.

Under this restriction the strict classes have precisely the homomorphisms from H as their images. One inclusion is the local calculation of Lemma 56.1. Conversely pull a Δ-equivariant map from H back to G_L by reciprocity and take its unique preimage under the restriction isomorphism. On inertia away from ℓ its finite class restricts to zero over L. Restriction is injective on local first cohomology in this direction because the inertia quotient has order dividing m. The same argument with decomposition groups at ℓ gives zero localization there. Thus the divisible global class satisfies every required local condition.

To take the separate characters, choose a generator of Δ. Then $\mathbb{Z}_\ell[\Delta] = \mathbb{Z}_\ell[X]/(X^m - 1)$ is the product of unramified integer rings indexed by Frobenius orbits. In fact the distinct irreducible factors modulo ℓ lift by Hensel's lemma and are pairwise coprime. For an orbit $\mathcal{O}$ the corresponding summand $H_{\mathcal{O}}$ of H is a module over its ring. For a faithful orbit that ring is O by Lemma 56.4, with the identification specified by the chosen character. The equivariant maps in the preceding paragraph identify with $\operatorname{Hom}_O(H_{\mathcal{O}}, O/\ell^a)$. On a cyclic summand O/ℓ^j their length is $\min(a, j)$. Finally $\log_\ell |H|$ is the sum of all component lengths weighted by their residue degrees. Summing over the distinct faithful components proves the inequality. □

Corollary 56.6 (One possible cyclic group at all half-residue twists)**.** *Take the growing layer C_l and the coefficient primes $\ell \equiv 5 \bmod 8$ of Corollary 56.3. For a fixed l, ℓ, there are two Frobenius orbits of faithful characters of C_l. At most one of them has nonzero strict cohomology at any half-residue twist. If it exists, the same orbit occurs at every such twist and its scalar group is cyclic over O. At $\ell \mid r$ this group is O/ℓ. For $1 \le r < t(x)$ the only possible contribution of these faithful characters to the truncated length, when their field average is zero, equals*

$$f \max\{0, k_{\ell,l}(r) - b_0(x)\}, \qquad f = 2^{l-2}.$$

Here $k_{\ell,l}(r)$ is the length of the one surviving scalar group, or zero in its absence. In particular the expression vanishes when $\ell \mid r$.

Proof. Here $m = 2^l$, $f = m/4$ and the number of faithful characters is $\varphi(m) = m/2$. The identity $\mathrm{ord}_{2^l}(\ell) = f$ gives the two orbits of size f. The estimate in the proof of Theorem 56.2 gives $|H| \le |\mathrm{Cl}(L)| < \ell^{m/2} = \ell^{2f}$. Since any nonzero faithful component of H has order at least ℓ^f, at most one of the two such components is nonzero, and its length over O is then one. The finite duality in Theorem 56.5 at $a = 1$ identifies the first layers for every twist in the residue with the duals of the same components. A nonzero ℓ-primary group has nonzero ℓ-torsion, so this detects all surviving orbits. Each scalar group is finite by Theorem 22.17. Over the discrete valuation ring O the dimension of its first torsion layer counts its cyclic summands, by the elementary divisor theorem. It is therefore cyclic whenever nonzero. When $\ell \mid r$, the exponent bound of Corollary 56.3 makes that cyclic group O/ℓ.

The two finite-level local conditions agree: $S^{N_*}(\beta, r) = S(\beta, r)$ by Lemma 22.16, since β has order prime to ℓ. The prime is also prime to the degree of E_x. An orbit of size f contributes f times the scalar length by the integral character decomposition. A cyclic group of length k modulo its subgroup killed by ℓ^{b_0} has length $\max\{0, k - b_0\}$. This proves the formula when the average is zero, as it is for the examples of Corollary 56.3. □

The first layer determines the orbit even at twists prime to ℓ. At those twists the larger exponents of its cyclic group still enter the comparison of Section 6.6.

56.3 Spacing of the weights with large strict cohomology

Fix a faithful character of a real dyadic layer C_j, and an odd prime $\ell \equiv 5 \bmod 8$. Assume $j \ge 3$ and $\ell > 4096(2^{j+2})^4$. Consider positive weights in the residue $r \equiv (\ell - 1)/2 \bmod \ell - 1$. The residual field L and group $\Delta = \mathrm{Gal}(L/\mathbb{Q})$ of Lemma 56.4 are common to all these weights and to all faithful characters of the layer. Put $f = 2^{j-2}$. The proof of Corollary 56.6 gives

$$H = \big(\mathrm{Cl}(L)/\langle [\lambda] \mid \lambda \mid \ell \rangle\big)[\ell^\infty], \qquad |H| < \ell^{2f}.$$

Consequently at most one faithful Frobenius orbit has a nonzero component in H. That component, if present, has length one over the unramified coefficient ring O of degree f. We shall use this length at a finite-order character to compare the groups at different integer weights.

Lemma 56.7 (One compact module for all weights in a fixed residue)**.** *Choose a faithful orbit, a character α representing it as in Lemma 56.4, and the lift $\widetilde{\tau}$ of its residual twist to roots of unity of order prime to ℓ. Put $J = \mathrm{Frac}(O)$ and $\Lambda = O[[T]]$. There is a compact Λ-module B such that B/TB is isomorphic to this orbit's component of H. For $t_r = (1+\ell)^{-r} - 1$ there are isomorphisms*

$$S(\alpha, r) \simeq \mathrm{Hom}_{O,\mathrm{cont}}\big(B/(T - t_r)B, J/O\big).$$

If the component of H is zero then $B = 0$. If it is nonzero then B is cyclic over Λ.

Proof. Let $\mathbb{Q}_\infty$ be the cyclotomic $\mathbb{Z}_\ell$-extension of $\mathbb{Q}$, and put $L_\infty = L\mathbb{Q}_\infty$. Since $|\Delta|$ is prime to ℓ, the Galois group is $\Delta \times \Gamma$, where Γ is identified with $1 + \ell\mathbb{Z}_\ell$ by the principal-unit part of the cyclotomic character. Let γ correspond to $1 + \ell$. From the maximal abelian pro-ℓ quotient of G_{L_∞}, divide out the closed subgroup generated by the images of all inertia groups away from ℓ and all decomposition groups at ℓ. Denote the resulting compact group by X. Conjugation induces commuting actions of Δ and Γ on X. The factor of $\mathbb{Z}_\ell[\Delta]$ corresponding to $\widetilde{\tau}$ is O, with δ acting by $\widetilde{\tau}(\delta)$. This follows by factoring the prime-to- ℓ cyclotomic polynomials into unramified factors, as in Theorem 56.5. Let B be the image in X of the idempotent of this factor and let T act by $\gamma - 1$.

For $t \in \ell O$, give J/O the action D_t on which Δ acts by $\widetilde{\tau}$ and γ by $1+t$. The latter action extends continuously to Γ by the binomial series. The coefficient action is trivial on G_{L_∞}. Restriction identifies global classes for D_t with continuous equivariant homomorphisms from G_{L_∞} to J/O. Indeed in the inflation–restriction sequence the outer groups in degrees one and two for $\Delta \times \Gamma$ vanish. Averaging over Δ kills its positive cohomology, and a nontrivial value of $\widetilde{\tau}$ differs from one by a unit, so $D_t^{\Delta} = 0$.

At a rational prime away from ℓ the image of inertia in $\Delta \times \Gamma$ has order prime to ℓ, since $\mathbb{Q}_\infty$ is unramified there. Restriction on its first inertia cohomology therefore has zero kernel after passage to L_∞. At ℓ, the image of a decomposition group in $\Delta \times \Gamma$ contains its projected prime-to-ℓ factor with trivial Γ-coordinate. To see this, take powers of an element whose exponent tends to zero ℓ-adically and is one modulo $|\Delta|$, and use closedness. That finite factor acts nontrivially through $\widetilde{\tau}$, since the tame quadratic twist ramifies at ℓ. Averaging over it gives zero first cohomology of the decomposition image, just as globally. Thus a class is zero at ℓ exactly when its restricted homomorphism kills every decomposition group above ℓ. These arguments identify the strict classes with the equivariant homomorphisms from X. The real places impose no condition at an odd prime. Equivariance takes the indicated idempotent component and imposes $T = t$. At $t = t_r$ the coefficient action is exactly $\alpha^{-1}\kappa_\ell^{-r}$, giving the asserted formula.

At $t = 0$ the coefficient action already factors through Δ. Restriction to G_L, with the same averaging argument globally, on inertia away from ℓ, and on the decomposition image at ℓ, identifies the strict group with the equivariant homomorphisms $H \to J/O$. Here global reciprocity identifies the unramified abelian group with the class group, and imposing splitting at the primes over ℓ kills their ideal classes [22]. We have therefore identified the continuous O-duals of B/TB and of the indicated component of H. Dualizing identifies the compact modules. Explicitly, the trace pairing identifies J/O with the $\mathbb{Z}_\ell$-dual of O with values in $\mathbb{Q}_\ell/\mathbb{Z}_\ell$, since O is unramified. The claimed biduality follows from ordinary finite abelian duality on the finite quotients and passage to inverse limits.

In particular $B/(\ell, T)B$ has dimension zero or one over $O/\ell O$. In dimension one choose a lift of a basis vector. The submodule it generates is compact as the image of Λ, hence closed. In dimension zero take the zero submodule. Its quotient Y satisfies $Y = (\ell, T)Y$. Every open additive subgroup contains an open subgroup stable under O and Γ. Indeed one can first intersect its inverse images under multiplication by a finite $\mathbb{Z}_\ell$-basis of O including one, obtaining an O-submodule, and then intersect its finitely many Γ-translates. The stabilizer is open by continuity of the action and compactness. On any finite stable quotient Q, the operator T is nilpotent modulo ℓ, since the action of Γ factors through a cyclic group of ℓ-power order. Thus $Q = (\ell, T)Q$ forces $Q/\ell Q = 0$ and then $Q = 0$. The finite quotients separate points, so $Y = 0$. □

Theorem 56.8 (Lengths of the faithful dyadic strict groups)**.** *For an orbit whose component of H is nonzero, write $k(r) = \operatorname{length}_O S(\alpha, r)$. Either $k(r) = 1$ at every indicated weight, or there exist $z \in \ell O$ with $v_\ell(z) = 1$ and $b \in \{1, 2, \ldots\} \cup \{\infty\}$ such that at every such weight*

$$k(r) = \min\{b, v_\ell(t_r - z)\}.$$

Here $v_\ell(\ell) = 1$ and $v_\ell(0) = \infty$. For every integer $a \geq 1$, the weights with $k(r) > a$, if any, lie in one residue class modulo $(\ell - 1)\ell^a$.

Proof. Write $B = \Lambda/I$ using Lemma 56.7. Since B/TB has length one, the ideal formed by the constant terms of elements of I is ℓO. Choose $F(T) = \ell + cT + T^2 G(T)$ in I. Every $P \in I$ satisfies $P(t) \in \ell O$ for $t \in \ell O$. If $c \in \ell O$, then $F(t)$ has valuation exactly one for every such t. Evaluation of I thus gives precisely ℓO, so every specialized dual has length one.

If c is a unit, F has a root $z \in \ell O$. For completeness, start with zero modulo ℓ. Given a root modulo ℓ^n, the correction modulo ℓ^{n+1} is unique because F' is congruent to c modulo ℓ at that point. Completeness gives the root, and the equation modulo ℓ^2 gives $v_\ell(z) = 1$. Division by $T - z$ in $O[[T]]$ gives $F(T) = (T - z)V(T)$, where the coefficient of T^i in V is $\sum_{n \geq i+1} [T^n] F \, z^{n-i-1}$. The series converge in O and the constant coefficient of V is congruent to c modulo ℓ. Thus $T - z \in I$. Evaluation at z identifies $\Lambda/(T - z)$ with O by the same division formula. The image of I in this ring is then $\ell^b O$, with the zero ideal written as $b = \infty$. It is proper because $B \neq 0$. Imposing $T = t_r$ now gives $O/(\ell^b, t_r - z)$. Its dual has the stated length. The strict groups at the positive weights under consideration are finite by Theorem 22.17.

If two distinct weights r, s have $k(r), k(s) > a$, the formula implies $v_\ell(t_r - t_s) \geq a + 1$. On the other hand

$$v_\ell(t_r - t_s) = v_\ell((1 + \ell)^{|r-s|} - 1) = 1 + v_\ell(r - s).$$

Indeed a power prime to ℓ preserves the valuation of a principal unit minus one, and raising it to the odd prime ℓ increases the valuation by exactly one, by the binomial theorem. Hence $\ell^a \mid r - s$. The weights already agree modulo $\ell - 1$, which proves the assertion. □

Corollary 56.9 (An interval bound with one possible exceptional weight)**.** *On an interval $[V, V^{3/2}]$ of Section 6.6, fix (ℓ, j). Include every weight r in the half residue for which $1 \leq r < t(x)$ at some point of the interval where the field contains the prescribed dyadic layer of index j as in Corollary 56.3 or Corollary 9.27, and where $\ell \equiv 5 \bmod 8$, $x^{16} \leq \ell \leq 2x^{16}$. Call this set $\mathcal{R}$. At sufficiently large V, there is at most one $r \in \mathcal{R}$ at which the faithful dyadic components can survive the truncation at $b_0(x)$ anywhere on the interval.*

More precisely, suppose that $\mathcal{R} \neq \varnothing$. Write $D = \max \mathcal{R} - \min \mathcal{R}$, take $k(r) = 0$ in the absence of a surviving orbit, and choose r_0 with maximal $k(r_0)$. Then

$$f \log \ell \sum_{\substack{r \in \mathcal{R} \\ r \neq r_0}} \max\{0, k(r) - 1\} \;\leq\; \frac{f D \log \ell}{(\ell - 1)^2}.$$

Proof. In both field families $2^j < 2x^{2+8\varepsilon}$, so the conductor hypothesis at the beginning of this subsection follows from $\ell \geq x^{16}$ for large V. The prime is prime to the field degree by Corollary 56.3. For fixed ℓ, j, the scalar group is independent of the choice of x realizing the weight. The stronger level condition and the scalar one agree by Lemma 22.16, and Theorem 22.17 gives descent on these same fields. The f conjugates in the orbit have the same length, since coefficient conjugation fixes t_r.

For each $a \geq 1$ a nonempty set of weights with $k(r) > a$ contains r_0. Its elements are spaced by at least $(\ell - 1)\ell^a$, by Theorem 56.8. On deleting r_0 at most $\lfloor D/((\ell - 1)\ell^a) \rfloor$ elements remain. Sum over $a \geq 1$ and use $\sum_{a \geq 1} \ell^{-a} = 1/(\ell - 1)$. This proves the displayed inequality. Finally put $t_* = \lfloor V^{(3/2)401} \rfloor$. For large V, every $b_0(x)$ is at least $\lceil \log_2(t_* + 1) \rceil$, since $b_0(x) = \lfloor \exp(x^\varepsilon/8) \rfloor$. With this last ceiling as a, the spacing exceeds $D < t_*$. Hence each $r \neq r_0$ has $k(r) \leq b_0(x)$ wherever it occurs. □

The estimate leaves the value of $k(r_0)$ open. Its size enters the truncated sum even when there is only one such weight. The other character components and the upper bound for the projected Gram determinant in Theorem 141.27 also enter the comparison on these intervals.

56.4 Full orders at weights outside the class group exceptions

Use the polynomial-conductor interval of Theorem 19.15, its largest field E_*, its degree n_*, and its modulus N_*. Put $t_* = \lfloor V^{1203/2} \rfloor$ and $t_- = \lfloor V^{401} \rfloor$. Consider primes $\ell \geq 5$ prime to

n_*N_*. For a fixed residue $s = 0$ or $s = (\ell-1)/2 \bmod \ell-1$, take the characters α of E_* with $\alpha(c) = (-1)^s$. We require that $\tau = \bar{\alpha}^{-1}\omega_\ell^{-s}$ be nontrivial on the decomposition group at ℓ. This includes every character of the indicated parity in the half residue. In the zero residue it means $\alpha(\ell) \neq 1$.

Fix a cyclic subgroup of the character group of E_*, and let α run through its generators that meet these conditions. Their residual fields L are equal by Lemma 56.4. For a Frobenius orbit $\mathcal{O}$ of the resulting characters of $\Delta = \mathrm{Gal}(L/\mathbb{Q})$, write O for its unramified coefficient ring, f for its residue degree, and

$$h_{\mathcal{O}} = \mathrm{length}_O\left((\mathrm{Cl}(L)/\langle[\lambda] \mid \lambda \mid \ell\rangle)[\ell^\infty]_{\mathcal{O}}\right).$$

For a representative α put $\lambda_{\mathcal{O}}(r) = \mathrm{length}_O S(\alpha, r)$ when $r > 0$ is in the chosen residue. The value is independent of the representative because coefficient conjugation preserves the local conditions.

Lemma 56.10 (The class group length bounds the number of large specializations)**.** *Set $h = h_{\mathcal{O}}$. If $h = 0$, all the scalar groups vanish. For $h > 0$ the weights with $\lambda_{\mathcal{O}}(r) > ha$ occupy at most h residue classes modulo $(\ell-1)\ell^a$, for every integer $a \geq 1$. In particular, among $1 \leq r < t_*$, at most h weights have*

$$\lambda_{\mathcal{O}}(r) > h\big(1 + \lfloor \log_\ell t_* \rfloor\big).$$

Proof. The construction in Lemma 56.7 applies to this residual field. Indeed Δ again has order prime to ℓ, and the lift of τ differs from one by a unit on some member of the local decomposition image. These two facts give the global and local restriction isomorphisms there. Away from ℓ the cyclotomic extension is unramified. At the finite-order specialization $T = 0$, reciprocity over L again identifies the dual with the indicated quotient of the class group. Thus a compact module B over $\Lambda = O[[T]]$ has B/TB of length h, and the specialization $B/(T - t_r)B$, where $t_r = (1+\ell)^{-r} - 1$, is dual to the strict group. The compact generation argument in that lemma works for any finite number of generators by lifting a basis of $B/(\ell, T)B$. In particular $h = 0$ implies $B = 0$.

For $h > 0$, choose a surjection $\Lambda^g \to B$ in this way, and write K for its kernel. In O^g the constant terms of K form a submodule with quotient B/TB, by right exactness. This submodule has rank g. Lift an O-basis of it to g columns in K. Their determinant $F(T)$ satisfies $v_\ell(F(0)) = h$ by the elementary divisor theorem. At every t_r the specialized columns are relations for $B/(T - t_r)B$. Taking determinants over O gives $\lambda_{\mathcal{O}}(r) \leq v_\ell(F(t_r))$, with the right side read as infinity if the determinant vanishes.

Suppose $h + 1$ weights r_i with $\lambda_{\mathcal{O}}(r_i) > ha$ lie in distinct classes modulo $(\ell-1)\ell^a$. Since their common residue modulo $\ell - 1$ is fixed, they are distinct modulo ℓ^a. Write $z_i = t_{r_i}$. The binomial identity from Theorem 56.8 gives $v_\ell(z_i - z_j) = 1 + v_\ell(r_i - r_j) \leq a$ for $i \neq j$. Each z_i is in ℓO. Successively dividing $F(T)$ by the linear factors $T - z_i$ gives

$$F(T) = Q(T)\prod_{i=1}^{h+1}(T - z_i) + R(T), \qquad Q \in O[[T]], \quad R \in O[T], \quad \deg R \leq h.$$

The divisions are integral by the convergent coefficient formula in Theorem 56.8. Interpolate R at the distinct z_i and evaluate at zero. The term corresponding to i is

$$F(z_i)\prod_{j \neq i}\frac{-z_j}{z_i - z_j}.$$

Its valuation exceeds $ha + h - ha = h$. The term containing $Q(0)$ has valuation at least $h + 1$. This contradicts $v_\ell(F(0)) = h$. Taking $a = 1 + \lfloor \log_\ell t_* \rfloor$ now gives the last claim, since $\ell^a > t_*$. □

Theorem 56.11 (A uniform weight count for characters nontrivial at the coefficient prime)**.** *There is one set $\mathcal{N}_V \subset [1, t_*] \cap \mathbb{Z}$ for the whole interval such that, uniformly for $t_- \le T \le t_*$,*

$$|\mathcal{N}_V \cap [1, T]| \ll_{\psi,\varepsilon} \frac{T \log\log T}{\log T}.$$

Outside this set, every orbit and prime specified above, at every weight $1 \le r < t_*$ in its residue, satisfies $\lambda_{\mathcal{O}}(r) \le h_{\mathcal{O}}(1 + \lfloor \log_\ell t_* \rfloor)$.

Proof. Put in $\mathcal{N}_V$ precisely those weights which exceed their last bound for at least one such orbit and prime. Only $\ell \le 2t_* + 1$ can occur, because $\ell - 1 \mid 2r$. For each ℓ we first count the possible weights without using this divisibility to estimate their number. Put $w(\ell) = \max\{v_2(\ell - 1), v_2(\ell + 1)\}$.

For a fixed cyclic subgroup of characters and one residue write $m = [L : \mathbb{Q}]$, let $C \mid N_*$ be the conductor of a generator, and let H be the ℓ-primary split class quotient occurring in the definition of $h_{\mathcal{O}}$. All its faithful factors have residue degree $f = \mathrm{ord}_m(\ell)$. Since they are distinct integral idempotent factors, $f \sum_{\mathcal{O}} h_{\mathcal{O}} \le \log |H| / \log \ell$. Every character of L has conductor dividing $C\ell$, so $|\operatorname{disc}(L)| \le (C\ell)^m$ by the conductor–discriminant formula. The field is totally real by parity. Minkowski's bound gives every class an integral ideal of norm at most $\sqrt{|\operatorname{disc}(L)|}$. Counting these ideals by the sum of their inverse squared norms gives

$$|H| \le |\operatorname{Cl}(L)| \le |\operatorname{disc}(L)| \zeta_L(2) \le (2C\ell)^m.$$

For the last inequality use the Euler factors and $\zeta(2) < 2$.

Let 2^j be the two-part of the order of the character α before twisting. Its odd part divides $o = [K_\psi : \mathbb{Q}]$, and the twist has order m divisible by 2^j and at most $2o\,2^j$. Since $2^j \mid \ell^f - 1$, one has $f \ge 2^{j - w(\ell)}$. In fact an odd power gives $v_2(\ell^f - 1) = v_2(\ell - 1)$, and for even f successive squaring gives $v_2(\ell^f - 1) = w(\ell) + v_2(f)$. Together with Lemma 56.10 the bounds just proved allow at most

$$\sum_{\mathcal{O}} h_{\mathcal{O}} \ll_\psi 2^{w(\ell)} \left(1 + \frac{\log(2N_*)}{\log \ell}\right)$$

exceptional weights for this cyclic subgroup and this residue.

At each fixed j there are $O_\psi(1)$ cyclic subgroups to count. Indeed the cyclic group of characters inflated from the largest real dyadic layer has index at most $4o$ in the full character group. In each coset the elements killed by $o_{\mathrm{odd}} 2^j$, where o_{odd} is the odd part of o, number at most 2^j, since any two of them differ by an element of the cyclic dyadic group killed by 2^j. Each subgroup with two-part 2^j has at least 2^{j-1} generators when $j \ge 1$, and at least one when $j = 0$. Generators of distinct cyclic subgroups are disjoint. There are $O_{\psi,\varepsilon}(\log V)$ possible j since $n_* \ll_\psi V^{3+12\varepsilon}$, and only two residues. As $\log N_* \ll_{\psi,\varepsilon} \log V$, the bound for all groups at this prime is $O_{\psi,\varepsilon}(2^{w(\ell)} (\log V)^2)$.

For $t_- \le T \le t_*$ split the primes at $Y = T/(\log T)^4$. For $a \ge 1$ the integers with $w(\ell) \ge a$ lie in the two classes $\pm 1 \bmod 2^a$. Counting up to Y and summing $2^a(Y/2^a + 1)$ for $a \le \log_2(Y + 1)$ shows that $\sum_{5 \le \ell \le Y,\ \ell \text{ prime}} 2^{w(\ell)} \ll Y \log(2Y)$. The small primes therefore allow $O_{\psi,\varepsilon}(T/\log T)$ weights.

For larger primes a weight $r \le T$ is a positive multiple of $(\ell - 1)/2$, and $\ell \le 2T + 1$. Their contribution to the count is at most

$$\sum_{Y < \ell \le 2T+1,\ \ell \text{ prime}} \frac{2T}{\ell - 1} \ll \frac{T \log\log T}{\log T}.$$

Indeed there are $O(\log\log T)$ dyadic intervals between Y and $2T + 1$. On each, Chebyshev's upper bound for the number of primes gives a reciprocal sum $O(1/\log Y)$, and $\log Y \asymp \log T$. The two counts establish the claimed bound for every prefix of the one fixed set. □

Corollary 56.12 (A polynomial bound for the full orders at the other weights)**.** *At each $x \in [V, V^{3/2}]$, consider all triples consisting of a prime ℓ, a weight $1 \le r < t(x)$ outside $\mathcal{N}_V$, and one of the specified character orbits occurring on E_x in the residue of r. Their full scalar groups satisfy*

$$\sum_{(\ell,r,\mathcal{O})} f_{\mathcal{O}} \lambda_{\mathcal{O}}(r) \log \ell \ll_{\psi,\varepsilon} n_*^2 t_*^2 (\log(2V))^3.$$

Each of these components contributes zero to $R_{\ell,r}(E_x)$ once V is sufficiently large.

Proof. Inflation of a character from E_x to E_* preserves its scalar coefficient action over $\mathbb{Q}$, hence also its strict group. The character decomposition is integral since $\ell \nmid n_*$. The comparison with the conductor-level group is the one in Theorem 22.17 and Lemma 22.16. From the bound for $|H|$ in the preceding proof and $m \le 2n_*$, each $h_{\mathcal{O}}$ is $O_{\psi,\varepsilon}(n_* \log(2V))$. The theorem then bounds each scalar length by $O_{\psi,\varepsilon}(n_*(\log(2V))^2)$. For one prime and weight, the sum of the orbit degrees is at most n_*, the total number of characters. There are at most $2t_*+1$ primes and at most t_* weights, and $\log(2t_*+1) \ll \log(2V)$. Multiplication proves the displayed inequality. Finally this polynomial bound on each length is smaller than $b_0(x)$ throughout a sufficiently distant interval. All the indicated primes are then at most $2t_* + 1 < P(x)$, so truncation kills their components. □

The class group comparison in this argument uses the nontrivial local residual action at ℓ. The groups on $\mathcal{N}_V$ and the zero-residue characters trivial on the decomposition group at ℓ are among the terms for which the estimate in Corollary 9.30 still needs an upper bound.

56.5 A finite class group determining the possible exceptional dyadic weight

Return to the faithful characters of the real dyadic field C_j and the primes and half-residue weights of Section 56.3. There are two faithful Frobenius orbits. An orbit absent from the split class quotient of L has zero strict group at every such weight by Lemma 56.7. For the possible nonzero orbit retain the notation $O, J, \widetilde{\tau}, B, \gamma, t_r$ from that lemma. In particular γ has cyclotomic principal-unit value $1 + \ell$. Put $u_r = 1 + t_r = (1 + \ell)^{-r}$.

For an integer $n \ge 0$, let $\mathbb{Q}_n$ be the degree-ℓ^n subfield of the cyclotomic $\mathbb{Z}_\ell$-extension $\mathbb{Q}_\infty$. Set $L_n = L\mathbb{Q}_n$ and define

$$H_n = \big((\mathrm{Cl}(L_n)/\langle [w] \mid w \mid \ell \rangle)[\ell^\infty]\big)_{\mathcal{O}}.$$

The subscript selects the same factor of $\mathbb{Z}_\ell[\Delta]$ as in Lemma 56.7. We use the action on ideals of the element of $\mathrm{Gal}(L_n/L)$ induced by γ. The fields L_n serve to calculate a scalar strict group on the period field E_x.

Lemma 56.13 (Specialization through an ordinary ideal class group)**.** *There is an isomorphism respecting the action of γ,*

$$H_n \simeq B/((1+T)^{\ell^n} - 1)B.$$

With $M^\vee = \mathrm{Hom}_{O,\mathrm{cont}}(M, J/O)$, one therefore has for every indicated weight

$$\big(S(\alpha, r)[\ell^{n+1}]\big)^\vee \simeq H_n/(\ell^{n+1} H_n + (\gamma - u_r)H_n).$$

Proof. Use the coefficient module $D_0 = (J/O)(\widetilde{\tau})$ over $\mathbb{Q}_n$, with trivial action in the cyclotomic $\mathbb{Z}_\ell$-direction. Over $L_\infty = L\mathbb{Q}_\infty$ it is trivial, and the quotient group over $\mathbb{Q}_n$ is $\Delta \times \langle \gamma^{\ell^n} \rangle$, where angular brackets denote the closed subgroup. Restrict global classes as in Lemma 56.7. Averaging over Δ gives zero first and second cohomology of this quotient because $D_0^\Delta = 0$. At

the prime above ℓ the quadratic inertia action remains nontrivial after the local extension of degree ℓ^n, since a subgroup of odd index cannot lie in the kernel of a quotient of order two. The finite part of the local decomposition image therefore still has zero invariants. Away from ℓ the cyclotomic extension is unramified, so the image of inertia has order prime to ℓ. These are the local injectivity arguments in that lemma. Consequently the strict classes of D_0 over $\mathbb{Q}_n$ are the continuous dual of the quotient of B imposing $\gamma^{\ell^n} = 1$.

Instead restrict the same classes to L_n. The quotient over $\mathbb{Q}_n$ is now the finite group Δ, still of order prime to ℓ. Restriction is again an isomorphism onto the equivariant homomorphisms satisfying the same local conditions. By global reciprocity these homomorphisms factor through the ideal class group with all classes of primes above ℓ killed, and every homomorphism of its indicated component occurs. Thus their group is $H_n^\vee$. The two restrictions commute with conjugation by the lift of γ which fixes L, and this lift acts trivially on D_0. Dualizing gives the first isomorphism with the asserted action.

The specialization formula of Lemma 56.7 identifies the dual of $S(\alpha, r)[\ell^{n+1}]$ with $B/(\ell^{n+1}, T - t_r)B$. Indeed the dual of the torsion subgroup killed by a scalar is the quotient of the compact dual by that scalar. In this quotient $(1+T)^{\ell^n} - 1$ acts as $u_r^{\ell^n} - 1$, of valuation $n + 1 + v_\ell(r)$ by the binomial theorem. Its action is therefore zero. We may first take the quotient in the first isomorphism and then impose $\ell^{n+1} = 0$ and $\gamma = u_r$, giving the second formula. □

Theorem 56.14 (A finite test for the full strict length to exceed a given depth)**.** *Let $n \geq 1$ and $k(r) = \operatorname{length}_O S(\alpha, r)$ for the possible surviving orbit. Then $k(r) > n$ if and only if*

$$H_n \simeq O/\ell^{n+1}O \quad \text{as an } O\text{-module}, \qquad \gamma|_{H_n} = u_r \operatorname{id}_{H_n}.$$

If these two conditions fail for a weight, its full length is the length of the finite quotient in Lemma 56.13.

Proof. Suppose $k(r) > n \geq 1$. In the proof of Theorem 56.8 a relation with nonunit linear coefficient would force $k(r) = 1$. The other case of that proof identifies B with $O/\ell^b O$, with $b = \infty$ denoting O, and γ acts by $1 + z$ for some $z \in \ell O$ of valuation one. The formula for $k(r)$ gives $b \geq n + 1$ and $1 + z \equiv u_r \bmod \ell^{n+1}O$. Raising $1 + z$ to the ℓ-th power increases the valuation of its difference from one by exactly one, as ℓ is odd and O is unramified. Induction gives $v_\ell((1+z)^{\ell^n} - 1) = n + 1$. The first isomorphism of Lemma 56.13 therefore gives precisely the cyclic group and action asserted.

Conversely, under the displayed conditions both relations in the second quotient of that lemma already hold on H_n. The dual of $S(\alpha, r)[\ell^{n+1}]$ then has length $n + 1$, forcing $k(r) > n$. Failure of either condition implies $k(r) \leq n$, in which case the entire scalar group is killed by ℓ^{n+1}. The same quotient computes its full length. □

Corollary 56.15 (One class group at level twenty-five on the period interval)**.** *Fix (ℓ, j) and the set of weights $\mathcal{R}$ in Corollary 56.9. In particular each eligible point has $x^{16} \leq \ell \leq 2x^{16}$. The group H_{25} with its ideal action determines the full strict orders for all but at most one weight of $\mathcal{R}$. All those determined by failure of the test have $k(r) \leq 25$. The remaining possible weight, if it exists, has $k(r) \geq 26$ and is specified as follows.*

First require $H_{25} \simeq O/\ell^{26}O$, and write v for the unit by which γ acts on it. Require also that v belong to the image of $1 + \ell\mathbb{Z}_\ell$ in $(O/\ell^{26}O)^\times$. Failure of either requirement leaves no such weight. Otherwise determine $a \bmod \ell^{25}$ by $(1+\ell)^{-a} = v \bmod \ell^{26}O$. The possible weight is the element of $\mathcal{R}$, if present, satisfying

$$r \equiv a \bmod \ell^{25}, \qquad r \equiv (\ell - 1)/2 \bmod \ell - 1.$$

The auxiliary field for this computation has degree $2^j\ell^{25}$ and conductor dividing $2^{j+2}\ell^{26}$.

