The generalized Riemann hypothesis for Dirichlet L-functions

27 November 2026 · Edition 930

Volume IV

Cyclotomic descent and relative strict orders

Abstract

We descend in the real cyclotomic tower, determine the ranges of coefficient primes and track exceptional twists. Norm maps compare the strict orders at consecutive layers.

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

Contents

IV Cyclotomic descent and relative strict orders **1**
19 Descent in the real cyclotomic tower . . . 3
19.1 A bound at all primes for a field of given degree . . . 3
19.2 Descent in the real cyclotomic tower . . . 5
19.3 Fixed odd primes through the full range of twists . . . 6
19.3.1 Stabilization over the full real cyclotomic tower . . . 8
19.4 The conductor and the range of full strict orders . . . 10
19.5 Polynomial conductor on the common interval . . . 12
19.6 All odd primes on a growing part of the same tower . . . 13
19.7 Bounds for deep torsion on the period field . . . 15
19.8 Strict cohomology on the fields of the norm theorem . . . 17
19.9 Strict cohomology in cyclic extensions of prime power degree . . . 19
19.10 The exact length over a cyclic group ring . . . 21
19.11 Determining a compact module from finitely many twists . . . 22
20 Uniform ranges of coefficient primes . . . 22
20.1 Cell counts and full primary orders . . . 22
20.2 All twists at a growing set of odd primes . . . 25
20.3 Testing whole character components on the common interval . . . 27
20.4 All complementary characters for a range of coefficient primes . . . 28
20.5 All odd primes in the polynomial range . . . 30
20.6 All twists on the quadratic invariants of the period fields . . . 31
20.7 Strict local conditions at these very theta primes . . . 32
20.8 An enlarged range of full orders on the same period field . . . 33
20.9 One exceptional set on a whole period interval . . . 34
20.10 Full orders at primes dividing the degree or conductor . . . 36
20.11 Endpoint bounds on the same fields as the period . . . 38
21 Residue data and exceptional twists . . . 39
21.1 Several twists in the same Bernoulli numerator . . . 39
21.2 Frobenius orbits in the exceptional twist count . . . 41
21.3 Common coefficient primes for the cohomology and the Gram minors . . . 42
21.4 A test on the common interval and the prime 37 . . . 44
21.5 One set of Frobenius parameters on the whole interval . . . 45
21.6 One finite field for the large-prime strict orders . . . 46

21.7 Residue valuations over ramified coefficient rings . . . 47
21.8 Frobenius orbits in the local cyclotomic sum . . . 48
21.9 Orders of the detected strict classes on the period interval . . . 49
21.10 Summing full strict orders across weights . . . 50
21.11 A single list of remaining twists on the period interval . . . 51
21.12 One auxiliary field for the ordinary congruences . . . 53
21.13 One prime detecting all the integral dual classes . . . 54
21.14 Interpolation at a fixed conductor . . . 55
21.15 Cuspidal congruences with prescribed auxiliary characters . . . 56
22 Relative orders through the norm map . . . 58
22.1 Strict orders on one cyclotomic field per interval and precision . . . 58
22.2 A common quotient bound for the residual twists . . . 59
22.3 Full relative strict orders in progressions of twists . . . 61
22.4 What two class groups determine about every twist . . . 62
22.5 Real logarithmic class groups at arbitrary precision . . . 63
22.6 An interval bound outside the factors detected by the norm kernel . . . 65
22.7 The strict group at each cyclotomic norm level . . . 66
22.8 The total contribution of the primes required to split . . . 67
22.9 Strict classes killed by one integer throughout an interval . . . 69
22.10 Simultaneous vanishing at the marked coefficient primes . . . 70
22.11 Vanishing of the critical sign at every required weight . . . 71
22.12 The full complementary order outside the class norm exceptions . . . 72
22.13 The local conditions at the conductor . . . 74
22.14 Ordinary class groups at every precision of the strict group . . . 76
22.15 The exceptional weights at small coefficient primes . . . 79
22.16 A fixed level for the rational strict groups . . . 81
22.17 Odd quadratic and quartic characters on the common fields . . . 84
22.18 Normalized Frobenius values on the original period fields . . . 86
22.19 The genus field contribution to the full strict length . . . 89
22.20 Local unit tests at arbitrary precision on the period fields . . . 91
22.21 The exact order of the quadratic summand at three . . . 94
22.22 The exact change in strict cohomology at split primes . . . 96
22.23 Division of strict classes by allowing tame ramification . . . 99
22.24 Measurement of the total residual length by ordinary class groups . . . 101
22.25 Which prime ideals can detect the residual strict classes? . . . 104
22.26 Recovering strict torsion from ray characters . . . 106
22.27 Ordinary class groups before cyclic descent . . . 108
23 References . . . 111

19 Descent in the real cyclotomic tower

19.1 A bound at all primes for a field of given degree

For a number field L, a rational prime p and an integer $r \geq 1$, set

$$A_{p,r} = \mathbb{Q}_p/\mathbb{Z}_p(-r), \qquad \mathcal{S}_{p,r}(L) = \ker\left(H^1(G_{L,S_p}, A_{p,r}) \longrightarrow \prod_{w|p} H^1(L_w, A_{p,r}) \right).$$

Here G_{L,S_p} allows ramification at the finite places over p only. The twist means that the cyclotomic character κ_p acts to the power $-r$. All cohomology is continuous. We write D_L for the absolute discriminant and $d_L = [L : \mathbb{Q}]$.

Theorem 19.1. *There is an absolute constant C with the following property. Let $L \subseteq \mathbb{Q}(\zeta_M)$ be totally imaginary and $r \geq 1$. Then*

$$\sum_p (\log p)\, \operatorname{length}_{\mathbb{Z}_p} \mathcal{S}_{p,r}(L) \;\leq\; \exp\bigl(C[d_L(r+2)]^{10} \log(2Md_L(r+2))\bigr). \tag{19.1}$$

The sum includes both conjugation eigenspaces at every odd prime and the full exponent of each group.

We prove an exponent bound and a bound on the number of generators separately. It matters that a single finite group accounts for the sum at all sufficiently large primes.

Lemma 19.2. *Set $i = 2r,\ n = 2i+8,\ d = d_L,\ W = 3^{dn}$. There are positive integers J, T such that*

$$\log(2JT) \leq \exp\bigl(C(nd)^9 \log(2Mnd)\bigr).$$

The integer $p^{i+4}JT$ kills $\mathcal{S}_{p,r}(L)$ for $p \leq W$. All larger primes together satisfy

$$\sum_{p>W} \log|\mathcal{S}_{p,r}(L)| \leq \log T.$$

Proof. First, the dual of $\mathcal{S}_{p,r}(L)$ embeds in $K_i(\mathcal{O}_L)[p^\infty]$. Here and below the dual is the group of continuous characters into $\mathbb{Q}_p/\mathbb{Z}_p$. Indeed, Poitou–Tate duality places this dual in $H^2_{\text{ét}}(\mathcal{O}_L[1/p], \mathbb{Z}_p(r+1))$ as the kernel of localization. The archimedean terms vanish since all archimedean places are complex. The Quillen–Lichtenbaum comparison identifies this H^2 with the p-adic completion of $K_{2r}(\mathcal{O}_L[1/p])$. The other possible term in even degree is $H^0(\mathbb{Z}_p(r)) = 0$ because the cyclotomic image is open and $r > 0$. In the localization sequence the finite residue fields at p have zero K_{2r} and K_{2r-1} of order prime to p. Thus one can use $\mathcal{O}_L$, and $K_{2r}(\mathcal{O}_L)$ is finite by finite generation and Borel's rank formula. These are the comparisons used in Proposition 11.4. [1, 3, 4]

Let $\Gamma = \mathrm{GL}_n(\mathcal{O}_L)$, and let Γ_3 be the kernel of its action on $\mathcal{O}_L^n/3\mathcal{O}_L^n$. Its index J divides $|\mathrm{GL}_{dn}(\mathbf{F}_3)| \leq 3^{(dn)^2}$. The principal congruence kernel is torsion free. Indeed, an element of prime order, viewed in $\mathrm{GL}_{dn}(\mathbb{Z})$, would have the form $I + 3^a B$, $a \geq 1$, $B \not\equiv 0 \bmod 3$. Taking its p-th power gives a nonzero leading term $p3^aB$ modulo 3^{a+1} for $p \neq 3$, and $3^{a+1}B$ modulo 3^{a+2} for $p = 3$. This excludes every element of prime order, hence every element of finite order other than the identity.

Put $T = |H_i(\Gamma_3, \mathbb{Z})_{\text{tors}}|$. We track the dependence on d, n in the cell count of Lemma 11.11. Ash's well-rounded retract for the free lattice $\mathcal{O}_L^n$ is contractible and has finite cell stabilizers.

Its cells are indexed by sets of shortest vectors of normalized metrics. Corollary 5.2 of Bayer-Fluckiger, Emery and Houriet gives a finite set Φ into which an element of Γ moves all shortest vectors of any one such metric. Its bound, valid since $L \neq \mathbb{Q}$ and $n \geq 5$, is

$$|\Phi| \leq n^{3n^2d^2}\, d^{5n^3d^4}\, D_L^{9n^3d^3}.$$

In particular $\log(2+|\Phi|) \leq C(nd)^4 \log(2ndD_L)$. [5, Sec. 2 and Cor. 5.2]

For completeness, the real vector space of metrics before positivity and normalization has dimension at most $D = dn^2$. The equation that a vector has squared trace length one is affine linear there. A consistent set of these equations is implied by at most $D+1$ of its members. Thus a cell can be encoded by at most $D+1$ of its shortest vectors. Indeed, if two choices of metrics give the same encoding, the full equations from either cell hold on both metrics, so the two sets of shortest vectors coincide. Along a chain of incident cells the shortest-vector sets are nested in reverse order. Move the largest such set into Φ. This encodes an entire flag by at most $D+1$ lists, each of length at most $D+1$. Allowing a padding symbol gives at most $(2+|\Phi|)^{(D+2)^2}$ orbits of simplices in the barycentric subdivision. The quotient by Γ_3 has at most J times that many simplices and computes its group homology. Call this last upper bound H. Each column of its integral boundary in degree $i+1$ has sum of absolute values at most $i+2$, even if faces become identified. Smith normal form and Hadamard's inequality give $\log T \leq H \log(i+2)$, since homology embeds in the cokernel of this boundary map. The conductor–discriminant formula gives $D_L \leq M^d$. Substitution, using $D+2 \ll (nd)^2$, proves the displayed bound for $\log(2JT)$.

Stability in the range $n \geq 2i+1$ identifies $H_i(\Gamma,\mathbb{Z})$ with the homology of $B\,\mathrm{GL}(\mathcal{O}_L)^+$. Transfer from Γ to Γ_3, followed by inclusion, is multiplication by J. It follows that JT kills the torsion in $H_i(\Gamma,\mathbb{Z})$. By Quillen's plus construction the ordinary Hurewicz map on this space has source $K_i(\mathcal{O}_L)$. Its kernel at p is killed by p^{i+4}. To see this last assertion, the adjunction from the suspension spectrum of the basepoint component of $\Omega^\infty\mathbf{K}(\mathcal{O}_L)$ to the connective K-spectrum takes the ordinary Hurewicz image of a sphere to its stable Hurewicz image. Thus Mathew's upper bound for the kernel of the stable map applies to the ordinary kernel. His Theorem 1.3(a,b) gives exponents at most $i+4$ at all primes. This proves the annihilator assertion. [5, Sec. 3.1][6, Thm. 1.3]

Every prime divisor of J is at most 3^{dn}, since the factors of $|\,\mathrm{GL}_{dn}(\mathbf{F}_3)|$ are powers of three and factors 3^h-1, $h \leq dn$. For $p > W$ the ordinary Hurewicz map is injective on p-torsion by Arlettaz's theorem, which applies already for $p > (i+1)/2$. Transfer is injective on this primary part as well, since $p \nmid J$. The direct sum of the large-primary parts of $K_i(\mathcal{O}_L)$ therefore embeds in the single finite torsion group of order T. Apply the injection at the beginning of the proof and take logarithms. [5, Sec. 3.1] □

Lemma 19.3. *For every prime p, the minimal number $b_{p,r}$ of cyclic summands of $\mathcal{S}_{p,r}(L)$ satisfies*

$$b_{p,r} \log p \leq C d_L p \log(2Mp).$$

Proof. The group is finite by Lemma 19.2, so $b_{p,r}$ is its dimension of p-torsion. The multiplication-by-p exact sequence on $A_{p,r}$ bounds that dimension by $\dim_{\mathbf{F}_p} H^1(G_{L,S_p}, \mathbf{F}_p(-r))$. Put $K = L(\mu_p)$, $a = [K:\mathbb{Q}] \leq d_L p$. Restriction to K is injective by corestriction since $[K:L] \mid p-1$. This extension is unramified outside p. Over K the coefficient becomes isomorphic to μ_p. For $R = \mathcal{O}_K[1/p]$, Kummer theory gives an extension of $\mathrm{Cl}(R)[p]$ by $R^\times/(R^\times)^p$ as this degree-one group. The unit term has dimension at most $2a$ by the S-unit theorem. Each ideal class in K has a representative of norm at most $B = 2^a D_K^{1/2}$ by Minkowski's bound. There are at most $B^2\zeta_K(2) \leq B^2\zeta(2)^a$ integral ideals of such norm, by the Dirichlet series

and the Euler factors. Since $\mathrm{Cl}(R)$ is a quotient of $\mathrm{Cl}(\mathcal{O}_K)$ and $D_K \le (Mp)^a$, the class group contributes at most $Ca\log(2Mp)/\log p$ to the dimension. Adding the unit term proves the lemma. □

Proof of Theorem 19.1. For $p \le W$, a cyclic summand has order at most $p^{i+4}JT$. Its logarithmic order is therefore at most $(i+4)\log W + \log(2JT)$. Sum over the generator bound of Lemma 19.3, using $\log p \ge \log 2$ and $\sum_{p\le W} p \le W^2$. The sum at these primes is bounded by

$$CdW^2 \log(2MW)\big((i+4)\log W + \log(2JT)\big).$$

Add the single $\log T$ from Lemma 19.2. Since $\log W = dn\log 3$ and $n = 4r+8$, increasing an absolute constant absorbs all factors in (19.1). □

19.2 Descent in the real cyclotomic tower

Fix a primitive Dirichlet character ψ of conductor F and order o, with fixed field K_ψ cut out by $\ker\psi$. Set $0 < \varepsilon < 1/52$, $\eta = \varepsilon/128$, $C_j = \mathbb{Q}(\zeta_{2^{j+2}})^+$ for $j \ge 0$, and let l be the least integer with $2^l \ge x^{2+8\varepsilon}$. The field in the prime count and a subfield of it are

$$E_x = K_\psi C_l(\sqrt{-q}, \sqrt{-d}),$$
$$L_x = K_\psi C_s(\sqrt{-q}, \sqrt{-d}), \qquad s = \lfloor \eta \log_2 x \rfloor.$$

The auxiliary primes q, d are those of Theorem 5.1. On its range they can be held fixed with $\log(qd) \ll_{\psi,\varepsilon} x^{\varepsilon/5}(\log(2x))^2$, and satisfy $q, d \equiv 3 \bmod 4$. In particular $M_x = 2^{l+2}Fqd$ is a cyclotomic modulus for both fields. We may use the same primes on the shorter intervals below.

Lemma 19.4 (Descent of strict classes)**.** *Let E/L be a finite Galois extension of degree prime to p, with group H. Restriction identifies $\mathcal{S}_{p,r}(L)$ with $\mathcal{S}_{p,r}(E)^H$.*

Proof. Work first with the absolute Galois groups so that ramification of E/L away from p is allowed. In inflation–restriction the higher cohomology of H on $A_{p,r}^{G_E}$ vanishes. Multiplication by $|H|$ is invertible there, and averaging gives exactness of invariants. Hence restriction is an isomorphism onto invariants on global H^1. For $v \nmid p$ the twist is unramified, so a cocycle restricted to inertia is a homomorphism and a coboundary restricts to zero. If it vanishes on inertia over E, it factors through an inertia quotient of order dividing $|H|$. Such a homomorphism into a p-primary group vanishes. Thus the descended class is unramified away from p, which is precisely the condition for inflation from G_{L,S_p}. At $v \mid p$, restriction followed by corestriction is multiplication by the local degree, a p-adic unit. Vanishing after restriction implies vanishing over L_v. The two local conditions are preserved in the forward direction as well. □

Theorem 19.5 (Both signs on a growing subfield)**.** *Write $H_x = \mathrm{Gal}(E_x/L_x)$. On the common intervals of Theorem 11.12, uniformly for all sufficiently large x in the interval,*

$$\sum_{1\le r\le x^\eta} \sum_{p>2} (\log p)\,\mathrm{length}_{\mathbb{Z}_p} \mathcal{S}_{p,r}(E_x)^{H_x} \le \exp(x^{2\varepsilon/3}). \tag{19.2}$$

The inner sum is over primes. The invariants are a direct summand over $\mathbb{Z}_p$; the estimate also holds for either complex-conjugation eigenspace separately.