Proof. If the orbit is absent at level zero, all orders are already one. Otherwise apply Theorem 56.14 with $n = 25$. An endomorphism of the indicated cyclic O-module is given by a unique scalar modulo ℓ^{26}. The reduction of $1+\ell\mathbb{Z}_\ell$ has ℓ^{25} elements and is generated by $1+\ell$, since $v_\ell((1+\ell)^{\ell^i}-1) = i+1$. The natural map of this finite group into $(O/\ell^{26}O)^\times$ is injective by unramifiedness. This gives the claimed exponent test. Its value is independent of the generator chosen for the cyclic module. Coefficient conjugation also preserves the test because every u_r lies in $\mathbb{Z}_\ell$.

The two congruences define one class modulo $(\ell-1)\ell^{25}$. For each $r \in \mathcal{R}$ there is an x with $x^{16} \le \ell$ and $r < t(x)$, so all such r lie between zero and $\ell^{401/16}$, even if they occur at different points of the interval. Since $401/16 = 25 + 1/16$ and $\ell - 1 > \ell^{1/16}$ for $\ell \ge 5$, the modulus exceeds this entire range. Thus there is at most one matching integer. The theorem gives its lower bound and the full orders at the other weights, by the finite quotient already described.

Finally L has degree 2^j prime to ℓ and conductor dividing $2^{j+2}\ell$. The field $\mathbb{Q}_{25}$ has degree ℓ^{25} and is contained in $\mathbb{Q}(\zeta_{\ell^{26}})$. Disjointness gives the stated degree and the compositum gives the conductor bound. These quantities are bounded by fixed powers of x on the prescribed window. The descent in Corollary 9.27 identifies the scalar components on the same E_x used for the periods. □

If the congruences select a weight, the level-twenty-five test gives a lower bound for its length. No bound for the excess above that depth follows here. At any higher level the theorem gives the same finite test, and finiteness of the strict group implies eventual failure for each fixed weight. A uniform bound for that level as ℓ, j, r vary would give additional control of the sum in Corollary 9.30.

56.6 Full cohomology lengths at locally split weights

Use the common fields $E_x \subseteq E_*$ and the interval $[V, V^{3/2}]$ of Theorem 19.15. Write $n_* = [E_* : \mathbb{Q}]$, let N_* be its cyclotomic modulus, and put $t_* = \lfloor V^{1203/2} \rfloor$, $t_- = \lfloor V^{401} \rfloor$. Fix a prime $\ell \ge 5$ with $\ell \nmid n_* N_*$, and take $s = 0$ or $s = (\ell-1)/2$. For a character α of $\mathrm{Gal}(E_*/\mathbb{Q})$ with $\alpha(c) = (-1)^s$, let $\tau = \alpha^{-1}\omega^{-s}$, where ω is the Teichmüller lift of the cyclotomic character modulo ℓ. Let L be its fixed-kernel field, $\Delta = \mathrm{Gal}(L/\mathbb{Q})$, $O = \mathbb{Z}_\ell[\tau(\Delta)]$, and $J = \mathrm{Frac}(O)$. The field L is totally real, $|\Delta|$ is prime to ℓ, and O is unramified. Subscript τ means the factor of $\mathbb{Z}_\ell[\Delta]$ determined by the coefficient Frobenius orbit of τ. We allow the trivial character, in which case $L = \mathbb{Q}$.

For $1 \le r < t_*$ in the residue s mod $\ell - 1$, write $k_\tau(r) = \mathrm{length}_O S(\alpha, r)$. The group $S(\alpha, r)$ consists of the classes over $\mathbb{Q}$ with coefficients $(J/O)(\alpha^{-1}\kappa_\ell^{-r})$ that are unramified away from ℓ and restrict to zero at ℓ. Put $t_r = (1+\ell)^{-r} - 1$. Let $\mathbb{Q}_1$ be the first layer of the cyclotomic $\mathbb{Z}_\ell$-extension of $\mathbb{Q}$, put $L_1 = L\mathbb{Q}_1$, and choose γ with principal cyclotomic value $1+\ell$. Its action on L_1 fixes L. Define

$$C_1 = ((\mathrm{Cl}(L_1)/\langle [w] \mid w \mid \ell \rangle)[\ell^\infty])_\tau\,, \qquad D_1 = C_1/\Phi_\ell(\gamma)C_1, \qquad \Phi_\ell(Y) = 1 + Y + \cdots + Y^{\ell-1}.$$

Fix a primitive ℓ-th root ζ and put $O' = O[\zeta]$, $J' = \mathrm{Frac}(O')$. The action of ζ by γ makes D_1 an O'-module. Set $h_\tau = \mathrm{length}_{O'} D_1$. Since O' and O have the same residue field, $h_\tau \le \mathrm{length}_O C_1$.

Lemma 56.16 (A primitive cyclotomic specialization at a split prime)**.** *There is a finitely generated compact $O[[T]]$-module B with*

$$S(\alpha, r) \simeq \mathrm{Hom}_{O,\mathrm{cont}}(B/(T - t_r)B, J/O), \qquad (B \otimes_O O')/(T - (\zeta - 1))(B \otimes_O O') \simeq D_1.$$

These conclusions hold also when every prime of L above ℓ has local degree one. If $\tau = 1$, then $B = 0$.

Proof. Put $L_\infty = L\mathbb{Q}_\infty$, where $\mathbb{Q}_\infty/\mathbb{Q}$ is cyclotomic with group $\Gamma = \langle\gamma\rangle \simeq \mathbb{Z}_\ell$. Take the maximal abelian pro-ℓ quotient of G_{L_∞} and kill the closed subgroup generated by inertia away from ℓ and all decomposition groups above ℓ. Let B be its τ-factor, with $T = \gamma - 1$. Conjugation gives the action because $\Delta \times \Gamma$ is the quotient over $\mathbb{Q}$ and inner conjugations act trivially on the abelian group. For the integral weights the coefficient on this quotient is τ on Δ and $1 + t_r$ on γ. At the auxiliary specialization use J'/O' with the same finite character and with γ acting by ζ.

Restriction from $\mathbb{Q}$ to L_∞ identifies the global classes at each of these points with equivariant homomorphisms. Indeed the first and second cohomology of the quotient vanish. For $\tau \neq 1$, average over Δ, whose invariants in the coefficient module vanish since some $\tau(\delta) - 1$ is a unit. For $\tau = 1$, the second group vanishes by ℓ-cohomological dimension one of Γ, and the first is the cokernel of multiplication by t_r or by $\zeta - 1$ on a divisible module. Both scalars are nonzero.

Away from ℓ the inertia image in the quotient has prime-to-ℓ order, so inflation contributes no inertia classes. At ℓ the decomposition image is $\Delta_w \times \Gamma$. Its projections are onto the respective local images, of coprime supernatural orders, and the cyclotomic extension is totally ramified. For the product assertion one can work in every finite layer, where a subgroup surjecting onto two factors of coprime orders has the full product order. Its first cohomology vanishes by averaging if $\tau|_{\Delta_w} \neq 1$, and otherwise by the same surjective scalar multiplication on the divisible module. Thus restriction detects zero at ℓ. At the real place the coefficient prime is odd. Equivariance on the resulting quotient gives the first isomorphism and gives the continuous O'-dual of the auxiliary specialization of B. The scalar extension here is a finite direct sum as a compact O-module.

For $\tau \neq 1$ compute that auxiliary group a second time, by restriction to L_1. Global averaging still kills degrees one and two for $\Delta \times C_\ell$. In the local quotient $\Delta_w \times C_\ell$ the only further case is the trivial action of Δ_w. The first cohomology of C_ℓ is then $\ker(1+\zeta+\cdots+\zeta^{\ell-1})/(\zeta-1)(J'/O') = 0$. Away from ℓ inertia is again of prime-to-ℓ order. Class field theory over L_1 identifies the unramified abelian quotient split above ℓ with the stated quotient of its ideal class group [22]. Equivariance selects C_1 and imposes $\gamma = \zeta$ after extension of coefficients. The resulting module is D_1, since $O' = O[Y]/(\Phi_\ell(Y))$ and the additional relation identifies Y with the action of γ. Both calculations give its continuous dual. Dualizing recovers the compact modules by finite abelian duality and inverse limits. Over a finite extension of $\mathbb{Z}_\ell$ the dualizing divisible module can be taken as the fraction field modulo the integers, since the inverse different is a principal fractional ideal.

For $\tau = 1$ the first cohomology of the global finite quotient C_ℓ is zero by the same calculation. Restriction therefore injects the auxiliary strict group into the dual of the split ℓ-class group of $\mathbb{Q}_1$. This class group is zero. Indeed its class field is Galois over $\mathbb{Q}$ with finite ℓ-group G. The inertia at ℓ has order ℓ and is cyclic. Its normal closure is G, since the fixed field of that closure would be everywhere unramified over $\mathbb{Q}$; the odd degree excludes real ramification and Minkowski excludes a nontrivial such field. A proper subgroup of a finite ℓ-group lies in a maximal subgroup, which is normal. The inertia therefore equals G. The split class field is $\mathbb{Q}_1$ itself. Both auxiliary modules consequently vanish.

In all cases the finite auxiliary specialization surjects onto $(B \otimes_O O')/(\zeta - 1, T)(B \otimes_O O')$, which identifies with $B/(\ell, T)B$. Lift a basis of the latter to B. The submodule generated over $O[[T]]$ by the lifts is closed as the continuous image of a compact finite free module. Its quotient Y satisfies $Y = (\ell, T)Y$. In every finite stable quotient T is nilpotent modulo ℓ, because γ acts

with ℓ-power order. These quotients separate points, by the open stable subgroup argument of Lemma 56.7. Thus $Y = 0$, including the case of an empty basis. □

Theorem 56.17 (A bound for full lengths after removing at most one weight per root)**.** *Let $I_s = \{1 \le r < t_* : r \equiv s \bmod \ell - 1\}$, $N = |I_s|$, and $h = h_\tau$. There is a set $D_\tau \subseteq I_s$ with $|D_\tau| \le h$ such that, if $N > 0$,*

$$k_\tau(r) \le h(1 + \lfloor \log_\ell t_* \rfloor) \qquad (r \in I_s \setminus D_\tau),$$
$$\sum_{r \in I_s \setminus D_\tau} k_\tau(r) \le h\left(N + \frac{N-1}{\ell - 1}\right).$$

In particular all the strict groups vanish if $D_1 = 0$.

Proof. If $h = 0$ the compact generation argument in the lemma gives $B = 0$. The empty progression also requires no choice. Otherwise put $B' = B \otimes_O O'$, $\pi = \zeta - 1$, $e = \ell - 1$, and normalize $v(\ell) = 1$, so $v(\pi) = 1/e$. Present B' as a quotient of $O'[[T]]^g$. At $T = \pi$ its relations map onto a full-rank sublattice of $(O')^g$ with cokernel of length h. Lift a basis of this sublattice to relation columns. Their determinant $F(T)$ satisfies $v(F(\pi)) = h/e$. At t_r these columns are again relations, hence $k_\tau(r) \le v(F(t_r))$, allowing infinity when the determinant vanishes. Indeed extension from O to O' multiplies length by e, and v divides the O'-length of a determinant by that same factor.

By Weierstrass preparation over the complete discrete valuation ring O', write $F = \pi^\mu U \prod_i (T - \beta_i)$ over a finite splitting field, where U is a unit power series, the β_i have positive valuation, and roots are repeated with multiplicity. The unit has valuation zero at all our points. For $v(\beta_i) < 1$ one has

$$v(t_r - \beta_i) = v(\beta_i) \le e\, v(\pi - \beta_i).$$

For $v(\beta_i) < 1/e$ the two distances have equal valuation. For $v(\beta_i) \ge 1/e$ the right side is at least one. Each root of valuation at least one contributes exactly $1/e$ at π. There are therefore at most h such roots. For each choose a weight $r_i \in I_s$ maximizing $v(t_{r_i} - \beta_i)$, allowing an infinite maximum. Take D_τ to be the union of these choices. For $r \ne r_i$ the ultrametric inequality gives

$$v(t_r - \beta_i) \le v(t_r - t_{r_i}) = 1 + v_\ell(r - r_i).$$

The equality follows by the binomial theorem for the principal unit $1 + \ell$. The constant π^μ, the roots of valuation below one, and one unit of valuation per remaining root cost at most $e\, v(F(\pi)) = h$. Thus outside D_τ the bound is $h + \sum_i v_\ell(r - r_i)$, with the sum only over the selected roots. This gives the first inequality.

Write the progression as $r_{\min} + a(\ell - 1)$ for $0 \le a < N$, and write a_i for the index of r_i. Summing $v_\ell(r - r_i)$ over the whole progression except r_i gives $v_\ell(a_i!) + v_\ell((N - 1 - a_i)!)$. Counting multiples of powers of ℓ bounds this by $(N - 1)/(\ell - 1)$. Summing over at most h roots proves the second inequality. □

Corollary 56.18 (One sparse exceptional set for both inertia residues)**.** *There is one set $D_V \subseteq [1, t_*] \cap \mathbb{Z}$ such that uniformly for $t_- \le T \le t_*$,*

$$|D_V \cap [1, T]| \ll_{\psi,\varepsilon} T/H(T),$$

where H is defined in Section 9.16. At every $x \in [V, V^{3/2}]$, take all the primes coprime to $n_* N_*$ and at least five, both residues above, and the character orbits occurring on E_x. With

$f_\tau = \operatorname{rank}_{\mathbb{Z}_\ell} O$ *denoting the unramified degree, their full lengths satisfy*

$$\sum_{\substack{(\ell,r,\tau)\\ 1\le r<\lfloor x^{401}\rfloor\\ r\notin D_V}} f_\tau k_\tau(r)\log\ell \ll_{\psi,\varepsilon} n_*^2 t_*^3(\log(2V))^3.$$

Here a triple is included only when r is in the residue defining τ. The bound includes the zero-residue characters for which $\alpha(\ell)=1$.

Proof. Inflating α to E_* preserves the scalar group over $\mathbb{Q}$, and the integral descent to E_x is that of Theorem 22.17 and Lemma 22.16. Take D_V to be the union of the sets in Theorem 56.17 for the characters of E_*. Only $\ell \le 2t_*+1$ occur since $\ell-1 \mid 2r$. The field L_1 has degree at most $2n_*\ell$ and conductor dividing $N_*\ell^2$. By the conductor–discriminant formula and the ideal-counting bound used in Theorem 56.11,

$$f_\tau h_\tau \log\ell \le \log|\operatorname{Cl}(L_1)| \le 2n_*\ell\log(2N_*\ell^2).$$

For $\ell \le Y = V^{100}$ there are at most $2n_*$ orbits over the two residues. Hence the total number of their selected weights is $O_{\psi,\varepsilon}(n_*^2Y^2\log(2V))$. The estimates $n_* \ll_\psi V^{3+12\varepsilon}$ and $\log N_* \ll_{\psi,\varepsilon} \log V$, with $\varepsilon < 1/52$, make this $o(t_-/\log t_*)$. Every weight selected for a larger prime belongs to the set in Lemma 9.28. Its count in every stated prefix is $O(T/H(T))$, which proves the first assertion.

For the mass, each $k_\tau(r)$ outside the union is $O_{\psi,\varepsilon}(n_*t_*(\log(2V))^2)$ by the class number bound and the first inequality of the theorem. At each prime and weight the sum of the orbit degrees is at most n_*. There are at most $2t_*+1$ primes and t_* weights. Multiplying and using $\log(2t_*+1) \ll \log(2V)$ gives the asserted polynomial bound. □

For sufficiently large V every individual length bounded here is smaller than $b_0(x)$ on the entire interval. At a weight in D_V the reference class group bounds the number of possible exceptions. Section 6.6 still requires control of the weighted sizes of those exceptional groups and of the projected theta periods on these fields.

56.7 Ideal classes at the primes testing the theta periods

Fix one interval of Corollary 56.9. For each pair (ℓ_i, j_i) from its dyadic family include the exceptional weight r_i if its strict length k_i exceeds 25. There is at most one such weight and one such orbit per pair by Corollary 56.15. Equivalently, one may work with any subset of this finite list. Put $f_i = 2^{j_i-2}$, let O_i be the corresponding unramified integer ring, and let L_i be the totally real cyclic field of the residual character τ_i of order 2^{j_i}. Choose an integer $1 \le n_i < k_i$ and set

$$K_i = L_i\mathbb{Q}_{i,n_i}, \qquad H_i = ((\operatorname{Cl}(K_i)/\langle [v] \mid v \mid \ell_i\rangle)[\ell_i^\infty])_{\tau_i},$$

where $\mathbb{Q}_{i,n_i}$ is the cyclotomic layer of degree $\ell_i^{n_i}$ over $\mathbb{Q}$. Theorem 56.14 gives $H_i \simeq O_i/\ell_i^{n_i+1}O_i$. The group $\operatorname{Gal}(L_i/\mathbb{Q})$ acts through the lift of τ_i, and the cyclotomic generator acts on H_i by $(1+\ell_i)^{-r_i}$. Let M_i/K_i be the abelian class field with group H_i, using arithmetic Frobenius as the Artin map on ideals. The defining subgroup is stable under $\operatorname{Gal}(K_i/\mathbb{Q})$, so $M_i/\mathbb{Q}$ is Galois. All primes above ℓ_i split in M_i/K_i.

Let $J/\mathbb{Q}$ be any finite Galois field containing the coefficients, torsion data, and normalizations of the chosen finite list of elliptic theta tests on the interval, as in Theorem 68.15. Additional residual splitting fields required for trace tests may be included in J. Write J^{ab} for its largest subfield abelian over $\mathbb{Q}$. Take a finite abelian field $A/\mathbb{Q}$ containing J^{ab}, all the K_i, and the period fields E_x on the interval. Such an A exists because the K_i and E_x are abelian and there

are only finitely many distinct E_x. Put $F = AJ$ and $M = A\prod_i M_i$, where the product denotes compositum.

Lemma 56.19 (Independence over the abelian fields of the interval)**.** *Restriction gives* $\mathrm{Gal}(M/A) = \prod_i H_i$. *For uniquely determined integers* $0 \le a_i \le n_i + 1$, *it gives*

$$\mathrm{Gal}(MF/F) = \prod_i \ell_i^{a_i} H_i, \qquad \prod_i \ell_i^{f_i a_i} = [M \cap F : A] \;\mid\; [J : J^{\mathrm{ab}}].$$

In particular enlarging the abelian field in this construction costs no factor in the stated upper bound.

Proof. The conjugation action on H_i of a lift of a generator of $\mathrm{Gal}(L_i/\mathbb{Q})$ with trivial cyclotomic component is multiplication by a primitive 2^{j_i}-th root of unity. Subtracting one gives a unit in O_i, since the reduction of a root of unity of order prime to ℓ_i has the same order. The commutators of this single lift with H_i thus fill H_i. The quotient by H_i is abelian. Consequently K_i is the largest abelian subfield of $M_i/\mathbb{Q}$ and $M_i \cap A = K_i$.

Let $W = \prod_i H_i$ and $D = \mathrm{Gal}(A/\mathbb{Q})$. There is a well-defined action of D on W through its quotients $\mathrm{Gal}(K_i/\mathbb{Q})$. We describe every D-stable subgroup of this finite abelian group. First separate its primary parts. For a given prime ℓ use the subgroup $D' \subset D$ of elements of order prime to ℓ. On each factor with $\ell_i = \ell$ it acts by τ_i. Indeed the projection of D' to the cyclotomic layer is trivial and its projection onto the prime-to-ℓ group $\mathrm{Gal}(L_i/\mathbb{Q})$ is surjective. The residual characters at this prime belong to distinct Frobenius orbits. Their orders 2^{j_i} differ, because the list contains at most one entry for each (ℓ, j_i).

The ring $\mathbb{Z}_\ell[D']$ has integral idempotents separating these orbits. To see this, over an unramified coefficient extension containing the character values use the character idempotents with denominator $|D'|$. Summing over one Frobenius orbit gives coefficients in $\mathbb{Z}_\ell$. On the selected factor the image of the ring is O_i, since the values of τ_i generate O_i. A stable subgroup is therefore the product of O_i-submodules of the separate cyclic modules H_i. Each such submodule is $\ell_i^{a_i} H_i$ with $0 \le a_i \le n_i + 1$.

The restriction of $\mathrm{Gal}(M/A)$ into W is injective, and its image is D-stable by conjugation in $\mathrm{Gal}(M/\mathbb{Q})$. Each projection is surjective by $M_i \cap A = K_i$. The subgroup description gives the first assertion. Restriction identifies $\mathrm{Gal}(MF/F)$ with $\mathrm{Gal}(M/M \cap F)$, which is again stable because $F/\mathbb{Q}$ is Galois. Its index in W is the stated product. This index divides $[F : A] = [J : J^{\mathrm{ab}}]$, since $J \cap A = J^{\mathrm{ab}}$. □

Theorem 56.20 (One prime representing the visible part of every exceptional class group)**.** *Fix* $0 < \delta < 1/4$. *For all sufficiently large* X, *a set of rational primes* $q \in [X, 2X]$ *of positive limiting relative density among those split in* F *has both of the following properties. For every marked elliptic factor, at every place over* q, *its recurrence scalar has multiplicative order greater than* $X^{1/4-\delta}$. *For each* i, *the* τ_i*-component of the class of a prime* $\mathfrak{q}_i$ *of* K_i *over* q *has additive order*

$$\ell_i^{n_i+1-a_i} \quad \text{in } H_i.$$

This order is independent of the choice of prime above q. *The* O_i*-multiples of the class fill* $\ell_i^{a_i} H_i$. *Every prime split in* F, *away from ramification in* MF, *gives a class in this subgroup.*

Proof. Choose g_i generating $\ell_i^{a_i} H_i$ over O_i; use zero for the zero group. By the lemma the tuple defines one element of $\mathrm{Gal}(MF/F)$. Viewed in the finite group $\mathrm{Gal}(MF/\mathbb{Q})$, its conjugacy class gives a positive Chebotarev density of rational primes. All split in F, and the dyadic-interval form of the theorem gives a positive limiting relative density there [24, §1A]. For each such prime choose a prime of MF with Frobenius equal to the chosen tuple. The restrictions to

M_i/K_i are the arithmetic Frobenius elements of the respective primes of K_i, since their residue degrees over $\mathbb{Q}$ equal one. Global reciprocity identifies them with the desired projections of ideal classes. Conjugating the prime acts on each H_i by a unit and preserves both the order and the submodule generated. All primes split in F give elements in the group of the lemma, which also proves the upper assertion. Finally Theorem 68.15 discards at most $O(X^{1-2\delta})$ primes for the entire list of elliptic data. For fixed fields this is $o(X/\log X)$, so the remaining relative density in the specified conjugacy class tends to one. □

Corollary 56.21 (A single degree bound for the loss in the weighted lengths)**.** *Take $n_i = k_i - 1$ and choose one prime q by the theorem. Write $\ell_i^{d_i(q)}$ for the order of the projected ideal class at q. For every subset S of the interval list and arbitrary cutoffs $b_i \ge 0$, put $(y)_+ = \max(y, 0)$. Then*

$$0 \;\le\; \sum_{i\in S} f_i \log \ell_i \big[(k_i - b_i)_+ - (d_i(q) - b_i)_+\big] \;\le\; \log[J : J^{\mathrm{ab}}].$$

If J is abelian over a number field K abelian over $\mathbb{Q}$, and $K \subseteq A \cap J$, then $d_i(q) = k_i$ for every i with $L_i \not\subseteq K$. In particular this holds for all entries if K is imaginary quadratic.

Proof. The theorem gives $k_i - d_i(q) = a_i$, and subtracting a fixed cutoff and taking the positive part decreases this difference. Sum the resulting bounds and take the logarithm of the index in Lemma 56.19. In particular the same prime works for the subset occurring on each E_x and for the actual cutoff $b_i = b_0(x)$.

In the last case $F = AJ$ is abelian over K, as a compositum of two extensions abelian over K. If $L_i \not\subseteq K$, choose an element of $\mathrm{Gal}(A/K)$ nontrivial on L_i. Its action on $H_i/\ell_i H_i$ is multiplication by a nonidentity value of the faithful residual character. Its action minus one is therefore invertible on H_i. On $\mathrm{Gal}(M \cap F/A)$ its action by conjugation is trivial since $M \cap F$ is abelian over K. The quotient $H_i/\ell_i^{a_i} H_i$ in that group must be zero. Thus $a_i = 0$. Every L_i here is totally real of degree $2^{j_i} \ge 8$, giving the assertion for imaginary quadratic K. □

The choice $n_i = 25$ in the theorem uses fixed layer indices throughout the interval. The corollary uses the full depths and allows its auxiliary prime to depend on them. To obtain the bound of Section 6.6 from this realization one still needs an upper bound for the orders $d_i(q)$ and control of the other components. The large orders of the elliptic recurrence scalars at this prime provide the tests of Corollary 68.17; their consequences for the actual projected period determinant require its global coefficient and rank estimates.

57 Units, regulators and relative class numbers

57.1 Global units modulo the coefficient prime and the opposite root

In the family of Section 47.2, retain the assumption $S(\alpha, r) \neq 0$ and write $\tau = \bar{\Psi}$, the character of the *opposite* root. The cyclic field L cut out by τ is also the residual field for the negative root. Its group Δ has order 2^j; at ℓ its inertia subgroup I has order two, since α is unramified and $\bar{\kappa}_\ell^r$ is the ramified quadratic character. The character τ restricts to the sign of I. Let $H_{\mathrm{rel}}(\tau) \subset H^1(\mathbb{Q}, k(\tau))$ consist of the classes unramified at all finite primes different from ℓ, with unrestricted localization at ℓ.

Lemma 57.1 (The ray class group at the rational ideal ℓO_L)**.** *Restriction to L gives a k-linear isomorphism*

$$H_{\mathrm{rel}}(\tau) \simeq \mathrm{Hom}_{\Delta}\left(\mathrm{Cl}_{\ell O_L}(L), k(\tau)\right),$$

where the maps on the right are additive group homomorphisms. The dimension is at most one. Here the modulus has exponent two at each prime over ℓ, independent of the weight.

Proof. Restriction to L identifies the global cohomology with the Δ-equivariant homomorphisms from G_L: averaging over Δ kills the two outer terms in inflation–restriction. At primes away from ℓ the same argument over inertia shows that the unramified conditions are exactly unramifiedness of the restricted homomorphism. Real places have order at most two, so they impose no distinction for these odd-primary homomorphisms.

Fix $\lambda \mid \ell$. In L_λ the absolute ramification index is two. Write $U^a = 1 + \lambda^a O_{L_\lambda}$ for $a \geq 1$. The ℓ-adic logarithm gives $(U^1)^\ell = U^3$. Indeed logarithm and exponential converge and are mutually inverse on the maximal ideal, since the normalized valuation of each element of that ideal is at least one, strictly greater than $2/(\ell - 1)$. They identify taking the ℓ-th power with multiplication by ℓ, of valuation two. Under local reciprocity the homomorphism therefore kills U^3. On $U^2/U^3 \simeq \lambda^2/\lambda^3$ inertia acts trivially. To see this, the nonidentity tame inertia element acts by -1 on λ/λ^2 via its faithful tame character and fixes the residue field. Its square character on λ^2/λ^3 is one. On the target it acts as -1, so equivariance kills U^2/U^3 as well. This proves the conductor bound. Conversely a homomorphism of the stated ray class group is unramified away from ℓ and provides the required global class by reciprocity [22]. Finally localization at ℓ on $H_{\mathrm{rel}}(\tau)$ has strict kernel zero by Lemma 47.4. Its target has dimension one by the local Euler characteristic and the local invariant vanishings in Theorem 47.2. □

Let $\kappa_\lambda = O_L/\lambda$, and let M_0 be the least common multiple of the integers $|\kappa_\lambda^\times|$ for $\lambda \mid \ell$. It is prime to ℓ. Define

$$B_\ell = \bigoplus_{\lambda \mid \ell} \lambda/\lambda^2, \qquad e_\tau = \frac{1}{|\Delta|} \sum_{\sigma \in \Delta} \tau(\sigma)^{-1} \sigma,$$
$$b(u) = \left(u^{M_0} - 1 \bmod \lambda^2\right)_{\lambda \mid \ell} \in B_\ell \qquad (u \in O_L^\times).$$

Here e_τ acts after tensoring B_ℓ from $\mathbb{F}_\ell$ to k.

Theorem 57.2 (A one-dimensional unit calculation for the ordinary root)**.** *The space $e_\tau(B_\ell \otimes_{\mathbb{F}_\ell} k)$ has dimension one. The relaxed group $H_{\mathrm{rel}}(\tau)$ vanishes if and only if some global unit u has $e_\tau b(u) \neq 0$. If every unit gives zero, $H_{\mathrm{rel}}(\tau)$ has dimension one. One may check any generating set of $O_L^\times$. All of these data are common to the half-residue weights for a fixed ℓ, j, α.*

Proof. Consider first the ordinary class group of L. Its faithful τ-component at ℓ vanishes. Indeed imposing splitting at the primes above ℓ gives the quotient in Lemma 47.4, with zero component there. The subgroup generated by the omitted prime classes has trivial I-action because Δ is abelian and each such prime is fixed by I. It has zero τ-component since $\tau|_I$ is nontrivial. One can take components integrally on the finite ℓ-primary groups by lifting τ to its prime-to-ℓ roots of unity. A component with zero residual quotient is zero by Nakayama's lemma.

The ray class exact sequence now shows that the only contribution at τ comes from $(O_L/\ell O_L)^\times$ modulo the global units. Its ℓ-primary subgroup is precisely B_ℓ: the product of the residue unit groups has order prime to ℓ and the kernel is identified with the additive groups λ/λ^2 by subtracting one. Raising a unit to M_0 kills the prime-to-ℓ part and acts as a unit scalar on the ℓ-part. The images of $b(u)$ therefore generate the contribution to be divided out. The map $u \mapsto b(u)$ is additive with respect to multiplication of units, as products of two displacements lie in λ^2. Taking components and extending the residue field are exact here. In particular, no extension from the ordinary class group changes this component.

To find its dimension before taking units, extend the coefficient field temporarily to an algebraic closure of $\mathbb{F}_\ell$. The line λ/λ^2 over κ_λ then splits into one line per residue-field embedding.

The group Δ acts transitively on the pairs consisting of a prime and such an embedding; the stabilizer of one pair is its inertia group I. On its line the action is the nontrivial tame character of I. The whole module is therefore the representation induced from this sign. Frobenius reciprocity gives multiplicity one for the character τ, since it restricts to that sign. Dimensions descend to k, where τ is defined. Thus quotienting by the projected $b(u)$ gives dimension zero or one as asserted, and its equivariant dual computes the relaxed group by the lemma. Finally, changing r in the prescribed residue preserves τ and L, hence also the unit calculation. □

Corollary 57.3 (Eliminating one parameter from the trace congruence)**.** *Write E for the positive-weight relation after diagonal elimination in Corollary 47.6. Its linear coefficient on x, reduced modulo ℓ, is nonzero if and only if the unit in Theorem 57.2 exists. In this case $e = yE$ eliminates U over O, and there are series $f_1', f_2' \in O[[V, W]]$ giving*

$$C = O[[V, W]]/(f_1', f_2'), \qquad C/(V, W)C = O/\ell^{k(r)}O.$$

In particular a characteristic-zero specialization of C with $V = W = 0$ is then impossible.

Proof. Consider global square-zero deformations on the positive symplectic root over $k[\epsilon]/(\epsilon^2)$. They are the global τ-cocycles unramified away from ℓ, normalized to have value zero at h. On this upper root every such cocycle satisfies the local ordinary condition: it fixes the coordinate flag and induces the split diagonal characters. The normalization selects exactly one representative of every relaxed class because $\tau(h) - 1$ is a unit. Away from ℓ the equivalence between unramifiedness of a class and factorization through H_q is the same inertia averaging used in Theorem 47.5.

In that presentation the only tangent coordinate of weight $(0, 1)$ is x. Of the relations only E can have a linear term in this coordinate. Consequently the relaxed group vanishes exactly when that coefficient is a unit, giving the equivalence by Theorem 57.2. On setting $v = w = 0$ in the first torus presentation, weight $+1$ forces $E = xg(xy)$ for some $g \in O[[U]]$. Here $g(0)$ is the same linear coefficient. Thus $e(U, 0, 0) = Ug(U)$ with $g(0)$ a unit under the stated condition. The formal inverse function theorem solves $e = 0$ uniquely as $U = H(V, W)$. The solution has $H(0, 0) = 0$, as the unique solution at $V = W = 0$ in the formal neighborhood of zero is $U = 0$. Substitution in the two f_i proves the presentation; Theorem 47.8 gives the indicated quotient. At a specialization with $V = W = 0$ the coefficient ring therefore factors through $O/\ell^{k(r)}O$. □

57.2 Norms of units at the exceptional dyadic weights

Fix a faithful character of $C_j = \mathbb{Q}(\zeta_{2^{j+2}})^+$ in Section 56.5, with $j \geq 3$, $\ell \equiv 5 \bmod 8$, and the stated conductor bound. At the half-residue weights write $k(r)$ for its full strict length. Let L be the residual field, $\Delta = \mathrm{Gal}(L/\mathbb{Q})$, and τ its faithful character with the unramified coefficient ring O. Write $L_a = L\mathbb{Q}_a$ as in Lemma 56.13. For any number field K write $U(K)$ for its group of global units, with its natural Galois action. The subscript τ on a finitely generated abelian group with Δ-action means to tensor with $\mathbb{Z}_\ell$ and take the idempotent of the orbit of τ. Set $C_a = \mathrm{Cl}(L_a)_\tau$.

Lemma 57.4 (The ramified prime and the ambiguous class sequence)**.** *There is exactly one prime above ℓ at each level L_a. Its square is principal. For $0 \leq a < n$ let $G = \mathrm{Gal}(L_n/L_a)$, let N be the norm, and write $j_{a,n}$ for extension of ideal classes. There is an exact sequence of O-modules*

$$0 \longrightarrow H^1(G, U(L_n))_\tau \longrightarrow C_a \xrightarrow{j_{a,n}} C_n^G \longrightarrow \big(U(L_a)/NU(L_n)\big)_\tau \longrightarrow 0.$$

Proof. The quadratic inertia character at ℓ in $\tau = \alpha^{-1}\omega^{-(\ell-1)/2}$ has order two, and $\tau^2 = \alpha^{-2}$ cuts out C_{j-1}. The image of ℓ generates $(\mathbb{Z}/2^{j+1}\mathbb{Z})^\times/\{\pm 1\}$. Indeed $\ell \equiv 5 \bmod 8$ gives $v_2(\ell^{2^t}-1) = 2+t$ for $t \geq 0$, by successive squaring, and no power is $-1 \bmod 4$. Thus the Frobenius on C_{j-1} has order 2^{j-1}. The decomposition group in L contains the inertia of order two and surjects onto this whole unramified quotient. There is one prime over ℓ, with ramification index two. Adjoining $\mathbb{Q}_a$ adjoins a totally ramified local extension of coprime degree ℓ^a. The local degree is the product by coprimality, and its ramification index is a multiple of the coprime indices 2 and ℓ^a. Its residue field contains that of L, of degree 2^{j-1}. The product of these lower bounds is the full global degree, so the ramification index is $2\ell^a$ and there is still just one prime. The prime in $\mathbb{Q}_a$ is generated by the norm to $\mathbb{Q}_a$ of $1-\zeta_{\ell^{a+1}}$. Indeed this generates the unique prime in the full cyclotomic field and the intermediate residue degree is one. Its ideal in L_a is the square of the unique prime there. In particular C_a equals the split class group factor H_a of Lemma 56.13.

In L_n/L_a the unique prime over ℓ is totally ramified and all other finite primes are unramified. Each unit of L_a is a local norm at those other primes, since units in an unramified local extension map onto the base units. The real places split. The product formula for local Artin symbols makes the symbol of the unit at the last prime trivial as well. By the local norm theorem and the Hasse norm theorem for a cyclic extension, every base unit is the norm of a field element. We need to distinguish which of them are norms of units. The prime-degree ambiguous class formulas are given in [25]. The following ideal calculation works for every cyclic degree ℓ^{n-a} and retains the character action.

Write I_K, P_K for fractional and principal ideals. The quotient $I_{L_n}^G/I_{L_a}$, with lower ideals extended, is a sum of cyclic groups of orders the ramification indices. This follows by taking the product of the primes in each orbit as the generator of its invariant ideal group. Only the prime at ℓ contributes, and Δ fixes it. The τ-factor of this quotient vanishes. Also $H^1(G, I_{L_n}) = 0$, since each prime orbit gives a permutation module with first cohomology $\mathrm{Hom}(G_w, \mathbb{Z}) = 0$. Hilbert's theorem 90 applied to $U(L_n) \to L_n^\times \to P_{L_n}$ gives

$$P_{L_n}^G/P_{L_a} \simeq H^1(G, U(L_n)), \qquad H^1(G, P_{L_n}) \simeq (U(L_a) \cap NL_n^\times)/NU(L_n).$$

The second isomorphism uses $H^2(G, D) = D^G/ND$ for cyclic G, first for units and then for field elements. The intersection on the right is all of $U(L_a)$ by the preceding paragraph. Now take invariants in $P_{L_n} \to I_{L_n} \to \mathrm{Cl}(L_n)$. The kernel of the map to invariant classes is supplied by invariant principal ideals, and its cokernel is $H^1(G, P_{L_n})$. After taking the τ-factor the invariant ideals come from L_a, as proved above. Dividing by P_{L_a} gives the displayed exact sequence. These operations are exact on the required terms by flatness of $\mathbb{Z}_\ell$ over $\mathbb{Z}$ and by the integral idempotent. The actions of Δ and G commute throughout. □

Theorem 57.5 (Capitulation and norm indices between every pair of levels)**.** *Suppose some half-residue weight has $k(r) > 1$. Use the scalar z and exponent b from the proof of Theorem 56.8, so $v_\ell(z) = 1$, $1 \leq b \leq \infty$ and $k(r) = \min(b, v_\ell(t_r - z))$. Put $s_a = \min(b, a+1)$. For $0 \leq a < n$ the kernel of $j_{a,n}$ and the τ-component of $U(L_a)/NU(L_n)$ are cyclic O-modules, each of length*

$$s_a - \max(0, s_n - (n-a)).$$

At level zero this length is zero for $n < b$ and one for $n \geq b$. Thus finite b is exactly the first level at which the nonzero faithful base class capitulates. It is also the first level at which the norms of units fail to generate the faithful base unit component.

Proof. The scalar description gives $B = O/\ell^b O$, where $b = \infty$ means $B = O$. The action of γ is $y = 1 + z$. By the binomial theorem $v_\ell(y^{\ell^a} - 1) = a + 1$. Lemma 56.13 therefore gives

$C_a = O/\ell^{s_a}O$, with the same scalar action. The invariants C_n^G are the kernel of $y^{\ell^a} - 1$ on C_n, hence have length s_a.

The ideal norm $C_n \to C_a$ is surjective. Indeed the unramified class field over L_a for C_a has trivial intersection with L_n over L_a, since every nontrivial intermediate field of L_n/L_a ramifies at its unique prime above ℓ. Its base change to L_n is unramified. Class field reciprocity, compatible with ideal norm under this restriction, gives the surjection on class groups and then on their τ-factors. Extension of the norm of an ideal is the product of all its G-conjugates, so $j_{a,n}C_a$ is the image on C_n of

$$\sum_{i=0}^{\ell^{n-a}-1} y^{i\ell^a} = \frac{y^{\ell^n} - 1}{y^{\ell^a} - 1}.$$

This scalar has valuation $n - a$. Its image thus has length $\max(0, s_n - (n - a))$. Both source and invariant target of $j_{a,n}$ are cyclic of length s_a. Their kernel and cokernel are cyclic of the claimed length, and the lemma identifies the cokernel with the unit norm quotient. For $a = 0$ the source has length one. Its entire nonzero class line survives exactly when $s_n = n + 1$, or $n < b$. □

Corollary 57.6 (A weight-uniform test using units modulo the first power)**.** *For $n \geq 1$, form the norm on ordinary units and reduce modulo ℓ to obtain*

$$e_\tau\big(U(L_n) \otimes \mathbb{F}_\ell\big) \longrightarrow e_\tau\big(U(L) \otimes \mathbb{F}_\ell\big),$$

where e_τ is the orbit idempotent. The target is a line over $O/\ell O$. If this map is zero, then $k(r) \leq n$ at every *indicated weight on the common interval. If a weight has $k(r) > n$, the unit norm map onto this line is surjective at each level $1, \ldots, n$. In particular a zero map at $n = 25$ rules out the exceptional weight for the entire pair (ℓ, j) on the tested orbit.*

Proof. The roots of unity in the totally real L have order at most two. Dirichlet's unit theorem identifies the real span of its free units, by equivariant logarithms of all absolute values, with the hyperplane of sum zero indexed by the real embeddings. The character of this representation is the regular character of Δ minus the trivial character. Its trace character comes from the integral unit lattice and is the same after scalar extension to characteristic zero at ℓ. The nontrivial orbit therefore contributes a free O-module of rank one to $U(L) \otimes \mathbb{Z}_\ell$. Reduction gives the stated line. Norm commutes with its idempotent.

If any $k(r) > n$, the hypothesis of the theorem holds and $b > n$. Its conclusion with $a = 0$ gives a surjective norm on completed faithful units at every level through n. Reduction proves the assertion and its contrapositive. If some weight has length greater than one, the first failure occurs exactly at finite b. Indeed for $n \geq b$ the image has index $|O/\ell O|$ and equals ℓ times the base lattice. Its reduction is then zero. Computing the displayed map requires only the images of a set of fundamental units of L_n in the base unit lattice modulo ℓ. The assertion at level 25 follows for all admissible weights by this same contrapositive. □

For every pair at which the displayed map vanishes at a depth at most $b_0(x)$, its faithful orbit contributes zero after truncation at that x. At pairs where these norm maps stay surjective the scalar congruence for γ in Theorem 56.14 still enters. The argument does not bound the number of successive surjective levels uniformly over the fields of Section 6.6.

57.3 A base unit test for all zero-residue weights

In Section 56.6 take $s = 0$ and $\alpha \neq 1$. Write $\tau = \alpha^{-1}$, $L = \overline{\mathbb{Q}}^{\ker \tau}$, $\Delta = \mathrm{Gal}(L/\mathbb{Q})$, and $O = \mathbb{Z}_\ell[\tau(\Delta)]$. The field L is totally real and for fixed α it is independent of ℓ. Take $\ell \geq 5$ prime

to n_*N_*. First suppose ℓ splits completely in L. For $n \geq 1$ write $L_n = L\mathbb{Q}_n$, $G_n = \mathrm{Gal}(L_n/L)$, and let $h^0_\tau = \mathrm{length}_O \mathrm{Cl}(L)_\tau$ in this subsection. Here the subscript on a group denotes its completed orbit component as in Section 57.2.

For a global unit u write $u_v \in \mathbb{Z}_\ell^\times$ for its image at $v \mid \ell$. In the decomposition $\mathbb{Z}_\ell^\times = \mu_{\ell-1} \times (1 + \ell\mathbb{Z}_\ell)$ denote the second coordinate by $\langle u_v \rangle$. Consider

$$\mathcal{L}(u) = \left(\frac{\log_\ell \langle u_v \rangle}{\log_\ell(1+\ell)} \right)_{v|\ell} \in \bigoplus_{v|\ell} \mathbb{Z}_\ell.$$

The logarithm here is its convergent principal-unit power series. The map is equivariant for the permutation of places. The target is a copy of the regular module $\mathbb{Z}_\ell[\Delta]$, and its τ-component is a free rank-one O-module. Define c_τ by requiring the image on the completed τ-component of the units to be ℓ^{c_τ} times this target component. We allow $c_\tau = \infty$ for zero image. Changing the identification of the target line multiplies it by a unit and preserves this definition.

Theorem 57.7 (Invariant ideal classes at a completely split coefficient prime)**.** *At every level $n \geq 1$ the ordinary class groups satisfy*

$$\mathrm{length}_O\big((\mathrm{Cl}(L_n)_\tau)^{G_n}\big) = h^0_\tau + \min(n, c_\tau).$$

If $h^0_\tau = c_\tau = 0$, then $\mathrm{Cl}(L_n)_\tau = 0$ at every level and $S(\alpha, r) = 0$ at every positive weight divisible by $\ell - 1$.

Proof. The primes of L above ℓ form a free transitive Δ-set. Each is totally ramified of degree ℓ^n in L_n, and all other finite primes are unramified. As in Lemma 57.4, extending ideals multiplies the generator of each invariant prime orbit by its ramification index. Thus $I_{L_n}^{G_n}/I_L$ is a copy of $(\mathbb{Z}/\ell^n)[\Delta]$ and its τ-factor has length n. Write $U' = U(L_n)_\tau$ and $U = U(L)_\tau$, and denote the norm on units by N. The equivariant logarithmic embedding in Dirichlet's unit theorem, now at all real places, gives the regular character of $\Delta \times G_n$ minus its trivial character on the rational unit lattice. Because τ is nontrivial, $U' \otimes_O \mathrm{Frac}(O)$ is the regular representation of G_n over $\mathrm{Frac}(O)$. Also U has rank one over O. There is no ℓ-torsion in these units since the fields are totally real.

We record the resulting equality of lengths

$$\mathrm{length}_O H^1(G_n, U') = \mathrm{length}_O(U/NU').$$

Indeed U' is commensurable equivariantly with $O[G_n]$ inside the common rational representation. For the regular lattice the two terms vanish by the cyclic cohomology formulas. For a finite module Q, with generator g of G_n, the quotients $\ker N/(g-1)Q$ and Q^{G_n}/NQ have equal orders. This follows by counting the kernels and images of N and $g-1$ separately. Their length difference is additive in exact sequences by the cyclic Tate cohomology sequence. Apply this to the intersection of the two lattices and their finite quotients. Finally $(U')^{G_n} = U$ by flatness and the orbit idempotent.

The group $(I_{L_n}^{G_n}/P_L)_\tau$ has length $h^0_\tau + n$. Passing to the subgroup of invariant classes represented by invariant ideals removes $(P_{L_n}^{G_n}/P_L)_\tau$, of length $\mathrm{length}_O H^1(G_n, U')$ by Hilbert 90. The cokernel of these ideal classes in all invariant classes is $\big((U(L) \cap NL_n^\times)/NU(L_n)\big)_\tau$, by the ideal cohomology argument of Lemma 57.4. Here we retain the indicated intersection because several primes ramify. Define $U^{\mathrm{norm}} = (U(L) \cap NL_n^\times)_\tau$. Together with the preceding equality of lengths this gives

$$\mathrm{length}_O\big((\mathrm{Cl}(L_n)_\tau)^{G_n}\big) = h^0_\tau + n - \mathrm{length}_O(U/U^{\mathrm{norm}}).$$

The Hasse norm theorem for cyclic extensions tests membership of a unit in $NL_n^\times$ at every place. Away from ℓ all units are local norms, including at the split real places. At $v \mid \ell$ the local field is $\mathbb{Q}_\ell$ and the extension is the degree-ℓ^n cyclotomic layer. Local reciprocity on its unit group is projection of the principal-unit exponent modulo ℓ^n, up to sign. This follows from the action of a local unit on the ℓ-power roots of unity by its cyclotomic exponent, with the prime-to-ℓ factor removed. Hence the norm condition is $\mathcal{L}(u) = 0 \bmod \ell^n$ at all coordinates. Completion and the integral idempotent preserve this finite-image calculation. The length of the image of the completed τ-map modulo ℓ^n is $\max(0, n - c_\tau)$, interpreted as zero for infinite c_τ. Substitution proves the formula.

If both invariants vanish, $(\mathrm{Cl}(L_n)_\tau)^{G_n} = 0$. A nonzero finite ℓ-group with an action of a cyclic ℓ-group has nonzero fixed elements. On its nonzero subgroup killed by ℓ, $g-1$ is nilpotent and thus has nonzero kernel. Hence the whole component is zero at every level. In particular its level-one split quotient D_1 in Lemma 56.16 is zero. Theorem 56.17 gives vanishing at every indicated positive weight. □

Corollary 57.8 (One class number product and a congruence on base units)**.** *There is a positive integer $D_{\mathrm{cl}}(V)$ depending only on E_* with*

$$\log D_{\mathrm{cl}}(V) \ll_\psi n_* \log(2N_*).$$

For $\ell \geq 5$ coprime to $n_* N_* D_{\mathrm{cl}}(V)$, a nonzero full component at a positive zero-residue weight on any E_x of the interval forces ℓ to split completely in its nontrivial residual field L. It also forces

$$e_\tau \left(\frac{u_v^{\ell-1} - 1}{\ell} \bmod \ell \right)_{v \mid \ell} = 0 \qquad \text{for every } u \in U(L).$$

Across all *primes $\ell \geq 5$ coprime to $n_* N_*$, the number of weights $1 \leq r < t_*$ exceptional in the sense of Lemma 56.10 for any zero-residue character nontrivial at its coefficient prime is $O_\psi(n_* \log(2N_*))$ on the entire interval.*

Proof. For each cyclic subgroup C generated by an even character of $\mathrm{Gal}(E_*/\mathbb{Q})$, take the field L_C cut out by a generator and put $D_{\mathrm{cl}}(V) = \prod_C |\mathrm{Cl}(L_C)|$. Its conductor divides N_*, and $m_C = [L_C : \mathbb{Q}] = |C|$. The discriminant and ideal count in Theorem 56.11 give $\log |\mathrm{Cl}(L_C)| \leq m_C \log(2N_*)$. The odd part of the order of any character divides $o = [K_\psi : \mathbb{Q}]$, because the other fields adjoined have degrees powers of two. Thus $m_C/\varphi(m_C) \leq \prod_{p \mid 2o} p/(p-1)$. The generators of distinct cyclic subgroups are disjoint and there are at most n_* characters in total. This proves the claimed bound on $\log D_{\mathrm{cl}}(V)$.

For $\ell \nmid D_{\mathrm{cl}}(V)$ every base ℓ-class component is zero. If the faithful residual character is nontrivial on the local decomposition group, Lemma 56.10 gives vanishing at every weight. If it is trivial on that group, the prime splits completely in L. A nonzero scalar group then requires $c_\tau \geq 1$ by the theorem. This condition says exactly that every projected local logarithm is zero modulo ℓ. The binomial expansion gives

$$\frac{u_v^{\ell-1} - 1}{\ell} \equiv (\ell - 1) \frac{\log_\ell \langle u_v \rangle}{\log_\ell(1 + \ell)} \pmod{\ell}.$$

The factor $\ell - 1$ is invertible. The globally trivial character has zero scalar group by Lemma 56.16. Integral character descent in Theorem 22.17 identifies the components on every E_x with their scalar groups for the inflated characters.

For the last assertion, the bound of Lemma 56.10 leaves at most the length of one split class group component per pair of prime and orbit. At a fixed field and prime, the sum of these

lengths multiplied by the residue degrees is at most $v_\ell(|\operatorname{Cl}(L_C)|)$, since the components have orthogonal integral idempotents. Multiplying by $\log \ell$ and summing over all primes and all C gives at most $\log D_{\mathrm{cl}}(V)$. Since all residue degrees are at least one and $\log \ell \geq 1$, this also bounds the number of exceptional weights in their union. □

Proposition 57.9 (The real quadratic layer $\mathbb{Q}(\sqrt{2})$)**.** *For the quadratic character of $\mathbb{Q}(\sqrt{2})$, a nonzero zero-residue component at a good $\ell \geq 5$ requires both*

$$\ell \equiv 1 \text{ or } -1 \bmod 8, \qquad (1+\sqrt{2})^{\ell-1} \equiv 1 \pmod{\ell^2 \mathbb{Z}[\sqrt{2}]}.$$

In particular its scalar group at $\ell = 7$ vanishes for every positive multiple of six. This gives the corresponding vanishing on the period fields whenever $7 \nmid n_* N_*$.

Proof. The field has discriminant eight, and Minkowski's bound $\sqrt{8}/2 < 2$ makes its class group trivial. A prime ℓ splits there exactly in the two displayed residue classes, by the quadratic supplement to reciprocity. At the inert primes under consideration Lemma 56.10 applies directly. At a split prime test the actual unit $u = 1+\sqrt{2}$. Its conjugate is $-u^{-1}$. Thus its two Fermat quotients modulo ℓ are opposites, and the nontrivial quadratic idempotent fixes their pair. Vanishing of that pair is equivalent to the displayed congruence because the two distinct primes over ℓ are coprime. The base class group is already trivial, so the proof of Corollary 57.8 applies independently of the class numbers of other subfields. At seven one has $(1+\sqrt{2})^6 = 99+70\sqrt{2}$, whose $\sqrt{2}$-coefficient is nonzero modulo 49. The scalar calculation uses only the field $\mathbb{Q}(\sqrt{2})$, whose degree and conductor are prime to seven. This proves the asserted vanishing. The quadratic field occurs in every sufficiently large real dyadic layer of the interval family. □

The Fermat quotient condition is necessary for a surviving split orbit with trivial base class component. The proof supplies no upper bound for its strict length when that condition holds. Such lengths, the other inertia residue, and the projected period comparison still enter Section 6.6.

57.4 Units supported at the coefficient prime and the real quadratic layer

Keep the nontrivial zero-residue character τ, its field L, and a completely split prime ℓ as in Section 57.3. Put $S = \{v : v \mid \ell\}$, $U_S = \mathcal{O}_L[1/\ell]^\times$ and $\operatorname{Cl}_S(L) = \operatorname{Cl}(L)/\langle [v] \mid v \in S\rangle$. For $u \in U_S$ define

$$\mathcal{L}_S(u)_v = \frac{\log_\ell \langle \ell^{-v_\ell(u_v)} u_v \rangle}{\log_\ell(1+\ell)} \qquad (v \in S).$$

Here $L_v = \mathbb{Q}_\ell$ and the angular brackets discard the Teichmüller component. Write $\ell^{c_{\tau,S}} O$ for the image of the completed S-units under this map on the τ-component of the local exponent lattice, identified with O as in Section 57.3.

Theorem 57.10 (The constant specialization computed in the residual field)**.** *For the compact module B of Lemma 56.16 there is an exact sequence*

$$0 \longrightarrow O/\ell^{c_{\tau,S}} O \longrightarrow B/TB \longrightarrow \operatorname{Cl}_S(L)_\tau \longrightarrow 0.$$

In particular $c_{\tau,S} \leq c_\tau$, where c_τ is the ordinary unit index of Theorem 57.7. These indices are finite. Write $b_S = c_{\tau,S} + \operatorname{length}_O \operatorname{Cl}_S(L)_\tau$. If $b_S = 0$, all the scalar groups at positive zero-residue weights vanish. In general the weights at which the full length exceeds ab_S occupy at most b_S residue classes modulo $(\ell-1)\ell^a$ for every $a \geq 1$.

Proof. Use the constant coefficient in the cyclotomic direction, $(J/O)(\tau)$ with $J = \mathrm{Frac}(O)$. Restriction from $\mathbb{Q}$ to $L_\infty = L\mathbb{Q}_\infty$ identifies its global first cohomology with the equivariant homomorphisms on G_{L_∞}. The outer groups in degrees one and two vanish by averaging over the prime-to-ℓ group Δ with nontrivial character, exactly as in Lemma 56.16. Requiring the resulting homomorphism to factor through the unramified, locally split quotient defining B gives the dual of B/TB, since γ acts trivially on the coefficient in this calculation.

Instead restrict first to L. The same averaging identifies the global classes with equivariant homomorphisms on G_L. At $v \nmid \ell$ their inertia condition is unchanged on passing to L_∞, which is unramified at v. At $v \mid \ell$ their restrictions to $G_{L_{\infty,w}}$ must be zero. Equivalently the local homomorphism on G_{L_v} factors through the local cyclotomic $\mathbb{Z}_\ell$-extension. Thus B/TB is the τ-component of the maximal abelian pro-ℓ quotient of G_L with these two local conditions. The equivalence follows by dualizing the same group of equivariant homomorphisms in the two descriptions.

By reciprocity, this quotient is computed by finite ideles. Keep the ideal valuations away from S. At $v \in S$ keep only the local principal-unit exponent. Indeed reciprocity for the cyclotomic extension of $\mathbb{Q}_\ell$ kills ℓ and the Teichmüller units and uses precisely this exponent up to a common sign. The ideal map outside S gives a surjection onto $\mathrm{Cl}_S(L)$ before the pro-ℓ quotient. Its kernel is the local exponent lattice $\bigoplus_{v\in S}\mathbb{Z}_\ell$ modulo $\overline{\mathcal{L}_S(U_S)}$. To verify this, an outside ideal trivial in $\mathrm{Cl}_S(L)$ can be removed by a principal idele. Two choices differ by an S-unit, and a principal idele with zero outside valuations comes from precisely an S-unit. The group of outside ideals is discrete, so taking closure changes only the local image in each such fiber. The kernel is compact pro-ℓ and the remaining ideal class group is finite. Consequently passing to the pro-ℓ quotient retains the kernel and takes the ℓ-primary part of the class group. The character idempotent gives the claimed exact sequence. This also identifies the nontrivial character component of the logarithmic class group described in Section 22.5.

Ordinary units belong to U_S, which proves the inequality for the indices. Leopoldt's theorem for abelian number fields gives full rational rank to the diagonal ℓ-adic logarithm on the ordinary unit lattice [26]. The nontrivial orbit has rank one over O in this lattice by Dirichlet's unit theorem. Its image in the local O-line is therefore nonzero, so both indices are finite. The exact sequence gives $\mathrm{length}_O(B/TB) = b_S$. The proof of Lemma 56.10 from this point uses only a finite presentation over $O[[T]]$, this constant length, and the specialization formula for $S(\alpha, r)$. Finite generation and that formula are available here by Lemma 56.16, and $O[[T]]$ is Noetherian. The determinant interpolation in Lemma 56.10 therefore gives the stated residue-class bound, also when the character is locally trivial. For $b_S = 0$, compact Nakayama gives $B = 0$. □

Proposition 57.11 (A prime where ordinary units alone leave a nonzero invariant class)**.** *For $L = \mathbb{Q}(\sqrt{2})$, its nontrivial character and $\ell = 31$, the ordinary class group at the first cyclotomic layer has invariant τ-component of length one. The compact module B is zero and the full strict group vanishes at every positive weight divisible by* 30*.*

Proof. Write $\eta = 1 + \sqrt{2}$. The units are generated by -1 and η. Indeed for a positive real unit $1 < u < \eta$ the conjugate is $u' = \pm u^{-1}$. In both cases $0 < (u - u')/(2\sqrt{2}) < 1$, whereas this is the integral coefficient of $\sqrt{2}$. Thus η is the least unit greater than one and its powers account for all positive units. The class number is one as in Proposition 57.9. At the prime over 31 with $\sqrt{2} \equiv 116 \bmod 961$ one has $116^2 \equiv 2 \bmod 961$ and $117^{30} \equiv 1 \bmod 961$. The latter follows by squaring successively, with residues $235, 448, 816, 844$ at exponents $2, 4, 8, 16$. The conjugate of η is $-\eta^{-1}$, so the same congruence holds at the other prime. Thus $c_\tau \geq 1$, and Theorem 57.7 gives invariant length one at level one.

The element $\pi = 7 + 3\sqrt{2}$ has norm 31, so it belongs to U_S. At the specified prime its value is 355 mod 961, which is a unit. The residues of its powers $2, 4, 8, 16$ are $134, 658, 514, 882$, giving $355^{30} \equiv 900 = 1 + 29 \cdot 31 \bmod 961$. Its local principal-unit exponent is therefore nonzero modulo 31. At the other prime the local value divided by 31 is the inverse of this unit since $\pi\bar{\pi} = 31$. The two exponents are negatives, so their pair already belongs to the nontrivial quadratic component. Its reduction generates the target line, giving $c_{\tau,S} = 0$. The split class group is also zero. The preceding theorem now proves the vanishing at every such weight. □

Corollary 57.12 (All coefficient primes through 10^7 in the real quadratic layer)**.** *For the quadratic character of $\mathbb{Q}(\sqrt{2})$, every prime $5 \le \ell \le 10^7$ and every positive multiple r of $\ell - 1$ satisfy $S(\alpha, r) = 0$. The conclusion transfers to its component on each period field of the interval for which the degree and modulus are prime to ℓ.*

Proof. For inert primes use the trivial base class group and Lemma 56.10. For the split primes first apply Proposition 57.9. Of the 332213 primes in this range congruent to 1 or 7 modulo eight, only 31 and 1546463 satisfy $\eta^{\ell-1} = 1 \bmod \ell^2$ in $\mathbb{Z}[\sqrt{2}]$. The following exact finite calculation is included for reproducibility. The pair (a, b) denotes $a + b\sqrt{2}$. Each loop over the binary digits squares the previous power and multiplies it by η when the digit is one. The sieve marks the proper multiples starting with the prime square, which exhausts the composites by their least prime factors.

```
from math import isqrt
bound = 10**7
prime = bytearray([1]) * (bound+1)
prime[:2] = bytes(2)
for d in range(2, isqrt(bound)+1):
    if prime[d]:
        prime[d*d::d] = bytes(1+(bound-d*d)//d)
survivors = []
count = 0
for p in range(5, bound+1):
    if not prime[p] or p % 8 not in (1, 7):
        continue
    count += 1
    m = p*p
    a, b = 1, 0
    for bit in bin(p-1)[2:]:
        a, b = (a*a+2*b*b) % m, (2*a*b) % m
        if bit == '1':
            a, b = (a+2*b) % m, (a+b) % m
    if (a,b) == (1,0):
        survivors.append(p)
assert (count, survivors) == (332213, [31, 1546463])
```

For the two survivors choose $\pi = A + B\sqrt{2}$ of norm ℓ. At the prime where π is a unit its residue modulo ℓ is $2A$. From $\pi(2A - \pi) = \ell$ we obtain the unit value $y = 2A - \ell(2A)^{-1} \bmod \ell^2$, with the inverse taken modulo ℓ. The last column in the table is $(y^{\ell-1} - 1)/\ell \bmod \ell$.

ℓ	A	B	$y \bmod \ell^2$	$(y^{\ell-1} - 1)/\ell \bmod \ell$
31	7	3	355	29
1546463	1601	713	534027699288	823555

The norm equalities follow from $A^2 - 2B^2 = \ell$. For an integer check of the final column, compute $\big(\operatorname{pow}(y, \ell-1, \ell^2) - 1\big)/\ell$ with modular exponentiation. Both residues are nonzero. At the conjugate prime the unit after division by ℓ is y^{-1} modulo ℓ^2. The argument of Proposition 57.11 gives $c_{\tau,S} = 0$ in each case. This proves vanishing for every indicated weight in the whole range of primes. Descent to E_x uses Theorem 22.17 and Lemma 22.16. □

The same S-unit test is defined at every larger split prime. An interval proof of the residual bound in Section 6.6 also requires uniform control at the unbounded primes, the other characters and the other inertia residue.

57.5 Two unit polynomials for the zero-residue strict groups

We compute the number of generators of the entire complementary strict group at weights divisible by $p - 1$, outside a fixed integer of controlled size for the interval. For a cyclic character the calculation also determines the full order whenever the constant specialization has length less than $1 + v_p(r)$. Keep $E_x \subseteq E_*$, $n_* = [E_* : \mathbb{Q}]$ and the cyclotomic modulus N_* of Theorem 19.15.

Let $L \neq \mathbb{Q}$ be a real cyclic subfield of E_*, $\Delta = \langle g \rangle = \operatorname{Gal}(L/\mathbb{Q})$, and $d = |\Delta|$. For each nontrivial subfield $K \subseteq L$, including L, let C_K be its conductor. Form the unit

$$w_K = N_{\mathbb{Q}(\zeta_{C_K})/K}(1 - \zeta_{C_K}), \qquad \epsilon_K = g(w_K)/w_K.$$

Here g restricts to a generator on every subfield. Let U_L^0 be generated by -1 and all conjugates of these ϵ_K.

Lemma 57.13 (Units of bounded index on the interval)**.** *Write $I_L = [\mathcal{O}_L^\times : U_L^0]$ and $h_L = |\operatorname{Cl}(L)|$. There is a positive integer*

$$J_U = 2n_*N_* \prod_{\substack{\mathbb{Q} \neq L \subseteq E_*^+ \\ L/\mathbb{Q} \text{ cyclic}}} I_L h_L, \qquad \log J_U \ll n_*^2 \log(2n_*N_*).$$

Proof. An automorphism above g takes ζ_C to ζ_C^a with a prime to C. The ratio $(1-\zeta_C^a)/(1-\zeta_C)$ is an algebraic integer by the geometric sum, and its inverse is integral by the same argument using an inverse of a modulo C. Its norm to K gives the asserted unit. At each embedding the logarithm of the absolute value of this unit has modulus at most $2N_* \log(2N_*)$. Indeed each conjugate of $1 - \zeta_C$ has absolute value between $2\sin(\pi/C)$ and two, and there are at most N_* factors in each of the two norms.

For a nontrivial complex character of Δ, let K be the field cut out by the character. Its primitive Dirichlet character ξ has conductor $C = C_K$ and is even. The ξ-coefficient of the logarithm vector of w_K is nonzero. To see this, unfold the norm to get $\sum_{a \bmod C} \bar{\xi}(a) \log|1-\zeta_C^a|$, summing over units. Replace ζ_C^a temporarily by $z\zeta_C^a$ for $0 < z < 1$ and expand the logarithm. The sums with frequencies j and $-j$ agree by evenness. The sum at frequency j is $\xi(j)G$, where $G = \sum_a \bar{\xi}(a)\zeta_C^a$. For invertible j change variables. Otherwise primitivity gives a unit congruent to one modulo $C/\gcd(C, j)$ on which ξ is nontrivial, so the sum is zero. Additive character orthogonality, summed over the frequencies, gives $|G|^2 = C$. Letting z increase to one now gives $-GL(1, \xi)$, by convergence of the Dirichlet series at one and Abel's limit theorem. The value is nonzero by Dirichlet's nonvanishing theorem. Passing to $g(w_K)/w_K$ multiplies by a nonzero difference between a character value and one. Repeating coordinates from K in the embeddings of L preserves nonvanishing in this component. The span of the logarithm vectors of the conjugates is invariant under Δ. The complex regular representation of a cyclic

group contains each character once, and the vectors consequently span the full hyperplane of coordinate sum zero. In particular I_L is finite by the unit theorem.