Proof. The extension E_x/L_x has degree a power of two. For odd p the averaging idempotent $|H_x|^{-1}\sum_{\sigma\in H_x}\sigma$ projects onto its invariants. It commutes with conjugation since $E_x/\mathbb{Q}$ is

abelian. Apply Lemma 19.4. The field L_x contains $\mathbb{Q}(\sqrt{-q})$ and has degree between 2^s and $4o2^s$. Moreover $\log(2M_x d_{L_x}(r+2)) \ll_{\psi,\varepsilon} x^{\varepsilon/4}$ on the indicated range. The exponent on the right of (19.1) is then

$$\ll_{\psi,\varepsilon} x^{20\eta+\varepsilon/4} = x^{13\varepsilon/32}.$$

Summing at most x^{η} copies of its exponential proves (19.2). In particular the bound is $o(\exp(x^{\varepsilon}/2))$, where the exponent in the latter expression is $\frac{1}{2}x^{\varepsilon}$. □

19.3 Fixed odd primes through the full range of twists

Fix an integer $a \geq 0$ and a finite set Π of odd primes. The field $B_a = K_\psi C_a$ embeds in every sufficiently high E_x. Write $H_{a,x} = \mathrm{Gal}(E_x/B_a)$, a group of order a power of two. The parameters a, Π can be prescribed before choosing an interval.

Theorem 19.6. *There are arbitrarily large V and a single pair q, d for each interval $[V, V^{3/2}]$ such that at every x there, with $t(x) = \lfloor x^{401} \rfloor$,*

$$\sum_{p\in\Pi} (\log p) \sum_{1\leq r<t(x)} \mathrm{length}_{\mathbb{Z}_p} \mathcal{S}_{p,r}(E_x)^{H_{a,x}} \leq \exp(x^{2\varepsilon/3}). \tag{19.3}$$

These same fields and intervals satisfy (19.2), the full dyadic bound of Theorem 11.12, and the odd-prime bound for the sign $(-1)^{r+1}$ in Theorem 11.1.

Lemma 19.7. *Let B be a fixed totally imaginary abelian number field and p a fixed odd prime. There is an integer $D = D(B,p) \geq 0$ such that, for every $T_0 \geq 2$, all but at most D of the integers $1 \leq r \leq T_0$ satisfy*

$$\mathrm{length}_{\mathbb{Z}_p} \mathcal{S}_{p,r}(B) \ll_{B,p} \log(2T_0).$$

Proof. Set $B_\infty = B(\mu_{p^\infty})$, $\Gamma = \mathrm{Gal}(B_\infty/B)$. Over $B(\mu_p)$ this is the cyclotomic $\mathbb{Z}_p$-extension. Its unramified abelian pro-p class module is finitely generated over $\mathbb{Z}_p$. Indeed, Iwasawa's theorem realizes it as a finitely generated torsion module over the one-variable Iwasawa algebra, and Ferrero–Washington gives $\mu = 0$ because $B(\mu_p)$ is abelian over $\mathbb{Q}$. The structure theorem then gives finite generation over $\mathbb{Z}_p$, including its finite submodule. Let X' be the quotient imposing complete splitting at the primes above p. It is also finitely generated over $\mathbb{Z}_p$. [2, 7]

To relate X' to degree one, restrict a cocycle to the kernel of the cyclotomic character in G_{B,S_p}. The action on $A_{p,r}$ becomes trivial and the restriction is a homomorphism. A strict class restricts to zero on all decomposition groups over p, so its homomorphism factors through X'. This uses only the maximal unramified quotient, since the initial Galois group already forbids ramification outside p. This description also follows by taking the maximal pro-p quotient of the kernel and killing its decomposition groups over p; the resulting extension is everywhere unramified and split over p, so it is a quotient of the unramified class module. Conjugation makes the homomorphism Γ-equivariant with scalar action κ_p^{-r} on its values.

Restriction is injective here. Write $\Gamma_1 = \Gamma \cap (1 + p\mathbb{Z}_p)$ under κ_p, choose its topological generator γ, and put $u = \kappa_p(\gamma)$. The procyclic resolution computes $H^1(\Gamma_1, A_{p,r}) = A_{p,r}/(u^{-r} - 1)A_{p,r} = 0$, since $u^{-r} - 1 \neq 0$ and the coefficient group is divisible. The index $[\Gamma : \Gamma_1]$ is prime to p, so $H^1(\Gamma, A_{p,r}) = 0$ by inflation–restriction and averaging. Thus $\mathcal{S}_{p,r}(B)$ injects into the dual of $X'/(\gamma - u^{-r})X'$. An injection suffices for the estimate.

Take a minimal generating surjection $\pi : \mathbb{Z}_p^D \to X'$ and lift the images under γ of its D generators to a matrix A satisfying $\pi A = \gamma\pi$. Reduction modulo p makes π an isomorphism on generator spaces, so A is invertible. If $D = 0$, all groups vanish. Otherwise right exactness and Smith normal form give

$$\mathrm{length}_{\mathbb{Z}_p} \mathcal{S}_{p,r}(B) \leq v_p(\det(A - u^{-r} I))$$

whenever the determinant is nonzero. All valuations are normalized by $v_p(p) = 1$. Put $e = v_p(u-1) \geq 1$, $J_0 = \lceil \log_p(T_0+1) \rceil$. The binomial formula at odd p gives

$$v_p(u^{-r} - u^{-s}) = e + v_p(r-s) \leq e + J_0 \qquad (1 \leq r \neq s \leq T_0).$$

For the equality, raising a principal unit to a power prime to p preserves the valuation of its difference from one, and taking its p-th power increases it by exactly one. If the determinant valuation exceeds $D(e+J_0)$, including when it is infinite, some eigenvalue α of A satisfies $v_p(\alpha - u^{-r}) > e + J_0$. Two distinct indices cannot satisfy this for the same eigenvalue by the displayed spacing and the ultrametric inequality. At most D indices are exceptional. The other indices satisfy the asserted bound. □

Proof of Theorem 19.6. Let $B = B_a(i)$. It is totally imaginary and abelian. Lemma 19.4 gives an injection from the strict groups of B_a into those of B at every odd prime, since their relative degree divides two. It also identifies the groups in (19.3) with those over B_a. For $p \in \Pi$, take D_p from Lemma 19.7 for B. Let $R_2(\psi)$ be the uniform bound on the number of exceptional twists at two in Theorem 11.7, and set

$$R = R_2(\psi) + \sum_{p \in \Pi} D_p, \qquad b = 401/\eta, \qquad K = 2(2b)^R.$$

These constants are fixed before the auxiliary primes. For arbitrarily large Z, choose q, d by Theorem 5.1 at the initial scale Z with upper endpoint Z^{K+1}. More explicitly, that theorem supplies fixed q, d with the character estimates throughout $[Z, Z^{K+1}]$ and $\log(qd) \ll_{\psi,\varepsilon,K} Z^{\varepsilon/5}(\log Z)^2$. Apply Lemma 19.7 with $T_0 = \lfloor Z^{401K} \rfloor$ and take the union of its exceptional sets over Π. Adjoin the exceptional set at two for the whole master interval $[Z, Z^K]$. Theorem 11.9 constructs the latter by using this same T_0 in its dyadic determinant estimate. Its cardinality is at most $R_2(\psi)$, independently of K, Z, q, d. The union has at most R elements.

Start with $U = K \log Z$ and associate to each exceptional r the point $a_r = (\log r)/401$. If any point is in $(U/(2b), U]$, discard it and replace U by $U/(2b)$. Discarded points are above the new range. After at most R divisions the band is empty. Put $V = \exp(U/2)$. Then $V \geq Z$, $V^2 \leq Z^K$. If $x \in [V, V^2]$ and an exceptional $r \leq x^{401}$, then $a_r \leq U$, so $a_r \leq U/(2b)$ and $r \leq x^\eta$. Restrict to $[V, V^{3/2}]$. The field and weight constructions in Theorem 11.9 now apply. The proof of Theorem 11.12 works with any smaller positive η than $\varepsilon/64$, since this only shortens the exceptional twist range. This gives the asserted simultaneous dyadic bound. The bounds for the critical sign and (19.2) held already before shortening.

For a nonexceptional twist the contribution from Π in (19.3) is $O_{\psi,\varepsilon,a,\Pi}(\log(2x))$, since $\log(2T_0) \ll_K \log(2x)$. The $O(R)$ exceptional twists with $r < t(x)$ satisfy $r \leq x^\eta$. For them apply (19.1) to the fixed field B and a fixed modulus for B. Its exponent is $O_{\psi,a,\varepsilon}(x^{10\eta}\log(2x))$. Consequently the entire sum is at most

$$C_{\psi,\varepsilon,a,\Pi}\, t(x) \log(2x) + R \exp\bigl(C_{\psi,\varepsilon,a} x^{10\eta} \log(2x)\bigr).$$

For sufficiently large Z this is at most $\exp(x^{2\varepsilon/3})$, as claimed. □

Corollary 19.8. *There is a sequence of disjoint intervals with $V_j \to \infty$ on which (19.3) holds with $a = j$ and Π the first j odd primes.*

Proof. At step j, fix these two parameters and use Theorem 19.6 with a lower endpoint larger than the preceding right endpoint and all thresholds for the new parameters. □

This choice by successive intervals gives no prescribed rate of growth for the number of primes in terms of V_j.

19.3.1 Stabilization over the full real cyclotomic tower

Fix an odd prime p. The fields $C_j = \mathbb{Q}(\zeta_{2^{j+2}})^+$ are the layers of the cyclotomic $\mathbb{Z}_2$-extension. We first describe exactly which degree-one classes detect the p-torsion of a strict group. This description will be independent of the positive twist.

Lemma 19.9 (Characters that are locally cyclotomic)**.** *Let L be a number field containing μ_p. Write $Y(L)$ for the space of continuous additive characters $G_L \to \mathbf{F}_p$ unramified outside p whose restriction at each $w \mid p$ factors through $\kappa_p(G_{L_w})$. For every $r \geq 1$, identify $A_{p,r}[p]$ with $\mathbf{F}_p$ using the coordinate $a/p \mapsto a \bmod p$. There is an exact sequence*

$$0 \longrightarrow \mathbf{F}_p\lambda_L \longrightarrow Y(L) \longrightarrow \mathcal{S}_{p,r}(L)[p] \longrightarrow 0, \tag{19.4}$$

where λ_L is a nonzero additive character of the global cyclotomic image of G_L, pulled back to G_L. The line it spans is independent of r. This sequence is equivariant under automorphisms over any base containing μ_p.

Proof. The finite coefficient action is trivial over L, so finite-coefficient cocycles are homomorphisms. From multiplication by p on $A = A_{p,r}$, every p-torsion cohomology class lifts to one of these homomorphisms. If its divisible-coefficient class is strict, then at every inertia group away from p it is a coboundary. The cyclotomic character is trivial there, so the homomorphism is zero there. On G_{L_w} for $w \mid p$ it has the form $g \mapsto (\kappa_p(g)^{-r} - 1)z_w$ in A. Hence it factors through the local cyclotomic image.

Conversely that image is an open subgroup of $1+p\mathbb{Z}_p$, since $L_w/\mathbb{Q}_p$ is finite and contains μ_p. For a topological generator u, multiplication by $u^{-r} - 1 \neq 0$ is surjective on A. A continuous cocycle on this procyclic group with values in A is therefore a coboundary: match its value at the generator and then use continuity and density of the integral powers. Thus every character of $Y(L)$ maps to a strict class.

The global image is likewise $1 + p^a\mathbb{Z}_p$ for some $a \geq 1$. The logarithm identifies its power $-r$ with multiplication by $-r$ on $p^a\mathbb{Z}_p$. Hence the ideal generated by all $\kappa_p(g)^{-r} - 1$ is $p^s\mathbb{Z}_p$, with $s = a + v_p(r)$. The global invariants of A are $p^{-s}\mathbb{Z}_p/\mathbb{Z}_p$. The kernel of the finite-to-divisible map is their quotient by multiplication by p, of dimension one. The connecting map sends a generator to the homomorphism $g \mapsto (\kappa_p(g)^{-r} - 1)p^{-s-1} \bmod \mathbb{Z}_p$. This factors through the global cyclotomic image and is nonzero on a generator. The space of additive characters of that image into $\mathbf{F}_p$ has dimension one, giving the stated independence. An automorphism fixing μ_p acts trivially on the finite coefficient coordinate and preserves κ_p under conjugation. These observations give equivariance. □

Theorem 19.10 (Simultaneous stabilization in every twist)**.** *Let $B/\mathbb{Q}$ be a fixed finite abelian field and $B_j = BC_j$. There is an integer $a = a(B,p)$, independent of r, such that restriction is an isomorphism*

$$\mathcal{S}_{p,r}(B_a) \longrightarrow \mathcal{S}_{p,r}(B_j) \qquad (j \geq a,\ r \geq 1).$$

The assertion concerns the full groups, including all exponents and both conjugation signs.

Proof. Suppose first that $\mu_p \subset B$. Washington's class number theorem for the cyclotomic $\mathbb{Z}_2$-extension of an abelian number field states that the p-parts of the class numbers of its layers eventually have constant order. The fields B_j give these layers after any repetitions at the bottom. Extension of ideals on p-primary ideal class groups is injective, since extension followed by norm is multiplication by the relative degree, a power of two. After a fixed layer it is therefore bijective. In particular $H = \mathrm{Gal}(B_j/B_a)$ acts trivially on the p-primary ideal class group for all $j \geq a$ once a is sufficiently large. [8]

The primes above p also stop splitting after a fixed layer. In the real cyclotomic tower over $\mathbb{Q}$, Frobenius at p has image p in $\mathbb{Z}_2^\times/\{\pm1\} \simeq \mathbb{Z}_2$. Its closed cyclic subgroup is open: $p \neq \pm1$ in $\mathbb{Z}_2$, and every nonzero closed subgroup of $\mathbb{Z}_2$ is open. Passing to the absolute Galois group of a finite local extension at p reduces this image by at most finite index. Thus the decomposition group of every prime of B over p is open in the tower over B. Enlarge a to ensure that H fixes every prime of B_j over p.

Consider the restriction map from $Y(B_j)$ to the direct sum over $w \mid p$ of the additive character spaces of $\kappa_p(G_{B_{j,w}})$. Its kernel consists of characters unramified everywhere and trivial at $w \mid p$. By the Hilbert class field theorem it is a subspace of the dual modulo p of the ideal class group. Here B_j is totally imaginary because it contains μ_p. The preceding stabilization makes the action of H on this kernel trivial. The action on the direct sum is trivial as well. Each place is fixed, and on its cyclotomic image conjugation by a lift of an element of H is trivial since κ_p is abelian. These statements concern actual Galois actions under the class field correspondence.

Since $|H|$ is a unit in $\mathbf{F}_p$, averaging over H is a projection. Its complementary projection kills the direct sum and the kernel just described. On $Y(B_j)$ its image is therefore contained in the kernel, where another application kills it. Idempotence then gives zero. By Lemma 19.9, H also acts trivially on $\mathcal{S}_{p,r}(B_j)[p]$ for all r. Apply the same complementary projection to the full strict group, now over $\mathbb{Z}_p$. A nonzero image would contain an element of order p, since the group is p-primary. The preceding conclusion excludes this. Lemma 19.4 identifies restriction with the invariant subgroup, proving the result.

For general B put $F_j = B_j(\mu_p)$. The first case gives a layer s above which $\mathrm{Gal}(F_j/F_s)$ acts trivially on every strict group. Choose $a \geq s$ with $F_s \cap \bigcup_j B_j \subset B_a$. Such an a exists since the intersection is a finite extension. For $j \geq a$, every element of $\mathrm{Gal}(B_j/B_a)$ fixes $B_j \cap F_s$, so it extends to an automorphism of $F_j = B_j F_s$ fixing F_s. This follows from the restriction isomorphism for a compositum of finite Galois fields. Restriction from B_j to F_j is injective by Lemma 19.4, because $[F_j : B_j] \mid p-1$. Equivariance of this restriction now gives triviality of $\mathrm{Gal}(B_j/B_a)$ on the strict group over B_j. Apply the lemma once more. □

Corollary 19.11 (The tower before the auxiliary quadratic extensions)**.** *For a prescribed finite set* Π *of odd primes, write* $B(x) = K_\psi C_l$ *and* $H_x^0 = \mathrm{Gal}(E_x/B(x))$*. There are arbitrarily distant common intervals of Theorem 19.6 on which*

$$\sum_{p\in\Pi} (\log p) \sum_{1\leq r<t(x)} \mathrm{length}_{\mathbb{Z}_p} \mathcal{S}_{p,r}(E_x)^{H_x^0} \leq \exp(x^{2\varepsilon/3}). \tag{19.5}$$

One may in particular include every odd prime dividing $\mathrm{ord}(\psi)$*. The bound holds throughout each interval with the same* q, d *as the dyadic and critical-sign estimates.*

Proof. Apply Theorem 19.10 to $B = K_\psi$ for each $p \in \Pi$ and take the largest of the finitely many stabilization indices. In Theorem 19.6 use this fixed layer, increased if necessary to meet any previously prescribed lower bound on a. For large x the index l exceeds it. At every twist the strict group over $B(x)$ is precisely the restriction of the one at the fixed layer. Lemma 19.4 identifies it with the invariants on the left of (19.5), since $[E_x : B(x)] = 4$. Substitution in (19.3) proves the claim. Every map commutes with complex conjugation, so both signs are included. □

Only the three summands on which at least one of the two auxiliary quadratic involutions acts by -1 can contribute at the primes in Π outside (19.5). This follows from the four averaging idempotents of $H_x^0 \simeq (\mathbb{Z}/2)^2$ at an odd prime. For a fixed pair q, d, Theorem 19.10

also applies with $B = K_\psi(\sqrt{-q}, \sqrt{-d})$. Its stabilization index can depend on that pair. As the pair varies with the interval, this last application supplies no uniform upper bound for the three remaining summands.

19.4 The conductor and the range of full strict orders

Let $0 < \varepsilon < 1/52$, fix the primitive character ψ of conductor F and order o, and let $C_j = \mathbb{Q}(\zeta_{2^{j+2}})^+$. On a selected interval let q, d_0 be the prescribed auxiliary primes. For each x put

$$L_j = K_\psi C_j(\sqrt{-q}, \sqrt{-d_0}), \qquad B_j = K_\psi C_j, \qquad E = L_J, \qquad t = \lfloor x^{401} \rfloor, \qquad b = \exp(x^\varepsilon).$$

Here J is the least index for which $[K_\psi C_J : \mathbb{Q}] \geq x^{2+8\varepsilon}$. The integral theta construction in Volume I uses this field E. The absolute logarithmic size of the two auxiliary primes can be reduced by placing the final interval farther into the range where the same two primes give the character estimates.

Lemma 19.12 (Choosing an interval with smaller auxiliary conductor)**.** *For every fixed $A \geq 1$ there are arbitrarily large Y, a single pair q, d_0 for each Y, and intervals $[V, V^{3/2}]$ with $V \geq Y^A$ on which the prime count, the uniform dyadic estimate, and the growing odd-prime estimate of Theorem 20.4 all hold. The period field and its finite-level and real estimates for the terminal periods may be taken on these intervals. Uniformly for x in them one has*

$$\log(2^{J+2} F q d_0) \ll_{\psi,\varepsilon,A} \log(2x) + x^{\varepsilon/(5A)} (\log(2x))^2. \tag{19.6}$$

Proof. Set $\eta = \varepsilon/80$, $b_1 = 401/\eta$, and let $R_2 = R_2(\psi)$ bound the number of exceptional dyadic twists in Theorem 11.7. Choose real constants

$$K_2 = 2A(2b_1)^{R_2}, \qquad W > K_2 + 2.$$

These are fixed before any field or prime is chosen. Begin the proof of Theorem 20.4 at Z, using this W. For clarity, $P_0 = \lceil \log\log Z \rceil$, $R = \lceil C_\psi P_0^5 \rceil$ and $K = W(Wb_1)^R$. By Lemma 20.3 the exceptional twists of the fields B_{a_p} for odd primes $p \leq P_0$ occupy at most R indices up to $\lceil Z^{401K} \rceil + 1$. These fields depend on ψ, p alone. The interval argument of Theorem 20.4 therefore supplies $Y \geq Z$ with $[Y, Y^W] \subset [Z, Z^K]$. Throughout that interval any of the listed exceptions below x^{401} is at most x^η.

Now choose the two auxiliary primes by Theorem 5.1 at the initial scale Y, with fixed upper power $K_2 + 1$. The twisted character estimates then hold on $[Y, Y^{K_2+1}]$ and $\log(qd_0) \ll Y^{\varepsilon/5}(\log(2Y))^2$. Use the dyadic determinant of Theorem 11.7 for all twists up to $\lfloor Y^{401K_2} \rfloor$. Its count of exceptional indices is at most R_2, independently of Y, q, d_0. Start with $U = K_2 \log Y$. If an exceptional index r has $(\log r)/401$ in $(U/(2b_1), U]$, replace U by $U/(2b_1)$. Such an index is then above every later endpoint. After at most R_2 replacements the half-open interval contains no exceptional index. Set $V = \exp(U/2)$. Then

$$V \geq \exp\left(\frac{K_2 \log Y}{2(2b_1)^{R_2}}\right) = Y^A, \qquad V^2 \leq Y^{K_2}.$$

For $x \in [V, V^2]$, each dyadic exception with $r \leq x^{401}$ satisfies $(\log r)/401 \leq U/(2b_1) \leq (\log x)/b_1$, so that $r \leq x^\eta$. All nonexceptional dyadic lengths and the fixed field for the exceptional ones are exactly those in Theorem 11.9. Its integral rounding keeps the required arguments of the prime sums in $[Y, Y^{K_2+1}]$. Its Theorem 11.2 applies since $\eta < \varepsilon/64$. The earlier odd-prime argument also applies since $[V, V^2] \subset [Y, Y^W]$. In particular its conversion of P_0 into a constant times $(\log\log x)^{1/5}$ still follows from $\log\log x \leq \log\log Z + \log K$. Constants may now depend on the fixed A.

Take $[V, V^{3/2}]$, as in the prime-count and theta constructions. It is a subinterval of the range just verified, with the same primes and the same field E at each x. The shortened cyclotomic index satisfies $J = O_\varepsilon(\log(2x))$ by minimality and $[C_j : \mathbb{Q}] = 2^j$. Since $Y \le x^{1/A}$ the conductor estimate follows. □

For an odd prime p write $S_{p,r} = \mathcal{S}_{p,r}(E)$. If $L \subset E$ with $[E : L]$ a power of two, write $e_L = [E : L]^{-1} \sum_{g \in \mathrm{Gal}(E/L)} g$. Its image on $S_{p,r}$ is exactly $\mathcal{S}_{p,r}(L)$ by restriction. Indeed averaging gives the isomorphism on global degree-one cohomology. Corestriction makes restriction injective locally at p, and at other finite primes a homomorphism on inertia vanishing upstairs factors through a group of two-power order. This proves descent with all strict local conditions and at every primary exponent.

Theorem 19.13 (A bound with a separate field degree for each twist)**.** *Fix $0 < \delta < 1$. For each of the following alternatives, use the indicated rule for $j(r)$ and set $e(r) = e_{L_{j(r)}}$. Choose the largest $0 \le j \le J$ satisfying the rule. When there is no such j, set $e(r) = 0$.*

$$\begin{aligned} &[2^j(r+2)]^5 \le x^{(1-\delta)\varepsilon}, && \text{using the published lattice bound,} \\ &2^j(r+2)^2 \le x^{(1-\delta)\varepsilon}, && \text{using the cell count of de la Torre Durán.} \end{aligned} \tag{19.7}$$

There are arbitrarily distant common intervals on which each alternative satisfies

$$\sum_{1 \le r < t} \sum_{p \text{ odd prime}} \log |e(r) S_{p,r}| \le \exp\bigl(C_{\psi,\varepsilon,\delta} x^{(1-\delta/2)\varepsilon}\bigr). \tag{19.8}$$

In particular the sum is $o(b^a)$ for every fixed $a > 0$. Both signs of complex conjugation and the full orders at all odd primes are included.

Proof. Choose A so that $1/(5A) < \delta/2$, then select the intervals of Lemma 19.12. Each L_j is totally imaginary, contains $\sqrt{-q}$, and has degree $d_j \le 4o\,2^j$. Its cyclotomic modulus divides $M = 2^{J+2} F q d_0$. Since $r < t$ and $d_j \le [E : \mathbb{Q}]$ are polynomially bounded in x, equation (19.6) gives

$$\log(2M d_j(r+2)) \ll_{\psi,\varepsilon,\delta} x^{\delta\varepsilon/2}.$$

The strict inequality in the choice of A absorbs the logarithmic factors. For one admitted twist apply Theorem 20.2 to L_j with this modulus. Its first bound uses $[d_j(r+2)]^5$ and its second uses $d_j(r+2)^2$ as the multiplier of this logarithm in the exponent. The respective hypotheses of (19.7) bound either multiplier by a constant times $x^{(1-\delta)\varepsilon}$. Thus the sum at this twist, over all primes, is at most the exponential in (19.8) with a fixed constant. Descent to the actual invariant group and summation over the at most x^{401} twists prove the claim after increasing the constant. The two cell estimates are those established in Section 20.1 from the published bound of Bayer-Fluckiger, Emery and Houriet and from the preprint of de la Torre Durán, respectively. [5, 9] □

Corollary 19.14 (Vanishing above the large coefficient cutoff)**.** *Let $P = \exp(x^\varepsilon/12)$. There is a positive constant c depending on ψ, ε such that, on every sufficiently distant admissible interval, for all odd primes $p > P$, all $0 \le j \le J$ and all $1 \le r < t$,*

$$2^j(r+2) \le c\left(\frac{\log x}{\log\log x}\right)^{1/5} \quad \Longrightarrow \quad e_{B_j} S_{p,r} = 0.$$

Using the second cell bound, the same conclusion follows from $2^j(r+2)^2 \le c(\log x)/(\log\log x)$.

Proof. Restriction first identifies $e_{B_j}S_{p,r}$ with $\mathcal{S}_{p,r}(B_j)$ since $[E : B_j]$ is a power of two. Restriction from there to $D_j = B_j(i)$ is injective by the same prime-to-p argument. The latter is a totally imaginary field of degree at most $2o\,2^j$ and has a modulus at most $2^{j+2}F$. These bounds involve neither auxiliary quadratic prime. Under either displayed size condition with $c \le 1$, $\log(2\operatorname{cond}(D_j)[D_j : \mathbb{Q}](r+2)) \le C_\psi \log\log x$ eventually. In the first case the exponent in (20.1) is at most $C_\psi c^5 \log x$. In the second case the exponent in (20.2) is at most $C_\psi c \log x$. Take c small enough that both are at most $(\varepsilon/2)\log x$. The sum of logarithmic orders over all primes for D_j is then at most $x^{\varepsilon/2}$. One nonzero p-primary summand would already contribute at least $\log p > x^\varepsilon/12$, which exceeds the entire bound for sufficiently large x. This proves the asserted vanishing on E. □

19.5 Polynomial conductor on the common interval

Theorem 19.15 (The same period fields with a polynomial conductor)**.** *Fix ψ, ε as in Lemma 19.12. There are arbitrarily distant intervals $[V, V^{3/2}]$, each with one pair of auxiliary primes q, d_0, on which one may use*

$$E_x = K_\psi C_J(\sqrt{-q}, \sqrt{-d_0}), \qquad N_x = 2^{J+2}Fqd_0, \qquad x^{2+8\varepsilon} \le [K_\psi C_J : \mathbb{Q}] < 2x^{2+8\varepsilon}$$

at every x, with the same minimal index J as above. There is a fixed $D = D(\psi, \varepsilon)$ for which $N_x \le x^D$ everywhere on the interval. The prime-sum bounds for the auxiliary characters, the dyadic strict-order bound and the growing odd-prime estimate of Theorem 20.4 on the fields B_J hold there. The integral weights and terminal-period data can be chosen on these same E_x.

There is also a choice retaining both original prime-size conditions at the initial scale of Theorem 5.1 in Volume I. For this choice the conclusions hold with $\log N_x \ll_{\psi,\varepsilon} \log(2x)(1 + \log\log(3x))^2$.

Proof. Put $\eta = \varepsilon/80$, $b_1 = 401/\eta$, and let $R_2 = R_2(\psi)$ be the bound from Theorem 11.7. Fix $K_0 = 2(2b_1)^{R_2}$ and $W > K_0 + 2$. Carry out the first, odd-prime selection in Lemma 19.12 with this W. At arbitrarily large H it gives a range $[H, H^W]$ on which each of the finitely many listed odd-prime exceptions below x^{401} is at most x^η. The count in Lemma 20.3 is uniform in the cutoff for the twists. The fields on which these lists are made are the $K_\psi C_{a_p}$, independent of both auxiliary primes. This explains the order of selection.

Let c, C be the constants of Theorem 5.6. Set $z = 2W\log H/c$ and $Y = z^{5/\varepsilon}$. Then $Y < H$ for large H and $e^{cz} = H^{2W}$. Use that theorem at Y, first with $U_2 = e^{Cz}$. It supplies a single pair with

$$\log(qd_0) \le (1 + C)z \ll_{\psi,\varepsilon} \log H.$$

Both auxiliary characters and their products with every permitted base character have the required estimates throughout $[H, H^W + 1]$. The congruences at two distinguish the two quadratic layers as in Theorem 11.7. In particular the number of dyadic exceptional indices is at most R_2 through $\lfloor H^{401K_0} \rfloor$ for this fixed pair. The ramified primes are distinct, avoid $2F$, and exceed H^{401W}, since $\log q > W\log H/c$ and $1/c > 401$. Every fixed odd prime needed to split in $\mathbb{Q}(\sqrt{-d_0})$ is eventually covered by $d_0 \equiv -1 \bmod p$.

For clarity, start with $U = K_0 \log H$. If $(U/(2b_1), U]$ contains $(\log r)/401$ for a dyadic exception, divide U by $2b_1$ and repeat. Each division puts a different exceptional index above the new upper endpoint. After at most R_2 divisions the range is empty of such indices. Set $V = e^{U/2}$. Then $H \le V$, $V^2 \le H^{K_0}$, and at every $V \le x \le V^2$ a dyadic exception with $r \le x^{401}$ has $r \le x^\eta$. Theorem 20.4 therefore gives its growing odd-prime estimate by exactly its bounds for the large and small twists, and the dyadic descent and bounded-degree estimate

of Theorems 11.9 and 11.12 bound the full dyadic sum. Their conductor input is an upper bound for $\log(2Fqd_0)$, which here is $O_{\psi,\varepsilon}(\log H)$.

Restrict to $[V, V^{3/2}]$. The rounded weight arguments $\lceil bx\rceil/b$, $b = \exp(x^{\varepsilon})$, belong to $[H, H^W + 1]$. The field construction and character average in Proposition 6.4, use the distinct quadratic ramification and these auxiliary character estimates. Restriction to the minimal layer J uses the descent through a two-power extension in Proposition 9.9. Since $[C_j : \mathbb{Q}] = 2^j$ and successive degrees $[K_\psi C_j : \mathbb{Q}]$ grow by at most two, minimality gives the displayed degree range and $2^{J+2} \ll_\psi x^{2+8\varepsilon}$. This proves the polynomial bound for the actual modulus. The ray-class estimate of Lemma 7.10 is uniform in the quadratic discriminant and modulus. For the split level primes and the common terminal prime its uses in Theorem 9.13 require the bound $\log(2N_x) = o(\log b)$, which follows here. The weights, ranks and tests in that construction are therefore available without a further change of field or interval.

Finally repeat the same selection using $U_2 = \exp(z(\log Y)^2)$. The initial prime-size and congruence conditions are now exactly those of Theorem 5.1 in Volume I. Here $\log Y = (5/\varepsilon)\log z$ and $z \asymp \log H$. This gives the second conductor estimate, and it still supplies all the conductor bounds just used. Both constructions concern the primes and intervals obtained by the stated selections. □

19.6 All odd primes on a growing part of the same tower

Fix the primitive character ψ of order o, its conductor F, and the parameter ε of Section 6.6. Throughout a selected interval write q, d_0 for the actual two auxiliary primes. We use d_0 here to distinguish this prime from a field degree. Put $C_j = \mathbb{Q}(\zeta_{2^{j+2}})^+$, and recall that l is least with $2^l \ge x^{2+8\varepsilon}$. For fixed $0 < u, v < 1$ set

$$E_x = K_\psi C_l(\sqrt{-q}, \sqrt{-d_0}), \qquad s = \lfloor u\varepsilon \log_2 x\rfloor,$$
$$L_{u,x} = K_\psi C_s(\sqrt{-q}, \sqrt{-d_0}), \qquad H_{u,x} = \mathrm{Gal}(E_x/L_{u,x}).$$

The sum in the next theorem is formed from the very strict groups on the left side of (L). We write logarithmic orders, so each cyclic summand of order p^a contributes $a \log p$. Define

$$B_{u,v}(x) = \sum_{1\le r\le x^{v\varepsilon}} \sum_{p \text{ odd prime}} \log\bigl|\mathcal{S}_{p,r}(E_x)^{H_{u,x}}\bigr|.$$

As elsewhere on these intervals, constants denoted by $C_{\psi,\varepsilon}$ may depend on additional parameters fixed before the choice of the two auxiliary primes.

Theorem 19.16 (Uniform bounds through the full primary exponents)**.** *On the common intervals of Section 6.6,*

$$B_{u,v}(x) = o\bigl(\exp(x^{\varepsilon}/2)\bigr) \quad \textit{if} \quad 5(u+v) + \tfrac{1}{5} < 1.$$

Using the cell-orbit bound of de la Torre Durán in Theorem 20.2 gives the same conclusion whenever $u + 2v + \frac{1}{5} < 1$. In particular the respective estimates at equal exponents are

$$B_{1/16,1/16}(x) \le \exp(C_{\psi,\varepsilon} x^{5\varepsilon/6}), \tag{19.9}$$
$$B_{1/4,1/4}(x) \le \exp(C_{\psi,\varepsilon} x^{23\varepsilon/24}). \tag{19.10}$$

Both eigenspaces of complex conjugation are included at each prime. Each assertion holds uniformly as the left endpoints of the intervals tend to infinity.