Delete one real coordinate from that hyperplane. For a nontorsion unit some $|\log|\sigma u||$ is at least $(\log 2)/2$. Otherwise every conjugate of the nonzero algebraic integer u^2-1 would have modulus strictly less than one. The deleted coordinate is the negative sum of the others. Thus in the remaining $d-1$ coordinates the logarithm lattice has minimum sup norm at least c/d, where $c=(\log 2)/2$. An open cube of side c/d injects up to its boundary into its real torus, giving covolume at least $(c/d)^{d-1}$. Select $d-1$ independent displayed unit vectors. Hadamard's bound on their determinant is at most $(2\sqrt{d}\,N_*\log(2N_*))^{d-1}$. Dividing the two bounds gives $\log I_L \ll d\log(2dN_*)$.

The conductor–discriminant formula gives $|\operatorname{disc} L| \le N_*^d$. Minkowski's bound supplies an integral ideal of norm at most $N_*^{d/2}$ in each ideal class. The number of ideals of norm at most Y is bounded by $Y^2\zeta_L(2) \le Y^2\zeta(2)^d$, by the Euler factors. Hence $\log h_L \ll d\log(2N_*)$. There are at most n_* cyclic subfields, since each corresponds to a cyclic subgroup of the character group with a generator. Summing proves the lemma. □

Suppose $p \ge 5$, $p \nmid J_U$, and p splits completely in L. Choose a place $v_0 \mid p$ and write $v_j = g^j v_0$. Choose β with $(\beta) = v_0^{h_L}$. For a unit z away from the places above p, put $z_j^\circ = p^{-v_j(z)} z_{v_j} \in \mathbb{Z}_p^\times$, where $v_j(p)=1$ and $L_{v_j}=\mathbb{Q}_p$. Define

$$\mathcal{L}_z(X) = \sum_{j=0}^{d-1} \frac{\log_p((z_j^\circ)^{p-1})}{(p-1)\log_p(1+p)} X^j,$$
$$f_z(X) = \sum_{j=0}^{d-1} \left(\frac{(z_j^\circ)^{p-1}-1}{p} \bmod p \right) X^j.$$

The first polynomial has coefficients in $\mathbb{Z}_p$, the second in $\mathbb{F}_p$. Their reductions differ by the unit factor $p-1$, as follows from $\log_p(1+pa) \equiv pa \bmod p^2$.

Theorem 57.14 (The first digits and the full lengths at divisible weights)**.** *Let α be any faithful character of Δ, $\tau=\alpha^{-1}$, $O=\mathbb{Z}_p[\tau(g)]$, and $r>0$ a multiple of $p-1$. Normalize $v_p(p)=1$ in this unramified coefficient ring. Put $s=1+v_p(r)$ and*

$$b_\tau = \min\bigl(v_p(\mathcal{L}_{\epsilon_L}(\tau(g))), v_p(\mathcal{L}_\beta(\tau(g)))\bigr).$$

A zero value is assigned infinite valuation. Then b_τ is finite. The finite strict group $S(\alpha,r)$ is cyclic over O, and for every $1 \le m \le s$ its subgroup killed by p^m has length $\min(m, b_\tau)$. If $b_\tau < s$, its full length is b_τ. It is nonzero precisely when the reduction of $\tau(g)$ is a common root of f_{ϵ_L} and f_β.

Proof. Identify the exponent lattice at the places above p with $\mathbb{Z}_p[X]/(X^d-1)$, by sending the place v_j to X^j. The action of g is multiplication by X. Evaluation at $\tau(g)$ is the projection to its orbit factor O, since $p \nmid d$. Under this identification the local principal-unit logarithm map of Theorem 57.10 sends z to $\mathcal{L}_z$. The completed units are generated by the conjugates of the ϵ_K since $p \nmid I_L$. If $K \ne L$, the logarithm vector is fixed by every element of $\mathrm{Gal}(L/K)$, and the faithful character component is zero. Conjugates of ϵ_L differ there by unit scalar multiplication.

The valuations at the v_j of the conjugates of β are the vectors $h_L e_j$. Since h_L is a p-adic unit, adjoining these elements to the ordinary units generates the completed S-units, where $S=\{v_j\}$. Indeed their valuations contain $h_L\mathbb{Z}^d$, and the kernel of the valuation map consists of ordinary units. Thus the image in O is generated by the two values displayed in the theorem.

The p-part of $\mathrm{Cl}_S(L)$ vanishes. Theorem 57.10 identifies B/TB with $O/p^{b_\tau}O$, with finite index, for the compact module B of Lemma 56.16.

Write $A_r = B/(T - t_r)B$, where $t_r = (1+p)^{-r} - 1$. This is the dual of the strict group by that lemma. The odd-prime binomial valuation gives $v_p(t_r) = s$. Consequently

$$A_r/p^m A_r = B/(p^m, T)B \simeq O/p^{\min(m,b_\tau)}O \qquad (1 \le m \le s).$$

The equality of quotients follows from equality of the two ideals after reduction modulo p^m. In particular the finite O-module A_r has at most one generator, by reduction modulo p. Its dual is cyclic with the same length. If $b_\tau < s$, a cyclic module with a longer elementary divisor would have larger length even after reduction modulo p^s. Taking $m = 1$ and reducing the two polynomial values proves the common-root assertion. □

Corollary 57.15 (The number of generators on every common period field)**.** *At every $p \ge 5$ outside J_U, throughout the interval, the dimension over $\mathbb{F}_p$ of the subgroup killed by p in the complementary sign of $\mathcal{S}_{p,r}(E_x)$ equals*

$$\sum_{\substack{\mathbb{Q} \neq L \subseteq E_x^+,\ L/\mathbb{Q} \text{ cyclic} \\ p \text{ splits completely in } L}} \deg \gcd\bigl(\overline{\Phi}_{[L:\mathbb{Q}]}(X), f_{\epsilon_L}(X), f_\beta(X)\bigr) \qquad (r > 0, \quad p - 1 \mid r).$$

The polynomials in each summand use its own L, g, v_0, β. In particular the same integer counts the generators at all such weights. If it is zero the entire complementary group vanishes.

Proof. The weights are even, so the complementary characters factor through E_x^+. The trivial one has zero strict group by Lemma 56.16. Each other character is faithful on the cyclic quotient cut out by its kernel. When p does not split completely in that field, the residual character is nontrivial on its decomposition group. Lemma 55.33 would force $p \mid h_L$ if the group survived. At a split prime the primitive d-th roots in characteristic p are distinct, since $p \nmid d$. The theorem gives one generator over the residue field for each surviving Frobenius orbit. Its degree over $\mathbb{F}_p$ is the orbit size, exactly the degree of the corresponding irreducible factor of the displayed gcd.

Finally the finite group of $E_x/\mathbb{Q}$ has order prime to p. Its integral orbit idempotents decompose the period-field group into these scalar groups by the coefficient descent in the proof of Theorem 22.17. At the primes away from p the additional conductor localizations cost zero by Lemma 22.16, since every inertia character here has order prime to p. Summing the residue dimensions proves the formula for the original group. □

Proposition 57.16 (The cubic field of conductor seven at thirteen)**.** *For each faithful character of $L = \mathbb{Q}(\zeta_7)^+$ the scalar strict group at $p = 13$ vanishes at every positive multiple of 12. This gives the same zero components on each period field containing L with $13 \nmid n_* N_*$.*

Proof. Put $t = \zeta_7 + \zeta_7^{-1}$, with minimal polynomial $t^3 + t^2 - 2t - 1$. Its discriminant is 49, so Minkowski's bound is at most $6\sqrt{49}/27 < 2$ and $h_L = 1$. Thirteen is -1 modulo seven and splits in the real subfield. With $g(t) = t^2 - 2$, one has $w_L = 2 - t$ and $\epsilon_L = 2 + t$. At the three local embeddings in the order v_0, gv_0, g^2v_0, the values of t modulo 169 can be taken as $34, 163, 140$. Indeed 34 solves the cubic modulo 169 with simple reduction and $g^{-j}(t)$ gives the other two entries in this order. Raising the corresponding values of $2 + t$ to the twelfth power modulo 169, subtracting one and dividing by thirteen gives $(9, 6, 11)$ mod 13. The polynomial $9 + 6X + 11X^2$ takes values $9, 5$ at $3, 9$, the two primitive cube roots modulo thirteen. Thus this single ordinary unit already generates each local exponent line over its coefficient ring. Together with the trivial class group the exact sequence of Theorem 57.10 gives $B/TB = 0$ for

both characters, so the specialized groups vanish. This calculation uses no index assumption on the other fields of the interval. □

When the common root occurs and $b_\tau \geq 1+v_p(r)$, the formula computes the indicated digits and leaves the possible excess length at that weight. The primes dividing J_U, the other weight residues, and the comparison of signed projected periods still enter Section 6.6.

57.6 Vanishing at zero-residue weights in the first three dyadic layers

Let $C_j = \mathbb{Q}(\zeta_{2^{j+2}})^+$. These are the actual real dyadic subfields of the period construction. We examine the whole strict group $\mathcal{S}_{p,r}(C_j)$ at weights $p-1 \mid r$. The rational and quadratic characters were treated in Lemma 56.16 and Corollary 57.12. We compute the remaining faithful contributions for the layers of degrees four and eight.

Lemma 57.17 (A single unit in the faithful part of a dyadic layer)**.** *Let $d = 2^j \geq 4$, $q = 4d$, $n = 2d$, $L = C_j$, and suppose that $p \geq 5$ is prime with $p \equiv \pm 1 \pmod q$. For the calculation use $Z = \zeta_q$, $t = Z + Z^{-1}$, and the following polynomial of degree less than n, with integer coefficients taken modulo p^2,*

$$A(Z) = (1 + Z - Z^{n-1})^{2(p-1)} - 1 \pmod{Z^n + 1,\ p^2}.$$

Each coefficient is divisible by p. Write $a_h \in \mathbb{F}_p$ for its quotient by p modulo p. For $0 \leq i < d/2$ take the representative e_i of $3^i \bmod q$ in $[0, q)$, and put

$$H_{p,d}(X) = \sum_{i=0}^{d/2-1} (-1)^{\lfloor e_i/n \rfloor} a_{e_i \bmod n} X^i.$$

If $p \nmid h_L$ and $\gcd(H_{p,d}, X^{d/2}+1) = 1$ in $\mathbb{F}_p[X]$, every faithful character of $L/\mathbb{Q}$ has zero scalar strict group at every positive multiple of $p-1$.

Proof. The group of the real field is cyclic of order d, generated by $g : Z \mapsto Z^3$ modulo complex conjugation. Indeed successive squaring gives $v_2(3^{2^i} - 1) = i + 2$ for $i \geq 1$, and no power of 3 is -1 mod 8. Its element $g^{d/2}$ takes t to $-t$, since $3^{d/2} \equiv 1 + 2d \bmod 4d$. Here $w_L = 2 - t$ and $\epsilon_L = (2 - t^3 + 3t)/(2 - t) = (1 + t)^2$. The ring $\mathbb{Z}[Z]/(Z^n + 1)$ realizes the integral cyclotomic coordinates. The prime splits in L, so the unit $\epsilon_L^{p-1} - 1$ is in $p\mathcal{O}_L$. It is therefore in $p\mathbb{Z}[\zeta_q]$. Since $Z^{-1} = -Z^{n-1}$, reduction gives exactly the polynomial in the statement and permits the coefficient division.

In the split ring $\mathcal{O}_L/p \simeq \prod_{v|p} \mathbb{F}_p$, the quotient by p just computed is the table of Fermat quotients of ϵ_L. The inclusion into $\mathbb{Z}[\zeta_q]/p$ is injective: an element of L integral after division by p in the larger field is already integral in L. Write $b_i = Z^{e_i} + Z^{-e_i}$ for $0 \leq i < d/2$. These lie in the (-1)-eigenspace of $g^{d/2}$. Their pairs of exponents modulo n, up to sign, are disjoint because 3 generates the real cyclotomic quotient and its order after factoring by $g^{d/2}$ is $d/2$. Their coefficients on those distinct exponent pairs are units. They form a basis of that eigenspace over $\mathbb{F}_p$: in the split ring the involution exchanges the places in pairs, so the eigenspace has dimension $d/2$. It is the direct sum of the faithful character components, whose eigenvalues for g are exactly the roots of $X^{d/2} + 1$.

Project to this eigenspace by $(1 - g^{d/2})/2$. This retains the odd exponents of the polynomial, since the involution acts there by $Z \mapsto -Z$. The coefficient of b_i is the coefficient at $Z^{e_i \bmod n}$ with the sign shown in the statement. Moreover $gb_i = b_{i+1}$, with $gb_{d/2-1} = -b_0$. In this basis the projection of the unit table is $H_{p,d}$ in the module $\mathbb{F}_p[X]/(X^{d/2} + 1)$. Its conjugates span that module if the two polynomials are relatively prime, by Bézout's identity. Consequently

each faithful local logarithm line is generated modulo p by ordinary units, hence integrally by Nakayama's lemma. With $p \nmid h_L$, Theorem 57.10 gives zero constant specialization at each such character. Lemma 56.16 and compact Nakayama give the asserted vanishing. □

Theorem 57.18 (Full strict vanishing in degrees four and eight)**.** *At every prime* $5 \le p \le 10^7$ *and every positive multiple* r *of* $p-1$*,*

$$\mathcal{S}_{p,r}(C_j) = 0 \qquad (0 \le j \le 3).$$

For $p \not\equiv \pm 1 \pmod{64}$ *in this same range, the equality holds at every* $j \ge 0$*.*

Proof. Fukuda and Komatsu prove that no prime below $1.2 \cdot 10^8$ divides the class number of any C_j [27, Corollary 1.1]. At a nonsplit prime the residual faithful character of C_j is nontrivial on the decomposition group, so Lemma 55.33 gives zero. At the split primes for $d = 4, 8$, the following finite calculation gives the number of primes tested and the number having a gcd of positive degree in Lemma 57.17, respectively:

d	split primes	positive gcd degree
4	166087	0
8	82993	0

Here are exact arithmetic instructions to reproduce the table. All coefficient lists start with the constant term. For each indicated prime reduce after each multiplication. In the quotient by $Z^n + 1$, form an ordinary convolution c with an extra zero at index $2n-1$, and return $(c_i - c_{i+n}) \bmod p^2$. Thus all intermediate coefficients may be computed as integers. The following pseudocode uses polynomial remainders over $\mathbb{F}_p$ in the last step.

```
prime[0..10000000] = true
for a from 2 through floor(sqrt(10000000)):
    if prime[a]: mark a*a, a*a+a, ... <= 10000000 false
for d in [4, 8]:
    count = 0; exceptional = 0; n = 2*d
    for p from 5 through 10000000:
        if not prime[p] or p mod (4*d) not in [1, 4*d-1]: skip p
        count = count+1
        u = 1+Z-Z^(n-1); b = 1; e = 2*(p-1)
        while e > 0:
            if e is odd: b = product(b,u)
            u = product(u,u); e = floor(e/2)
        b = b-1
        check that p divides each coefficient of b
        h = 1; H = 0
        for i from 0 through d/2-1:
            H = H + (-1)^floor(h/n)*(b[h mod n]/p)*X^i
            h = (3*h) mod (4*d)
        F = X^(d/2)+1; G = H reduced modulo p
        while G is nonzero: (F,G) = (G,remainder(F,G))
        if degree(F) > 0: exceptional = exceptional+1
    record (count, exceptional)
```

The sieve removes exactly the composites, each of which has a prime factor at most its square root. Repeated squaring preserves the product of the accumulator and the remaining power of

the base. The loop over i reads the faithful basis in the order of the lemma. The Euclidean algorithm terminates with a scalar multiple of the gcd. This justifies the finite computation independently of any choice of roots in a residue field.

Each character of C_3 is either trivial or faithful on exactly one of C_1, C_2, C_3. The rational component vanishes by Lemma 56.16. The quadratic component vanishes by Corollary 57.12. The lemma and the table account for the other two layers. All these fields are totally real and of degree prime to p. Character descent, or the prime-to-p idempotents in Theorem 22.17, gives vanishing of the entire strict group. For the final assertion Theorem 24.28 identifies the group at any layer with one of the four groups just treated. □

Corollary 57.19 (The corresponding summand on the period fields)**.** *At x let $C_j \subseteq E_x$ be any layer covered by Theorem 57.18, and assume $p \nmid [E_x : C_j]$. For each of its weights the field average onto C_j has zero image on $\mathcal{S}_{p,r}(E_x)$.*

Proof. The integral average has image the invariants under $\mathrm{Gal}(E_x/C_j)$. Restriction identifies these with the lower strict group: global cohomology descends by averaging, and restriction on the local conditions is injective by corestriction at the primes over p and on inertia elsewhere. The lower group is zero by the theorem. □

This removes the indicated real dyadic character components at all their matching weights on the common intervals. Characters involving the other factors of E_x and the other twist residues still occur in the local sum of Section 6.6.

57.7 The two possible characters in the full real dyadic tower

For an odd prime p put $q = 2^{\max(v_2(p-1),v_2(p+1))}$ and $d = q/4$. Thus $L = \mathbb{Q}(\zeta_q)^+$ has degree d. It is the highest real dyadic layer in which p splits completely: the splitting condition at conductor 2^h is $p \equiv \pm 1 \bmod 2^h$. For the primes through 10^7 the class numbers at all levels are prime to p by Fukuda and Komatsu [27, Corollary 1.1]. Consequently at a positive multiple of $p-1$ every faithful character from a level above L has zero strict group by Lemma 55.33 for $p \geq 5$. We evaluate the logarithms on all levels up to L simultaneously.

Lemma 57.20 (A single transform for all the split layers)**.** *Suppose $d \geq 4$. Choose a primitive q-th root z in the unramified extension of $\mathbb{Z}_p$ of residue degree one if $p \equiv 1 \bmod q$, two otherwise. Write $g(\zeta_q) = \zeta_q^3$ on the real field. Set $u_i = 2 - z^{3^i} - z^{-3^i}$ for $0 \leq i < d$. These are in $\mathbb{Z}_p^\times$. Put*

$$c_i = \frac{u_i^{p-1} - 1}{p} \bmod p, \qquad A_k = \sum_{i=0}^{d-1} c_i \omega^{ki}, \qquad \omega = (z \bmod p)^4, \quad 0 \leq k < d.$$

Let τ be the lifted scalar character with reduction $\bar{\tau}(g) = \omega^{-k}$ and order $e = d/\gcd(k,d) \geq 4$. On the unique subfield of degree e its faithful ordinary unit ϵ of Section 57.5 generates the local logarithm component if $A_k \neq 0$.

Proof. The Frobenius of the unramified coefficient extension sends the chosen Teichmüller root to its p-th power, which is itself or its inverse. The traces $z^{3^i} + z^{-3^i}$ are therefore rational p-adic integers. Modulo p, each u_i is nonzero since a primitive root of order q raised to an odd exponent is different from one. These values are the conjugates of $w_L = (1-\zeta_q)(1-\zeta_q^{-1})$ at a fixed place. The indexing is by g^i acting on the element, hence by g^{-i} acting on the place. This gives precisely the inverse in $\bar{\tau}(g)$.

For a smaller nontrivial layer K the norm of w_L to K is w_K with compatible choices of primitive roots. At a single step this follows in the full cyclotomic field from $(1-Z)(1+Z) =$

$1-Z^2$; then take the norm to the real subfield. The logarithm turns a norm into the sum over the fibers. The same holds for Fermat quotients modulo p since $(1+pa)(1+pb) \equiv 1+p(a+b) \bmod p^2$. Thus the weighted sum for an inflated character is its logarithm at the field of that character, up to the common unit normalizing the logarithm. The unit $g(w_K)/w_K$ supplies the further factor $\omega^{-k}-1$, which is a unit for the indicated orders. The value $A_k \neq 0$ consequently gives a generator modulo p, hence a generator of the rank-one local exponent lattice. □

Theorem 57.21 (Full dyadic strict groups outside two coefficient primes)**.** *Let $3 \le p \le 10^7$ be prime, and let $r > 0$ be divisible by $p-1$. At every $j \ge 0$ one has $\mathcal{S}_{p,r}(C_j) = 0$ unless $p = 18433$ or $p = 114689$. At the former prime only a single character of degree-256 quotient can contribute, and at the latter only a single character of degree-1024 quotient can contribute. In the table, k follows the root convention specified in the proof, e is the character order, and the last column is $\bar{\tau}(g)$ in $\mathbb{F}_p$.*

p	d	k	e	$\bar{\tau}(g)$
18433	512	426	256	13924
114689	4096	1420	1024	34058

For each such prime the possible group is cyclic over $\mathbb{Z}_p$ and is obtained by restriction from the layer of degree e once $2^j \ge e$. If $p \mid r$ its order is at most p.

Proof. At three the vanishing follows from Theorem 24.28. For $p \ge 5$ the rational and quadratic components are zero by Theorem 57.18. It remains to test the characters in the lemma. We give the complete finite calculation. All powers, including those in a quadratic ring, may be taken by binary exponentiation. For $p \equiv 1 \bmod 4$, take the smallest positive quadratic nonresidue h and put

$$z_0 = h^{(p-1)/q} \bmod p, \qquad z = z_0^p \bmod p^2.$$

For $p \equiv 3 \bmod 4$, work in $(\mathbb{Z}/p^m)[i]$, $i^2 = -1$, with $m = 1, 2$ as specified. Take the least positive integer h for which h^2+1 is a quadratic nonresidue. Such an h exists: the equation $v^2 - h^2 = 1$ has $p-1$ solutions by factoring the left side, so $\sum_h (\frac{h^2+1}{p}) = -1$. The term at zero is one. Take $z_0 = (h+i)^{(p^2-1)/q} \bmod p$, lift its two coefficients to $[0, p)$, and take $z = z_0^p \bmod p^2$ in that ring. The norm of $h+i$ is a nonsquare, hence $h+i$ is a nonsquare in the cyclic residue multiplicative group. Raising a nonsquare to the group order divided by q gives exact order q because q is a power of two. This also proves the order assertion in degree one. The subsequent p-th power kills the possible principal-unit error of the lifted root modulo p^2 and preserves exact order. In degree two it selects the conjugate residue root, which defines the allowed choice of embedding.

For each prime in the sieve of Theorem 57.18 the following operations suffice. The symbol $F(c, w)$ denotes the list of the values of the polynomial with coefficient list c on the consecutive powers of w, starting with exponent zero.

```
if d < 4: skip this prime
s = z + z^(q-1) modulo p^2
for j from 0 through d-1:
    c[j] = (least_residue((2-s)^(p-1),p^2)-1)/p
    s = (s^3-3*s) modulo p^2
w = (z modulo p)^4
values = F(c,w)
for k from 1 through d-1, omitting d/2:
    if values[k] == 0: record (p,d,k,d/gcd(d,k))
```

The initial s has zero imaginary part, by the order and Frobenius properties proved above. The recurrence is the identity $x^3+x^{-3}=(x+x^{-1})^3-3(x+x^{-1})$. To implement F, return the input for length one. Otherwise set $b=F(c_{\mathrm{even}},w^2)$ and $a=F(c_{\mathrm{odd}},w^2)$, with each subsequence in its original order. For input length D the entries at $i, i+D/2$ are $b_i+w^i a_i, b_i-w^i a_i$ for $0\le i<D/2$. This follows by separating the even and odd exponents and using $w^{D/2}=-1$. These instructions thus evaluate the sums of the lemma using only integer arithmetic and pairs of residues.

There are 166087 primes with $d\ge 4$ in this range. In total 5211578 character values of order at least four are tested. The zero values give exactly the two rows displayed in the theorem. For additional counts, the numbers tested at orders 2^j, for $j=2,\dots,18$ successively, are

$$332174, 331972, 331752, 331840, 330432, 331904, 333056, 331008, 333312,$$
$$331776, 327680, 311296, 335872, 327680, 262144, 196608, 131072.$$

Here the counts can also be checked directly by adding $\varphi(2^j)$ for each prime with $2^j\mid d$. For every nonzero test value, the class-number theorem and Theorem 57.10 now give zero constant specialization and hence vanishing at every indicated weight. The same two pairs of prime and layer degree occur in Gras’s computations of the ordinary p-adic regulator [28]. The strict local condition here also allows units supported at p.

To bound the two remaining components we retain one more digit. Both primes are $1 \bmod q$, so this calculation takes place in the integers. For each displayed row lift z_0 by $z=z_0^{p^2} \bmod p^3$, set $w=z^{4k} \bmod p^2$, and run the same trace recurrence modulo p^3. For each u_i let $b_i=((u_i^{p-1} \bmod p^3)-1)/p$, taking the least residue first. The resulting values are

p	h	z_0	$w \bmod p$	$p^{-1}\sum_i w^i(b_i-pb_i^2/2) \bmod p$
18433	5	17660	12072	921
114689	3	2187	2401	99260

To reproduce the last column, accumulate the sum modulo p^2, using the inverse of two there, and then divide its least residue by p. The logarithm series gives $p^{-1}\log(1+pb_i)\equiv b_i-pb_i^2/2 \bmod p^2$ since $p\ge 5$. Changing to the normalization in Theorem 57.14 multiplies the entire sum by a unit. The norm to the smaller layer and the factor from $g(w_L)/w_L$ in the lemma preserve this valuation. Thus the indicated ordinary unit has valuation exactly one in each of the two logarithm lines. The additional p-units can only enlarge its image.

The class group term is zero by Fukuda and Komatsu. Hence the constant specialization B/TB of Theorem 57.10 is either zero or $\mathbb{Z}/p$ in the two possible characters. Their coefficient rings are $\mathbb{Z}_p$ because $e\mid p-1$. Reduction of $B/(T-t_r)B$ modulo p gives at most one generator. For $p\mid r$ we may reduce modulo p^2 and replace $T-t_r$ by T, as in Theorem 57.14; the resulting quotient has order at most p, forcing the full cyclic group to have order at most p. The character decomposition over the totally real fields is integral since the degrees are powers of two. Restriction on these towers of degree prime to p identifies the individual characters with their inflations, including the strict local conditions, as in Corollary 57.19. This proves the theorem. □

Corollary 57.22 (A single arithmetic progression for longer groups)**.** *At each of the two primes either all indicated lengths are at most one, or there exists $z_p\in\mathbb{Z}_p^\times$ such that for every positive r divisible by $p-1$ and every j,*

$$\log_p|\mathcal{S}_{p,r}(C_j)|\le 1+v_p(r-z_p).$$

Here $v_p(0)=+\infty$. In particular lengths greater than a are confined to at most one residue class modulo $(p-1)p^a$ for each integer $a\ge 1$.

Proof. It suffices to consider the one possible field and character. If $B/TB = 0$, compact Nakayama gives $B = 0$. Otherwise a single generator gives $B = \mathbb{Z}_p[[T]]/I$, since its reduction modulo (p, T) has dimension one. Constant terms of elements of I form exactly $p\mathbb{Z}_p$ by the constant specialization. Choose $F = p + Tc(T) \in I$. For $t \in p\mathbb{Z}_p$, each specialization has length at most $v_p(F(t))$. If $c(0)$ is divisible by p, this valuation is one for all t. Otherwise F has a unique root $u \in p\mathbb{Z}_p$: beginning at zero modulo p, each lift of a root modulo p^a changes the next digit with unit coefficient $c(0)$ mod p. Completeness gives the root. For $t \in p\mathbb{Z}_p$ the integral divided difference $(F(t) - F(u))/(t - u)$ is a unit, by the same reduction, whenever $t \neq u$. Also $u = -p/c(u)$ has valuation one. Thus $z_p = -\log(1 + u)/\log(1 + p)$ is a unit, and $v_p(t_r - u) = 1 + v_p(r - z_p)$ by the odd-prime logarithm. This proves the inequality. Length greater than a forces $r \equiv z_p \bmod p^a$; combining with the weight residue proves the final assertion. □

Corollary 57.23 (The real dyadic image in the residual sum on the common interval)**.** *Include* $18433, 114689$ *in the fixed finite set* Π *of Section 6.6 when selecting the common intervals. Let* $C_j \subset E_x$ *be a real dyadic layer. For every odd prime* $p \leq 10^7$ *and every weight in the residual sum divisible by* $p - 1$*, the image of* $\mathcal{S}_{p,r}(C_j)$ *in* $R_{p,r}(E_x)$ *is zero on every sufficiently distant such interval. The fields and terminal primes can be those of Corollary 9.34.*

Proof. Only the two displayed primes require consideration. Every incoming class is restricted from C_8 or C_{10}, whenever its supplying layer is present, by the theorem. For $r \leq x^{\eta}$ both fixed layers lie in the real dyadic part of L_x for large V. For $r > x^{\eta}$ both lie in $B(x)$, and the prime belongs to Π. In either case the field average $J_{p,r}$ fixes the restricted class, since it comes from the fixed field of that average. The factor $1 - J_{p,r}$ in the definition of $R_{p,r}$ therefore kills it already before truncation. This argument concerns the image of restriction even if a larger extension has degree divisible by p. The common field and prime selection allows an arbitrary fixed finite set Π containing the required odd divisors, so the same choices apply to the signed period calculation. □

The other character components of E_x, other weights and the larger coefficient primes must still be included in the full local estimate. The two possible nonzero strict groups in the real dyadic tower were removed here by the actual field averages.

57.8 Relative regulators at the half-residue weights

Let $C_j = \mathbb{Q}(\zeta_{2^{j+2}})^+$. We treat the residual character at the second of the two weights in Corollary 54.14. Suppose $j \geq 1$, put $2n = 2^j$, and let α be a faithful character of $C_j/\mathbb{Q}$. Its primitive conductor is $c = 8n$. Let $p \equiv 1 \pmod 4$ be prime and write η_p for the quadratic character of conductor p. For $r \equiv (p-1)/2 \pmod{p-1}$ the residual character of Section 55.10 is the reduction of $\lambda = \alpha^{-1}\eta_p$. Write L for the field fixed by the kernel of λ and $F = C_{j-1}$, with $C_0 = \mathbb{Q}$. The two characters have coprime conductors, so L is real cyclic of degree $2n$, F is cut out by λ^2, and L/F is quadratic. We compare their ordinary class numbers h_L, h_F.

Lemma 57.24 (The relative unit lattice at a ramified prime)**.** *For these fields, with the usual regulators and* $R_{\mathbb{Q}} = 1$*,*

$$\frac{R_L}{R_F} \geq \frac{[n(\frac{1}{2}\log p - \log 2)]^n}{n!}.$$

Also extension of ideals injects $\mathrm{Cl}(F)$ *into* $\mathrm{Cl}(L)$*.*

Proof. Pair the real embeddings of L over those of F, choosing one member τ_i of each pair. Let s generate $\mathrm{Gal}(L/F)$. The kernel of the norm on units modulo signs consists of units u with

$u\,s(u) = \pm 1$, modulo $\{1, -1\}$. Their log vectors $a_i = \log|\tau_i(u)|$ form a lattice Γ of rank n in $\mathbb{R}^n$. Indeed the full logs are $(a, -a)$, and the image of the norm on units contains the squares of units of F. Dirichlet's unit theorem gives the rank, discreteness and full span.

For a nonzero vector of this lattice one has $u \notin F$, since a unit of F with square ± 1 is ± 1. The relative discriminant divides the discriminant $(u - s(u))^2$ of the order with basis $1, u$, as seen by passage to local integral bases. At p the field F is unramified and the inertia in L has order two, from the factor η_p. Thus every prime of F above p ramifies tamely in the quadratic extension and occurs in the relative discriminant. Their product has norm p^n. Consequently

$$p^{n/2} \le \prod_{i=1}^{n} |\tau_i(u - s(u))| \le 2^n \exp\!\left(\sum_i |a_i|\right).$$

Every nonzero vector of Γ has ℓ^1-norm at least $b = n(\tfrac{1}{2}\log p - \log 2) > 0$. The cross-polytope of this radius has volume $2^n b^n/n!$. Minkowski's convex body theorem, first for smaller radii and then in the limit, gives $\det\Gamma \ge b^n/n!$.

Complete a basis of the relative units modulo signs by lifts of a basis of the image of the norm. In the regulator matrix omit the last conjugate row. Add the first $n-1$ rows to the corresponding conjugate rows. The bottom rows now give the logs of norms, zero on the first n columns. The two diagonal determinants in absolute value are $\det\Gamma$ and R_F times the index of the norm image in the units of F modulo signs. This proves the regulator assertion, including $n = 1$.