Proof. The index $[E_x : L_{u,x}]$ is a power of two, since adjoining C_l completes the extension. For odd p, restriction identifies $\mathcal{S}_{p,r}(L_{u,x})$ with $\mathcal{S}_{p,r}(E_x)^{H_{u,x}}$. For the global degree-one group this is inflation–restriction, since higher cohomology of the finite group $H_{u,x}$ on a p-primary group vanishes. At a place above p, corestriction composed with restriction is multiplication by a local degree prime to p, so local triviality descends. Away from p the twist is unramified. An inertia homomorphism that becomes zero upstairs factors through a group of order prime to p, so it vanishes. This also proves descent at places that ramify in the field extension. The invariant group is a direct summand under the averaging idempotent, which commutes with complex conjugation.

Write $d_L = [L_{u,x} : \mathbb{Q}]$. Since $[C_s : \mathbb{Q}] = 2^s$,

$$2^s \le d_L \le 4o\,2^s \le 4o\,x^{u\varepsilon}.$$

The field contains $\sqrt{-q}$, is totally imaginary, and is contained in $\mathbb{Q}(\zeta_N)$ for $N = 2^{l+2}Fqd_0$. The common interval construction in Sections 7.1 and 11.3 has $\log(qd_0) \ll_{\psi,\varepsilon} Z^{\varepsilon/5}(\log(2Z))^2$ at its initial scale $Z \le x$. Any fixed extra parameters in that construction are held fixed here. Since $l = O_\varepsilon(\log(2x))$, for $1 \le r \le x^{v\varepsilon}$ this gives

$$\log(2Nd_L(r+2)) \ll_{\psi,\varepsilon} x^{\varepsilon/5}(\log(2x))^2 \ll_{\psi,\varepsilon} x^{5\varepsilon/24}.$$

No auxiliary prime or interval has been reselected.

Use first the published lattice bound in Theorem 20.2. At one twist the logarithmic order summed over all primes is at most $\exp(C[d_L(r+2)]^5 \log(2Nd_L(r+2)))$. Inserting the preceding estimates and summing at most $x^{v\varepsilon}$ such terms gives

$$B_{u,v}(x) \le x^{v\varepsilon} \exp\bigl(Cx^{[5(u+v)+1/5]\varepsilon}(\log(2x))^2\bigr).$$

If $5(u+v)+1/5 < 1$, the logarithm of this upper bound is $o(x^\varepsilon)$, proving the first assertion. With $u = v = 1/16$, using $5\varepsilon/24$ for the logarithmic factor yields $5(1/16+1/16)+5/24 = 5/6$. Absorbing $x^{v\varepsilon}$ gives (19.9).

For the second assertion use the other bound in that same theorem. Its exponent is $Cd_L(r+2)^2\log(2Nd_L(r+2))$. This replaces $5(u+v)$ by $u+2v$ in the preceding argument. At $u = v = 1/4$ the exponent with $5/24$ is $3/4+5/24 = 23/24$. This proves (19.10) with all odd primes included. In each calculation all constants are independent of q, d_0, x once the interval construction and the indicated parameters are fixed. □

Corollary 19.17 (The contribution outside the bounded summands)**.** *Choose either range of Theorem 19.16, with its stated hypotheses. Write $t = \lfloor x^{401} \rfloor$. On $S = \mathcal{S}_{p,r}(E_x)$ for odd p put*

$$e_r = \frac{1+(-1)^r c}{2}, \qquad \pi_{p,r} = \begin{cases} |H_{u,x}|^{-1} \displaystyle\sum_{\sigma \in H_{u,x}} \sigma, & r \le x^{v\varepsilon}, \\ 0, & r > x^{v\varepsilon}, \end{cases}$$

where c is complex conjugation. Then

$$\mathcal{L}(x) - \sum_{1 \le r < t} \sum_{p \text{ odd prime}} \log\bigl|(1-\pi_{p,r})e_r\mathcal{S}_{p,r}(E_x)\bigr| = o\bigl(\exp(x^\varepsilon/2)\bigr). \tag{19.11}$$

One may also omit from the sum the character components certified by Theorem 20.5 at $p \nmid N[E_x : \mathbb{Q}]$.

Proof. For odd p the commuting idempotents give the direct sum

$$S = (1 - e_r)S \ \oplus \ \pi_{p,r} e_r S \ \oplus \ (1 - \pi_{p,r}) e_r S.$$

The sum of the logarithmic orders of the first terms is bounded by the polynomial critical-sign estimate in Theorem 11.1. The middle terms together contribute at most $B_{u,v}(x)$. The dyadic groups in $\mathcal{L}(x)$ contribute $o(\exp(x^{\varepsilon}/2))$ on these same intervals by Theorem 11.17 and its proof. This gives (19.11). At a prime of the stated kind we may extend scalars to the unramified character ring of Theorem 20.5. Its character projections commute with $\pi_{p,r}$ and e_r. Projecting a certified component again only decreases its length. Thus the total cost of omitting these components, with lengths normalized as in that theorem, is polynomial in x. This proves the final assertion. □

For $r > x^{v\varepsilon}$ the last sum still contains the whole complementary eigenspace, before the possible character omissions. For smaller r it still contains the part that does not descend to $L_{u,x}$. The full field contains C_l of degree $2^l \geq x^{2+8\varepsilon}$, whereas $[C_s : \mathbb{Q}] \leq x^{u\varepsilon}$. A uniform bound for those remaining orders is open. The height estimate for the arithmetically normalized theta-period map in Corollary 87.3 is also open on these fields.

19.7 Bounds for deep torsion on the period field

Let $E = \widetilde{E} = K_{\psi} C_{l'}(\sqrt{-q}, \sqrt{-d_0})$ be the field carrying the periods in Proposition 9.9. Throughout this paragraph $x \in [V, V^{3/2}]$, with the same V, q, d_0 as in that proposition. Write $b = \exp(x^{\varepsilon})$, $P = b^{1/12}$, $t = \lfloor x^{401} \rfloor$, $n = [E : \mathbb{Q}]$, and take N from the common construction, so

$$E \subset \mathbb{Q}(\zeta_N), \qquad n \ll_{\psi} x^{2+8\varepsilon}, \qquad \log(2N) \ll_{\psi,\varepsilon} x^{\varepsilon/4}.$$

We use the original small-ε range $0 < \varepsilon < 1/52$. For an odd prime p, write $S_{p,r} = \mathcal{S}_{p,r}(E)$. Its elements are global classes with coefficients $(\mathbb{Q}_p/\mathbb{Z}_p)(-r)$, unramified away from p and locally zero at every prime above p. Put

$$D_{p,r} = \frac{p-1}{\gcd(p-1, r)}, \qquad M_{p,r} = \tfrac{1}{2}(1 + (-1)^r c) S_{p,r}.$$

Lemma 19.18 (Two bounds for the subgroup killed by p)**.** *For every odd prime p and every $r \geq 1$,*

$$\log |S_{p,r}[p]| \ll n D_{p,r} \log(2Np). \tag{19.12}$$

For $p > P$, all sufficiently large x, and the full range of twists used by the periods, one also has

$$\sum_{1 \leq r < t} \log |M_{p,r}[p]| \ll np \log(2Np). \tag{19.13}$$

The constants in these two inequalities are absolute.

Proof. Let F/E be the field cut out by $\bar{\kappa}_p^{-r}$. Then $F \subset E(\mu_p)$ and $[F : E] \leq D_{p,r}$ since the r-th powers in $\mathbf{F}_p^{\times}$ form a group of that order. The estimate at $j = 1$ in Theorem 11.22 gives

$$\log |S_{p,r}[p]| \leq \log h(F) + [F : \mathbb{Q}] \log p.$$

Here $h(F)$ is the ordinary class number. For any subfield H of $\mathbb{Q}(\zeta_{Np})$ of degree m, the conductor–discriminant formula gives $|\operatorname{disc} H| \leq (Np)^m$. Each ideal class has an integral representative of norm at most $Y = 2^m |\operatorname{disc} H|^{1/2}$ by Minkowski's theorem. The number of integral ideals of norm at most Y is bounded by $Y^2 \zeta_H(2) \leq Y^2 \zeta(2)^m$, by comparison of Euler factors. Thus $\log h(H) \ll m \log(2Np)$, which proves (19.12).

For $p > P$ one has $p > t+1$ and $p \nmid nN$ for all sufficiently large x, by the displayed bounds on n, N. Let $T = (E\mathbb{Q}(\mu_p))^+$. The groups in (19.13) use distinct eigenspaces in its ideal class group modulo p. We recall the argument. Work over an unramified coefficient ring containing the values of the characters α of $\mathrm{Gal}(E/\mathbb{Q})$. Descent by the character idempotent, as in Theorem 24.1 and Corollary 24.17, gives the strict character over $\mathbb{Q}$ with residual action $\alpha^{-1}\bar{\kappa}_p^{-r}$. The descent uses averaging over the prime-to-p group, on global cohomology and on each local restriction. In the complementary summand $\alpha(c) = (-1)^r$, so this character factors through $\mathrm{Gal}(T/\mathbb{Q})$. It is nontrivial on inertia at p since $0 < r < p-1$ and $p \nmid N$. Finite and divisible coefficients therefore give the same zero local condition at p for a class killed by p. Over T it gives an unramified homomorphism, hence one from the class group. Restriction is injective since $[T : \mathbb{Q}]$ is prime to p.

The cyclotomic factors of conductors N, p are disjoint. On their product the second factor determines r in this range and the first determines α. Thus the pairs (r, α) use pairwise distinct idempotents. Sum their dimensions over the residue field. Extension of the coefficient field preserves dimension, so after multiplication by $\log p$ the sum is at most $\log h(T)$. Applying the preceding class-number estimate with $[T : \mathbb{Q}] \le np$ proves (19.13). □

Define two depths, with $\lfloor y \rfloor = 0$ for $0 \le y < 1$, by

$$u_{p,r} = \left\lfloor \frac{x^{-420} b^{1/2}}{p D_{p,r}} \right\rfloor, \qquad j_p = \begin{cases} \left\lfloor x^{-4} b^{1/2} / p^2 \right\rfloor, & p > P, \\ 0, & p \le P. \end{cases} \qquad k_{p,r} = \max(u_{p,r}, j_p).$$

We use $M[p^0] = 0$.

Theorem 19.19 (Growing depths at all the twists of the period field)**.** *Uniformly on the selected intervals,*

$$\sum_{1 \le r < t} \sum_{p \text{ odd prime}} \log |M_{p,r}[p^{k_{p,r}}]| \ll_{\psi,\varepsilon} x^{-1} b^{1/2}. \tag{19.14}$$

For all $p \le P$, every $k_{p,r}$ is at least $\lfloor x^{-420} b^{1/3} \rfloor$. For $P < p \le b^{1/5}$ it is at least $\lfloor x^{-4} b^{1/10} \rfloor$. The whole first layer at every $P < p \le x^{-2} b^{1/4}$ is included.

Proof. If A is a finite abelian p-group with elementary divisors p^{d_i}, then for every integer $j \ge 0$

$$\log |A[p^j]| = (\log p) \sum_i \min(j, d_i) \le j \log |A[p]|.$$

This permits estimates at growing j on the field of the first layer. For a maximum of two depths we can bound the logarithmic order by the sum of their two bounds.

Set $U = x^{-420} b^{1/2}$. The inequality $u_{p,r} \ge 1$ implies $p(p-1) \le U \gcd(p-1, r) \le Ut$. Thus $p \le Z = 1 + \sqrt{Ut}$ whenever this depth contributes. Using $M_{p,r}[p] \subset S_{p,r}[p]$ and (19.12), the sum for the depths $u_{p,r}$ is at most

$$CtnU \log(2NZ) \sum_{p \le Z} \frac{1}{p} \;\le\; CtnU \log(2NZ)(1 + \log Z).$$

Here $\log(2NZ)$ and $1 + \log Z$ are both $O_{\psi,\varepsilon}(x)$, and $n \ll_\psi x^3$. This bound is $O_{\psi,\varepsilon}(x^{-14} b^{1/2})$.

Put $U' = x^{-4} b^{1/2}$. For the depths j_p sum first over r using (19.13). We obtain

$$CnU' \sum_{P < p \le \sqrt{U'}} \frac{\log(2Np)}{p} \ll_{\psi,\varepsilon} nU' x^{2\varepsilon} \ll_{\psi,\varepsilon} x^{-2+10\varepsilon} b^{1/2}.$$

Indeed $\log(2Np) \ll_{\psi,\varepsilon} x^{\varepsilon}$ in this range, and the harmonic sum over all integers up to $\sqrt{U'}$ is $O(x^{\varepsilon})$. Since $10\varepsilon < 1$, this proves (19.14). For $p \le P$ use $D_{p,r} \le p$ and $P^2 = b^{1/6}$. The two assertions above P follow from $p^2 \le b^{2/5}$ and $p^2 \le x^{-4} b^{1/2}$, respectively. □

Corollary 19.20 (The order still required on the same interval)**.** *Use the averaging projector $\pi_{p,r}$ of Proposition 9.9 on E, in either range allowed there and with its corresponding hypotheses. Put $Q_{p,r} = (1 - \pi_{p,r})M_{p,r}$, and let $\mathcal{L}_E(x)$ denote the left side of* (L) *on E. Then*

$$\mathcal{L}_E(x) = \sum_{1 \le r < t} \sum_{p \text{ odd prime}} \log |p^{k_{p,r}} Q_{p,r}| + o(b^{1/2}). \tag{19.15}$$

Each pair for which the finite orders of $S_{p,r}[p^{k_{p,r}}]$ and $S_{p,r}[p^{k_{p,r}+1}]$ agree contributes zero to this sum. Both orders are given by Corollary 11.23.

Proof. Proposition 9.9 gives (19.11) on E with these projectors. For each $Q = Q_{p,r}$ and $k = k_{p,r}$, multiplication by p^k gives $\log |Q| - \log |p^k Q| = \log |Q[p^k]|$. Its right side is nonnegative and at most $\log |M_{p,r}[p^k]|$. Substitution of Theorem 19.19 into (19.11) proves (19.15), with the stated uniform error. Equal finite orders at the indicated consecutive depths force $p^{k_{p,r}} S_{p,r} = 0$ by the cyclic decomposition, including when $k_{p,r} = 0$. This also kills $Q_{p,r}$. □

For comparison, Proposition 6.11 removes depth $\lfloor b^{1/8} \rfloor$ at $p \le P$, and Proposition 7.7 removes at most four layers above P. Theorem 19.19 controls growing depths on both sides of P, on the field used by the period itself. For any fixed $\delta > 0$, a bound by $(1 - \delta)b^{1/2}$ for the sum in (19.15) on arbitrarily distant common intervals would give (L). The sizes of the terms surviving these depths and a nonzero integral comparison on the projected theta image are still required.

19.8 Strict cohomology on the fields of the norm theorem

Let $E = K_\psi C_J(\sqrt{-q}, \sqrt{-d_0})$ be the field of Theorem 87.10, with $J = l'$, $t = \lfloor x^{401} \rfloor$ and $A = \mathrm{Gal}(E/C_J)$. We give a full-depth estimate for a collection of summands in the strict cohomology sum (L). At $p \equiv 3 \bmod 8$, $p > 3$, put $\lambda(v) = (v/p)$ and take the twists

$$r + 1 \equiv (p - 1)/2 \pmod{p - 1}.$$

They are even, so the A-invariant classes on this real cyclotomic subfield have the complementary sign in (19.15).

Fix a nontrivial character α of C_J with primitive conductor f_0, and fix an embedding of its values in an unramified coefficient ring O over $\mathbb{Z}_p$. Choose a positive $a_0 \equiv 1 \bmod p$ prime to f_0 with $\alpha(a_0) \ne 1$. This choice may be kept for the entire Frobenius orbit of α. For any p-adic unit v write $\omega(v)$ for its Teichmüller lift and $\langle v \rangle = v/\omega(v)$. For integers $s \ge 0$ put

$$A_m(s) = \sum_{\substack{1 \le v \le f_0 p^m \\ (v, f_0 p) = 1}} \left\lfloor \frac{a_0 v}{f_0 p^m} \right\rfloor \bar{\alpha}(v) \lambda(v) \langle v \rangle^{-s} \pmod{p^m O}. \tag{19.16}$$

When $s = r + 1$ in the indicated congruence this is exactly the annihilator for the p^m-torsion in the strict component, by the floor-sum test in Sections 24.3 and 25.3.

Lemma 19.21 (Finite differences of the annihilator)**.** *The residues in* (19.16) *define $A(s) \in O$. Put $\bar{q}(v) = (\langle v \rangle - 1)/p \bmod p$ and let M be the sum at modulus $f_0 p^2$ with weight $\bar{\alpha}(v)\lambda(v)\bar{q}(v)$ in the residue field. For distinct nonnegative integers s, s' one has*

$$\frac{A(s') - A(s)}{p(s' - s)} \in O, \qquad \frac{A(s') - A(s)}{p(s' - s)} \equiv -M \pmod{pO}.$$

At $s = 0$ the value is $(a_0 - \alpha(a_0)\lambda(a_0))B_\alpha$, where B_α is the algebraic integer of Lemma 25.6.

Proof. Let $n = f_0 p^i$ and pass from n to kn with k a power of p. Above a unit $v \bmod n$ the representatives are $v + bn,\ 0 \le b < k$. The sum of their floor coefficients is

$$\lfloor a_0 v/n \rfloor + (a_0 - 1)(k-1)/2.$$

Indeed the residues of $a_0 b \bmod k$ run through a complete system, and summing the integer parts followed by the fractional parts gives the displayed identity. The extra constant has zero sum against the reduced weights, which are odd under $v \mapsto -v$ since λ is odd and $\langle -v \rangle = \langle v \rangle$. This proves compatibility modulo p^i. At $s = 0$ the weight comes from modulus $f_0 p$ itself. The same calculation gives exact equality of the weighted floor sums at every modulus. The permutation by a_0 at the first modulus gives the stated value, as in equation 24.19 with the identity for floors proved there.

Let $d = v_p(s' - s)$. At modulus $f_0 p^{d+2}$, for each unit v the binomial expansion or the p-adic logarithm gives

$$\langle v \rangle^{-s'} - \langle v \rangle^{-s} \equiv -p(s' - s)\bar{q}(v) \pmod{p^{d+2}}.$$

For instance $\log\langle v \rangle / p \equiv \bar{q}(v) \bmod p$, and exponentiating $-(s' - s)\log\langle v \rangle$ preserves its linear term at this precision since p is odd. Also $\langle v \rangle^{-s} \equiv 1 \bmod p$. After summing and division by $p(s' - s)$, the remaining weights factor modulo $f_0 p^2$ and are still odd under negation. The floor identity therefore reduces their sum to M. This proves both claims about the finite difference. □

Theorem 19.22 (At most one exceptional twist per conductor)**.** *For every sufficiently large x on the common intervals and every prime*

$$x^4 < p \le 2t + 1, \qquad p \equiv 3 \bmod 8,$$

all but at most $J - 2$ of the twists in the stated congruence with $1 \le r < t$ satisfy

$$p^{101} \mathcal{S}_{p,r}(E)^A = 0. \tag{19.17}$$

More precisely, at each conductor 2^{j+2}, $3 \le j \le J$, and for every $m \ge 1$, at most one class of $r + 1 \bmod p^m$ can escape the exponent bound p^m for its character components. This class, when present, is nonzero modulo p. The conditions can be tested by (19.16) with precision p^{m+1}.

Proof. The bound on the period degree in Proposition 9.9 gives $2^{J+2} \le x^3$ for all sufficiently large x. Throughout the prime range $2^{J+2}(2 + \log(2^{J+2}p))^2 < p$, since $\log p \ll \log x$. Also $p > |A|$ since $|A| \le 4[K_\psi : \mathbb{Q}]$. Prime-to-$p$ descent with the local conditions identifies $\mathcal{S}_{p,r}(E)^A$ with $\mathcal{S}_{p,r}(C_J)$.

The first four labels vanish by Theorem 24.25. At a conductor 2^{j+2} with $j \ge 3$ there are just two Frobenius orbits of primitive labels. By Lemma 25.6 and the proof of Corollary 25.8, the sum of the two valuations of B_α is strictly less than two. They are nonnegative integers. Thus there can be only one orbit where the valuation is nonzero, and there it is one. The factor multiplying B_α in Lemma 19.21 is a unit. The finite differences show $A(s) \equiv A(0) \bmod pO$ for every s. A unit at zero therefore kills its strict component for every relevant twist by the test at $m = 1$.

For the possible other orbit $v_p(A(0)) = 1$. If $M = 0$, the lemma gives $A(s) \equiv A(0) \bmod p^2 O$ for all s, and p kills every component in that orbit. If $M \neq 0$, the same lemma gives exactly

$$v_p(A(s') - A(s)) = 1 + v_p(s' - s).$$

If two values of A are both zero modulo p^{m+1}, their arguments must thus coincide modulo p^m. Conversely that congruence of arguments preserves the residue of A modulo p^{m+1}. No such

argument is zero modulo p, as that would give $A(s) \equiv A(0) \bmod p^2 O$. The Frobenius-conjugate labels in the orbit give conjugate annihilators at each integer, with the same valuation. If $A(s) \neq 0 \bmod p^{m+1}$ for $s = r+1$, the test at precision p^{m+1} kills the entire strict component by p^m. Indeed its valuation is at most m, and an element of larger order would yield one of order p^{m+1}. This proves the assertion about classes at every conductor.

Finally $p^{101} > x^{404} > t$. At each of the $J-2$ conductors the possible exceptional residue at $m = 101$ can contain at most one integer $r+1$ in the required range. All of the other twists satisfy the bound at every character. The character idempotents are integral after unramified coefficient extension since p is odd. Faithful scalar extension gives (19.17) for the entire invariant group. □

Corollary 19.23 (The logarithmic order on the common interval)**.** *Sum the full logarithmic orders of $\mathcal{S}_{p,r}(E)^A$ over the primes and quadratic residual twists covered by (19.17), omitting the possible exceptional twists. Uniformly on the same intervals used for the period construction the sum is*

$$\ll [E:\mathbb{Q}]\, t^2 \log(2Nt) = o\big(\exp(x^{\varepsilon}/2)\big).$$

At every included pair this invariant group is killed by the depth $p^{k_{p,r}}$ of Theorem 19.19.

Proof. By cyclic decomposition, (19.17) bounds each logarithmic order by $101 \log|\mathcal{S}_{p,r}(E)[p]|$. Lemma 19.18 bounds this by $C[E:\mathbb{Q}]p\log(2Np)$. For each prime the number of twists is at most $1 + t/(p-1)$. Summing over the integers from two to $2t+1$ bounds $\sum_p p(1+t/(p-1))$ by $O(t^2)$. The degree, t and $\log(2Nt)$ are all polynomially bounded in x, proving the little-oh estimate for fixed $\varepsilon > 0$. All those coefficient primes satisfy $p \le 2t+1 \le P = \exp(x^{\varepsilon}/12)$ eventually. The lower bound for $k_{p,r}$ in Theorem 19.19 consequently exceeds 101. □

These groups lie on the field carrying the automorphic periods. The estimate leaves the possible exceptional twists, the components nontrivial on A, and other ranges of primes and twists in the full cohomological sum. The norm identity of Theorem 87.10 on these fields still requires control of the omitted real tail and an integral normalization for the prescribed theta periods.

19.9 Strict cohomology in cyclic extensions of prime power degree

Let $B/\mathbb{Q}$ be cyclic of degree p^a, for an odd prime p, with conductor b prime to p. Fix a primitive character χ of order prime to p and conductor f prime to pb. Put $O = \mathbb{Z}_p[\chi]$, $J = \operatorname{Frac} O$. Take $r \ge 1$ with $\chi(-1) = (-1)^r$, and put $A = (J/O)(\chi^{-1}\kappa_p^{-r})$. Write $S(B,A)$ for the subgroup of $H^1(B,A)$ of classes unramified away from p and zero at every place over p. For each $0 \le j \le a$, choose a character λ_j of $\mathrm{Gal}(B/\mathbb{Q})$ of exact order p^j, with $\lambda_0 = 1$. Write $d_j = d_{p,r,\chi\lambda_j}(fb)$ for the cyclotomic index on the open set of Theorem 27.3.

Theorem 19.24 (Integral bounds through the cyclic character quotients)**.** *Suppose that $\bar\chi^{-1}\omega^{-r}$ is nontrivial on $G_{\mathbb{Q}_p}$, where $\omega = \kappa_p \bmod p$. Suppose also that $\bar\chi(q) \neq 1$ at every prime $q \mid b$. Then*

$$\max_{0\le j\le a} d_j \;\le\; \operatorname{length}_O S(B,A) \;\le\; \sum_{j=0}^{a} d_j.$$

The group vanishes exactly when $d_0 = 0$.

Proof. Put $\Sigma = \{v : v \mid pfb\}$ for the finite primes in question. Every $q \mid b$ is $1 \bmod p$. Indeed its inertia in the abelian extension is a nontrivial tame p-group, hence a quotient of $\mathbb{F}_q^{\times}$ by local reciprocity. For $v \mid f$ the residual finite character is nontrivial on inertia. At $q \mid b$ its

Frobenius value differs from one and $\omega(q) = 1$. Thus at every $v \mid fb$ both the residual line $\bar{A} = \bar{\chi}^{-1}\omega^{-r}$ and its Tate dual have zero invariants. The local Euler characteristic formula away from p, together with local duality in degree two, gives zero degree-one cohomology as well. The same conclusions apply after a local extension of p-power degree, since a nontrivial character of order prime to p stays nontrivial there. Filtering finite coefficients by residual lines and passing to their union proves local vanishing for the divisible coefficients below. Every simple constituent of the regular representation of a cyclic p-group in characteristic p is trivial, by $X^{p^a} - 1 = (X - 1)^{p^a}$. This justifies the filtration also for the regular representation and its lattice quotients. At p we use only degree-zero vanishing, which follows from the first hypothesis by the same filtration.

For these coefficients M over $\mathbb{Q}$, write $S(M)$ for the kernel of localization at all $v \in \Sigma$ in cohomology unramified outside Σ. At primes dividing fb the local condition is automatic by the preceding paragraph. Set $O_j = O[\zeta_{p^j}]$, $J_j = \mathrm{Frac}(O_j)$ and $A_j = (J_j/O_j)((\chi\lambda_j)^{-1}\kappa_p^{-r})$. In the Poitou–Tate sequence the dual of $S(A_j)$ identifies with the kernel of localization on degree two for the dual lattice. All its local degree-two terms vanish, by local duality and the degree-zero vanishing just proved. The trace dual of O_j is a free fractional O_j-ideal, so choosing a generator identifies this lattice with $O_j(\chi\lambda_j\kappa_p^{r+1})$. Theorem 27.3 now gives $\mathrm{length}_{O_j} S(A_j) = d_j$. Indeed any extra prime factor in its Euler product divides b, and the reduction of the factor is $1-\bar{\chi}(q)$. The extension O_j/O is totally ramified, since $O/\mathbb{Z}_p$ is unramified and the translated cyclotomic polynomial is Eisenstein. The two lengths agree over O on every finite O_j-module, by filtering it by the common residue field.

Put $R_i = O[X]/(X^{p^i} - 1)$, with X the action of a generator of the cyclic quotient. Shapiro's lemma identifies $S(A \otimes_O R_a)$ with $S(B, A)$, including each local restriction. Sending X to the inverse character value chosen for λ_i gives quotient O_i, for $i \geq 1$. Multiplication by $\Phi_{p^i}(X)$ identifies the kernel with R_{i-1}, by cancellation of this monic factor in $O[X]$. Tensoring with A preserves exactness because the quotient is O-free. In a resulting short exact sequence the global degree-one map from the first term is injective, since the last term has zero global invariants. Its image on strict groups is the kernel of the map to the third strict group. Indeed a global lift from the first term is locally zero at every required prime by injectivity on local degree one, which follows from local degree-zero vanishing for the third term. Applying the resulting order inequality successively proves the upper bound. For the lower bound, O_j embeds in R_a by multiplication by $(X^{p^a} - 1)/\Phi_{p^j}(X)$, using $\Phi_1 = X - 1$ at $j = 0$. Its quotient is again O-free and has only the indicated residual line after twisting. The same injection therefore gives the lower bound for each j.

Finally let b_j be the conductor of λ_j. It is squarefree, as the higher unit groups at a tame prime $q \mid b$ are pro-q. Modulo the maximal ideal of O_j, λ_j becomes trivial. The corestriction defining the reduced class may therefore be taken first from level fpb_j to level fp, with the tensor basis carried along. Removing each new q gives

$$N_{\mathbb{Q}(\zeta_{mq})/\mathbb{Q}(\zeta_m)}(1 - \zeta_{mq}) = \frac{1 - \zeta_m}{1 - \zeta_m^{q^{-1} \bmod m}} \qquad (q \nmid m,\ \zeta_{mq}^{q} = \zeta_m).$$

This follows by taking the product over the q roots of $X^q - \zeta_m$ and omitting the unique root in μ_m. Moving inverse Frobenius on the second Kummer class across the corestriction acts on the tensor basis by $\chi(q)q^r$. Thus the reduced class is the reduction of the $j = 0$ class times $\prod_{q \mid b_j}(1 - \bar{\chi}(q)q^r)$, a unit. Both classes are compared on the same open set with the same residue field. The multiplication exact sequence identifies the kernel of reduction on the free degree-one lattice with its maximal-ideal multiple. Hence $d_j = 0$ exactly when $d_0 = 0$. The two bounds prove the last assertion. □

19.10 The exact length over a cyclic group ring

Let p be odd, $r \geq 1$, and χ a finite character of order prime to p with $\chi(-1) = (-1)^r$. Write $O = \mathbb{Z}_p[\chi]$, $k = O/pO$ and $T = O(\chi\kappa_p^{r+1})$. Let P be the Galois group of a cyclic degree-p^a extension of $\mathbb{Q}$. Choose N divisible by its conductor and that of χ, and put $U = \operatorname{Spec}\mathbb{Z}[1/(Np)]$. Fix a generator of P. For $i = 0, \dots, a$ put $R_i = O[X]/(X^{p^i} - 1)$, with the chosen generator acting by multiplication by X. Put $D_i = O[\zeta_{p^i}]$, with the generator acting by ζ_{p^i}, and $D_0 = O$. In every tensor with T use the diagonal Galois action. Denote by M_i and H_i the O-lengths of $H^2(U, T \otimes R_i)$ and $H^2(U, T \otimes D_i)$, respectively.

Theorem 19.25 (The length lost on separating two integral lattices)**.** *Fix $1 \leq i \leq a$, put $m = p^{i-1}$ and $W = k[X]/(X^m - 1)$. Map R_{i-1} to W by reduction and map D_i to W by $\zeta_{p^i} \mapsto X$. Let I_0, I_1 be the respective images of integral degree-one cohomology in $H^1(U, T \otimes W)$. Then both have k-dimension m, and*

$$M_i = M_{i-1} + H_i - m + \dim_k(I_0 \cap I_1).$$

In particular $0 \leq \sum_{j=0}^{a} H_j - M_a \leq (p^a - 1)/(p - 1)$. For a cyclic extension of degree p the correction is zero when the two residue lines agree and one when they are distinct.

Proof. Write $g = X^m - 1$, $h = \Phi_{p^i}(X)$. In $O[X]/g$ one has $h = p$, by summing the first p powers of X^m. Consequently $O[X]/(g, h) = W$. The intersection of the ideals $(g), (h)$ is (gh). Indeed the two monic polynomials are coprime over $\operatorname{Frac} O$, and monic division gives the asserted divisibility already over O. Taking the difference of the two quotient maps therefore gives an exact sequence of Galois modules

$$0 \longrightarrow R_i \longrightarrow R_{i-1} \oplus D_i \longrightarrow W \longrightarrow 0.$$

For surjectivity onto the pairs with equal images, if polynomial representatives u, v differ by $gA + hB$, use the common lift $u - gA = v + hB$. In D_i reduction means quotient by the element $\delta = \zeta_{p^i}^m - 1$. The field extension for D_i/O is totally ramified, so $D_i/\delta D_i \simeq W$ has dimension m over k.

After tensoring with the free lattice T, all the integral groups in degree two are finite. For D_i this follows from Theorem 27.3, since the orders of the two finite characters are coprime and their product generates the coefficient ring. For R_i use its decomposition over the fraction field and finite generation of global cohomology. There is no cohomology above degree two here. For finite coefficients this is the odd-p cohomological dimension bound with p inverted. Passage to compact lattices preserves it since the finite cohomology groups satisfy the Mittag–Leffler condition. The degree-one group for D_i is free of rank one over D_i by the same theorem. For R_{i-1} the rational decomposition gives rank m over O. Complex conjugation acts by -1 on the lattice modulo p, since its image in P is trivial. Thus the invariant subgroup is zero modulo p, and the multiplication sequence shows that degree one is torsion free, hence free over O.