The class number of F is odd. For completeness, if it were even, the Hilbert class field for the ordinary ideal classes would give a nontrivial maximal elementary abelian unramified two-extension D/F split at the real places. It is Galois over $\mathbb{Q}$ by invariance of these conditions; its Galois group is a two-group. The only possible finite ramification over $\mathbb{Q}$ is at two, which is totally ramified in F. Inertia in $D/\mathbb{Q}$ there has order $[F : \mathbb{Q}]$, hence is proper. A maximal subgroup containing it is normal of index two. Its fixed field would be quadratic and unramified at every finite prime, contrary to the quadratic discriminant formula. Finally the norm after extension of ideal classes is squaring. Its kernel on the odd class group of F is trivial. □

Lemma 57.25 (The joint mean of the faithful Dirichlet values)**.** *Uniformly for $p \to \infty$ and*

$$n \le \frac{(\log p)^2}{\log\log(3p)},$$

one has

$$\left(\frac{1}{n}\sum_{\substack{a \bmod 2n\\ a \text{ odd}}} |L(1, \alpha^a\eta_p)|^2\right)^{1/2} \le (1 + o(1))\frac{\log p}{4\sqrt{n}}.$$

Proof. All the indicated characters are primitive of conductor $D = cp$. Put $y = \lceil\sqrt{D}\,\log^2(2D)\rceil$. For any primitive nonprincipal character of conductor D, its sum over an interval is $O(\sqrt{D}\log(2D))$, with an absolute constant. Indeed its additive Fourier coefficients vanish at nonunits and have modulus $\sqrt{D}$ at units by the primitive Gauss sum identity. Expand the indicator of a residue interval using its geometric sums, bounded at frequency $1 \le h < D$ by $D/(2\min(h, D-h))$, and divide by D. The zero frequency for the character vanishes, and full periods may first be omitted. Partial summation therefore permits truncating the Dirichlet series at y with error $O(1/\log(2D))$ per character.

Let $G_0 = (\mathbb{Z}/c\mathbb{Z})^\times/\{1, -1\}$, of order $2n$. Form $s_g = \sum_{m \le y,\ [m]=g} \eta_p(m)/m$ on this group. For the representative $1 \le a < c/2$ of a class $g = \{a, c-a\}$, bounding the two harmonic sums

separately gives

$$|s_g| \le \frac{2\log y}{c} + e_g, \qquad e_g = \frac{1}{a} + \frac{1}{c-a} + \frac{2}{c}, \qquad \sum_g e_g^2 \ll 1.$$

For each progression, terms after its first are bounded by the harmonic sum up to y divided by c. The squared error estimate follows by summing reciprocal squares and the constant terms. The truncated character values are precisely the Fourier sums of the same s_g at the odd powers of α. Orthogonality on G_0, enlarged to all characters before applying Parseval, gives their root mean square over the n odd powers at most

$$\sqrt{2}\,\|s\|_2 \le \sqrt{2}\left(\sqrt{2n}\frac{2\log y}{c} + O(1)\right) = \frac{\log y}{2\sqrt{n}} + O(1).$$

By the bound on n, $\log y = \frac{1}{2}\log p + O(\log\log(3p))$ and $\sqrt{n}/\log p \to 0$ uniformly. The truncation error and the absolute $O(1)$ term are absorbed, which gives the assertion. □

Theorem 57.26 (Vanishing in a growing range of dyadic layers)**.** *There is an absolute p_0 such that for $p \ge p_0$, $p \equiv 1 \pmod 4$, and n in the range of Lemma 57.25,*

$$\frac{h_L}{h_F p^{n/2}} \le \frac{n!}{n^n}\left(\frac{1}{\sqrt{2}} + o(1)\right)^n < 1.$$

The error in the parenthesis is uniform. If $\operatorname{ord}_{2n}(p) \ge n/2$, then $S(\alpha, r) = 0$ for every positive $r \equiv (p-1)/2 \pmod{p-1}$, with the strict local conditions of Section 55.10. In particular this proves vanishing at every such weight on all the indicated layers when $p \equiv 5 \pmod 8$, and on the quadratic and quartic layers for both prime classes $1, 5 \pmod 8$.

Proof. The characters of L outside those of F are exactly the n odd powers of λ, whose conductors are all cp. The conductor–discriminant formula gives $|\Delta_L|/|\Delta_F| = (cp)^n$. Divide the analytic class number formulas for these two totally real fields, both with two roots of unity [29, Theorem 19.12]. Factor their Dedekind zeta functions into primitive Dirichlet functions. The common factors cancel in the quotient of the residues at one, giving

$$\frac{h_L}{h_F} = \frac{(cp)^{n/2}}{2^n}\,\frac{R_F}{R_L}\prod_{\substack{a \bmod 2n \\ a \text{ odd}}} |L(1, \alpha^a \eta_p)|.$$

The product of the absolute values equals the positive residue ratio since nonreal characters are paired with their conjugates. By the arithmetic–geometric mean the product is at most the n-th power of the root mean square in the preceding lemma. Insert its bound and the regulator bound. After division by $p^{n/2}$ the result is

$$\frac{n!}{n^n}\left(\frac{\sqrt{8n}}{2}\,\frac{(1+o(1))\log p}{4\sqrt{n}\,(\frac{1}{2}\log p - \log 2)}\right)^n.$$

The parenthesis tends uniformly to $1/\sqrt{2}$. Since $n! \le n^n$ the strict inequality follows.

Suppose the strict group were nonzero. Its first torsion layer gives a nonzero equivariant homomorphism from $\mathrm{Cl}(L)$ to the additive residual character module, by the proof of Lemma 55.33. Its local hypothesis holds because inertia at p acts by η_p. The image has size at least $p^{\operatorname{ord}_{2n}(p)}$, since it is stable under a primitive $2n$-th root after reduction. Classes extended from F are fixed by s. The character of s on the target is -1, and p is odd, so the homomorphism kills those classes. By Lemma 57.24 the available quotient has order h_L/h_F. This contradicts the class number bound whenever the stated residue degree condition holds.

For $p \equiv 5 \pmod 8$ one has $v_2(p^{2^a} - 1) = a + 2$ for $a \geq 0$, by successive squaring. Hence the order modulo 2^j is $2^{\max(j-2,0)}$, at least $n/2$. For $j = 1, 2$ every $p \equiv 1 \pmod 4$ has order one modulo 2^j, which also suffices. □

Corollary 57.27 (The half-residue summands on the period fields)**.** *On the fields and intervals of Section 6.6, the faithful components from the layers and primes in Theorem 57.26, with $C_j \subset E_x$ and $p \nmid [E_x : \mathbb{Q}]$, contribute zero to $R_{p,r}$ for every indicated $1 \leq r < t(x)$. One may include the bounded coefficient primes in the fixed set Π so that the inflated contributions from the same degree range at these smaller primes are removed by the field averages as well.*

Proof. The integral character comparison of Theorem 22.17 identifies the component over E_x with the scalar group subject also to its conductor conditions. This is a subgroup of the strict group just shown to vanish. Increase the absolute cutoff by the fixed prime divisors of $[K_\psi : \mathbb{Q}]$ if necessary to cover all possible odd divisors of the field degrees. For the finitely many smaller primes the displayed degree range involves only finitely many C_j. All these fields lie in both L_x and $B(x)$ for sufficiently large x. Include those primes in Π. The applicable field average then fixes every class inflated from these subfields and $1 - J_{p,r}$ kills it. This argument only uses invariance for the small primes, even when the whole character decomposition over E_x fails to be integral. The choice of Π is fixed before the intervals and is compatible with the period primes in Corollary 96.8. □

Corollary 57.28 (Every weight on a common growing subfield)**.** *For a sufficiently distant period interval $[V, V^{3/2}]$, let $D_V = C_j$ for the largest $j \geq 1$ with*

$$2^{j-1} \leq \frac{(\log V)^2}{2 \log\log(3V)}.$$

Its degree is of order $(\log V)^2 / \log\log(3V)$. For every x in the interval, $V \leq p \leq P(x)$ with $p \equiv 5 \pmod 8$, and every $1 \leq r < t(x)$, the field average onto D_V acts as zero on the actual residual quotient $R_{p,r}$ over E_x. For $p > P(x)$ in the same progression the sum of the log orders coming from D_V, over all such primes and weights, is $O_{\psi,\varepsilon}(V^C)$ for a fixed C.

Proof. The field D_V lies in every E_x on the interval because the available real dyadic degrees grow at least as a fixed positive power of V, by Theorem 19.15. All the indicated primes are prime to $[E_x : \mathbb{Q}]$ for large V. The field average commutes with the sign and field averages defining $R_{p,r}$. Its image on the full strict group is restriction from D_V by descent through a prime-to-p extension. We bound this latter group before forming the quotient.

At a multiple of $p - 1$, Theorem 24.28 gives zero at every real dyadic level when $p \equiv 5 \pmod 8$. At the half residue the twist is even. The rational component vanishes by Proposition 20.6. The other components are faithful on some dyadic subfield of D_V. Each satisfies the size condition of Theorem 57.26, because $(\log z)^2 / \log\log(3z)$ is increasing for sufficiently large z and $p \geq V$. They all vanish by that theorem and integral character descent. At every remaining weight, $p - 1 \nmid 2r$. Lemma 9.31 bounds each full log order by $\log J(V) \ll V^C$, uniformly. This bounds its exponent in powers of p by $V^{O(1)} < b_0(x)$, so its image is killed in the formation of $R_{p,r}$ for $p \leq P(x)$. Finally $P(x) > 2\lfloor V^{1203/2} \rfloor + 1$ for large V. The product divisibility in the same lemma bounds the total log order at the larger primes by $\log J(V)$. This proves both claims. □

Corollary 57.29 (The full real dyadic tower at primes three modulo eight)**.** *Write $C_{J(x)}$ for the real dyadic field used to construct E_x, and e_D for the field average onto D. For $V \leq p \leq P(x)$*

with $p \equiv 3 \pmod 8$, $e_{C_{J(x)}} R_{p,r} = 0$ *at every* $1 \le r < t(x)$. *More generally, for* $p \equiv 3 \pmod 4$ *and* $p \not\equiv -1 \pmod{64}$ *in this range,*

$$e_{C_{J(x)}} R_{p,r} = e_{C_{\min(3,J(x))}} R_{p,r}.$$

The total log order from these real dyadic subfields at $p > P(x)$ *is polynomially bounded in* V.

Proof. At separated weights use Lemma 9.31 and the truncation argument of Corollary 57.28. At the half residue, $(p-1)/2$ is odd. Complex conjugation fixes the real subfield, hence acts as the identity on the image of its field average. The complementary sign projector $(1-c)/2$ kills that image. At the zero residue Theorem 24.28 gives zero for $p \equiv 3 \pmod 8$. For the other indicated primes it gives descent of the entire dyadic strict group to a layer of degree at most eight. Consequently the field averages onto $C_{J(x)}$ and $C_{\min(3,J(x))}$ have the same image on this group. They are nested commuting idempotents, so this equality passes to the sign, field and truncation quotients. The large-prime bound follows on E_* from Lemma 9.31 and descends to every $C_{J(x)}$ by prime-to-p restriction. □

The estimate here includes twists prime to p as well as multiples of p. Its range grows with the coefficient prime. The highest dyadic layers of the period fields, all the other residue characters outside the earlier bounds, and the full marked period comparison still enter Section 6.6.

57.9 Relative class numbers in complex dyadic layers

Write $C_j = \mathbb{Q}(\zeta_{2^{j+2}})^+$. Let $j \ge 2$, $2n = 2^j$, and let β be a faithful character of $C_j/\mathbb{Q}$. Its primitive conductor is $c = 8n$. Let ξ be a quadratic character or the trivial character, and let a be the odd part of its primitive conductor. Take an odd prime $p \nmid a$. Write η_p for the quadratic character of conductor p, and put

$$\lambda = \beta^{-1}\xi\eta_p, \qquad D = acp.$$

Every odd power of λ is primitive of conductor D. Indeed an odd power of β still has conductor c. The dyadic conductor of a quadratic character divides eight, and $c \ge 16$, so twisting leaves this conductor exponent unchanged. The characters at the odd factors of a and at p are nontrivial quadratic characters on separate factors.

Lemma 57.30 (A geometric mean at one for all the odd powers)**.** *With an absolute implied constant,*

$$\left(\prod_{\substack{b \bmod 2n \\ b \text{ odd}}} |L(1, \lambda^b)| \right)^{1/n} \ll \big(\log(3D)\big)^{1/n}.$$

Proof. First consider any primitive nonprincipal Dirichlet character χ of conductor D. For real $\sigma \ge 1$, the absolute value of its completed function $\Lambda(\sigma, \chi)$ is nondecreasing. Here is the zero argument. The entire function of order at most one

$$\Lambda(1/2 + w, \chi)\Lambda(1/2 + w, \bar\chi)$$

is even by the functional equations, including their conjugate root numbers. Its zeros belong to $|\operatorname{Re} w| \le 1/2$ by the Euler product and the functional equations. Pair each nonzero zero z with $-z$, counting multiplicities. By Hadamard factorization the paired factors are $1 - w^2/z^2$ and the central factor is w^{2h} for some $h \ge 0$. The remaining factor is a constant because the entire function is even and its exponential prefactor has degree at most one. The paired product

converges on compact sets, since the sum of $|z|^{-2}$ converges away from zero. At real $w > 1/2$ each of $1/(w-z)$ and $1/(w+z)$ has positive real part. Their sum is the logarithmic derivative of the paired factor. The central factor contributes $2h/w$. This proves the monotonicity since the product of the two completed functions is the positive number $|\Lambda(1/2+w,\chi)|^2$ there. Continuity gives the endpoint. Taking $\sigma = 1 + 1/\log(3D)$, the conductor power and ratio of gamma factors between 1 and σ are bounded by an absolute constant for either parity. Hence

$$|L(1,\chi)| \ll |L(\sigma,\chi)|.$$

At this $\sigma > 1$ take logarithms of the absolutely convergent Euler products. Prime powers of exponent at least two contribute $O(1)$ to the average of their real logarithms, uniformly in all data. At a prime $q \nmid D$ the average of $\lambda(q)^b$ over odd b is zero unless $\beta(q)^2 = 1$, by the finite geometric series. In that case its real part is at most one. Enlarging the prime set to $q \nmid c$ in this nonnegative upper bound and using orthogonality gives

$$\begin{aligned}\frac{1}{n}\sum_{b\ \mathrm{odd}} \log|L(\sigma,\lambda^b)| &\le \sum_{\substack{q\nmid c\\ \beta(q)^2=1}} q^{-\sigma} + O(1)\\ &= \frac{1}{n}\sum_{j'=0}^{n-1} \log|L_c(\sigma,\beta^{2j'})| + O(1).\end{aligned}$$

The sum over q is over primes. The subscript c means that every character is read modulo c, so all its Euler factors at two are omitted. The term for $j' = 0$ is bounded by $\log\zeta(\sigma) \le \log(1 + 1/(\sigma-1))$.

For the other j', a partial sum of the character has absolute value at most c by periodicity and zero mean. Partial summation bounds the tail after c of its Dirichlet series by an absolute constant for $1 < \sigma \le 2$. The mean square of the first c terms, averaged over all n characters, is bounded absolutely. In fact orthogonality groups $1 \le m \le c$, m odd, by their value under β^2. Every fiber has $\varphi(c)/n = 4$ members. Cauchy–Schwarz on each fiber bounds the mean square by $4\sum_{m\ge1} m^{-2}$. It follows that the mean of $\log^+|L_c(\sigma,\beta^{2j'})|$ over the nonprincipal terms, divided by n, is $O(1)$. Exponentiate the resulting bound and use the transfer from σ to 1. This proves the assertion. □

Theorem 57.31 (The half residue after a fixed quadratic twist)**.** *Suppose $\xi(-1) = \eta_p(-1)$, let L be the field cut out by λ, and put $F = C_{j-1}$. There is an absolute constant C for which*

$$\left(\frac{h_L}{h_F p^{n/2}}\right)^{1/n} \le \frac{(n!)^{1/n}}{n}\,\frac{C\sqrt{an}\,(\log(3acp))^{1/n}}{\log p - 2\log 2} \qquad (p > 4).$$

For each fixed ξ there is $b_\xi > 0$ such that for all sufficiently large p of this parity and every $2 \le n \le b_\xi(\log p)^2$, the right hand side is less than one. If in addition $\mathrm{ord}_{2n}(p) \ge n/2$, the strict group $S(\beta\xi, r)$ vanishes at every positive $r \equiv (p-1)/2 \bmod (p-1)$.

Proof. The character λ is even of order $2n$. Its square cuts out F, so L/F is quadratic and both fields are totally real. At every prime over p this extension is ramified of index two, whereas p is unramified in F. The relative regulator estimate of Lemma 57.24 applies also to this extension. To verify the dependence on the quadratic twist, for a nontrivial relative unit modulo signs let s be the involution and take one embedding above each embedding of F. The ideal of the relative discriminant divides the ideal of $(u - su)^2$, since $u \notin F$ generates L/F. The product of the norms of primes of F above p is p^n. Consequently

$$p^{n/2} \le \prod_{\tau} |\widetilde{\tau}(u - su)| \le 2^n \exp\left(\sum_{\tau} |\log|\widetilde{\tau}u||\right).$$

Here the relative unit is in the kernel of the norm modulo signs, so that $|\widetilde{\tau} s u| = |\widetilde{\tau} u|^{-1}$. The lattice of these n log coordinates has full rank because norms of units contain the squares of units of F. The cross-polytope of radius $n(\frac{1}{2}\log p - \log 2)$ has no nonzero lattice point in its interior. Minkowski's theorem gives covolume at least the n-th power of this radius divided by $n!$. The regulator determinant, with one row omitted, gives R_L/R_F equal to this covolume times the index of the norm image modulo signs, as computed in Lemma 57.24. This proves the required regulator inequality without any condition on a.

Exactly the n odd powers of λ occur in the quotient of the zeta functions for L and F. Each has conductor acp. The conductor–discriminant formula and the analytic class number formulas therefore give

$$\frac{h_L}{h_F} = \frac{(acp)^{n/2}}{2^n} \frac{R_F}{R_L} \prod_{b \text{ odd}} |L(1, \lambda^b)|.$$

Insert the two estimates and $c = 8n$, absorbing the fixed numerical factor into C. For fixed a, take first $2 \le n \le \log\log(3p)$. Then $\sqrt{n}(\log(3acp))^{1/n}/\log p$ is $O_a(\sqrt{\log\log(3p)/\log p})$. For $\log\log(3p) < n \le b_\xi(\log p)^2$, we may take $b_\xi \le 1$, and the factor $(\log(3acp))^{1/n}$ is at most four eventually. Choosing b_ξ small enough in terms of a, C gives a strict upper bound less than one.

If $S(\beta\xi, r) \neq 0$, the argument of Lemma 55.33 supplies an equivariant homomorphism out of the ordinary class group of L with image of order at least $p^{\mathrm{ord}_{2n}(p)}$. Inertia at p acts nontrivially on the residual character, as required there. The involution of L/F acts as minus one on this image, so the homomorphism kills classes extended from F. The class number of the real dyadic field F is odd by Lemma 57.24, and extension of its ideal classes is injective because norm after extension is squaring. Thus the available quotient has order h_L/h_F. In the indicated range it has order less than $p^{n/2}$, contradicting the lower bound on the image. □

Corollary 57.32 (Every weight on a growing complex subfield)**.** *Let K_ξ be any fixed imaginary quadratic field contained in $K_\psi C_\infty$, with associated character ξ. There exists $b > 0$ such that, on each sufficiently distant original interval, one can take the largest $j \ge 1$ with $2^{j-1} \le b(\log V)^2$ and put $D_V = K_\xi C_j$. Then D_V is contained in every actual E_x of the interval, and its degree is of order $(\log V)^2$. At every odd prime $V \le p \le P(x)$ with $p \equiv 3, 5 \bmod 8$ and every $1 \le r < t(x)$,*

$$R_{p,r}(E_x)^{\mathrm{Gal}(E_x/D_V)} = 0.$$

At $p > P(x)$ the total logarithmic order of the complementary groups on this subfield, summed over those primes and all these weights, is $O_{\psi,\varepsilon}(V^A)$ for some A. If K_ξ is omitted, the same assertions hold for the real subfields C_j on every original family.

Proof. Take b at most the two constants in the theorem for ξ and the trivial character. The fixed quadratic field is contained in a fixed base layer. The available real dyadic degree in E_x grows at least as a fixed positive power of V, by Theorem 19.15. This gives the inclusions, and successive real dyadic degrees double. Since the quadratic field is imaginary it has intersection $\mathbb{Q}$ with the real tower.

For $p \ge V$ the odd prime p is prime to the degrees of the actual fields for large V. At a separated weight $p - 1 \nmid 2r$, Lemma 9.31 bounds the strict length on D_V by $\log J(V)/\log p < b_0(x)$. At $p - 1 \mid r$ the complementary sign is plus. Its component descends to C_j by the order-two projection and vanishes by Theorem 24.28 in both progressions.

At the half residue the sign is odd for $p \equiv 3 \bmod 8$ and even for $p \equiv 5 \bmod 8$. The corresponding characters are respectively $\xi\beta'$ and β', with β' a character of C_j. If β' is faithful on a layer of order $2n' \ge 4$, the theorem applies with $n' \le b(\log p)^2$. Indeed $v_2(p^2 - 1) = 3$ in both progressions, and each successive squaring from p^2 increases the valuation of its difference

from one by one. The order modulo $2n'$ is at least $n'/2$, including modulus four by inspection. If β' has order at most two, the finitely many resulting nontrivial quadratic characters vanish here by Proposition 22.27 at all sufficiently large p. The trivial character at an even half-residue weight is covered by Proposition 20.6. These scalar vanishings give vanishing of the corresponding sign summand on D_V by prime-to-p character descent. For the real field alone the minus component is already zero by conjugation.

The field average onto D_V commutes with the sign, the other field averages and the high-power truncation in Proposition 6.11. On the strict groups its image is restriction from D_V, by prime-to-p descent. Thus in every case the indicated residual invariant group is zero. For $p > P(x)$, all weights in question are separated for sufficiently large V, since $P(x) > 2t(x) + 1$. The local divisibilities of Lemma 9.31 on $D_V \subset E_*$ bound the total logarithmic order by $\log J(V) \ll V^A$. □

This argument allows arbitrary fixed odd conductor in the quadratic twist. On the original fields the two moving ramified quadratic characters and primes in the other residue classes still occur in the complementary estimate.

57.10 Fixed characters at the limiting residue degree

For a Dirichlet character γ, let K_γ be the fixed field of its kernel in the abelian closure of $\mathbb{Q}$. We always take the primitive L-function of a character, except when the modulus of an imprimitive Euler product is indicated explicitly. We use the strict group $S(\alpha, r)$ of Section 22.17. Its local condition at the coefficient prime p is zero.

Theorem 57.33 (A class number bound at the limiting residue degree)**.** *Let α be a fixed primitive character of conductor M and order d. Write $m = \operatorname{lcm}(d, 2) = 2n$ and suppose $n \geq 2$. For an odd prime $p \nmid Md$ let η_p be the quadratic character of conductor p. If $\alpha(-1) = \eta_p(-1)$, the field $L = K_{\alpha^{-1}\eta_p}$ is totally real and*

$$h_L \ll_\alpha \frac{p^{n/2}}{(\log p)^{n-1}}.$$

Consequently, at every sufficiently large prime of this parity with $\operatorname{ord}_m(p) \geq m/4$, one has $S(\alpha, r) = 0$ for all positive $r \equiv (p-1)/2 \bmod (p-1)$.

Proof. Put $\lambda = \alpha^{-1}\eta_p$. The conductor factors are coprime, so the two characters attain their values independently. It follows that λ has order $2n$ and $\lambda^2 = \alpha^{-2}$ has order n. Write $F = K_{\alpha^2}$, a fixed field of degree n. The parity assumption makes its quadratic extension L totally real. The inertia at p has order two in L and trivial image in F.

We first prove

$$\prod_{\substack{b \bmod 2n \\ b \text{ odd}}} |L(1, \lambda^b)| \ll_\alpha \log(3Mp). \tag{57.1}$$

Every odd power has conductor divisible by p and dividing Mp. Thus it is nonprincipal. Take $\sigma = 1 + 1/\log(3Mp)$. The completed-function inequality in the proof of Lemma 57.30 gives $|L(1, \lambda^b)| \ll |L(\sigma, \lambda^b)|$ with an absolute constant. Indeed the primitive conductor $D_b \leq Mp$ contributes a factor $D_b^{(\sigma-1)/2} \leq \sqrt{e}$, and the two possible gamma ratios are bounded on this interval.

At a prime $q \nmid Mp$, the mean of $\lambda(q)^b$ over these n exponents is zero unless $\alpha(q)^2 = 1$. This follows by summing a geometric progression with ratio $\lambda(q)^2$. Its mean has real part at most one when the ratio is one. Terms of exponent at least two in the logarithms of the Euler

products have sum bounded absolutely by $\sum_q \sum_{k\ge 2} q^{-k}/k$. The Euler factors belonging to the fixed primes $q \mid M$ can increase the mean logarithm by at most $\sum_{q\mid M} -\log(1-1/q)$. All factors at p are omitted. We can include $q = p$ when taking an upper bound for the resulting nonnegative sum of prime terms. For $q \nmid M$, orthogonality expresses the indicator of $\alpha(q)^2 = 1$ as the average of the n powers of $\alpha(q)^2$. Restoring prime powers of exponent at least two in this new average costs another absolute constant. Hence

$$\frac{1}{n}\sum_{b \text{ odd}} \log|L(\sigma,\lambda^b)| \le \frac{1}{n}\sum_{i=0}^{n-1} \log|L_M(\sigma,\alpha^{2i})| + O_\alpha(1),$$

where L_M omits the factors at $q \mid M$. Only $i = 0$ is principal. Its absolute value is at most $\zeta(\sigma) \le 1 + 1/(\sigma-1)$. Each nonprincipal term is bounded in absolute value before taking its logarithm, uniformly in $1 < \sigma \le 2$. In fact the partial sums of a nonprincipal character modulo M have absolute value at most M, and partial summation bounds its Dirichlet series by M there. Multiply the inequality by n, which is fixed, and exponentiate. The transfer to $s = 1$ proves (57.1).

Exactly the odd powers of λ occur in ζ_L/ζ_F. The conductor–discriminant formula gives $|\operatorname{disc} L|/|\operatorname{disc} F| = \prod_{b \text{ odd}} D_b \le (Mp)^n$. In the analytic class number formula the two totally real fields both have two roots of unity. Taking the quotient of their residues therefore gives

$$h_L = \frac{h_F}{2^n}\left(\prod_{b \text{ odd}} D_b\right)^{1/2} \frac{R_F}{R_L} \prod_{b \text{ odd}} |L(1,\lambda^b)|.$$

The regulator argument of Lemma 57.24 applies because p is unramified in F and every prime of F above p ramifies in L/F. More explicitly, the discriminant of $1, u$ for a nontrivial relative unit modulo signs has norm at least p^n. The logarithms at one embedding in every conjugate pair thus have total absolute value at least $n(\frac{1}{2}\log p - \log 2)$. The cross-polytope and determinant calculation of that lemma gives

$$\frac{R_L}{R_F} \ge \frac{\left[n(\frac{1}{2}\log p - \log 2)\right]^n}{n!} \qquad (p > 4).$$

The field F and its class number are fixed. Inserting the last inequality and (57.1) proves the claimed estimate for all sufficiently large p. A single larger constant includes the remaining primes.

At a half-residue weight the residual scalar character is the reduction of λ. Its order stays m because $p \nmid m$. Its restriction to inertia at p is nontrivial. Lemma 55.33 therefore makes $p^{\operatorname{ord}_m(p)}$ a divisor of h_L if there is a nonzero strict class. Since $n \ge 2$, the class number estimate gives $h_L < p^{n/2}$ for all sufficiently large p. This contradicts the divisibility even when $\operatorname{ord}_m(p) = m/4$. □

Let D_8 be the compositum of the character fields of order dividing eight in $K_\psi C_\infty$. To see that it is finite, observe that the Galois group of this tower has an open procyclic pro-two subgroup. Its subgroup of eighth powers has finite index and every indicated character kills it. In particular D_8 has degree a power of two and is contained in $K_\psi C_{j_0}$ for some fixed j_0.

Corollary 57.34 (Odd weights on the subfield of exponent eight)**.** *On the intervals of Theorem 19.15, with $t = \lfloor x^{401} \rfloor$, there is a fixed A such that*

$$\sum_{p>2} \sum_{\substack{1\le r<t \\ r \text{ odd}}} \log\left|\mathcal{S}_{p,r}(D_8)^{c=-1}\right| \ll_{\psi,\varepsilon} V^A + \exp(x^{2\varepsilon/3}).$$

For each such r and every odd $p \le P(x)$, $R_{p,r}(E_x)^{\operatorname{Gal}(E_x/D_8)} = 0$ throughout every sufficiently distant interval.

Proof. Each odd character of D_8 has order two, four, or eight. Choose p_0 larger than the finitely many conductor primes, the prime divisors of $[K_\psi : \mathbb{Q}]$, the exceptional primes of Lemma 9.31, and the thresholds in Proposition 22.27 and the theorem above for these characters. At an odd half-residue weight one has $p \equiv 3 \bmod 4$. In both resulting residue classes modulo eight the order of p modulo eight is two. The theorem therefore kills every character of order eight at this weight for $p > p_0$. Orders two and four are covered by Proposition 22.27. Over the unramified coefficient ring containing the eighth roots of unity the character projectors are integral since p is odd. Prime-to-p restriction, globally and at each local condition, identifies the sign summand with these scalar summands as in Theorem 22.28. Faithful flatness gives zero before extending coefficients. The zero residue has no odd weights. The product of the orders at the remaining weights and $p > p_0$ divides $J(V)$ by Lemma 9.31, and $\log J(V) \ll V^A$.

For $2 < p \le p_0$ restrict from D_8 to the actual B_J. Corestriction kills the kernel after multiplication by $[B_J : D_8]$, whose p-valuation is at most $v_p([K_\psi : \mathbb{Q}])$. At each of these finitely many primes the p-rank on D_8 is bounded independently of r. Indeed the Kummer calculation in Theorem 22.28 uses only the p-units and the p-torsion in the class group of the fixed $D_8(\mu_p)$ with p inverted. Thus the kernel costs $O_\psi(1)$ in logarithmic order per weight, and Theorem 20.4 bounds the sum of the logarithmic orders of the images by $\exp(x^{2\varepsilon/3})$. Absorb the $O_\psi(t)$ losses by increasing A.

Write $H = \mathrm{Gal}(E_x/D_8)$. If $p \nmid |H|$, averaging identifies strict invariants with restriction from D_8 and gives exact invariants on the subsequent quotients. For large V the displayed bound divided by $\log p$ is less than $b_0(x) = \lfloor \exp(x^\varepsilon/8) \rfloor$. The quotient by the subgroup killed by $p^{b_0(x)}$ therefore removes the invariant summand. If $p \mid |H|$, then p lies in the fixed prime set Π of Proposition 6.11. Both $B(x)$ and L_x there contain the fixed D_8 for large V. Hence the subgroup defining its average $J_{p,r}$ is contained in H. The average acts as the identity on every H-invariant and as zero on the residual quotient, proving the assertion. □

Theorem 57.35 (One growing subfield down to the smallest coefficient primes)**.** *Fix a quadratic field K_ξ as in Corollary 57.32, or take $K_\xi = \mathbb{Q}$. Set*

$$Y_V = \tfrac{1}{2} c_{\psi,\varepsilon} (\log\log V)^{1/5}$$

with the constant of Theorem 20.4. There is a choice of $D'_V = K_\xi C_j$, common to all $x \in [V, V^{3/2}]$, with $[D'_V : \mathbb{Q}] \asymp_{\psi,\varepsilon,\xi} (\log\log\log V)^2$, for which

$$R_{p,r}(E_x)^{\mathrm{Gal}(E_x/D'_V)} = 0 \qquad (1 \le r < \lfloor x^{401} \rfloor)$$

at every odd $p \le Y_V$ and at every odd $p \le P(x)$ congruent to three or five modulo eight. For $p > P(x)$ the logarithmic order on D'_V, summed over all such primes and weights, is $O_{\psi,\varepsilon}(V^A)$.

Proof. Choose b as in Corollary 57.32 and take j largest with $2^{j-1} \le b(\log Y_V)^2$. Successive degrees in the real tower double and $\log Y_V = \frac{1}{5}\log\log\log V + O_{\psi,\varepsilon}(1)$. This proves the degree estimate, since adjoining the fixed quadratic field changes the degree by at most two. For all sufficiently large V we have $j = O(\log\log Y_V)$ and any fixed initial layer containing K_ξ is available. Thus D'_V lies in B_J and in each of the two fields $B(x), L_x$ used for the averages in Proposition 6.11. In particular this choice works throughout the original interval.