Reduction of degree one for R_{i-1} has kernel its multiple by p. For D_i the kernel is the multiple by δ, by the corresponding multiplication sequence. These prove the two dimensions in the statement. Put $u = \dim_k H^2(U, T \otimes R_{i-1})[p]$. Reduction by p and vanishing in degree three give

$$\dim_k H^1(U, T \otimes W) = m + u, \qquad \dim_k H^2(U, T \otimes W) = u.$$

For the second equality a finite O-module has equally many elements in its p-torsion and its quotient modulo p. In the long exact sequence of the displayed pair of lattices, the cokernel in degree one has dimension $m + u - \dim_k(I_0 + I_1)$. It injects into degree two for R_i. The next image has length $M_{i-1} + H_i - u$, by surjectivity onto degree two for W. Adding and using $\dim_k(I_0 + I_1) = 2m - \dim_k(I_0 \cap I_1)$ gives the formula. Summing in i and using $M_0 = H_0$ proves the bounds. □

19.11 Determining a compact module from finitely many twists

Theorem 19.26 (A finite determination of a cyclic cyclotomic module)**.** *Let p be prime, $\Lambda = \mathbb{Z}_p[[T]]$, and Y an inverse limit of finite abelian p-groups with surjective maps and a compatible continuous Λ-action. Suppose $1+T$ acts on each finite group with p-power order. Write $Y(z) = Y/(T-z)Y$ for $z \in p\mathbb{Z}_p$. Let $b \geq 2$. Suppose $|Y(z_*)| = p$ for some $v_p(z_*) = 1$, and $|Y(z_j)| = p^b$ for p elements z_j representing all classes of $p^b\mathbb{Z}_p/p^{b+1}\mathbb{Z}_p$. Then Y itself is cyclic of order p^b, and T acts by zero.*

Proof. The quotient $Y/(p,T)Y$ equals $Y(z_*)/pY(z_*)$, hence is one-dimensional over $\mathbb{F}_p$. Lift a generator to y. Its image generates each finite group as a Λ-module. Indeed the quotient of that group by the image of Λy is equal to its multiple by (p,T). On this finite quotient p is nilpotent, and modulo p some p-power of T is zero by the hypothesis on $1+T$. A power of the ideal (p,T) consequently kills the quotient, forcing it to vanish. The image of Λy is compact and surjects onto every finite level, so it equals Y. Write $Y = \Lambda/I$.

Evaluation at $z \in p\mathbb{Z}_p$ gives $\Lambda/(T-z) = \mathbb{Z}_p$, with convergence of every series. Its kernel description also follows by dividing $H(T) - H(z)$ by $T - z$ term by term. Thus the ideal of values $I(z)$ has index $|Y(z)|$. For $H \in I$ one has $H(0) \equiv H(z_j) \equiv 0 \bmod p^b$. Choose $H \in I$ with $v_p(H(z_*)) = 1$, using $I(z_*) = p\mathbb{Z}_p$. In $H(z_*)$ the constant and all terms of degree at least two are zero modulo p^2. Hence the linear coefficient is a unit. Starting from $0 \bmod p^b$, the unit derivative gives a unique Hensel lift at each successive precision. The limit is a root $a \in p^b\mathbb{Z}_p$.

Write $H(T) = (T-a)U(T)$. The coefficient of T^i in U is $\sum_{n>i} H_n a^{n-1-i}$, with H_n the coefficients of H. It converges in $\mathbb{Z}_p$, and the constant coefficient reduces to $H_1 \neq 0 \bmod p$. Thus U is a unit and $T - a \in I$. It follows that $Y = \mathbb{Z}_p/J$ for an ideal J, with T acting by a. Choose j with $z_j \equiv a \bmod p^{b+1}$. The quotient by $J + (a - z_j)$ has order p^b, so this ideal is $p^b\mathbb{Z}_p$. Since $a - z_j \in p^{b+1}\mathbb{Z}_p$, the valuation of ideals in $\mathbb{Z}_p$ forces $J = p^b\mathbb{Z}_p$. Finally $a \in p^b\mathbb{Z}_p$ acts as zero on Y. □

20 Uniform ranges of coefficient primes

20.1 Cell counts and full primary orders

Let $L \subseteq \mathbb{Q}(\zeta_M)$ be totally imaginary, with degree d and absolute discriminant D_L. Fix $r \geq 1$, put $i = 2r$, $n = 2i+8$, and write $\Gamma = \mathrm{GL}_n(\mathcal{O}_L)$. We use the free lattice $\Lambda = \mathcal{O}_L^n$. In this section all logarithms are natural. We will bound the order of a cohomology group by counting cells in just two degrees. This allows us to retain torsion at the small primes when passing from the lattice estimate to Galois cohomology.

Lemma 20.1 (Cells and their incidences)**.** *Let a be an upper bound for the number of Γ-orbits of cells in each of dimensions i and $i+1$ of Ash's well-rounded retract. Put $J = [\Gamma : \Gamma_3]$, where Γ_3 is the principal subgroup of level three. Write D for the real dimension of the space of Hermitian metrics before positivity and normalization, so $D = dn^2/2$ for this totally imaginary field. If $T = |H_i(\Gamma_3, \mathbb{Z})_{\mathrm{tors}}|$, then*

$$\log T \;\leq\; Ja\big\{\log(2Ja) + (D+1)\log(1+3^{dn})\big\}.$$

Proof. A metric h gives a positive definite real quadratic form on the rank dn lattice Λ by taking the archimedean trace. Write $h[v]$ for its value and $S(h)$ for the set of vectors of squared length one when the minimum is one. For a well-rounded metric $S(h)$ spans L^n over L. Ash's retract is contractible, has finite cell stabilizers, and has one open cell for each such set $S(h)$. Closing a cell allows additional shortest vectors. [5, Sec. 2.3]

Here is the geometry of these closures. Write P for the set of positive definite metrics with $h[v] \geq 1$ for all $v \in \Lambda \setminus \{0\}$. For $S = S(h_*)$ the closed cell is

$$F_S = \{h \in P : \ h[v] = 1 \quad (v \in S)\}.$$

Indeed the open segment from any point of this set to h_* has exactly S as its shortest vectors. To see compactness, take an L-basis among S. In the corresponding basis at every embedding, each diagonal coefficient is bounded above since it contributes positively to a trace of value one. Cauchy–Schwarz then bounds every entry. A limit could only leave the positive cone if the determinant of the real trace form tended to zero in a fixed lattice basis. To apply Minkowski's first theorem, observe that the ellipsoid of squared length less than one contains no nonzero lattice vector, and its volume is a fixed positive constant divided by the square root of that determinant. Minkowski's bound on this volume bounds the determinant away from zero. Thus F_S is compact inside the open cone. Enclose it in the interior of a compact polytope in that cone, for instance by taking the convex hull of finitely many small closed cubes about points of F_S. On that polytope the smallest eigenvalue of the trace form has a positive lower bound. Only finitely many vectors can therefore reach length at most one anywhere on it. The displayed intersection is a convex polytope. At a relative interior point, the inactive inequalities are locally strict.

The functional $h \mapsto h[v]$ is real linear in the metric. A basis of the span of the functionals for $v \in S$ determines the whole face by setting those basis values equal to one and intersecting with P. In fact every further functional in S is a linear combination of this basis, and its coefficients sum to one by evaluation at h_*. If F_S is a face of another cell, that cell has a defining set contained in S. A list of at most D members of S therefore specifies each cell containing F_S. Open balls of radius $1/2$ about the shortest vectors in the trace norm have disjoint interiors and fit inside the ball of radius $3/2$ about zero. Comparing volumes gives $|S| \leq 3^{dn}$. Thus a fixed cell lies in at most $B = (1 + 3^{dn})^{D+1}$ closed cells.

The level-three subgroup is torsion free by Lemma 19.2, so its cell stabilizers are trivial. In each of the two degrees the quotient has at most Ja cells. Count orbits of pairs consisting of an i-cell and a containing $(i+1)$-cell, beginning with the i-cell. There are at most JaB such pairs up to Γ_3. The distinct facets of a fixed $(i+1)$-cell give distinct pair orbits, since an identification between the pairs would stabilize that cell. Its boundary therefore has sum of absolute coefficients at most JaB, including after faces are identified in the quotient. Each incidence in the polytope before identification contributes one sign. The quotient is a classifying space for Γ_3. The torsion in its degree i cellular homology embeds in the torsion of the cokernel of the degree $i+1$ boundary. If that boundary has rank $s > 0$, the latter torsion order is the greatest common divisor of its nonzero s-rowed minors, by Smith normal form. Hadamard's inequality bounds each by $(JaB)^s$, with $s \leq Ja$. For $s = 0$ the cokernel is free. This proves the estimate. □

Theorem 20.2 (Two uniform bounds for full strict orders)**.** *With $b = r + 2$, write $U(L, r) = \sum_p \log |\mathcal{S}_{p,r}(L)|$. The sum includes every rational prime and every elementary divisor at that prime. There is an absolute constant C with*

$$U(L, r) \ \leq \ \exp\bigl(C(db)^5 \log(2Mdb)\bigr). \tag{20.1}$$

Using the cell-orbit estimate in Theorem 3.9 of the November 2026 preprint of de la Torre Durán gives the further bound

$$U(L, r) \ \leq \ \exp\bigl(Cdb^2 \log(2Mdb)\bigr). \tag{20.2}$$

Proof. For (20.1), use the finite set Φ in Corollary 5.2 of Bayer-Fluckiger, Emery and Houriet. Some element of Γ moves the entire shortest-vector set of any given well-rounded metric into Φ. The assumptions $n \ge 5$ and $L \neq \mathbb{Q}$ hold here. The basis of defining functionals in Lemma 20.1 then bounds the number of cell orbits in each degree by $a = (1 + |\Phi|)^{D+1}$. By the explicit bound for Φ in Lemma 19.2,

$$\log(2 + |\Phi|) \ll n^2 d^2 \log(2n) + n^3 d^4 \log(2d) + n^3 d^3 \log D_L,$$
$$\log(2a) \ll (nd)^5 \log(2Mnd).$$

Here $D_L \le M^d$ by the conductor–discriminant formula. This proves the orbit bound needed for the first assertion. [5]

For (20.2) we relate the two required cell degrees to the dimensions in the preprint. For a metric h in a j-cell take the cone $V(h)$ generated by vv^* for $v \in S(h)$ in the real space of Hermitian matrices. The trace pairing identifies these matrices with the defining functionals above. The cone has linear dimension $D - j$, since near h the defining equalities cut out precisely the cell. It is a face of a perfect-form cone. To see this choose a vertex h_0 of the compact polytope $F_{S(h)}$. If its active functionals failed to span the dual space, a short segment about h_0 annihilating their linear parts would lie in that polytope, contradicting extremality. Thus h_0 is perfect. On $V(h_0)$ the functional $h - h_0$ is nonnegative, and its zero face is exactly $V(h)$. Moreover $\sum_{v \in S(h)} vv^*$ is positive definite at every embedding because $S(h)$ contains an L-basis. A relative interior point of this cone is a positive combination of its generating vectors, so the relative interior lies in the positive cone.

Distinct cells give distinct cones. In fact, suppose $V(h) = V(h')$. For $v \in S(h)$ express $vv^* = \sum_{w \in S(h')} c_w ww^*$ with $c_w \ge 0$. Pairing with h gives $1 \ge \sum c_w$, and pairing with h' gives $h'[v] = \sum c_w \ge 1$. Hence $v \in S(h')$. Reversing the roles gives equality of shortest-vector sets. Change of lattice basis preserves this correspondence, acting on normals by the inverse adjoint to its action on metrics. It therefore gives an injection on Γ-orbits.

In the dimension convention of the preprint, $V(h)$ has dimension $k = D - j - 1$. For $j = i, i + 1$ one has $dn - 1 \le k \le D - 1$, because $D = dn^2/2$ and $n = 2i + 8$. This verifies the lower dimension cutoff in its Theorem 3.9. The field L is abelian and totally imaginary. Its subfield fixed by complex conjugation is totally real of index two, so the CM case of the cited theorem counts all the required cone orbits with an upper bound

$$a \;\le\; \exp\!\big(Cdn^2 \log(2nd)\big)\, D_L^{4n(n+1)}.$$

Thus we may use $\log(2a) \ll dn^2 \log(2Mnd)$. Its separate Theorem 4.5 estimates K-torsion above a prime cutoff. Here Theorem 3.9 supplies the cell count before the passage to cohomology. [9]

We finish the arithmetic argument for either choice of a. Reduction modulo three gives $J \le 3^{dn^2}$, by counting matrices over the ring $\mathcal{O}_L/3$ of cardinality 3^d. Each prime factor of J is at most $W = 3^{dn}$, by the embedding of the reduction group in $\mathrm{GL}_{dn}(\mathbf{F}_3)$. Write $A = (nd)^5 \log(2Mnd)$ for the first bound and $A = dn^2 \log(2Mnd)$ for the second. Lemma 20.1 now gives $\log(2JT) \le \exp(CA)$ in both cases. Indeed $\log(2Ja) \ll A$, while $(D + 1)\log(1 + 3^{dn}) \ll d^2 n^3$ appears only as a multiplicative factor in the bound for $\log T$.

Recall the arithmetic steps of Lemmas 19.2 and 19.3. Duality and the comparison in even K-theory embed the dual of $\mathcal{S}_{p,r}(L)$ in $K_i(\mathcal{O}_L)\{p\}$. A stable homology torsion class transfers into the group of order T for Γ_3. Composing this transfer with inclusion multiplies by J, so JT kills the class. The Hurewicz kernel on its p-part is killed by p^{i+4}. For $p > W$, both Hurewicz and transfer are injective on that part. Hence all $p > W$ together contribute at most $\log T$ because there is a single target torsion group of that order. For $p \le W$, each cyclic summand

has logarithmic order at most $(i+4)\log W + \log(2JT)$. The Kummer bound of Lemma 19.3 gives at most $Cdp\log(2Mp)/\log p$ summands at p, independently of their exponents. Summing and using $\sum_{p\le W} p \le W^2$ gives

$$U(L,r) \le \log T + CdW^2\log(2MW)\big((i+4)\log W + \log(2JT)\big).$$

Since $\log W = dn\log 3$ and $n = 4(r+2)$, enlarging the absolute constant gives (20.1) and (20.2). □

20.2 All twists at a growing set of odd primes

Fix ψ of conductor F and retain $B_j = K_\psi C_j$. Write $M_{p,r}(L) = \frac{1}{2}(1+(-1)^r c)\mathcal{S}_{p,r}(L)$ at an odd prime p. The layer a_p of Theorem 25.17 works at every twist r. We use this fact to make the number of excluded indices independent of the length of the interval over which the auxiliary primes will be selected.

Lemma 20.3 (Exceptional twists on the fixed prime-dependent layers)**.** *For every $P \ge 3$ and integer $T \ge 2$ there is a set $\mathcal{D} \subseteq [1,T]\cap\mathbb{Z}$ with $|\mathcal{D}| \ll_\psi P^5$ such that, for every $1 \le r \le T$ outside $\mathcal{D}$ and every $J \ge 0$,*

$$\sum_{\substack{2<p\le P\\ p \text{ prime}}} \log|M_{p,r}(B_J)| \ll_\psi P^{10}(1+\log(2T)). \tag{20.3}$$

Proof. For each p it suffices to prove the estimates in B_{a_p}, by Theorem 25.17. Let n_p be its degree and $N_p = F2^{a_p+2}$ a cyclotomic modulus. Both are $O_\psi((p+1)4^{e_p})$, with $e_p = v_2(p^D-1)$ and $D = 2\varphi([K_\psi:\mathbb{Q}])$. Both are $O_\psi(p^3)$. For p fixed, apply Corollary 25.13 to the characters of the prime-to-p part of this field's Galois group, on $[1,T]$ using the upper endpoint $T+1$ in that corollary. If its p-part has order d, a rational conjugacy orbit $\mathcal{O}$ contributes $O(d|\mathcal{O}|p\log(2N_pp)/\log p)$ exceptions for each residual index h. Sum over at most $p-1$ indices and use $\sum_{\mathcal{O}} d|\mathcal{O}| = n_p$. Since $\log(2N_pp)/\log p \ll_\psi 1$, the resulting number is $O_\psi(n_pp^2)$. This argument includes $p \mid n_p$.

To sum the exceptions, write $w_p = \max(v_2(p-1), v_2(p+1))$. Then $e_p = w_p + v_2(D)$, by equation 25.13 and its proof. For $P \ge 3$ one has

$$\sum_{2<p\le P} 4^{e_p} \ll_\psi \sum_{1\le m\le P+1} 4^{v_2(m)} \ll P^2.$$

Indeed the map from primes p to either $p-1$ or $p+1$ at which the maximum is attained has multiplicity at most two. There are at most $(P+1)/2^a$ integers of valuation a. Sum the geometric progression for $2^a \le P+1$. The union over the primes thus has size $O_\psi(\sum_{p\le P} p^3 4^{e_p}) = O_\psi(P^5)$.

At every other twist the exponent of $M_{p,r}(B_{a_p})$, written as a power of p, has exponent $O_\psi(P^4(1+\log(2T)))$. Indeed (25.10) bounds each $1+V_{\alpha,h}$ by $O_\psi(n_pp)$. The interpolation estimate in Corollary 25.13 multiplies this by $O(1+\log(2T))$ and adds at most $2(1+v_p(n_p)+\log_p(T+1))$. The components exhaust the group.