First take $p \le Y_V$. If $p \mid [E_x : \mathbb{Q}]$, its odd part comes from $[K_\psi : \mathbb{Q}]$, so $p \in \Pi$. The average argument at the end of the preceding corollary applies because both its candidate fields contain D'_V. If $p \nmid [E_x : \mathbb{Q}]$, restriction injects the complementary strict group on D'_V into the corresponding one on B_J. Theorem 20.4 bounds their logarithmic orders even after summing over all weights and primes up to Y_V, since $x \ge V$. The resulting bound divided by

$\log p$ is less than $b_0(x)$ for large V. Prime-to-p invariants are exact, so the truncation again removes the entire indicated summand.

Now take $Y_V < p \le P(x)$ in either specified progression. Eventually p exceeds every fixed prime excluded in Lemma 9.31 and is prime to $[E_x : \mathbb{Q}]$. Here $2^{j-1} \le b(\log p)^2$, the precise size condition used at the half residue in Theorem 57.31. For each character in the required sign summand the dyadic order is a power of two. At orders at least four, $v_2(p^2-1) = 3$ gives the residue-degree bound in that theorem. The characters of order at most two are covered by Propositions 22.27 and 20.6, as in the proof of Corollary 57.32. At a multiple of $p-1$ the sign is plus and descends to the real C_j, where Theorem 24.28 applies. At all separated weights Lemma 9.31 bounds the length by $\log J(V)/\log p < b_0(x)$. These arguments require only the lower bound $p > Y_V$ just verified, so they also cover the primes below V. Exactness of averaging gives the claimed vanishing. Finally $p > P(x) > 2\lfloor V^{1203/2} \rfloor + 1$ on sufficiently distant intervals. All weights under consideration are separated and the same integer $J(V)$ bounds the summed logarithmic order. □

The subfields in the last two statements belong to the fixed tower $K_\psi C_\infty$. Section 6.6 also requires estimates on components involving the two quadratic characters whose conductors vary with the interval.

57.11 Half-residue weights over a fixed abelian field of two-power degree

The field cut out by the square of a character need not be a pure cyclotomic layer. Working over that field gives a uniform estimate as the order and the conductor both vary. For a finite Dirichlet character ν, let K_ν be its character field and let $\mathrm{cond}(\nu)$ be its primitive conductor, equal to one for the trivial character. All L-values in this subsection have their primitive Euler factors.

Lemma 57.36 (An upper bound over the field of the squared character)**.** *Let λ be a Dirichlet character of order $2n$, $n \ge 2$. Put $B = \mathrm{cond}(\lambda^2)$, $D = \max_{b \text{ odd}} \mathrm{cond}(\lambda^b)$, where exponents are read modulo $2n$, and set*

$$H(B,n) = \min\left\{ 1 + \log(2B),\ \frac{B}{\varphi(B)}\left(1 + \sqrt{\frac{\varphi(B)}{n}}\right)\right\}.$$

There is an absolute constant A such that

$$\left(\prod_{b \text{ odd}} |L(1,\lambda^b)|\right)^{1/n} \le A\,(\log(3D))^{1/n} H(B,n)^{\,1-1/n}.$$

Proof. Write $L = K_\lambda$, $F = K_{\lambda^2}$, and $\sigma = 1 + 1/\log(3D)$. For each odd power, the comparison of completed functions proved in Lemma 57.30 gives $|L(1,\lambda^b)| \le A_1 |L(\sigma,\lambda^b)|$. Indeed the conductor factor from 1 to σ is at most $\sqrt{e}$, and the gamma ratios for both parities are bounded on $[1,2]$.

The product of the absolute values at σ is $\zeta_L(\sigma)/\zeta_F(\sigma)$, by abelian factorization and conjugate pairing. At a prime ideal of F of norm Q, the Euler factor of this quotient is $(1-Q^{-\sigma})^{-1}$, $(1+Q^{-\sigma})^{-1}$, or 1, according as the prime splits, is inert, or ramifies in L/F. Each is bounded above by the Euler factor of $\zeta_F(\sigma)$. Thus the entire quotient is at most $\zeta_F(\sigma)$, including at primes dividing B.

Factor this last zeta function using the n powers of $\nu = \lambda^2$. The principal factor is $\zeta(\sigma) \le 1 + 1/(\sigma-1)$. For a nonprincipal primitive character of conductor $b_0 \mid B$, periodicity bounds

its partial sums by b_0. Summing the initial b_0 terms and using partial summation for the tail gives an upper bound $A_2(1+\log(2B))$ for the absolute value of each such factor.

For a second bound, first read all powers of ν modulo B. For each nonprincipal power the tail after B is bounded by an absolute constant, again by partial summation and periodicity. Let T_i denote the sum of the first B terms for ν^i at σ, including $i=0$. Orthogonality gives

$$\frac{1}{n}\sum_{i=0}^{n-1}|T_i|^2=\sum_{z\in\operatorname{im}\nu}\left|\sum_{\substack{1\le a\le B,\ (a,B)=1\\ \nu(a)=z}}a^{-\sigma}\right|^2\le\frac{\varphi(B)}{n}\sum_{a\ge1}a^{-2}.$$

Every fiber has $\varphi(B)/n$ members, which gives the inequality by Cauchy–Schwarz. Restoring omitted Euler factors increases each absolute value by a factor at most $\prod_{\ell\mid B}(1-1/\ell)^{-1}=B/\varphi(B)$. The arithmetic mean over the $n-1$ nonprincipal factors is therefore at most $A_3H(B,n)$, using $n/(n-1)\le 2$ and taking the better of the two bounds. Their geometric mean satisfies the same estimate. Insert the principal factor and take the n-th root. □

Theorem 57.37 (A uniform necessary inequality for a half-residue class)**.** *Let α have order d and conductor M, let $2n=\operatorname{lcm}(2,d)$ with $n\ge2$, and let $p\ge5$ be a prime not dividing Md. Suppose that $r\equiv(p-1)/2 \bmod (p-1)$, $r>0$, and $\alpha(-1)=(-1)^r$. Put $f=\operatorname{ord}_{2n}(p)$, $B=\operatorname{cond}(\alpha^2)$, and*

$$M_{\mathrm{o}}=\left(\prod_{\substack{b \bmod 2n\\ b\ \text{odd}}}\operatorname{cond}(\alpha^b)\right)^{1/n}.$$

If the full strict scalar group $S(\alpha,r)$ of Section 22.13 is nonzero, then, for an absolute A,

$$p^{f/n}\ \le\ A\,\frac{\sqrt{pM_{\mathrm{o}}}}{\log(p/4)}(\log(3Mp))^{1/n}H(B,n)^{\,1-1/n}.$$

Proof. Let η_p be the quadratic character of conductor p, $\lambda=\alpha^{-1}\eta_p$, $L=K_\lambda$, and $F=K_{\lambda^2}$. The conductor factors of λ are coprime, so that its order is $2n$ and its odd powers have conductors $p\operatorname{cond}(\alpha^b)$. The parity condition makes L totally real. Every prime over p ramifies in the quadratic extension L/F because F is unramified at p and inertia acts there on λ by η_p.

Suppose a strict class survives. Its residual character is $\bar\lambda$, and inertia at p acts nontrivially. The proof of Lemma 55.33 supplies an equivariant homomorphism u from $\mathrm{Cl}(L)$ to an additive group of characteristic p whose image has at least p^f elements. The involution s of L/F acts on that image by minus one. For every ideal class a, the class $a/s(a)$ has trivial norm and its image is $2u(a)$. Thus the kernel of the norm already maps onto the image, since two is invertible there.

In this extension the class group norm is surjective. Indeed the ordinary Hilbert class field H_F has $H_F\cap L=F$ by the ramification at p. The compositum H_FL/L is unramified at finite places and split at the real places. Reciprocity on L maps its class group onto $\mathrm{Gal}(H_FL/L)$; restriction to H_F identifies this map with the ideal norm followed by reciprocity on F. This proves

$$p^f\le|\ker N_{L/F}|=h_L/h_F.$$

The regulator estimate used in Theorem 57.31 depends only on total reality, quadratic relative degree, and full ramification over the unramified rational prime p. To recall its content, for a nontrivial relative unit v modulo signs the order with basis $1,v$ has discriminant $(v-s(v))^2$.

The norm of the relative discriminant is at least p^n. For one embedding τ of L above each embedding of F, this gives

$$p^{n/2} \le \prod_{\tau} |\tau(v - s(v))| \le 2^n \exp\left(\sum_{\tau} |\log |\tau(v)|| \right).$$

Here $vs(v) = \pm 1$. The volume of the resulting empty open cross-polytope and the norm determinant of Lemma 57.24 give $R_L/R_F \ge [n \log(p/4)/2]^n/n!$. The conductor–discriminant and class number formulas, with two roots of unity in both fields, now give

$$\frac{h_L}{h_F} = \frac{(pM_{\mathrm{o}})^{n/2}}{2^n} \frac{R_F}{R_L} \prod_{b \text{ odd}} |L(1, \lambda^b)|.$$

Apply Lemma 57.36, use $D \le Mp$, and take the n-th root. The factor $(n!)^{1/n}/n$ is at most one. □

Corollary 57.38 (Half-residue vanishing on the mixed subfield throughout the interval)**.** *Let K be the maximal subfield of K_ψ of two-power degree, including $K = \mathbb{Q}$. There is a constant $b_\psi > 0$ with the following property on every sufficiently distant interval of Theorem 19.15. Take j largest with $2^j \le b_\psi (\log V)^2$, and put $T_V = KC_j$. This one field is contained in every E_x on the interval. For every $p \ge V$ congruent to three or five modulo eight and every half-residue weight $1 \le r < t(x)$, one has*

$$\mathcal{S}_{p,r}(T_V)^{c=(-1)^r} = 0, \qquad R_{p,r}(E_x)^{\mathrm{Gal}(E_x/T_V)} = 0.$$

Proof. The initial field K is fixed and cyclic; write $a = [K : \mathbb{Q}]$. The cyclotomic degree available in every E_x grows as a positive power of V by Theorem 19.15, so all contain T_V. A character of T_V is a product $\alpha = \gamma\beta$ with γ from K and β from C_j. Indeed the Galois group embeds in the product for the two factors, and a character of a subgroup of a finite abelian group extends to the whole group. One may extend a generator at a time by taking a root of its prescribed power.

If α has order $2n \ge 4$, then $\mathrm{ord}(\beta) \le \max(2n, a)$, since both factors have two-power order. A nontrivial character of exact order 2^i in the real dyadic tower first occurs at C_i and has conductor 2^{i+2}. Consequently $M \le A_\psi n$, also $B \le M$, and every prime dividing B divides the fixed integer $2\,\mathrm{cond}(\psi)$. Hence $H(B, n) \le A'_\psi$. The possible $2n$ are at most 2^j once $2^j \ge a$. For $p \equiv 3, 5 \bmod 8$, $v_2(p^2 - 1) = 3$ and every subsequent squaring increases the valuation by one. This gives $\mathrm{ord}_{2n}(p) \ge n/2$, including modulus four. By the theorem a nonzero group would require

$$1 \le A''_\psi \frac{\sqrt{n}\,(\log(3A_\psi np))^{1/n}}{\log(p/4)}.$$

Put $y = \log\log(3p)$. For $2 \le n \le y$ the right side is $O_\psi(\sqrt{y/\log p})$, which tends to zero uniformly. If $y < n \le b_\psi(\log p)^2$ and $b_\psi \le 1$, the factor with exponent $1/n$ is at most four for large p. Choosing b_ψ sufficiently small makes the right side strictly less than one in this range as well.

The characters of order at most two in KC_∞ have bounded conductor by the same argument for $\gamma\beta$. For them $L = K_{\alpha^{-1}\eta_p}$ is real quadratic of discriminant $O_\psi(p)$ when the signs match. Minkowski gives a representative of norm at most $Y = O_\psi(\sqrt{p})$ for every ideal class, with $Y \ge 1$. The quadratic Euler factors bound the number of ideals of each norm by the divisor function, so $h_L \le Y(1 + \log Y) < p$ eventually. This contradicts Lemma 55.33, including when α is trivial.

All primes in question are prime to $[E_x:\mathbb{Q}]$ and to the conductors of the characters of T_V for large V. The character decomposition with the strict local conditions from Theorem 22.17 therefore proves the first equality. Restriction identifies this group with the invariants of the matching sign group on E_x, since averaging is exact for the relative group of order prime to p, also locally. Field averages and the truncation in Proposition 6.11 commute with this projection. This proves the second equality at every indicated x. □

For instance, a quartic character modulo 17 is even and its square has conductor 17. The corollary applies to all its twists by the indicated growing dyadic characters. The two varying auxiliary quadratic conductors of E_x can enter M_{o} in the theorem. Their contribution to the full sum in Section 6.6 still requires an estimate.

57.12 Descent at the zero residue over a fixed real cyclic field

At weights divisible by $p-1$, the places over p give local coordinates for a strict class killed by p. To use these coordinates one must control the ordinary class group of the field on which they are taken. We give a uniform bound as the cyclotomic layer grows.

Lemma 57.39 (A lower bound for the relative regulator in totally real degree two)**.** *Let L/F be a quadratic extension of totally real fields with $[F:\mathbb{Q}]=n$. Put $c_0=\frac{1}{2}\log(3\sqrt{3}/2)>0$. Then $R_L/R_F\ge (c_0 n)^n/n!$.*

Proof. For every real number z,

$$|z(z^2-1)|\le \frac{2}{3\sqrt{3}}\max(1,|z|)^4.$$

On $0\le t=|z|\le 1$, the maximum of $t(1-t^2)$ is $2/(3\sqrt{3})$. For $t\ge 1$, dividing by t^4 gives the same function at $1/t$. Let s be the involution of L/F, and choose a nontrivial unit u in the kernel of the norm on units modulo signs. Then $u\neq\pm1$, so $u(u^2-1)$ is a nonzero algebraic integer. Its absolute norm is at least one. In each pair of real embeddings over F, the two absolute values of u are reciprocal since $u\,s(u)=\pm1$. Taking the product of the scalar inequality over all $2n$ embeddings gives

$$1\le \left(\frac{2}{3\sqrt{3}}\right)^{2n}\exp\left(4\sum_{\tau}|\log|\tau(u)||\right),$$

where one member τ of each pair occurs in the sum. Thus every nonzero log vector of the relative units has ℓ^1-norm at least $c_0 n$. These vectors form a full lattice in $\mathbb{R}^n$, since norm images contain the squares of the units of F. The cross-polytope estimate and the determinant computation of Lemma 57.24 give the result. □

Theorem 57.40 (Large primes in the class groups of mixed real layers)**.** *Fix a totally real cyclic number field K, allowing $K=\mathbb{Q}$. Write $a=[K:\mathbb{Q}]$ and let a_{odd} be its odd part. Put $U_j=KC_j$, with $C_j=\mathbb{Q}(\zeta_{2^{j+2}})^+$, and $C_0=\mathbb{Q}$. There is A_K, independent of j, such that for every $j\ge 0$ and every prime $p\equiv 3,5 \bmod 8$,*

$$p>A_K(1+2^j)^{a_{\mathrm{odd}}}\quad\Longrightarrow\quad \mathrm{Cl}(U_j)\{p\}=0.$$

The bound is linear in 2^j when a is a power of two.

Proof. Enlarge A_K to exclude all primes dividing $2a$ or $\mathrm{cond}(K)$. Here the conductor of K is the least cyclotomic modulus containing it. Suppose that $\mathrm{Cl}(U_j)[p]\neq 0$. Its Galois action

is semisimple over $\overline{\mathbb{F}}_p$, because p is prime to the abelian Galois group. Choose an occurring character, lift its values to roots of unity of order prime to p, and call it α. Put $m = \mathrm{ord}(\alpha)$, $L = K_\alpha$. The character also occurs in the class group of L after reduction to its p-torsion and extension of scalars. In fact, on the p-part of the class groups, extension followed by norm is multiplication by $[U_j : L]$, a unit. Extension of the norm is the sum over $\mathrm{Gal}(U_j/L)$, which is that same unit times the averaging idempotent. This identifies the class group of L at p with the invariant subgroup and is compatible with taking p-torsion.

Write $\alpha = \gamma\beta$ with γ from K and β from C_j, as in Corollary 57.38. The order of β divides the two-part of $\mathrm{lcm}(m, a)$. If m is odd or $m = 2$, this puts L in one fixed finite extension of $\mathbb{Q}$. There are only finitely many such subfields and their class numbers have bounded prime factors. Enlarge A_K to cover them.

It remains to consider $m = 2n$, $n \geq 2$. Set $F = K_{\alpha^2}$ and denote the involution of L/F by s. The Frobenius orbit of the faithful residual character has size $f = \mathrm{ord}_m(p)$: it is the least exponent for which raising a primitive m-th root to p^f fixes it. All its conjugates occur, as the class group action is defined over $\mathbb{F}_p$. They contribute dimension at least f to the minus eigenspace of s. The norm kills this space, because it has the same value on a class and its s-conjugate, and two is a unit on the p-torsion.

The image of the ideal norm from L has index at most two in $\mathrm{Cl}(F)$. To see this, form the compositum of L with the ordinary Hilbert class field H_F. Class field reciprocity on L maps onto $\mathrm{Gal}(H_F L/L)$, with restriction to H_F given by the ideal norm. Its image in $\mathrm{Gal}(H_F/F)$ has index $[H_F \cap L : F] \leq 2$. Thus $p^f \leq |\ker N_{L/F}| \leq 2h_L/h_F$.

Put $M = \mathrm{cond}(\alpha)$, $B = \mathrm{cond}(\alpha^2)$. The order bound on β and the conductor $4\,\mathrm{ord}(\beta)$ of a nontrivial real dyadic tower character give $M \leq C_K m$. The primes dividing B belong to the fixed set dividing $2\,\mathrm{cond}(K)$, and $B \leq M$. It follows that $H(B, n)$ of Lemma 57.36 is bounded in terms of K. The same is true of $(\log(3M))^{1/n}$. All the odd powers of α have conductor at most M. As L and F are totally real, dividing their class number formulas and applying that lemma and Lemma 57.39 yields

$$(h_L/h_F)^{1/n} \leq \frac{\sqrt{M}}{2}\left(\frac{R_F}{R_L}\prod_{b \text{ odd mod } 2n} |L(1, \alpha^b)|\right)^{1/n} \leq C'_K\sqrt{m}.$$

Here the first inequality uses the conductor–discriminant formula for the odd powers, and $(n!)^{1/n}/n \leq 1$ in the second.

Write $m = 2^v w$ with w odd. Then $w \mid a_{\mathrm{odd}}$. For the indicated primes the order modulo 2^v is at least 2^{v-2}, by $v_2(p^2 - 1) = 3$ and successive squaring, with $v = 1, 2$ covered directly. Hence $f \geq m/(4w)$. Combining the lower and upper bounds gives $p^{1/(2w)} \leq p^{f/n} \leq C''_K\sqrt{m}$. Since $m \mid \mathrm{lcm}(a, 2^j)$, this implies $p \leq A_K(1 + 2^j)^{a_{\mathrm{odd}}}$ after increasing A_K. This contradicts the assumed lower bound for p. □

Corollary 57.41 (Descent of the full strict group to a bounded cyclic field)**.** *Under the size and congruence conditions in Theorem 57.40, let σ_p be Frobenius in $U_j/\mathbb{Q}$, and put $P_{p,j} = U_j^{\langle\sigma_p\rangle}$. For every positive r divisible by $p - 1$, restriction gives*

$$\mathcal{S}_{p,r}(P_{p,j}) \;\simeq\; \mathcal{S}_{p,r}(U_j).$$

The field $P_{p,j}$ is cyclic of degree at most a and is contained in $KC_{v_2(a)}$. For $j \geq v_2(a)$ it equals $P_{p,v_2(a)}$.

Proof. The prime p is unramified in U_j. By Lemma 24.27, triviality of its ordinary p-class group embeds $\mathcal{S}_{p,r}(U_j)[p]$, equivariantly, in the permutation module on the primes over p modulo the constant line. The decomposition group $\langle\sigma_p\rangle$ fixes every such prime since the extension

is abelian. Its average therefore fixes the entire p-torsion. Any nonzero element in the complementary summand would have a multiple of order p there. Thus it fixes the full strict group. Restriction from the fixed field identifies the lower strict group with these invariants: the relative group has order prime to p, so restriction and averaging give descent on global cohomology. Local restriction is injective at p, and at every other prime an inertia homomorphism which vanishes upstairs factors through a group of order prime to p. This proves the isomorphism.

The projection of σ_p generates $\mathrm{Gal}(C_j/\mathbb{Q})$. In fact choose $u = \pm p$ with $u \equiv 1 \bmod 4$. Then $v_2(u-1) = 2$, and $v_2(u^{2^i}-1) = 2+i$ for $i \geq 0$, by repeated factorization. This gives order 2^j in the quotient modulo signs at conductor 2^{j+2}. It follows that the quotient by $\langle \sigma_p \rangle$ is generated by the image of $\mathrm{Gal}(U_j/C_j)$, a subgroup of the cyclic group $\mathrm{Gal}(K/\mathbb{Q})$. This proves cyclicity and the degree bound. For any character $\gamma\beta$ trivial on σ_p, one has $\beta(p) = \gamma(p)^{-1}$. Since p generates the dyadic quotient, the order of β equals that of $\beta(p)$, and divides $2^{v_2(a)}$. Every such character therefore factors through $KC_{v_2(a)}$. If $j \geq v_2(a)$, Frobenius there is the restriction of the same σ_p; its characters trivial on this element are exactly the ones just identified. This proves the last two assertions. □

Corollary 57.42 (The remaining summand on the original intervals)**.** *For the actual fields of Theorem 19.15, take $K = K_\psi^+$, the maximal totally real subfield of K_ψ. For $j \leq J(x)$ satisfying the hypotheses of Theorem 57.40 and $p \nmid [E_x : \mathbb{Q}]$, write e_D for averaging onto a subfield D on $R_{p,r}(E_x)$. At every $1 \leq r < t(x)$ divisible by $p-1$,*

$$e_{KC_j} R_{p,r}(E_x) = e_{P_{p,j}} R_{p,r}(E_x).$$

In particular the assertion applies to the entire real subfield of $K_\psi C_{J(x)}$ whenever the size bound holds at $j = J(x)$.

For T_V of Corollary 57.38 one also has, for every x on the interval and every $V \leq p \leq P(x)$ congruent to three or five modulo eight,

$$e_{T_V} R_{p,r}(E_x) = \begin{cases} e_{P'} R_{p,r}(E_x), & p-1 \mid r, \\ 0, & p-1 \nmid r, \end{cases} \qquad 1 \leq r < t(x).$$

Here P' is the decomposition field of p in T_V^+; it belongs to a finite list depending only on ψ.

Proof. Since $p-1 \mid r$, the complementary sign is plus. Apply Corollary 57.41 to KC_j and restrict into E_x. The field averages, the sign projector and the quotient by the subgroup of bounded exponent in Proposition 6.11 all commute. Exactness of averaging gives the first equality after these operations. The fixed field of complex conjugation on the compositum with the real C_j is $K_\psi^+ C_j$: adjoining K_ψ to this field has degree at most two, and conjugation acts nontrivially if K_ψ is imaginary.

For the second assertion the same argument identifies T_V^+ as the compositum of C_j with the real part of the fixed two-power subfield of K_ψ. Its degree condition at p holds uniformly since $2^j \ll_\psi (\log V)^2$ and $p \geq V$. At the zero residue apply the first argument with this fixed real field as K; the preceding corollary supplies the finite list. At the half residue apply Corollary 57.38. For all other r, Lemma 9.31 bounds the logarithmic order on T_V by $\log J(V) \ll_{\psi,\varepsilon} V^C$. Dividing by $\log p$ gives a length smaller than $b_0(x)$ on every sufficiently distant interval. The truncation for $p \leq P(x)$ then kills the summand. This accounts for every positive weight in the stated range. □

The decomposition fields in the formula are totally split at p. The local unit conditions on these fixed fields can still contribute at multiples of $p-1$; the descent identifies the group carrying that contribution.

57.13 Descent at varying Frobenius orders in the real dyadic tower

At zero-residue weights the part of the strict group detected above a decomposition field depends on the class group of the real layer. We keep track of the order of Frobenius in that layer for each odd coefficient prime. This lets us use a single lower field across almost all the large primes of a common interval, with an explicit bound on the exceptional prime and weight pairs.

Let $K/\mathbb{Q}$ be totally real cyclic of degree a, and write a_{o} for its odd part. Let $C_j = \mathbb{Q}(\zeta_{2^{j+2}})^+$, $U_j = KC_j$. For an odd prime p put

$$h(p) = v_2(p^2-1) - 3 = \max\{v_2(p-1), v_2(p+1)\} - 2.$$

This integer is nonnegative. We use the usual Frobenius acting by p-th power on unramified roots of unity. The real layer and its Frobenius are also specified in the archive at `Formalism/FrobeniusOrbits/Statement.lean`, line 156.

Theorem 57.43 (A class number bound with the dyadic Frobenius order)**.** *There is a constant $A_K \geq 2$ such that for every odd prime p and $j \geq 0$,*

$$p > \left[A_K(1+2^j)\right]^{2^{h(p)}a_{\mathrm{o}}} \quad \Longrightarrow \quad \mathrm{Cl}(U_j)\{p\} = 0.$$

Proof. Increase A_K to exceed the prime divisors of $2a\,\mathrm{cond}(K)$. If the class group has nonzero p-torsion, choose an occurring character over $\overline{\mathbb{F}}_p$ and write α for its lift to roots of unity of order prime to p. Put $m = \mathrm{ord}(\alpha)$. Its component descends to $L = K_\alpha$ by extension and norm of ideals, since $p \nmid [U_j : L]$. Write $\alpha = \gamma\beta$ with γ from K and β from C_j. Such a factorization follows by extending the character of the subgroup $\mathrm{Gal}(U_j/\mathbb{Q})$ to the product of the two cyclic Galois groups. If m is odd or $m = 2$, the order of β divides the two-part of $\mathrm{lcm}(m, a)$, which is bounded in terms of K. Here the characters are viewed on the absolute Galois group of $\mathbb{Q}$, where the same order bound follows from $\beta = \alpha\gamma^{-1}$. These L belong to one fixed finite extension. Enlarge A_K to cover the finitely many prime factors of their class numbers.

Suppose $m = 2n \geq 4$. Put $F = K_{\alpha^2}$ and $f_p = \mathrm{ord}_m(p)$. The distinct p-power conjugates of the faithful character in the class group of L give at least f_p dimensions over $\mathbb{F}_p$ in the minus part for L/F. This part is killed by the ideal norm, whose image in $\mathrm{Cl}(F)$ has index at most two. Hence $p^{f_p} \leq 2h_L/h_F$, as in the proof of Theorem 57.40. Its relative class number estimate $(h_L/h_F)^{1/n} \leq C_K\sqrt{m}$ applies to this L/F for every such p. Indeed its proof uses the conductor of α, the relative regulator bound of Lemma 57.39 and the product of the complex L-values in Lemma 57.36. None of those quantities involves the congruence class of the coefficient prime. We have proved $p^{f_p/n} \leq C'_K\sqrt{m}$.

Write $m = 2^v w$ with w odd, so $w \mid a_{\mathrm{o}}$. Choose $u \in \{p, -p\}$ with $u \equiv 1 \bmod 4$. Then $v_2(u-1) = h(p) + 2$. Successive squaring gives $v_2(u^{2^i} - 1) = h(p) + 2 + i$, because each factor $u^{2^i} + 1$ has valuation one. Raising to a further odd power leaves this valuation unchanged. In the quotient modulo signs at conductor 2^v the order of p is consequently $2^{\max(0, v-2-h(p))}$ for $v \geq 2$. A power of u is $1 \bmod 4$, so cannot be $-1 \bmod 2^v$ there. At $v = 1$ use order one. In all cases

$$f_p \geq \frac{m}{4\,2^{h(p)}w}, \qquad p^{1/(2\,2^{h(p)}w)} \leq C'_K\sqrt{m}.$$

Now $m \mid \mathrm{lcm}(a, 2^j)$ and $m \leq a(1+2^j)$. Raising to the indicated power and increasing A_K proves the theorem. □

Theorem 57.44 (The full strict group on the decomposition field)**.** *Assume the prime bound of Theorem 57.43. For $P_{p,j} = U_j^{\langle \mathrm{Frob}_p \rangle}$ and every $r > 0$ divisible by $p-1$, restriction gives*

$$\mathcal{S}_{p,r}(P_{p,j}) \simeq \mathcal{S}_{p,r}(U_j).$$

Moreover,

$$[P_{p,j} : \mathbb{Q}] \le a\, 2^{\min(j,h(p))}, \qquad P_{p,j} \subseteq KC_{\min(j,h(p)+v_2(a))}.$$

For every $j \ge h(p)+v_2(a)$, the decomposition field itself equals $P_{p,h(p)+v_2(a)}$, also independently of the prime bound on the class number.

Proof. At the unramified p the class group bound and Lemma 24.27 embed the p-torsion of the strict group in the permutation module on primes over p modulo constants. Its decomposition group fixes all these primes by commutativity. Its order is prime to p, and averaging fixes the full strict group since a nonzero complementary p-primary summand would have nonzero p-torsion. Restriction from the decomposition field identifies its strict group with these invariants. Indeed averaging gives global cohomological descent, restriction at p is injective, and away from p an inertia homomorphism becoming zero upstairs would factor through a group of order prime to p.

The order of Frobenius on C_j is $2^{\max(0,j-h(p))}$ by the calculation at conductor 2^{j+2} above. This bounds its order on U_j from below. Since $[U_j : \mathbb{Q}] \le a2^j$, the degree bound follows. For each character $\alpha = \gamma\beta$ trivial on this Frobenius, the order of $\beta(p) = \gamma(p)^{-1}$ divides $2^{v_2(a)}$. The subgroup generated by p in the cyclic dyadic group has index $2^{\min(j,h(p))}$. Hence the order of β divides $2^{h(p)+v_2(a)}$. Every such α factors through the lower field displayed in the theorem. Conversely every character there that is trivial on its Frobenius inflates to one trivial on the upper Frobenius. These equal character groups prove stabilization. □

Corollary 57.45 (One lower field and the exceptional prime and weight pairs)**.** *On a common interval of Theorem 19.15 take $K = K_\psi^+$, or any fixed real cyclic subfield of K_ψ. Fix $A > 0$ and choose j with $2^j \le (\log V)^A$. Put*

$$H = \left\lfloor \log_2 \frac{\log V}{4a_{\mathrm{o}}(A+1)\log\log V} \right\rfloor, \qquad M = 2^{H+3}, \qquad W = KC_{\min(j,H+v_2(a))}.$$

For all sufficiently large V, for every $x \in [V, V^{3/2}]$, $p \ge V$, and $1 \le r < t(x)$ with $p-1 \mid r$, one has

$$(e_{U_j} - e_W)R_{p,r}(E_x) = 0 \qquad \text{if } p \not\equiv \pm 1 \bmod M.$$

Here e_D is the average onto the field D in the original local-length test. Uniformly for $V \le R \le V^{602}$, the number of pairs (p,r) with $p \ge V$, $1 \le r < R$, $p-1 \mid r$ in the two omitted progressions is

$$O_{K,A}\!\left(R\,\frac{\log\log V}{\log V}\right).$$

Proof. Eventually $H \ge 0$. Every U_j under consideration is in every E_x, since the available dyadic degree grows as a positive power of V. For these primes the field averages exist integrally. The only odd primes dividing $[E_x : \mathbb{Q}]$ divide the fixed degree of K_ψ. The congruence condition in the display is exactly $h(p) \le H$. In this case

$$2^{h(p)} a_{\mathrm{o}} \log[A_K(1+2^j)] < \log V$$

for large V, by the choice of H. The two theorems give $\mathcal{S}_{p,r}(U_j)$ by restriction from $P_{p,j} \subseteq W$. Thus its image in $\mathcal{S}_{p,r}(E_x)$ coincides with the image from W. This equality survives the sign and field projections and the quotient by bounded-exponent torsion defining $R_{p,r}$, because the averages commute and give direct summands.

For the count, write $N(y)$ for the number of primes at most y in the two residue classes. For $y \ge V$ the two classes are reduced, $M \asymp_{K,A} \log V/\log\log V$, and $\log(y/M) \ge \frac{1}{2}\log y$ eventually. The Brun–Titchmarsh inequality gives $N(y) \ll y/(M\log y)$, since $\varphi(M) = M/2$. We use the

bound $2y/(\varphi(M)\log(y/M))$ per class, with $y > M$. H. L. Montgomery and R. C. Vaughan, *The large sieve*, Theorem 2 (1973). Each $p \le R+1$ contributes at most $R/(p-1)$ weights. By partial summation,

$$\sum_{\substack{V\le p\le R+1\\ p\equiv\pm1 \bmod M}} \frac{1}{p-1} \ll \frac{N(R+1)}{R+1} + \int_V^{R+1} \frac{N(y)}{y^2}\,dy \ll \frac{1}{M}.$$

In the last inequality $\log(R+1)/\log V$ is bounded by an absolute constant. Multiplying by R proves the claim. □

Corollary 57.46 (The entire real dyadic layer at large coefficient primes)**.** *On the same intervals take the actual index $J = J(x)$. Whenever $x^{300} \le p$, $p \not\equiv \pm1 \bmod 1024$, and $p-1 \mid r$ with $1 \le r < t(x)$, one has*

$$\mathcal{S}_{p,r}(C_J) \simeq \mathcal{S}_{p,r}(C_{\min(J,h(p))}), \qquad h(p) \le 7.$$

The corresponding field averages of $R_{p,r}(E_x)$ agree.

Proof. Use $K = \mathbb{Q}$ in the two theorems. The congruence condition is $h(p) \le 7$, hence $2^{h(p)} \le 128$. The actual degree bound gives $2^J \le [K_\psi C_J : \mathbb{Q}] < 2x^{2+8\varepsilon}$. For $0 < \varepsilon < 1/52$ we have $128(2+8\varepsilon) < 300$, so the prime bound holds uniformly at sufficiently large x. In the cyclic group of C_J the index of the Frobenius subgroup is exactly $2^{\min(J,h(p))}$. Its fixed field is the unique subfield of that degree. Apply restriction and the same commuting averages as in the preceding corollary. □

These results concern full strict groups at the specified weights. The count of omitted pairs bounds their number. Their individual lengths, the surviving classes over the decomposition fields, and the components involving the two varying quadratic inputs still enter the weighted sum in Section 6.6.

57.14 The relative class group at the half-residue weights

At a half-residue weight all the odd powers of a chosen Galois character can be tested in one relative class group. Keeping the different coefficient Frobenius orbits together determines their combined torsion at each available precision. In particular the bound for a relative class number can be used once for all these orbits.

Let α be a Dirichlet character of order m_0 and conductor M_0. Fix $p \ge 5$ prime to m_0M_0, and $r > 0$ with $r \equiv (p-1)/2 \bmod (p-1)$ and $\alpha(-1) = (-1)^r$. Put $2n = \operatorname{lcm}(2, m_0)$, let η_p be the quadratic character of conductor p, and set

$$\lambda = \alpha^{-1}\eta_p, \qquad L = K_\lambda, \quad F = K_{\lambda^2}, \quad \Delta = \operatorname{Gal}(L/\mathbb{Q}).$$

Here K_χ is the fixed field of $\ker\chi$. The conductors of the two factors of λ are coprime, hence its order is $2n$. Its parity is even, so L is totally real. Write ι for the involution of L/F and

$$C^- = \tfrac{1}{2}(1-\iota)\operatorname{Cl}(L)\{p\}.$$

Index odd powers by odd residue classes $b \bmod 2n$. For one representative in each orbit of $b \mapsto pb$, put $O_b = \mathbb{Z}_p[\lambda^b(\Delta)]$, $J_b = \operatorname{Frac}(O_b)$, and $S_b = S(\alpha^b, r)$, with coefficients in J_b/O_b. The same coefficient ring is generated by α^b since the quadratic factor has values in $\mathbb{Z}_p$. If the remaining members of an orbit are used, they have the corresponding conjugate coefficient modules.

Theorem 57.47 (All odd powers at one precision)**.** *For $1 \le z \le 1 + v_p(r)$, there are isomorphisms of finite modules*

$$S_b[p^z] \simeq \mathrm{Hom}_{\mathbb{Z}_p[\Delta]}(C^-, (J_b/O_b)[p^z](\lambda^b)).$$

In particular

$$\prod_{b \text{ one per orbit}} |S_b[p^z]| = |C^-[p^z]|, \qquad |C^-| = (h_L/h_F)_p.$$

The last subscript denotes the p-part of a positive integer. If N_z counts the odd labels b whose full strict group has an element of order p^z, counting every character label, then

$$N_z \le \log_p \frac{|C^-[p^z]|}{|C^-[p^{z-1}]|} \le \frac{\log_p(h_L/h_F)}{z}.$$

Proof. On divisible coefficients the scalar action is $\theta_b = \alpha^{-b}\kappa_p^{-r}$. On p^z-torsion it equals λ^b: the Teichmüller factor of the power of κ_p gives η_p, and raising a member of $1 + p\mathbb{Z}_p$ to r gives one modulo $p^{1+v_p(r)}$. This last assertion follows by factoring out the prime-to-p part of r and then applying the binomial theorem successively. At p inertia acts nontrivially on the residual character because η_p is ramified and α is unramified. An inertia element therefore acts by a scalar whose difference from one is a unit. Both the local and the global invariants of the divisible coefficients vanish. The sequence for multiplication by p^z consequently identifies the subgroup of p^z-torsion in global H^1 with H^1 on the finite coefficients, and the same assertion holds locally at p.

The finite coefficients are trivial on G_L, and $p \nmid |\Delta|$. Restriction identifies their global H^1 with the equivariant continuous homomorphisms on G_L, by averaging in inflation–restriction. A strict class gives a homomorphism killing the decomposition groups over p. At a finite prime away from p, inertia intersected with G_L acts trivially even on the divisible coefficients: both cyclotomic characters are unramified there and $\alpha^{-1} = \lambda\eta_p$ on this inertia. A finite cocycle whose divisible class is unramified consequently vanishes on that intersection. Conversely, an equivariant homomorphism unramified everywhere and zero at the decomposition groups over p gives a strict class. At each finite place in this converse, the class restricted to inertia away from p, or to the full decomposition group at p, restricts to zero over L. The kernel of that restriction is zero by averaging over a subgroup of Δ. Real inertia has order two. Class field theory now gives all the homomorphisms from the ordinary class group killing the classes of the primes over p.

The element ι belongs to inertia at p, and Δ is abelian. Thus it fixes every such prime, whereas $\lambda^b(\iota) = -1$. Every homomorphism with these target coefficients already kills the prime classes and the entire plus part. This proves the first isomorphism, in both directions. On the p-primary group the plus part identifies with the class group of F at p by extension and norm: their two composites are multiplication by two and $1 + \iota$, respectively. The ideal norm on the full class groups is surjective here. Indeed L/F is quadratic ramified above p, so its intersection with the ordinary Hilbert class field of F is F; reciprocity on their compositum gives surjectivity as in Theorem 57.37. These facts give the claimed order of C^-.

Since $p \nmid 2n$, the roots of $X^{2n} - 1$ are simple modulo p. Factoring over $\mathbb{F}_p$ and lifting the coprime factors gives a product of unramified integer rings for $\mathbb{Z}_p[\Delta]$, with one ring for each coefficient Frobenius orbit. The minus factor uses precisely the odd labels. In the factor for b the target in the first display is O_b/p^zO_b under the corresponding action. On a cyclic summand O_b/p^uO_b of the class module the homomorphisms to this target number $|O_b/pO_b|^{\min(u,z)}$. This is the order of the p^z-torsion of the same summand. Multiplying gives the product identity.

The orbit size equals $[O_b : \mathbb{Z}_p]$, the residue degree. Passing from $z-1$ to z adds exactly that many to the base-p logarithm for each cyclic summand of length at least z. An orbit carrying an element of order p^z therefore contributes at least its number of labels to the increase. The full logarithmic order of each such class summand is at least z times its contribution to the increase. This proves both inequalities. □

Corollary 57.48 (A bound uniform in the Frobenius order)**.** *Fix a cyclic abelian field K and use characters of KC_j. There is $c_K > 0$ such that whenever V is sufficiently large, $2^j \le c_K(\log V)^2$, and $p \ge V$, each family above with $n \ge 2$ satisfies*

$$N_z < \frac{n}{2z} \qquad (1 \le z \le 1 + v_p(r)).$$

For $n = 1$ the full strict group is zero. In particular, at least half the odd labels in every such family have zero full strict group at every fixed half-residue weight of the required parity. If $[K : \mathbb{Q}]$ is a power of two, the bound by one half also holds for the proportion of surviving labels among all characters of KC_j of the required parity, whenever that set is nonempty.

Proof. Let $a = [K : \mathbb{Q}]$. As in Theorem 57.43, write $\alpha = \gamma\beta$ with γ from K and β dyadic. The order of β divides the two-part of $\operatorname{lcm}(a, 2n)$. The conductor of a nontrivial real dyadic character of order 2^i is 2^{i+2}. Thus $M_0 \le A_K n$; the primes dividing $\operatorname{cond}(\alpha^2)$ belong to a fixed finite set, and $n \le a2^j$. For $n \ge 2$ the quantity $H(\operatorname{cond}(\alpha^2), n)$ of Lemma 57.36 is bounded in terms of K. The regulator and relative class number calculation in the proof of Theorem 57.37, before the use of any one residual component, therefore gives

$$\frac{(h_L/h_F)^{1/n}}{\sqrt{p}} \le C_K \, \frac{\sqrt{n}\,(\log(3A_K np))^{1/n}}{\log(p/4)}.$$

Put $y = \log\log(3p)$. For $2 \le n \le y$ the right side is $O_K(\sqrt{y/\log p})$. For $y < n \le ac_K(\log p)^2$, the logarithmic factor with exponent $1/n$ is bounded by four for large p. Choosing c_K small enough makes the displayed right side strictly less than one throughout both ranges. Thus $h_L/h_F < p^{n/2}$, and the theorem applies. For $n = 1$, the conductor of α is bounded in terms of K. The quadratic field L has discriminant $O_K(p)$ and class number $O_K(\sqrt{p}\log(2p)) < p$, by the ideal count in the proof of Corollary 57.38. The theorem at $z = 1$ gives zero p-torsion, hence zero strict group. For the last assertion, partition the character group into the generators of its cyclic subgroups. In a two-group the generators of a nontrivial cyclic subgroup are exactly the odd powers of any generator, and their parities are equal. Apply the result to each eligible subgroup, counting the trivial character separately. □

Corollary 57.49 (Full exponent control on the mixed subfield)**.** *In the original fields and intervals take $K = K_\psi$, including its odd-degree part. Let a_{o} be the odd part of $[K : \mathbb{Q}]$, $2^j \le c_K(\log V)^2$, $U = KC_j$, and $h(p) = v_2(p^2 - 1) - 3$. At $p \ge V$ put $z_p = 2^{h(p)}a_{\mathrm{o}}$. For every x on the interval and $1 \le r < t(x)$ satisfying*

$$r \equiv (p-1)/2 \bmod (p-1), \qquad 1 + v_p(r) \ge z_p,$$

the full complementary-sign strict group on U is killed by $p^{z_p - 1}$. In the notation of Section 6.6,

$$e_U R_{p,r}(E_x) = 0.$$

Proof. Every eligible α has λ of order $2n = 2^v w$ with $w \mid a_{\mathrm{o}}$. The coefficient orbit of $b = 1$ has size $\operatorname{ord}_{2n}(p)$. The dyadic order calculation in Theorem 57.43 gives

$$\operatorname{ord}_{2n}(p) \ge \frac{2n}{4\,2^{h(p)}w} \ge \frac{n}{2z_p}.$$

If $n \geq 2$, the entire orbit would contribute to N_{z_p} if its strict group had an element of order p^{z_p}. The strict inequality in the preceding corollary excludes this. The case $n = 1$ has already vanished. Every element of order larger than p^{z_p-1} would have a multiple of order exactly p^{z_p}. Integral character decomposition at $p \nmid [U : \mathbb{Q}]$ therefore bounds the exponent on U by p^{z_p-1}, using Theorem 22.17.

The dyadic degree allowed in every E_x grows as a positive power of V, so U is a subfield throughout this same interval. Field averaging identifies its contribution upstairs by prime-to-p descent. A half-residue weight in the given range has $p \leq 2t(x)+1 < P(x)$ for sufficiently large x. Also $z_p - 1 \leq v_p(r) \leq \log_2 t(x) < b_0(x)$. The quotient removing the $p^{b_0(x)}$-torsion therefore kills this entire summand, including after the other commuting field projections. □

For example, at $h(p) = 1$ and $a_{\mathrm{o}} = 1$, divisibility of a half-residue weight by p suffices on this mixed field. At weights with fewer available digits the relative class group still determines their initial torsion. A uniform bound on the length beyond this precision and the estimate for the full fields in Section 6.6 remain open.

57.15 A single class number for the half-residue weights of the interval

Fix one of the intervals of Theorem 19.15, with largest field $E = E_*$, cyclotomic modulus $N = N_*$, degree $n_* = [E : \mathbb{Q}]$, and $R = t_* = \lfloor V^{1203/2} \rfloor$. Fix $p \geq 5$ with $p \nmid n_* N$, and put $s = (p-1)/2$. Only $p \leq 2R+1$ can have a weight $1 \leq r < R$ congruent to s mod $(p-1)$. Let η_p be the quadratic character of conductor p, let D_p be its quadratic field, and put

$$H = (ED_p)^+, \qquad H_0 = E^+.$$

The superscript denotes the maximal real subfield. Write c for complex conjugation. We consider the individual characters α of E with $\alpha(c) = (-1)^s$. If this list is empty, all the sums below are empty.

Lemma 57.50 (The class group for all the characters of the given parity)**.** *For a nonempty list, H/H_0 is quadratic. Let ι be its nonidentity automorphism. Put*

$$C = \tfrac{1}{2}(1-\iota)\,\mathrm{Cl}(H)\{p\}, \qquad B_p = \log_p |C|.$$

For an orbit of $\alpha \mapsto \alpha^p$ on the list, put $\tau = \alpha^{-1}\eta_p$, $O_\tau = \mathbb{Z}_p[\tau]$, and $f_\tau = [O_\tau : \mathbb{Z}_p]$. Let h_τ be the O_τ-length of the corresponding factor of C. Then

$$\sum_{\text{orbits}} f_\tau h_\tau = B_p = v_p(h_H/h_{H_0}).$$

The compact module for $S(\alpha, r)$ in Lemma 56.16 has constant specialization of length h_τ.

Proof. The prime p is unramified in E and ramified in D_p. Thus $E \cap D_p = \mathbb{Q}$, and the Galois group of ED_p is the direct product. Its element acting only on D_p descends to ι in H. The characters on the list give exactly the characters of the product trivial on c and nontrivial on this element, by writing them as $\alpha^{-1}\eta_p$. Nonemptiness shows that ι is nontrivial. Its fixed field in H is $E \cap H = H_0$.

The order of $\mathrm{Gal}(H/\mathbb{Q})$ is prime to p. Its integral group algebra over $\mathbb{Z}_p$ splits into unramified integer rings indexed by Frobenius orbits of characters. Indeed the exponent is prime to p, so the roots of unity in a splitting ring remain distinct after reduction. The character projectors over that ring are integral, and their Frobenius orbits descend to the indicated factors. A factor of length h_τ therefore has order $p^{f_\tau h_\tau}$. Extension and norm for H/H_0 identify the plus part

of $\mathrm{Cl}(H)\{p\}$ with $\mathrm{Cl}(H_0)\{p\}$, since their composites are 2 and $1+\iota$ and 2 is a unit at p. This gives the displayed equality.

For the constant specialization of a character let $L = K_\tau$. The calculation at $T = 0$ in Lemma 56.10 identifies its length with the τ-factor of $\mathrm{Cl}(L)\{p\}$ modulo the classes at p. Here inertia contains the image of ι, which fixes every prime above p and acts by -1 on the factor. The prime classes consequently make no contribution. For H/L, extension and norm identify $\mathrm{Cl}(L)\{p\}$ with the invariants upstairs: the degree is prime to p, and the group sum divided by the degree is the projector onto invariants. The τ-factor upstairs already belongs to these invariants. This proves the constant specialization assertion. □

For the following elementary estimate, normalize each extension of v_p by $v_p(p) = 1$. Put

$$W = 1 + \lfloor \log_p R \rfloor, \qquad d_r = 1 + v_p(r), \qquad H_\tau(r) = h_\tau + (W - d_r)\lfloor h_\tau / d_r \rfloor.$$

Write $k_\alpha(r) = \mathrm{length}_{O_\tau} S(\alpha, r)$. In an inequality this length can be read as $+\infty$ if the specialized module has positive rank.

Theorem 57.51 (A weighted bound over characters and weights)**.** *Count every character label, including the distinct conjugates over $\mathbb{Z}_p$. For every $R \geq 2$ as above,*

$$\sum_{\alpha} \sum_{\substack{1 \leq r < R,\ r \equiv s \pmod{p-1} \\ k_\alpha(r) > H_\tau(r)}} (1 + v_p(r)) \ \leq \ B_p.$$

The same inequality holds for any subset of the characters and weights. In particular one need only count characters of E once when passing through the nested fields E_x.

Proof. Fix one orbit. Its compact module B is finite type over $O_\tau[[T]]$; its specialization at $t_r = (1+p)^{-r} - 1$ is dual to the strict group by Lemma 56.16. For $h = h_\tau = 0$ the module vanishes by compact Nakayama. For $h > 0$ there is a relation determinant $A(T)$ with

$$v_p(A(0)) = h, \qquad k_\alpha(r) \leq v_p(A(t_r)).$$

Indeed take a finite free cover of B. At $T = 0$ the images of its relations form a full rank lattice of colength h. Lifting a basis of this lattice to relations gives a square matrix. The cokernel of its specialization surjects onto the specialized module, which proves both claims.

Weierstrass preparation writes A as p^μ times a unit times a distinguished polynomial. In a splitting field write its roots, with multiplicity, as β. Each has $v_p(\beta) > 0$, none is zero, and $\mu + \sum_\beta v_p(\beta) = h$. For u, v distinct positive integers the binomial theorem gives

$$v_p(t_u) = 1 + v_p(u), \qquad v_p(t_u - t_v) = 1 + v_p(u - v).$$

In fact taking a power prime to p preserves the valuation of a principal unit minus one, and taking its p-th power increases that valuation by one. This also applies to inverses. In particular the distinct t_r under consideration have mutual differences of valuation at most W.

Only roots of valuation d_r can make $v_p(t_r - \beta) > v_p(\beta)$. There are at most $\lfloor h/d_r \rfloor$ such roots. If every distance valuation is at most W, their total increase above their contribution at zero is at most $(W - d_r)\lfloor h/d_r \rfloor$; all other roots have contribution at most their value at zero. It follows that a weight with $k_\alpha(r) > H_\tau(r)$ has a root with $v_p(t_r - \beta) > W$, necessarily of valuation d_r. One root cannot serve two such weights, by the bound for $v_p(t_r - t_{r'})$ and the ultrametric inequality. Assigning one root to each weight gives $\sum d_r \leq \sum_\beta v_p(\beta) \leq h$ within this orbit. Conjugation preserves the lengths. Multiplication by the orbit size f_τ and summation give the theorem by Lemma 57.50.

Finally a character inflated from E_x defines the same scalar Galois module over $\mathbb{Q}$ and the same local conditions as the original character. Thus its exceptional weights are already counted at the largest field. □

Corollary 57.52 (Application on the full period fields)**.** *On the polynomial-conductor intervals, for all good primes* $5 \le p \le 2R+1$*,*

$$B_p \ll n_*(1+\log N_*/\log p).$$

For $p \ge V$ *the weighted number of exceptional pairs in Theorem 57.51 is* $O_{\psi,\varepsilon}(n_*)$ *per prime, including characters involving either moving quadratic field. For every* $x \in [V, V^{3/2}]$*, the total logarithmic order of the nonexceptional half-residue components of these good primes at* $1 \le r < t(x)$ *is* $O_{\psi,\varepsilon}(V^A)$ *for a fixed* A*. Each such component vanishes after quotienting by the subgroup killed by* $p^{b_0(x)}$*, for sufficiently large* V*.*

Proof. The absolute discriminant of H is at most $(pN_*)^{[H:\mathbb{Q}]}$ by the conductor-discriminant formula. Minkowski's bound supplies an integral ideal of norm at most $\sqrt{|\operatorname{disc}(H)|}$ in each class, since H is totally real. The number of ideals of norm at most $Y \ge 1$ is at most $Y^2\zeta_H(2)$, and the Euler factors give $\zeta_H(2) \le \zeta(2)^{[H:\mathbb{Q}]}$. Use $B_p \le \log_p h_H$ and $[H:\mathbb{Q}] \le 2n_*$. The bound for $p \ge V$ follows since N_* is polynomial in V on these intervals.

At a nonexceptional weight the length in a single orbit is at most Wh_τ. Even if different orbits are exceptional at different weights, the sum of f_τ times the nonexceptional lengths for a fixed p, r is at most WB_p. The logarithmic order further multiplies this by $\log p$. There are at most R weights and $2R+1$ possible primes, and $W \le 1+\log_5 R$. All these quantities, n_*, and $\log N_*$ are polynomially bounded in V. Prime-to-p descent to the scalar factors on E_x uses the same exact group algebra decomposition as in Lemma 57.50, or the descent in Theorem 57.47. Finally the exponent of a finite module of length k over an unramified integer ring divides p^k. Uniformly in p, WB_p is polynomial in V, whereas $b_0(x) = \lfloor \exp(x^\varepsilon/8) \rfloor$ exceeds every fixed power of V eventually. This proves the vanishing. □

For the odd powers of one α on KC_j, the same root argument uses $v_p(h_L/h_F)$ in Theorem 57.47. Thus under the hypotheses of Corollary 57.48 with $n \ge 2$ the sum of $1+v_p(r)$ over all its exceptional label and weight pairs is strictly less than $n/2$, even when all half-residue weights in the interval are included at once. For $n = 1$ the same corollary gives vanishing. On the full period fields the bound above controls the number and the weight divisibility of the exceptional pairs. Condition (L) also requires an upper bound for the lengths at the exceptional pairs themselves.

57.16 Quantitative unit indices at split coefficient primes

The zero-residue weights involve an index of local logarithms when the coefficient prime splits completely in the character field. We give a bound for this index in terms of the conductor, the degree and the number of character components being tested. The bound also controls the invariant ordinary ideal classes at every level of the cyclotomic tower of that field.

Let L be a totally real cyclic field of degree $d \ge 2$ and conductor M. Let $p \ge 5$ be prime to dM and split completely in L. For a faithful character τ of $\Delta = \mathrm{Gal}(L/\mathbb{Q})$, write $O_\tau = \mathbb{Z}_p[\tau]$. Recall from Theorem 57.7 that $p^{c_\tau}O_\tau$ is the image of the completed ordinary units in the τ-component of the local cyclotomic exponent lattice. This lattice is identified with $\mathbb{Z}_p[\Delta]$ by numbering the places over p. List all $\varphi(d)$ faithful characters at one embedding of the character values into $\overline{\mathbb{Q}}_p$, including individual Frobenius conjugates, and order their c_τ

in decreasing order, denoting the result by $c^{(1)}, c^{(2)}, \ldots$. Set

$$A(d,p,M) = d^2 \log(2d) + d \log(2pM).$$

Theorem 57.53 (Simultaneous bounds for the split unit indices)**.** *There is an absolute constant C such that for $1 \le m \le \varphi(d)$,*

$$\log(2 + c^{(m)}) \le C \left(\frac{A(d,p,M)}{m} + \log(2d) + \log\log(3pM) \right).$$

In particular for a character of coefficient residue degree f_τ the bound with $m = f_\tau$ holds for c_τ.

Proof. Take a generator g of Δ, fix a place v_0 over p, and label the places by $v_j = g^j v_0$, $0 \le j < d$. Put

$$w = N_{\mathbb{Q}(\zeta_M)/L}(1 - \zeta_M), \quad u = g(w)/w, \qquad z_j = \log_p \left((g^{-j} u)^{p(p-1)} \right)$$

in the embedding at v_0. The unit calculation in Lemma 57.13 gives $h(u) \le 2M \log(2M)$ for the absolute logarithmic Weil height, and the logarithmic archimedean vector of u has nonzero coefficient at every faithful character. Indeed the norm on w unfolds the coefficient to the Gauss sum times the nonzero Dirichlet value $L(1,\chi)$ of the primitive even character. The factor $g-1$ multiplies it by a nonzero scalar. At v_0 the conjugates of u are in $\mathbb{Z}_p^\times$. Their $p(p-1)$-th powers belong to $1 + p^2\mathbb{Z}_p$, so the z_j have absolute value at most p^{-2}, and their exponentials are the indicated algebraic units.

Let $T_z \subset \mathbb{Q}^d$ be the smallest rational subspace whose scalar extension contains the vector $z = (z_j)$. We need the rank, on this subspace, of the Fourier forms $\ell_\tau(Z) = \sum_{j=0}^{d-1} \tau(g)^j Z_j$. For an integral vector (a_j), the relation $\sum a_j z_j = 0$ is equivalent to $\prod_j (g^{-j}u)^{p(p-1)a_j} = 1$. This follows by the logarithm and exponential on $1 + p^2\mathbb{Z}_p$ and injectivity of the field embedding. The relations are therefore stable under cyclic shifts. They all vanish also on the vector of real numbers $(\log |g^{-j}u|)_j$, using any fixed real embedding. Clearing denominators treats rational relations. Thus $T_z \otimes \mathbb{C}$ contains that real vector and its cyclic shifts. Projection in the complex group algebra onto each faithful eigenline gives a nonzero vector by the archimedean calculation. Every faithful eigenline is therefore contained in the complexification. The same inclusion holds over $k = L(\zeta_d)$: these eigenlines are defined over k and membership in T_z is tested by rational linear equations. Distinct Fourier forms pair with distinct such lines. In particular any m faithful forms restrict to rank m on $T_z \otimes k$.

Apply Gaudron's simultaneous p-adic logarithm bound over k to these m forms and the d logarithms z_j. We spell out the parameter dependence because both the field and p vary. The degree $D = [k : \mathbb{Q}]$ is at most d^2, the coefficients of the forms have height zero, and the heights of the exponentials are at most $H = 2p^2 M \log(2M)$. The rank parameter in the theorem is the codimension on T_z, hence is m. Its real radius parameter may be taken equal to $\exp(1)$, since $p^{-2} \le \exp(-1) p^{-2/(p-1)}$ for $p \ge 5$. Take each logarithmic height parameter equal to H and the logarithmic coefficient parameter equal to D. The auxiliary integer in the bound is then at most $a = 2 + \lceil D \log(\exp(1) + D + dH) \rceil$. For any set $\mathcal{T}$ of m distinct faithful labels the theorem gives, with an absolute constant,

$$-\log \max_{\tau \in \mathcal{T}} |\ell_\tau(z)|_p \ \ll \ (10d)^{59 d^2/m} \, a^{1/m} (D + a + D \log(2D))(1 + DH)^{d/m}.$$

Here the product in the logarithm theorem runs over a maximal rationally independent subfamily, of size at most d. This application does not require multiplicative independence of all

the conjugates. The published estimate and its parameter conventions are in Gaudron, *Bulletin de la Société Mathématique de France* 142 (2014), Theorem 2.1, p. 5.

For u itself the image in the local exponent lattice at the τ-factor is the evaluation of its logarithm vector at $\tau(g)$, namely $\ell_\tau(z)/(p(p-1)\log_p(1+p))$. The denominator has valuation two under $v_p(p)=1$. The image ideal of all ordinary units contains this element, so $v_p(\ell_\tau(z)) \ge 2+c_\tau$. For a singleton the rank computation and Gaudron's theorem also give nonvanishing. Taking the m indices of largest c_τ lower bounds the left side of the preceding display by $(2+c^{(m)})\log p$. Take ordinary logarithms. The power of $10d$ contributes $O(d^2\log(2d)/m)$; the product contributes $O(d\log(2dpM)/m)$. The remaining factors contribute $O(\log(2d)+\log\log(3pM))$ by the bound on a. Absorbing $d\log(2d)$ into $d^2\log(2d)$ proves the claim. Conjugating coefficients preserves the index and the orbit has f_τ members, which gives the last assertion. □

Corollary 57.54 (Uniformity in the cyclotomic layer at the split primes)**.** *Use the intervals and full fields $E_x \subseteq E_*$ of Theorem 19.15. For each cyclic $L \subset E_*^+$ as above and each good split prime $p \le t_*+1$, put*

$$L_i = L\mathbb{Q}_i, \quad G_i = \mathrm{Gal}(L_i/L), \qquad h_\tau^0 = \mathrm{length}_{O_\tau}\,\mathrm{Cl}(L)\{p\}_\tau,$$

where $\mathbb{Q}_i$ is the degree p^i cyclotomic layer. Except for at most

$$O_{\psi,\varepsilon}\left(\frac{d^2\log(2d)+d\log(2V)}{V^\varepsilon}\right)$$

faithful character labels for this L,p, both

$$\sup_{i\ge1}\mathrm{length}_{O_\tau}\left((\mathrm{Cl}(L_i)\{p\}_\tau)^{G_i}\right) \quad \textit{and} \quad \mathrm{length}_{O_\tau}(B/TB)$$

are at most $h_\tau^0+\exp(V^\varepsilon/16) < b_0(x)$ throughout the interval for sufficiently large V. Here B is the compact module for the zero-residue weights of $\alpha=\tau^{-1}$. For every fixed $0<\delta<1$ the exceptional fraction tends uniformly to zero for $2 \le d \le V^{(1-\delta)\varepsilon}$. There are no exceptional labels for $d \le V^{\varepsilon/3}$ once V is sufficiently large.

Proof. The hypotheses give $p, M, n_* \le V^{C_{\psi,\varepsilon}}$. If there are $m>0$ indices larger than $\exp(V^\varepsilon/16)$, the theorem bounds m as stated: its additive logarithmic terms are $O_{\psi,\varepsilon}(\log V) = o(V^\varepsilon)$. This argument includes primes dividing class numbers or indices of circular units. Theorem 57.7 gives the first length at level i as $h_\tau^0+\min(i,c_\tau)$. Theorem 57.10 gives the second as an S-class length plus the local index for S-units, where S consists of the primes over p. Ordinary units belong to the S-units and the S-class group is a quotient of the ordinary class group. Both displayed quantities are consequently bounded by $h_\tau^0+c_\tau$. Minkowski's ideal bound and the conductor-discriminant formula, as in Corollary 57.52, give $h_\tau^0 \le \log_p h_L \ll d\log(2M)/\log p$, a polynomial bound in V. This proves the comparison with $b_0(x)$.

The degree d has odd part dividing the fixed order of ψ, since E_* is obtained from K_ψ by extensions of degree a power of two. Thus $\varphi(d) \gg_\psi d$. Dividing the bound on the number of exceptions by $\varphi(d)$ gives a quantity tending uniformly to zero in the stated degree range. In the smaller range the bound for the number itself tends to zero. Subfields occurring at any x are already included at the top field. □

At a positive zero-residue weight the actual strict group is dual to $B/(T-((1+p)^{-r}-1))B$. The corollary bounds the constant specialization and the invariant ordinary classes at all levels. Controlling the exceptional positive-weight specializations in Section 6.6 still requires information on the cyclotomic action.

57.17 One class group quotient for the sum at the half-residue weights

We retain the lengths at the exceptional weights of Theorem 57.51. Their sum, including every digit through an arbitrarily prescribed precision, can be measured by imposing one polynomial relation on one finite ordinary class group. The additive error below is independent of that precision.

Use $E = E_*, D_p, H = (ED_p)^+$, $H_0 = E^+$, ι, and B_p as in Lemma 57.50. We consider only primes with a nonempty list in that lemma. Let $\mathbb{Q}_j$ be the cyclotomic layer of degree p^j, set $H_j = H\mathbb{Q}_j$ for $j \geq 1$, and write H itself for the base layer. In particular $H_0 = E^+$ continues to mean the fixed field of ι. Let $\Delta = \mathrm{Gal}(H/\mathbb{Q})$, and choose γ in the cyclotomic direction with principal cyclotomic value $1 + p$. Put

$$C(j) = \tfrac{1}{2}(1 - \iota)\,\mathrm{Cl}(H\mathbb{Q}_j)\{p\} \quad (j \geq 0), \qquad \mathbb{Q}_0 = \mathbb{Q}, \qquad u_r = (1 + p)^{-r}.$$

Then $\log_p |C(0)| = B_p$. Fix a union of coefficient Frobenius orbits of the allowed characters α. Let $e \in \mathbb{Z}_p[\Delta]$ be the sum of the idempotents for their characters $\tau = \alpha^{-1}\eta_p$.

Lemma 57.55 (Finite precision in the ordinary class group)**.** *There is a norm isomorphism*

$$C(j)/(\gamma - 1)C(j) \simeq C(0).$$

Let $r \equiv (p-1)/2 \bmod (p-1)$ be positive, $k \geq 1$, and $j \geq \max(0, k - 1 - v_p(r))$. Then

$$\sum_{\alpha \text{ selected, one per orbit}} \log_p |S(\alpha, r)[p^k]| = \log_p \left| eC(j)/(p^k, \gamma - u_r)eC(j) \right|.$$

Proof. The finite Galois group of $H\mathbb{Q}_j/\mathbb{Q}$ is $\Delta \times \langle\gamma\rangle$, the second factor of order p^j, because $p \nmid [H : \mathbb{Q}]$. The indicated lower bound on j makes the principal part of the coefficient character trivial modulo p^k on the absolute Galois group of $H\mathbb{Q}_j$, by $v_p(u_r^{p^j} - 1) = 1 + v_p(r) + j$. On the finite quotient the actions are τ and u_r. The central element ι acts by -1 and lies in the inertia image at every prime over p: its tame image was already present in H, and a subgroup of a product of groups of coprime orders contains the pure factors of each of its elements. Thus global invariants of the divisible coefficient and invariants at p vanish as in Theorem 57.47. One can use the lift of tame inertia whose principal cyclotomic part is one, or just use its action modulo p, whose difference from one is a unit. Multiplication by p^k identifies p^k-torsion in the global and p-local first cohomology with first cohomology on the finite coefficients.