The logarithmic order of its subgroup killed by p is $O(n_pp\log(2N_pp))$. To recall the first-layer argument, pass to the field L/B_{a_p} cut out by the residual cyclotomic twist, of relative degree at most $p-1$. Theorem 11.22 bounds the first-layer logarithm by $\log h(L) + [L:\mathbb{Q}]\log p$, where $h(L)$ is the class number. The conductor–discriminant formula for $L \subseteq \mathbb{Q}(\zeta_{N_pp})$ gives $|\operatorname{disc} L| \le (N_pp)^{[L:\mathbb{Q}]}$. Minkowski's bound for representatives and $\zeta_L(2) \le \zeta(2)^{[L:\mathbb{Q}]}$ give the asserted estimate, also for totally real fields at an odd prime. For a finite abelian group killed by p^j, its logarithmic order is at most j times the first-layer logarithm, term by term in its elementary divisors. Multiplying the two bounds above, then summing over at most P primes, proves (20.3). □

Theorem 20.4 (An explicit growing prime range at every twist)**.** *For fixed $0 < \varepsilon < 1/52$ there is $c_{\psi,\varepsilon} > 0$. On arbitrarily distant intervals $[V, V^{3/2}]$ carrying the auxiliary fields and weights of Section 6.6, one has for every x in the interval and every $J \geq 0$*

$$\sum_{\substack{2<p\leq c_{\psi,\varepsilon}(\log\log x)^{1/5}\\ p \text{ prime}}} \sum_{1\leq r<\lfloor x^{401}\rfloor} \log|M_{p,r}(B_J)| \;\leq\; \exp(x^{2\varepsilon/3}). \tag{20.4}$$

Proof. Choose $\eta = \varepsilon/80$ and $b = 401/\eta$. Fix a constant $W > 2$ large enough for the dyadic interval selection of Theorem 11.9. Specifically take $W > 2(2b)^{R_2} + 1$, where $R_2 = R_2(\psi)$ is the bound there for the number of dyadic exceptions. For a sufficiently large Z, set $P = \lceil \log\log Z \rceil$ and choose an integer $R = \lceil C_\psi P^5 \rceil$ using Lemma 20.3. Form

$$K = W(Wb)^R, \qquad T = \lceil Z^{401K} \rceil + 1.$$

The estimate for R is independent of T, so we may now use the lemma with this T and obtain a set $\mathcal{D}$. All the fields in that use of the lemma are the specified B_{a_p}. They are independent of the auxiliary quadratic primes.

Start at $U = K \log Z$. Place the points $(\log r)/401$, $r \in \mathcal{D}$, on the real line. If some point is in $(U/(Wb), U]$, lower U to $U/(Wb)$. The point just encountered exceeds the new upper endpoint, and so cannot be encountered again. After at most R such divisions the band is empty. Set $Y = \exp(U/W)$ at this stage. Since $U \geq K \log Z/(Wb)^R = W \log Z$, one has $Y \geq Z$ and $Y^W \leq Z^K$. Throughout $[Y, Y^W]$, an exceptional r with $r \leq x^{401}$ satisfies $\log r/401 \leq U$. The empty band forces $\log r/401 \leq U/(Wb) \leq (\log x)/b$, or $r \leq x^\eta$. This conclusion holds for every $p \leq P$ at once.

Now select the two auxiliary primes at the initial scale Y by Theorem 5.1, with the fixed upper power $W + 1$. The dyadic construction in the proof of Theorem 11.9 takes place inside $[Y, Y^{2(2b)^{R_2}}]$, since that is its initial range for the dyadic exceptional indices. Its proof applies at every sufficiently large initial scale. It produces $[V, V^{3/2}] \subseteq [Y, Y^W]$ with the specified fields, weights and dyadic bounds. The estimates on ranks, auxiliary primes and real period levels in Volume I then apply at the points of this interval. In particular the auxiliary-prime selection has used a power fixed before Z, although K used for the independent cyclotomic layers grows with Z.

If x is in this interval, then $\log\log x \leq \log\log Z + \log K \ll_{\psi,\varepsilon} P^5$. Choose $c_{\psi,\varepsilon}$ small enough that every prime in (20.4) is at most P. All its twists lie in $[1, T]$. For the twists outside $\mathcal{D}$ their total contribution is at most

$$C_\psi x^{401} P^{10}(1 + \log(2T)).$$

Its logarithm is $O_{\psi,\varepsilon}(\log x + P^5 + \log\log Z)$, which is $o(x^{\varepsilon/3})$ uniformly since $x \geq Z$ and $P = \lceil \log\log Z \rceil$.

For an exceptional $r < x^{401}$ we have $r \leq x^\eta$. Theorem 25.17 embeds $M_{p,r}(B_J)$ into $M_{p,r}(B_{a_p})$, using the inverse of its isomorphism if $J > a_p$. Restriction through the extension of degree at most two then embeds this latter group into $\mathcal{S}_{p,r}(B_{a_p}(i))$. The latter field is totally imaginary of degree $O_\psi(P^3)$ and has modulus $O_\psi(P^3)$. Bound its single-prime logarithmic order by the all-prime estimate (19.1). The exponent on the right of that estimate is

$$O_\psi((P^3(x^\eta + 2))^{10} \log(2P^6(x^\eta + 2))) \;\leq\; x^{\varepsilon/3}$$

eventually, since $10\eta = \varepsilon/8$. There are at most PR pairs to count in this part. Consequently the two parts together are at most $\exp(x^{2\varepsilon/3})$ for all sufficiently large Z, uniformly in J. Letting Z tend to infinity proves the assertion. □

20.3 Testing whole character components on the common interval

Keep $E = E_x$, its degree n_E, modulus N, and $t = \lfloor x^{401} \rfloor$ as in Theorem 11.17. For each odd $\ell \nmid Nn_E$, take a finite unramified coefficient ring $O/\mathbb{Z}_\ell$ containing the character values of $\mathrm{Gal}(E/\mathbb{Q})$. For a character α of sign $(-1)^r$ put $\vartheta = \kappa_\ell^{-r}\alpha^{-1}$. Denote the corresponding strict group over $\mathbb{Q}$ by $S(\vartheta)$, as in Sections 24.1 and 24.7. It gives the α-summand of the strict group over E after extending scalars. The normalized length is length_O; summing it over all characters recovers the original $\mathbb{Z}_\ell$-length since $O/\mathbb{Z}_\ell$ is unramified.

Theorem 20.5 (A polynomial bound for all components certified by a finite test)**.** *Put $h = 1 + v_\ell(r)$. For $\bar\vartheta \neq 1$ let C_h be the finite class group component of Theorem 24.20. Include a triple (ℓ, r, α) in the following sum if ℓ^{h-1} kills $C_h/\ell^h C_h$. Also include every triple with $\bar\vartheta = 1$. Then on every indicated field*

$$\sum_{\substack{\text{included triples}\\ 1\le r<t}} (\log \ell)\,\mathrm{length}_O\, S(\vartheta) \;\ll\; n_E^2 t^2 \log(2Nt)\log(2t).$$

The groups in this estimate are taken with their full exponents. The bound is $o(\exp(x^\varepsilon/2))$ uniformly on the common intervals.

Proof. If $\bar\vartheta = 1$, restrict first to inertia at ℓ. The character α is unramified there, so $\ell - 1 \mid r$. Then κ_ℓ^{-r} is trivial modulo ℓ globally, and $\alpha = 1$ since its values have order prime to ℓ. The twist r is even. By Proposition 11.19 its group over $\mathbb{Q}$ is zero, since the trivial eigenspace of the class group modulo ℓ in $\mathbb{Q}(\zeta_\ell)$ comes from $\mathrm{Cl}(\mathbb{Q}) = 0$. Indeed the norm of an extended class is its $(\ell-1)$-st power, and extending the norm gives the product of all Galois conjugates. Dividing by $\ell - 1$ on the ℓ-primary group gives the invariant part.

For the other included triples put $L = \overline{\mathbb{Q}}^{\ker\bar\vartheta}$. Corollary 24.21, shows that the entire strict group is killed by $\ell^{v_\ell(r)}$. Its number of cyclic summands is at most $1 + \log|\mathrm{Cl}(L)|/\log\ell$. For a nonsplit prime this follows directly from the class group description at level one. For a split prime the ray class sequence adds at most one generator on the character component, since the permutation module on the primes over ℓ is the regular representation. The S-class group is a quotient of the ordinary class group.

The field L has degree at most $n_E(\ell - 1)$ and conductor dividing $N\ell$. The conductor–discriminant formula gives $\log|\mathrm{disc}\, L| \le [L:\mathbb{Q}]\log(N\ell)$. Every ideal class has an integral representative of norm at most $2^{[L:\mathbb{Q}]}|\mathrm{disc}\, L|^{1/2}$ by Minkowski's theorem. There are at most $Y^2\zeta(2)^{[L:\mathbb{Q}]}$ integral ideals of norm at most Y, by bounding the ideal Dirichlet series prime by prime. It follows that $\log|\mathrm{Cl}(L)| \ll n_E\ell\log(2N\ell)$. Thus the contribution from one triple is at most

$$v_\ell(r)\big(\log\ell + Cn_E\ell\log(2N\ell)\big).$$

Only primes dividing r give a positive contribution. There are at most n_E characters for each prime and each r. Use $\ell \le r$ at these primes and $\sum_{\ell\mid r} v_\ell(r) \le \log r/\log 2$, then sum over $r < t$. This proves the stated bound. The field degree, t, and $\log(2N)$ are all at most fixed powers of x, which proves the uniform assertion. □

Proposition 20.6 (The rational integer bound in the source)**.** *Let $r \ge 2$ be even. If ℓ is an odd prime with $\ell - 1 \mid 2r$, then $K_{2r}(\mathbb{Z})\{\ell\} = 0$. For any choice of coefficient fields in the source's rational integer bound the exact equality*

$$\sup_P \sum_{\ell\in P} (\log\ell)\,\frac{\mathrm{length}_{O_\ell} S_\ell^{(2)}(r; O_\ell)}{e(O_\ell/\mathbb{Z}_\ell)} = \log|K_{2r}(\mathbb{Z})| \tag{20.5}$$

holds, where P runs over finite sets of primes $\ell \geq 5$ with $\ell - 1 \nmid 2r$. Here $S_\ell^{(2)}$ uses coefficients $(\operatorname{Frac} O_\ell/O_\ell)(-r)$, local triviality at ℓ and at 2, and trivial restriction to inertia at all other finite primes. Consequently a polynomial bound in r for the sums in (20.5) is equivalent to one for $\log|K_{2r}(\mathbb{Z})|$ at even r.

Proof. By Proposition 11.19 the rank modulo ℓ is the dimension of the ω^{-r}-part of the real cyclotomic class group modulo ℓ. The order of that character divides two when $\ell - 1 \mid 2r$. Its eigenspace descends to the field cut out by the character. Indeed the subgroup fixing that field has order prime to ℓ. Extension of ideals followed by norm multiplies by its order, and in the reverse order is the sum of its elements on ideal classes. Thus ideal extension identifies the downstairs ℓ-primary class group with the invariants upstairs, also after reduction modulo ℓ.

The trivial character gives $\mathbb{Q}$. A nontrivial quadratic character here is even and cuts out $\mathbb{Q}(\sqrt{\ell})$, of discriminant ℓ. This follows also from the conductor–discriminant formula for its single nontrivial character. In this real quadratic field each ideal class has an integral ideal of norm at most $Y = \sqrt{\ell}/2$. There are at most $\sum_{n \leq Y} \sum_{a \mid n} 1 \leq \lfloor Y \rfloor^2$ such ideals. Indeed the number at a prime power p^j is at most $j + 1$ by prime factorization of quadratic ideals, and each pair counted in the last sum has two positive coordinates at most Y. Hence the class number is less than ℓ. Its ℓ-part vanishes. The computed dimension is zero in both cases, so the finite ℓ-primary K-group vanishes.

For odd ℓ the dual of the rational strict group with $\mathbb{Q}_\ell/\mathbb{Z}_\ell$ coefficients is all $K_{2r}(\mathbb{Z})\{\ell\}$, by the duality argument of Corollary 11.18. Requiring local triviality at 2 in addition does not change its order. An unramified local class at 2 is determined by its value at Frobenius, modulo multiples by $2^{-r} - 1$ on $(\mathbb{Q}_\ell/\mathbb{Z}_\ell)(-r)$. This is a nonzero scalar in $\mathbb{Z}_\ell$, so multiplication is surjective. All such local classes vanish. The same statement holds after finite scalar extension to O_ℓ. Concretely $(\mathbb{Q}_\ell/\mathbb{Z}_\ell) \otimes_{\mathbb{Z}_\ell} O_\ell = \operatorname{Frac}(O_\ell)/O_\ell$. This finite free base change commutes with the cochains and with the restriction kernels. On a cyclic summand $\mathbb{Z}_\ell/\ell^a$ the resulting length is $a\, e(O_\ell/\mathbb{Z}_\ell)$. This accounts for the denominator in (20.5).

There is no dyadic torsion in $K_{2r}(\mathbb{Z})$ for positive even r, by the number-ring computation at two in [10, Ch. VI, Cor. 9.8]. The prime 3 always satisfies $\ell - 1 \mid 2r$. All omitted primes have therefore been accounted for. There are only finitely many prime divisors of the group order, so the supremum equals the stated logarithm. □

The rational inequality in the supplied archive is formulated at `Development/AutomorphicArithmetic/AutomorphicVarieties/SmallClassNumbers/ClassNumberThree.lean`, line 16. Its deduction at line 89 of that file uses the comparison of strict lengths with Frobenius-trace congruences. The single-character inequality is written at `Development/AutomorphicArithmetic/AutomorphicVarieties/UnitaryThreeGroups/KatoUse.lean`, line 54. Proposition 20.6 identifies its rational target. A uniform upper bound for that target would require the comparison or an independent bound on the orders. The theta-period height in Corollary 87.3 is a further requirement on the same intervals.

20.4 All complementary characters for a range of coefficient primes

We continue on the field $E = K_\psi C_{l'}(\sqrt{-q}, \sqrt{-d_0})$ of the period, with $n = [E : \mathbb{Q}]$, conductor dividing N, and $t = \lfloor x^{401} \rfloor$. Write $M_{p,r} = \frac{1}{2}(1 + (-1)^r c)\mathcal{S}_{p,r}(E)$. This time the bound is for that whole eigenspace on E. There is no restriction of r to a prescribed residue class.

Theorem 20.7 (A full-field bound away from an exceptional set of twists)**.** *Take any odd prime $p \nmid n$ with $p \leq x^{199}$. On every sufficiently large common interval, there is a subset*

$\mathcal{E}_p \subset \{1, \dots, t-1\}$ *with*

$$|\mathcal{E}_p| \ll np^2 \frac{\log(2Np)}{\log p}, \tag{20.6}$$

$$p^{\lceil x^{202} \rceil} M_{p,r} = 0 \qquad (1 \le r < t,\ r \notin \mathcal{E}_p). \tag{20.7}$$

The implicit constant in (20.6) *is absolute. In particular, uniformly over these primes,*

$$\frac{|\mathcal{E}_p|}{t-1} \ll_{\psi,\varepsilon} x^{-1+33\varepsilon/4}.$$

Proof. Extend scalars to an unramified p-adic coefficient ring containing the values of all characters of $\mathrm{Gal}(E/\mathbb{Q})$. Character descent as in Theorem 24.1 and the integral idempotents for this prime-to-p group split $M_{p,r}$ into the strict components with $\alpha(-1) = (-1)^r$. Theorems 25.9 and 25.10 apply to each component in each class of r mod $(p-1)$. They include the case $p \mid N$, with the tame part ω^i at p separated from α'. The components with trivial residual character already vanish.

To count exceptions, group the characters α into their orbits $\mathcal{O}$ under rational Galois conjugacy. Use $h = r + 1 + i \bmod (p-1)$ as the index of the residue class for each α. Holding h fixed holds fixed the integer $k \in [2, p]$ used to evaluate the annihilator in equation 25.7. The parity condition becomes $\alpha'(-1) = (-1)^{h-1}$. It is invariant throughout each orbit even when its tame exponent i changes. For any allowed orbit and h, write $V_{\alpha,h}$ for the valuation of that nonzero evaluation. Then

$$\sum_{\alpha \in \mathcal{O}} (V_{\alpha,h} + 1) \ll |\mathcal{O}| \left(1 + k \frac{\log(2Np)}{\log p}\right). \tag{20.8}$$

Indeed $V_{\alpha,h} = 1 + v_p(B_{k,\bar{\alpha}'})$ by the proof of Theorem 25.9. The conductor f_0 of α' is fixed on the orbit. The number $f_0(k+1)!\, B_{k,\bar{\alpha}'}$ is an algebraic integer, and each of its conjugates has modulus at most $\exp(Ck \log(2Np))$, as shown there. Regard it in the value field of α. The embeddings of that field correspond bijectively to $\mathcal{O}$. Repeated restrictions to the value field of α' give exactly the multiplicities in its rational norm. The sum of the valuations of all these conjugates at a fixed p-adic embedding is the valuation of that norm. Its absolute size gives (20.8) since clearing a denominator never decreases valuation. One may include the already vanishing residual components in this upper bound using the same evaluation formula.

By Theorem 25.10, for an individual pair (α, h) at most $2(V_{\alpha,h}+1)$ distinct twists escape its exponent bound. Take the union over all pairs, including only their stipulated residue classes. There are at most $p-1$ choices of h per orbit and $\sum_{\mathcal{O}} |\mathcal{O}| = n$. Using $k \le p$ in (20.8) now proves (20.6).