The finite quotient and the local decomposition quotient at p have vanishing positive-degree cohomology on these coefficients. Indeed first take cohomology of the central subgroup $\langle\iota\rangle$: averaging kills positive degrees and its invariants vanish. Inflation–restriction therefore gives the equivariant homomorphisms on the upper field and detects the zero local class. Away from p the inertia quotient is of order prime to p. Over the upper field, inertia away from p acts trivially also on the divisible coefficients, since the finite character there is trivial on inertia and the cyclotomic part is unramified. Consequently the unramified condition descends and ascends by restriction, just as in Theorem 57.47. The real places contribute no odd-primary inertia. Reciprocity over $H\mathbb{Q}_j$ now computes the homomorphisms from its ordinary class group that kill the classes above p. These prime classes are fixed by ι and already map to zero in every selected factor. In the τ-factor, equivariance imposes $\gamma = u_r$ and the coefficient precision imposes $p^k = 0$. Finite duality preserves the order of each factor over its unramified integer ring. Multiplying over the selected orbits proves the second formula.

For the norm assertion take the base of cohomology to be E^+ and the divisible coefficient $\mathbb{Q}_p/\mathbb{Z}_p$ twisted only by the character of H/E^+. On $\mathrm{Gal}(H\mathbb{Q}_j/E^+) = \langle\iota\rangle \times \langle\gamma\rangle$, the two actions are now -1 and 1. The very same global and local averaging arguments identify the dual of the

strict group with $C(j)/(\gamma-1)C(j)$. Computing over H instead gives $C(0)$. Restriction of the homomorphisms corresponds to ideal norm by functoriality of reciprocity. Dualizing therefore gives the indicated norm isomorphism, which is compatible with the Δ-action. □

Theorem 57.56 (The product of the weight relations)**.** *Let $\mathcal{R}\subset[1,R)$ be any finite set of positive half-residue weights and put*

$$P_{\mathcal{R}}(Y)=\prod_{r\in\mathcal{R}}(Y-u_r),\qquad D(\mathcal{R})=\sum_{\substack{r,s\in\mathcal{R}\\ r<s}}(1+v_p(s-r)).$$

For $1\le k\le m$ use one layer $j=m-1$ and define

$$q_k=\log_p\left|eC(j)/(p^k,P_{\mathcal{R}}(\gamma))eC(j)\right|,\qquad a_k=\sum_{r\in\mathcal{R}}\sum_{\alpha\text{ selected, one per orbit}}\log_p|S(\alpha,r)[p^k]|.$$

Then

$$0\le a_k-q_k\le\log_p|eC(0)|\,D(\mathcal{R}).$$

In particular the two differences a_m-a_k and q_m-q_k differ in absolute value by at most this same bound, independent of m. For the empty set the quotient by the empty product is zero and the logarithms of orders are zero.

Proof. Set $A=eC(j)/p^keC(j)$ and enumerate the weights as $r_1,\dots,r_n$. Write $D_i=\gamma-u_{r_i}$ acting on A, $Q_0=1$, and $Q_i=D_iQ_{i-1}$. By the lemma, $a_k=\sum_i\log_p|\ker D_i|$, since an endomorphism of a finite group has equal kernel and cokernel orders. The order of $Q_{i-1}A/Q_iA$ is $|\ker D_i\cap Q_{i-1}A|$; this is the kernel-cokernel equality for the restriction of D_i to $Q_{i-1}A$. These latter logarithms sum to q_k. Their termwise deficits are nonnegative.

On $\ker D_i$ the operator Q_{i-1} acts by the nonzero scalar $\prod_{h<i}(u_{r_i}-u_{r_h})$, of valuation $b_i=\sum_{h<i}(1+v_p(r_i-r_h))$. Therefore $\ker D_i\cap Q_{i-1}A$ contains $p^{b_i}\ker D_i$. The deficit at i is at most b_i times the number of cyclic generators of the finite abelian p-group $\ker D_i$. All u_r are one modulo p; the subgroup killed by p in $\ker D_i$ is precisely $A[p]^{\gamma=1}$. Its dimension is at most $\log_p|\ker(\gamma-1:A\to A)|$, which equals $\log_p|A/(\gamma-1)A|$. The latter is at most $\log_p|eC(0)|$ by the norm assertion and right exactness of quotienting. Summing over i gives the inequality. Subtracting two numbers in the same interval $[0,\log_p|eC(0)|D(\mathcal{R})]$ proves the assertion about differences. □

Corollary 57.57 (A finite test for the entire half-residue tail)**.** *At $x\in[V,V^{3/2}]$ let $H(x)$ be the contribution to $\mathcal{R}(x)$ of Proposition 6.11 from good $p\ge5$ and half-residue weights. Let $X>0$ be any proposed bound in natural logarithmic order, $b=b_0(x)$, and, for each contributing prime, take*

$$m_p=b+\lfloor X/\log p\rfloor+1.$$

At fixed p, split the half-residue weights $1\le r<t(x)$ into those with $r\le x^\eta$ and those with $r>x^\eta$. On each set take e to select precisely the characters inflated from E_x surviving $1-J_{p,r}$ in Section 6.6. Use the theorem on each such set, at $m=m_p$, and add $(q_{m_p}-q_b)\log p$ over the sets and primes, obtaining $Q(x,X)$. Define

$$\mathcal{D}(x)=\sum_{p,\,\mathcal{R}}(\log p)\log_p|eC(0)|\,D(\mathcal{R}).$$

There is $A=A_{\psi,\varepsilon}$ with $\mathcal{D}(x)\ll_{\psi,\varepsilon}V^A$ uniformly on the interval and independently of X. One has both implications

$$\begin{aligned}Q(x,X)+\mathcal{D}(x)\le X&\implies H(x)\le X,\\ H(x)\le X&\implies Q(x,X)\le X+\mathcal{D}(x).\end{aligned}$$

Proof. The idempotent is constant on each indicated set by the definition of $J_{p,r}$. Prime-to-p character descent identifies the contribution on E_x with the selected scalar groups: averaging is exact globally and locally, and the inertia quotients away from p have order prime to p. All these primes satisfy $p \le 2R+1 < P(x)$ for large V, so their truncation is at b. Capping the elementary divisors at m_p gives a truncated total $H_{\mathrm{cap}} = \sum_{p,\mathcal{R}} (a_{m_p} - a_b) \log p$, with $0 \le H_{\mathrm{cap}} \le H(x)$. Its difference from $Q(x,X)$ is bounded by $\mathcal{D}(x)$ by the theorem. For each set $D(\mathcal{R}) \le R^2(1+\log_p R)$. Corollary 57.52 bounds $\log_p |eC(0)|$ by $O(n_*(1+\log N_*/\log p))$. There are at most $2(2R+1)$ sets, and the interval parameters here are polynomial in V. This proves the uniform error bound.

If any elementary divisor in the sum were longer than m_p, its contribution alone to H_{cap} would be at least $(m_p - b)\log p > X$. Thus $H_{\mathrm{cap}} \le X$ forces $H_{\mathrm{cap}} = H(x)$. This proves the first implication, and the second follows from $H_{\mathrm{cap}} \le H(x)$. □

The action of γ is essential to this test. For example, as a calculation with finite modules, fix a weight r_0 prime to p and an integer $M \ge 2$. On $\mathbb{Z}/p^{j+1}\mathbb{Z}$ let γ act by $u_{r_0} + p^M$. Its difference from one has valuation one, so this action factors through order p^j; reduction gives the maps between the layers. The orders p^{j+1} and the coinvariant orders p are independent of M, whereas the length at u_{r_0} is $\min(M, j+1)$. The arithmetic quotients in the corollary retain the actual action of the period fields. Their required size on arbitrarily distant intervals has yet to be bounded.

57.18 All weights at a good prime in one ordinary class group

We include the zero residue at the completely split primes and retain the original averaging operator at each weight. Write $E = E_*$, $N = N_*$, $R = t_*$, and take $5 \le p \le 2R+1$, $p \nmid n_* N$, on a common interval. Put

$$F = (E\mathbb{Q}(\mu_p))^{+}, \quad F_j = F\mathbb{Q}_j, \quad C_j = \mathrm{Cl}(\mathcal{O}_{F_j}[1/p])\{p\}, \quad \Delta = \mathrm{Gal}(F/\mathbb{Q}).$$

Thus C_j is an ordinary ideal class group modulo the classes of the primes above p. Its degree-zero logarithmic analogue will not be needed. The cyclotomic layers $\mathbb{Q}_j$ and generator γ are normalized as in Section 57.17. The degree of F is prime to p. In particular F is disjoint from $\mathbb{Q}_\infty$, and locally at p its intersection with the totally ramified cyclotomic $\mathbb{Z}_p$-extension is trivial.

Given a character α of E and $0 \le s < p-1$ with $\alpha(c) = (-1)^s$, the finite character $\tau = \alpha^{-1}\omega^{-s}$ is an even character of $E\mathbb{Q}(\mu_p)$, where ω is the Teichmüller cyclotomic character. Every character of F occurs once this way: $E \cap \mathbb{Q}(\mu_p) = \mathbb{Q}$ by unramifiedness and total ramification at p. Frobenius conjugation of the coefficients preserves s. Write e_τ for the integral orbit idempotent in $\mathbb{Z}_p[\Delta]$.

Lemma 57.58 (Ordinary class groups at the split places)**.** *Suppose $\tau \ne 1$, $m \ge 1$ and $r > 0$ is congruent to s mod $(p-1)$. Put $u_r = (1+p)^{-r}$. For $j \ge m$, the finite O_τ-dual of $S(\alpha, r)[p^m]$ is*

$$e_\tau C_j / (p^m, \gamma - u_r) e_\tau C_j.$$

This holds also when τ is trivial on the entire decomposition group at p.

Proof. Write $D = (\mathrm{Frac}(O_\tau)/O_\tau)(\tau\langle\kappa_p\rangle^{-r})$ and $d_r = 1 + v_p(r)$. The finite quotient over $\mathbb{Q}$ is $\Delta \times \langle\gamma\rangle$, with the second factor of order p^j. Over F_j the coefficient on $D[p^m]$ is trivial because $j + d_r \ge m$. The global invariants of D vanish: a nonidentity value of the prime-to-p character is different from one modulo p. Hence $H^1(\mathbb{Q}, D)[p^m] = H^1(\mathbb{Q}, D[p^m])$. Averaging over Δ gives zero invariants and zero higher cohomology on the finite coefficient, so restriction identifies this

first cohomology with equivariant homomorphisms on G_{F_j}. Away from p the inertia quotient has order prime to p and inertia over F_j acts trivially even on D. Consequently unramifiedness of the divisible class is equivalent to vanishing of the homomorphism on that inertia.

At p the decomposition quotient is $\Delta_w \times \langle\gamma\rangle$. Its projections are onto and their orders are coprime. If τ is nontrivial on Δ_w, averaging there proves local injectivity, and local invariants of D are zero. Suppose instead that $\tau|_{\Delta_w} = 1$. The principal cyclotomic image on $G_{\mathbb{Q}_p}$ is all of $1 + p\mathbb{Z}_p$. Its image on $G_{F_{j,w}}$ is the subgroup of p^j-th powers: the local degree of F is prime to p. A finite cocycle whose divisible local class is zero has the form $g \mapsto (\theta(g) - 1)y$ locally, with $\theta = \tau\langle\kappa_p\rangle^{-r}$. Then $p^m y$ lies in $D^{G_{\mathbb{Q}_p}} = D[p^{d_r}]$. On $G_{F_{j,w}}$ the difference $\theta(g) - 1$ is divisible by p^{j+d_r}. The assumption $j \geq m$ therefore makes the finite cocycle itself zero there.

Conversely a local cocycle that vanishes on this upper group has divisible class inflated from the local quotient on $D^{G_{F_{j,w}}} = D[p^{j+d_r}]$. Average out Δ_w, which is acting trivially in this case. For the remaining cyclic group, first cohomology is the kernel of $1 + u_r + \cdots + u_r^{p^j-1}$ modulo the image of $u_r - 1$. Their valuations are j and d_r; the first kernel and the second image on $D[p^{j+d_r}]$ are both $p^{d_r}D[p^{j+d_r}]$. Thus the divisible local class is zero. The real places impose no odd-primary condition. Class field theory now gives C_j, with equivariance imposing τ and $\gamma = u_r$. Taking finite O_τ-duals proves the formula. □

Fix x. For each nontrivial orbit τ, let $\mathcal{R}_\tau$ consist of the weights $1 \leq r < t(x)$ in its residue for which α is inflated from E_x and survives $1 - J_{p,r}$. Put $\mathcal{R}_1 = \varnothing$: the only trivial pair is $\alpha = 1, s = 0$, whose scalar group is zero by Lemma 56.16. Define one polynomial over the integral group algebra and one finite group at the chosen precision:

$$P(Y) = \sum_{\tau} e_\tau \prod_{r \in \mathcal{R}_\tau} (Y - u_r),$$
$$Z_m = C_m/(p^m, P(\gamma))C_m.$$

Empty products are one. Let Y_m be the direct sum of the groups on the right of Lemma 57.58 at $j = m$ over all the indicated orbits and weights. Set

$$a_p = \max_{\tau,\ r \in \mathcal{R}_\tau} \sum_{\substack{r' \in \mathcal{R}_\tau \\ r' \neq r}} (1 + v_p(r - r')),$$

taking zero when there are no weights.

Theorem 57.59 (Two-sided bounds for all the surviving elementary divisors)**.** *There are homomorphisms between Z_m and Y_m in both directions whose two composites are multiplication by p^{a_p}. Thus for every integer $b \geq a_p$,*

$$|p^{b+a_p} Z_m| \ \leq \ |p^b Y_m| \ \leq \ |p^{b-a_p} Z_m|.$$

If g_p is the number of primes of F above p, the base-p logarithms of the two outer orders differ by at most

$$2a_p R\,(v_p(h_F) + g_p - 1).$$

This error is uniform in the cyclotomic level m, including at primes that divide the indices of global units.

Proof. Work on one nonempty orbit factor $A = e_\tau C_m/p^m e_\tau C_m$. List its distinct roots $u_1, \ldots, u_n$, let $P_0(Y) = \prod_i (Y - u_i)$, and let $P_i(Y) = P_0(Y)/(Y - u_i)$. The diagonal quotient map from $A/P_0(\gamma)A$ goes to $\bigoplus_i A/(\gamma - u_i)A$. For the reverse map, lift the entries x_i and send them to the class of

$$\sum_i \frac{p^{a_p}}{P_i(u_i)} P_i(\gamma) x_i.$$

All the coefficients lie in $\mathbb{Z}_p$ by the difference valuation in Theorem 57.51; that valuation holds for any two distinct positive integers. Changing a lift changes the sum by a multiple of $P_0(\gamma)$. Evaluation in the i-th quotient gives $p^{a_p}x_i$, and the interpolation identity $\sum_i p^{a_p}P_i(Y)/P_i(u_i) = p^{a_p}$ gives the other composite. Summing the maps over the orbit factors proves the assertion for Y_m, Z_m. Factoring multiplication by p^{b+a_p} through p^bY_m, and multiplication by p^b on Y_m through $p^{b-a_p}Z_m$, proves the two inequalities.

It suffices to bound the number of abelian p-group generators of Z_m, since lowering a power of p by one increases the logarithmic order by at most that number. Modulo p, on each factor the polynomial is $(Y-1)^{|\mathcal{R}_\tau|}$. Consequently Z_m/pZ_m is a quotient of $C_m/(p,(\gamma-1)^R)C_m$. The filtration by powers of $\gamma-1$ has at most R quotients, each an image of $C_m/(p,\gamma-1)C_m$.

For completeness the latter dimension is bounded at the bottom of the tower even when its full coinvariant length is large. All the primes over p in F are totally ramified in F_m/F. In the abelian p-class field of F_m split above p, a decomposition group at one such prime lifts $\langle\gamma\rangle$ isomorphically. The Galois group over F is thus the semidirect product of C_m and this lift. Its abelianization replaces C_m by $C_m/(\gamma-1)C_m$. To make every prime over p split, kill the chosen lift and the differences with the other g_p-1 decomposition generators. This gives exactly the split class group of F: its class field base-changes into the corresponding split class field of F_m, and the constructed quotient has the required ramification and splitting. Hence at most g_p-1 more generators are needed than for $\mathrm{Cl}(\mathcal{O}_F[1/p])\{p\}$, which itself needs at most $v_p(h_F)$. This proves the stated width without an upper bound for any unit index. □

Corollary 57.60 (A simultaneous ordinary class group test for the good primes)**.** *Let $G(x)$ be the part of $\mathcal{R}(x)$ in Proposition 6.11 from all primes $p \geq 5$ prime to n_*N_*, including all weights. For $X > 0$ put $b = b_0(x)$ and $m_p = b + \lfloor X/\log p \rfloor + 1$. Over the good primes through $2R+1$ form the two quantities*

$$T_{\mathrm{low}} = \sum_p \log|p^{b+a_p}Z_{m_p}|, \qquad T_{\mathrm{up}} = \sum_p \log|p^{b-a_p}Z_{m_p}|.$$

For all sufficiently large V these are defined, and $0 \leq T_{\mathrm{up}} - T_{\mathrm{low}} \ll_{\psi,\varepsilon} V^A$ for some fixed A, independently of X. On the same fields and intervals one has

$$\begin{aligned} T_{\mathrm{up}} + \log J(V) \leq X &\implies G(x) \leq X, \\ G(x) \leq X &\implies T_{\mathrm{low}} \leq X, \end{aligned}$$

where $J(V)$ is the integer of Lemma 9.31, with $\log J(V) \ll_{\psi,\varepsilon} V^C$.

Proof. For $p \leq 2R+1$ we have $p < P(x)$ eventually, and $a_p \leq R(1+\log_p R) < b$. The theorem and prime-to-p descent as in Corollary 57.57 bracket the actual capped total on these primes between the two sums. The corresponding F has degree at most $n_*(p-1)$ and conductor dividing pN_*. Hence both g_p and $v_p(h_F)$ are polynomially bounded in V, by the Minkowski estimate of Corollary 57.52. Summing the displayed width of the theorem with the factors $\log p$ gives the asserted polynomial width.

Every prime beyond $2R+1$ satisfies $p-1 \nmid 2r$ for every weight in question. For sufficiently large V it also lies outside the fixed finite exceptional set of Lemma 9.31. That lemma bounds the total logarithm of the full orders there by $\log J(V)$. If the capped total is at most X, an elementary divisor longer than m_p at a prime in the test would contribute at least $(m_p - b)\log p > X$ to that total. Thus the cap has lost nothing at those primes. Combining these facts gives the first implication. For the second, T_{low} is at most the capped total, itself at most $G(x)$. □

The two numbers now measure the contribution at all good primes within polynomial uncertainty, using the original weight-dependent field averages. Their absolute size still depends on the action on ideal classes in the common cyclotomic layer. An upper bound for that size on arbitrarily distant intervals, the other coefficient primes, and the integral signed period comparison remain necessary.

57.19 Prime ideal generators at exact cyclotomic depth

The splitting restriction in Corollary 22.54 has a converse for the scalar groups whose residual character is nontrivial at the coefficient prime. We construct rational primes at the least possible common depth for an entire list. Several weights on the same character and several coefficient primes may occur together.

Fix one interval with largest field E_*, degree n_* and modulus N_*. Use the scalar characters and weights of Section 57.18. An entry consists of a good prime $p \geq 5$, $p \nmid n_* N_*$, a positive weight $r < t(x)$, and a character α of E_x with $\alpha(c) = (-1)^r$. Inflate to E_*, and let $\tau = \alpha^{-1}\omega_p^{-r}$ be nontrivial, with ω_p the Teichmüller character. One can restrict the list to the characters selected by the original field averages. Write $F = (E_*\mathbb{Q}(\mu_p))^+$, $F_j = F\mathbb{Q}_j$, where $[\mathbb{Q}_j : \mathbb{Q}] = p^j$ in the cyclotomic $\mathbb{Z}_p$-extension. Put $d_r = 1 + v_p(r)$ and $u_r = (1+p)^{-r}$. For an integer $m \geq 1$ let Q be the finite dual of $S(\alpha, r)[p^m]$ over its unramified coefficient ring. For an abelian p-group we use the additive convention.

Lemma 57.61 (A class field at the precision of the twist)**.** *Choose the layer index*

$$j = \begin{cases} \max(0, m - d_r), & \tau \text{ nontrivial on a decomposition group at } p, \\ m, & \tau \text{ trivial there.} \end{cases}$$

There is a finite Galois extension $M/\mathbb{Q}$, abelian over F_j, with $\mathrm{Gal}(M/F_j) = Q$. The class map on F_j is the quotient

$$e_\tau C_j/(p^m, \gamma - u_r)e_\tau C_j, \qquad C_j = \mathrm{Cl}(\mathcal{O}_{F_j}[1/p])\{p\}.$$

The largest subfield of M abelian over $\mathbb{Q}$ is F_j.

Proof. Lemma 57.58 gives this class quotient for $j = m$. We justify the smaller layer when τ is locally nontrivial. Over F_j the principal cyclotomic character raised to $-r$ is trivial modulo p^m, since $v_p(u_r^{p^j} - 1) = j + d_r$. The remaining finite character already factors through F. Globally and at p the finite quotient is the product of its prime-to-p part and its cyclic p-part. At p this follows also from the fact that a subgroup of a finite abelian group contains the prime-to-p and p-parts of each of its elements. In each quotient a prime-to-p element acts on the finite coefficient by a root of unity differing from one by a unit. Averaging over its cyclic subgroup kills the invariants and all higher cohomology. Inflation–restriction now gives equivariant homomorphisms over F_j and detects zero localization at p. The invariants of the divisible coefficient vanish in the same two places, so the exact sequence for multiplication by p^m identifies the divisible and finite conditions through that precision. Away from p the inertia quotient in $F_j/\mathbb{Q}$ has order prime to p. On the upper inertia the finite and divisible coefficients have trivial action, since the cyclotomic extension is unramified there and the finite character is trivial on that inertia. Thus the condition is unramifiedness, by restriction and averaging. Class field theory gives the asserted quotient, with the scalar relation on γ coming from equivariance.

The map from the ordinary class group to Q has Galois-stable kernel. Its abelian class field M/F_j is consequently Galois over $\mathbb{Q}$. Choose an element of the prime-to-p factor whose

τ-value is nontrivial. It acts on Q with its difference from the identity a unit on the whole orbit component. The commutators with any lift of this element therefore generate Q. Conversely all commutators in $\mathrm{Gal}(M/\mathbb{Q})$ belong to Q, since $F_j/\mathbb{Q}$ is abelian. Its commutator subgroup is exactly Q, proving the last assertion. □

Theorem 57.62 (Simultaneous generators with prescribed Frobenius depth)**.** *Let $i = 1, \dots, s$, $s \geq 1$, be a finite list as above, with entries $p_i, r_i, \tau_i, m_i, j_i, Q_i$. Assume that Q_i has exponent $p_i^{m_i}$. This can always be arranged for a nonzero truncated group by reducing its precision to its exponent. For each occurring p define*

$$N_p = 1 + \max_{i : p_i = p} j_i.$$

Let $d = \max_i \dim_{\mathbf{F}_{p_i}} Q_i/p_i Q_i$. There are $h = d + \lceil \log_2(2s) \rceil$ distinct rational primes q_a, outside any prescribed finite set, such that all split in E_* and

$$v_p(q_a - 1) = N_p \quad \text{for every } a, p.$$

For each i one can choose primes over these q_a in F_{i,j_i} whose images generate Q_i as an abelian group. The choices over different fields can be taken from one prolongation per rational prime.

If every entry at p has τ_i nontrivial locally at p, then

$$N_p = \max(\{1\} \cup \{m_i - v_p(r_i) : p_i = p\})$$

is the least possible common depth for generating these groups by primes split in E_* and congruent to one modulo p. The same necessity holds when one requires the multiplied prime classes only to generate $p^{b_i} Q_i$, provided $0 \leq b_i < m_i$.

Proof. For the finite set of coefficient primes take

$$A = \mathbb{Q}(\mu_{N_* \prod_p p^{N_p}}), \qquad C = \mathbb{Q}(\mu_{N_* \prod_p p^{N_p+1}}).$$

Every F_{i,j_i} lies in A by the choice of N_p. The Chinese remainder theorem prescribes an automorphism σ of C which is one modulo N_* and $1 + p^{N_p}$ modulo p^{N_p+1} at every p. It fixes A. Let $K = C \prod_i M_i$, using the class fields of the lemma, and $G = \mathrm{Gal}(K/\mathbb{Q})$. Since $C/\mathbb{Q}$ is abelian, $M_i \cap C = F_{i,j_i}$. Consequently restriction maps $\mathrm{Gal}(K/C)$ onto each Q_i. This follows by extending an automorphism first to $M_i C$ over C and then to the Galois extension K/C.

The lifts of σ to G form a coset of this subgroup. Each fixes all F_{i,j_i}. A uniform choice in the coset therefore maps uniformly to each Q_i. Take h independent choices. At a given i, failure to span the reduction modulo p_i puts all h entries in one hyperplane. For dimension d_i there are $(p_i^{d_i} - 1)/(p_i - 1)$ hyperplanes, each of relative size $1/p_i$. The failure probability is at most $p_i^{d_i - h} \leq 2^{d-h}$. The sum of these bounds over the list is at most $1/2$. Thus a tuple spanning every reduction exists, including when some weight quotients are correlated. Spanning modulo p_i implies generation of the full finite group, by iteration of multiplication by p_i on its quotient by the span.

Apply Chebotarev's theorem in $K/\mathbb{Q}$ to each chosen element. There are infinitely many unramified rational primes in its conjugacy class, and conjugating the prolongation realizes the element itself. Choose the primes successively with the stated exclusions. Their actions on C give the exact valuations and complete splitting in A. Thus their residue degrees over each F_{i,j_i} above $\mathbb{Q}$ are one. Their restrictions to M_i are precisely the relative arithmetic Frobenius elements, hence the ideal class images under reciprocity. These are the generating elements just chosen. [24]

For necessity, take any candidate prime q unramified in the fields in question, split in E_*, and congruent to one modulo p. Its Frobenius on F is trivial. In the cyclotomic direction it acts on Q_i by q^{-r_i}. Indeed q is a principal p-adic unit, and the relation on the chosen generator is $\gamma = (1+p)^{-r_i}$. Frobenius fixes the class of each prime above q in F_{i,j_i}. Thus every image is killed by $q^{r_i} - 1$, also when the prime does not split completely at level j_i. Its order has base-p exponent at most $v_p(q-1) + v_p(r_i)$, by binomial expansion. To generate a group of exponent p^{m_i} at least one generator must have that order. To generate $p^{b_i} Q_i$ with $b_i < m_i$, at least one multiplied class must have order $p^{m_i - b_i}$, with the same consequence for the original class. Taking the maximum gives the lower bound for any common depth. In the locally nontrivial case our chosen $1 + j_i$ is exactly $\max(1, m_i - v_p(r_i))$, proving attainment. □

This also gives the cost of a simultaneous choice of such primes for the independent symplectic inertia characters of Theorem 62.23. For a fixed p, the h primes just constructed have local separating ideal $p^{h N_p} \mathcal{O}$. Any set of probes of depth at most D at p misses generators for a component with $m_i > D + v_p(r_i)$. This statement concerns the prime ideal images in the indicated class groups. The construction lets the probes depend on the actual exponents. An upper bound for those exponents, or for their weighted sum on the interval, is still required in Section 6.6.

58 References

[1] T. Liu, *Torsion p-adic Galois representations and a conjecture of Fontaine*, Ann. Sci. École Norm. Sup. (4) **40** (2007), 633–674, Sections 1 and 7.3. Original paper.

[2] M. Kisin, *The structure of potentially semi-stable deformation rings*, Theorem 1.2.2. See also *Potentially semi-stable deformation rings*, J. Amer. Math. Soc. **21** (2008), 513–546.

[3] K. Kato, *p-adic Hodge theory and values of zeta functions of modular forms*, Astérisque **295** (2004), 117–290, Theorem 14.2(1) and Section 14.10.

[4] J. Newton and J. A. Thorne, *Adjoint Selmer groups of automorphic Galois representations of unitary type*, J. Eur. Math. Soc. **25** (2023), 1919–1967, Theorem A and Section 2.5.

[5] D. Geraghty, *Modularity lifting theorems for ordinary Galois representations*, Math. Ann. **373** (2019), 1341–1427, Section 2. Published paper. Proposition and lemma numbers refer to the original manuscript.

[6] S. Bloch and K. Kato, *L-functions and Tamagawa numbers of motives*, in *The Grothendieck Festschrift*, Vol. I, Progr. Math. **86** (1990), 333–400, Section 3.

[7] L. Pan, *The Fontaine–Mazur conjecture in the residually reducible case*, J. Amer. Math. Soc. **35** (2022), 1031–1169. Author's paper.

[8] J. Arthur and L. Clozel, *Simple Algebras, Base Change, and the Advanced Theory of the Trace Formula*, Annals of Mathematics Studies 120, Princeton University Press, 1989, Chapter III.

[9] T. Barnet-Lamb, T. Gee, D. Geraghty and R. Taylor, *Local-global compatibility for $l = p$, II*, Ann. Sci. Éc. Norm. Supér. (4) **47** (2014), 165–179, Theorem A. Published paper.

[10] S. W. Shin, *Galois representations arising from some compact Shimura varieties*, Ann. of Math. **173** (2011), 1645–1741. Theorem 1.2.

[11] T. Saito, *Modular forms and p-adic Hodge theory*, Invent. Math. **129** (1997), 607–620. See also *Hilbert modular forms and p-adic Hodge theory*, Compos. Math. **145** (2009), 1081–1113.

[12] G. Chenevier, *The p-adic analytic space of pseudocharacters of a profinite group and pseudorepresentations over arbitrary rings*, in *Automorphic Forms and Galois Representations*, Vol. 1, Cambridge University Press, 2014, 221–285, Introduction and Theorem A. Original paper.

[13] N. Katz, *p-adic properties of modular schemes and modular forms*, in *Modular Functions of One Variable III*, Lecture Notes in Mathematics 350, Springer, 1973. Original paper.

[14] N. Billerey and R. Menares, *On the modularity of reducible mod ℓ Galois representations*, Math. Res. Lett. **23** (2016), 15–41, Section 1. Published paper.

[15] P. Deligne and M. Rapoport, *Les schémas de modules de courbes elliptiques*, in *Modular Functions of One Variable II*, Lecture Notes in Mathematics 349, Springer, 1973, 143–316. Original paper.

[16] F. Diamond and J. Im, *Modular forms and modular curves*, in *Seminar on Fermat's Last Theorem*, CMS Conf. Proc. **17** (1995), 39–133. Authors' text.

[17] P. Deligne, *Formes modulaires et représentations ℓ-adiques*, Séminaire Bourbaki, Exp. 355 (1969). Paper.

[18] H. Carayol, *Sur les représentations ℓ-adiques associées aux formes modulaires de Hilbert*, Ann. Sci. École Norm. Sup. (4) **19** (1986), 409–468. T. Saito, *Modular forms and p-adic Hodge theory*, Invent. Math. **129** (1997), 607–620.

[19] C. M. Skinner and A. J. Wiles, *Ordinary representations and modular forms*, Proc. Natl. Acad. Sci. USA **94** (1997), 10520–10527. Published paper.

[20] S. Gelbart and H. Jacquet, *A relation between automorphic representations of* GL(2) *and* GL(3), Ann. Sci. École Norm. Sup. (4) **11** (1978), 471–542.

[21] P. B. Allen and F. Calegari, *Finiteness of unramified deformation rings*, Algebra Number Theory **8** (2014), 2263–2272, Theorem 1. Original paper.

[22] J. S. Milne, *Class Field Theory*, version 4.03 (2020), Chapter V, Sections 1 and 3, and the reciprocity law. Author's notes.

[23] X. Zhang, *Modular points and dimensions of Eisenstein deformation spaces*, arXiv:2512.21249v4 (2026), Appendix A, Proposition A.1.4 and Theorem A.3.1. Author's preprint, version 4.

[24] J. Thorner and A. Zaman, *A unified and improved Chebotarev density theorem*, Algebra Number Theory **13** (2019). Theorem 1.4 and Theorem 3.1.

[25] F. Lemmermeyer, *The ambiguous class number formula revisited* (2013), Theorem 1 and Proposition 1. Author's paper.

[26] A. Brumer, *On the units of algebraic number fields*, Mathematika **14** (1967), 121–124. Original paper.

[27] T. Fukuda and K. Komatsu, *Weber's class number problem in the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}$, II*, J. Théor. Nombres Bordeaux **22** (2010), 359–368, Corollary 1.1. Published paper.

[28] G. Gras, *Weber's class number problem and p-rationality in the cyclotomic $\widehat{\mathbb{Z}}$-extension of $\mathbb{Q}$*, arXiv:2009.05278, v3 (2020), §7. Author's paper.

[29] A. V. Sutherland, *The analytic class number formula*, MIT 18.785, Lecture 19 (2018), Theorem 19.12. Lecture notes.