For an individual component the common upper bound for its exponent as a power of p away from that union is

$$C \left(1 + np \frac{\log(2Np)}{\log p}\right) \left(1 + \frac{\log t}{\log p}\right).$$

This uses the individual estimate of equation 25.8, and the definition $L = V + 2(V+1)\lfloor \log_p t \rfloor$. Here $n \ll_\psi x^{2+8\varepsilon}$, $\log(2Np) \ll_{\psi,\varepsilon} x^{\varepsilon/4}$, and $p \le x^{199}$. In the bound for the conductor one uses also $\log x = O_\varepsilon(x^{\varepsilon/4})$. Since $0 < \varepsilon < 1/52$, the displayed bound is at most x^{202} for sufficiently large x, uniformly in the prime. Taking all the integral character summands and using faithful scalar extension gives (20.7). Finally (20.6), $p^2 \le x^{398}$, and $t - 1 \asymp x^{401}$ give the asserted proportion. The interval and field choices are precisely those of Proposition 9.9. □

Corollary 20.8 (The nonexceptional part of the strict cohomology sum)**.** *On these same intervals,*

$$\sum_{\substack{2<p\le x^{199}\\ p\text{ prime},\ p\nmid n}}\ \sum_{\substack{1\le r<t\\ r\notin\mathcal{E}_p}} \log|M_{p,r}| = o(\exp(x^{\varepsilon}/2)).$$

At each included pair the remaining summand in (19.15) *is zero.*

Proof. By the elementary-divisor calculation in Theorem 19.19, each logarithm on the left is at most $\lceil x^{202}\rceil \log|\mathcal{S}_{p,r}(E)[p]|$. Lemma 19.18 bounds the latter logarithm by $Cnp\log(2Np)$. Bounding the sum of the primes by the sum of all positive integers at most x^{199}, the result is $O_{\psi,\varepsilon}(x^{202}nt\,x^{398}\log(2Nx^{199}))$. This is polynomial in x, which proves the claimed estimate for fixed $\varepsilon>0$. Moreover $x^{199}<\exp(x^{\varepsilon}/12)$ eventually. The lower bound for $k_{p,r}$ at these primes in Theorem 19.19 therefore exceeds $\lceil x^{202}\rceil$. As $Q_{p,r}\subseteq M_{p,r}$, this gives $p^{k_{p,r}}Q_{p,r}=0$, as asserted. □

A bound on the number of exceptions leaves their individual orders undetermined. Within this prime range, the sum over $\mathcal{E}_p$ and the odd primes dividing n therefore still requires an estimate. Primes above x^{199} also occur in (L). The height-restricted norm identity and the compact row types from Theorems 87.10 and 87.12 apply on exactly the fields treated here.

20.5 All odd primes in the polynomial range

Work on the interval of Proposition 9.9. Use its field $E=K_{\psi}C_{l'}(\sqrt{-q},\sqrt{-d_0})$ and retain $n=[E:\mathbb{Q}]$, N, $t=\lfloor x^{401}\rfloor$ and $M_{p,r}=\frac{1}{2}(1+(-1)^r c)\mathcal{S}_{p,r}(E)$. The next estimate includes the odd prime divisors of n.

Theorem 20.9 (Simultaneous control of the complementary groups)**.** *For each odd prime $p\le x^{199}$ there is a set $\mathcal{E}_p\subset\{1,\dots,t-1\}$ with*

$$|\mathcal{E}_p|\ll np^2\,\frac{\log(2Np)}{\log p},\qquad p^{\lceil x^{202}\rceil}M_{p,r}=0\quad(1\le r<t,\ r\notin\mathcal{E}_p).$$

The implied constant is absolute, and x is sufficiently large in the common intervals. In particular the exceptional proportion is $O_{\psi,\varepsilon}(x^{-1+33\varepsilon/4})$ uniformly in these primes. For the smaller range $p\le Y=x^{133-3\varepsilon}$ there is a single set $\mathcal{E}\subset\{1,\dots,t-1\}$ with

$$\frac{|\mathcal{E}|}{t-1}\ll_{\psi,\varepsilon} x^{-3\varepsilon/4},\qquad p^{\lceil x^{202}\rceil}M_{p,r}=0\quad\text{for every odd prime } p\le Y,\ r\notin\mathcal{E}. \tag{20.9}$$

Proof. Write $\mathrm{Gal}(E/\mathbb{Q})=P\times H$ with P its p-Sylow subgroup of order d. Over the unramified coefficient ring containing the characters of H, the idempotents for H are integral because $p\nmid|H|$. Complex conjugation lies in H. The components of $M_{p,r}$ are therefore exactly those indexed by $\alpha\in\widehat{H}$ with $\alpha(-1)=(-1)^r$. Restriction identifies each component with the corresponding strict group over E^H by Lemma 24.8. This descent keeps the entire action of P on that component.

For each character and each residue class of r mod $(p-1)$, Corollary 25.13 bounds its exponent outside at most $2(V_{\alpha,h}+1)$ twists in that class. Here $h=r+1+i \bmod (p-1)$ if the factor of α at p is ω^i. As in Theorem 20.7, fixing h fixes the moment index $k\le p$, and the parity condition on the prime-to-p character is constant on each rational conjugacy orbit $\mathcal{O}$. Taking the union of the exceptional twists and summing equation 25.10 over the orbits and the at most $p-1$ values of h proves the asserted cardinality, since $\sum_{\mathcal{O}} d|\mathcal{O}|=n$. The estimate also covers characters for which the twisted coefficient becomes trivial modulo p on G_{E^H}.

For each character separately, (25.10) gives $V_{\alpha,h}+1 \ll np\log(2Np)/\log p$. The two additional scalar factors in the exponent have total valuation at most $2(1+v_p(d)+\log_p t)$, by Lemma 25.11. By Corollary 25.13, the power of p required for every component outside the union thus has exponent at most

$$Cnp\,\frac{\log(2Np)}{\log p}\left(1+\frac{\log t}{\log p}\right)+2(1+\log_p n+\log_p t).$$

Here C is absolute. On the stated fields we have $n \ll_\psi x^{2+8\varepsilon}$ and $\log(2Np) \ll_{\psi,\varepsilon} x^{\varepsilon/4}$ for $p \le x^{199}$. Also $\log t = O_\varepsilon(x^{\varepsilon/4})$, so the dominant term is $O_{\psi,\varepsilon}(x^{201+17\varepsilon/2})$. Since $0<\varepsilon<1/52$, the whole exponent is at most x^{202} eventually. Faithful scalar extension yields the bound on $M_{p,r}$ itself. Dividing the cardinality bound by $t-1 \asymp x^{401}$ gives the first exceptional proportion.

For the joint assertion take $\mathcal{E}=\bigcup_{2<p\le Y}\mathcal{E}_p$, the union being over primes. Bounding $\sum_{p\le Y}p^2$ by the sum of squares of the integers up to Y gives

$$|\mathcal{E}| \ll_{\psi,\varepsilon} x^{2+8\varepsilon+\varepsilon/4}\,Y^3 = x^{401-3\varepsilon/4}.$$

Every remaining twist then satisfies the exponent bound for all the indicated primes simultaneously. □

Corollary 20.10 (The remaining prime and twist pairs)**.** *On these fields and intervals,*

$$\sum_{\substack{2<p\le x^{199}\\ p\text{ prime}}}\ \sum_{\substack{1\le r<t\\ r\notin\mathcal{E}_p}} \log|M_{p,r}| = o(\exp(x^\varepsilon/2)).$$

In (19.15) *the sum over odd primes may be restricted to $p>x^{199}$ and to $p\le x^{199}$ with $r\in\mathcal{E}_p$.*

Proof. At an included pair the elementary-divisor inequality bounds the logarithmic order by $\lceil x^{202}\rceil\log|\mathcal{S}_{p,r}(E)[p]|$. Lemma 19.18 bounds the first-layer logarithm by $Cnp\log(2Np)$ for every odd prime. Summing as in Corollary 20.8 gives a polynomial bound in x, hence the stated little-oh estimate for every fixed $\varepsilon>0$. For $p\le x^{199}$ the assigned depth $k_{p,r}$ of Theorem 19.19 exceeds $\lceil x^{202}\rceil$ eventually. Thus $p^{k_{p,r}}Q_{p,r}=0$ at each included pair, which proves the restriction on the sum. □

This reduction leaves the orders at the exceptional twists and at larger primes to be bounded. The arithmetic normalization and the untruncated period comparison of Section 6.6 on E are also required to deduce the prime-sum estimate (W) by this argument.

20.6 All twists on the quadratic invariants of the period fields

Fix ψ of conductor F, put $o=[K_\psi:\mathbb{Q}]$, and take $0<\varepsilon<1/52$. For a number field L in the abelian family and an odd prime p, write

$$M_{p,r}(L)=\tfrac12(1+(-1)^r c)\mathcal{S}_{p,r}(L).$$

Here c is complex conjugation, and $\mathcal{S}_{p,r}(L)$ is the strict degree-one group with coefficients $\mathbb{Q}_p/\mathbb{Z}_p(-r)$. A strict class vanishes on inertia away from p and locally at each place over p. All logarithms of finite-group orders below include the full primary exponent.

Theorem 20.11 (The quadratic invariants at every prescribed twist)**.** *There is a constant $c_{\psi,\varepsilon}>0$ and there are arbitrarily distant intervals $[V,V^{3/2}]$ with fixed auxiliary primes q,d_0 on each interval. For every x in such an interval use precisely the period field of Proposition 9.9,*

$$J=l',\qquad B_J=K_\psi C_J,\qquad E=B_J(\sqrt{-q},\sqrt{-d_0}),\qquad H_0=\mathrm{Gal}(E/B_J).$$

Then

$$\sum_{\substack{2<p\le c_{\psi,\varepsilon}(\log\log x)^{1/5}\\ p\ \text{prime}}}\ \sum_{1\le r<\lfloor x^{401}\rfloor} \log|M_{p,r}(E)^{H_0}| \ \le\ \exp(x^{2\varepsilon/3}). \tag{20.10}$$

On these very fields and intervals, (87.5) *holds for the height-truncated theta-period seeds of Theorem 87.10.*

Proof. Choose the intervals of Theorem 20.4. There the auxiliary prime pair is chosen after the exceptional twists on the fields B_j have been located, and the resulting interval still satisfies the hypotheses of Proposition 9.9 and Theorem 87.10. Neither q nor d_0 divides $2F$. Each of the three quadratic subfields of $\mathbb{Q}(\sqrt{-q},\sqrt{-d_0})$ ramifies at one or both of these primes, whereas B_J is unramified at both. Thus H_0 has order four. Averaging over H_0 is exact on p-primary modules. Inflation–restriction on absolute Galois groups identifies degree-one cohomology over B_J with the invariants over E. Restriction on local degree-one groups at p is injective by corestriction, as the local degree divides four. Away from p the coefficient is unramified and an inertia homomorphism which vanishes upstairs factors through a group of order dividing four. Its p-primary image is zero. The strict local conditions therefore descend. These identifications commute with c. Hence each group in (20.10) is isomorphic to $M_{p,r}(B_J)$. Theorem 20.4 gives the asserted sum uniformly in J, in particular at $J = l'(x)$. □

For the primes in (20.10) this also shortens the remaining sum in (19.15), including its terms at the exceptional twists of Theorem 20.9. Indeed put $e_0 = |H_0|^{-1}\sum_{h\in H_0} h$. It commutes with the projector $\pi_{p,r}$ there since the field is abelian. The logarithm of the order of $p^{k_{p,r}}e_0Q_{p,r}$ is at most $\log|M_{p,r}(E)^{H_0}|$. The direct sum decomposition for e_0 therefore permits replacing $Q_{p,r}$ in these terms by $(1-e_0)Q_{p,r}$ with total error at most $\exp(x^{2\varepsilon/3}) = o(b^{1/2})$, where $b = \exp(x^{\varepsilon})$. This leaves the other three characters of H_0 in these terms.

20.7 Strict local conditions at these very theta primes

Let E be the period field, $d = [E:\mathbb{Q}]$, $t = \lfloor x^{401}\rfloor$, and R_0 the squarefree product of the primes dividing $2Ng_1g_2T$. For p prime, $r \ge 1$, use the actual coefficient $A_{p,r} = (\mathbb{Q}_p/\mathbb{Z}_p)(-r)$ of Section 6.6.

Theorem 20.12 (The local cost on the interval of the integral comparison)**.** *On the same fields and intervals as Theorems 20.11 and 104.26, the two auxiliary prime ideals for the theta construction can be chosen above distinct rational primes ℓ_1,ℓ_2 split completely in E, larger than $t+2$ and every prime-power cutoff in the period count, and with logarithms polynomial in x. Put $R = R_0\ell_1\ell_2$ and let W be all places of E over its divisors. In the strict group $\mathcal{S}_{p,r}(E)$, relax the conditions at W by allowing all local classes away from p and unramified classes above p. Denote the resulting group by $\mathcal{S}^W_{p,r}(E)$. Then*

$$\sum_{1\le r<t}\ \sum_{p} \log|\mathcal{S}^W_{p,r}(E)/\mathcal{S}_{p,r}(E)| \ll dt^2\log(2Rdt) \ll_{\psi,\varepsilon} x^C = o(b^{1/2}). \tag{20.11}$$

The same bound holds for the increase of the sum of the orders in logarithmic form on the right of (19.15) *under this relaxation. The final compact integral norm* (104.10) *holds with these choices.*

Proof. For each required narrow class use the construction of Theorem 72.30 with one additional cyclotomic factor. Take an odd prime l outside the original rational primes to avoid and with logarithm at most the logarithm of one plus their product, by taking a prime divisor of that integer. Choose a least positive with $l^a > Y+1$, where Y exceeds the cutoffs and $t+2$. One may

choose $Y = O(t+xb)$ with a sufficiently large implied constant since the numerators of the count are $O(xb)$ and all weights are at least one. The extra extension $E^{+}(\zeta_{l^a})/E^{+}$ is totally ramified at l, where the prior auxiliary class field is unramified. Thus its Frobenius can be prescribed as $-1 \bmod l^a$ independently of the given narrow class. The same unconditional least-prime theorem gives a degree-one prime of norm exceeding Y and with logarithm polynomial in x, by the abelian conductor bound. Excluding its rational prime for the next class gives distinct primes. Both are unramified and split completely in E.

For a finite place $w \nmid p$, put $q = Nw$. Unramified cohomology is zero because the nonzero multiplier $q^{-r} - 1$ acts surjectively on $\mathbb{Q}_p/\mathbb{Z}_p$. Inertia restriction identifies the full local cohomology with the Frobenius invariants in the maps from the pro-p tame inertia $\mathbb{Z}_p(1)$ to $A_{p,r}$. Its order is therefore $p^{v_p(q^{r+1}-1)}$. At $w \mid p$, the allowable unramified group is a quotient of the inertia invariants. The cyclotomic inertia image has index dividing the absolute ramification index e_w in $\mathbb{Z}_p^{\times}$, so these invariants have logarithmic order at most $(2+v_p(r)+v_p(e_w))\log p$. At either new rational prime, when it is the coefficient prime, the completion is $\mathbb{Q}_p$ and $p-1 > r$. A primitive Teichmüller unit then acts nontrivially modulo p and the invariants vanish.

The quotient of the global groups injects into these local groups by restriction. Its away-from-p contributions sum to at most $d(t-1)(t+2)\log R/2$ by factoring $q^{r+1}-1$. At the residue characteristics the total for a fixed twist is at most $d(2\log R + \log r + \log d)$, since every e_w divides d. This proves (20.11). The original and the relaxed groups are Galois-stable, and the quotient of their images under the sign and group-ring operators in (19.15) is a quotient of the increase already bounded. The prime choices preserve the ideals and local properties used in Theorems 104.25 and 104.26. Full proofs are in Section 11.5. □

Every original strict class already vanishes on restriction to every place in W. Thus (20.11) measures the cohomological cost of the finite theta test places. The orders of the classes in the original strict kernel on the right of (19.15) still require a uniform bound. In the integral period, (104.10) identifies the last coefficient exactly. Its nonvanishing and height after the preceding lifts, finite class sums and the prescribed projection are the other outstanding estimates for the interval bound.

20.8 An enlarged range of full orders on the same period field

The exponent $1/5$ from the two auxiliary conductors in Theorem 19.16 measures their size at the initial scale of prime selection. The final interval can start later while retaining those same primes. This also permits the depth of the subfield in the real cyclotomic tower to depend on the twist.

Theorem 20.13 (Removing a growing family of complete summands)**.** *Fix $0 < \delta < 1$. On arbitrarily distant admissible intervals take $E = K_\psi C_J(\sqrt{-q}, \sqrt{-d_0})$ as in (19.15). For each $1 \le r < t$ let $j(r)$ be the largest $0 \le j \le J$ with*

$$[2^j(r+2)]^5 \le x^{(1-\delta)\varepsilon}.$$

Let e'_r project to the classes invariant over the subfield $K_\psi C_{j(r)}(\sqrt{-q}, \sqrt{-d_0})$, and put $e'_r = 0$ if there is no such j. The contribution of these summands, at every odd prime and with full primary exponents, is $o(b^a)$ for every fixed $a > 0$. Using the cell count of de la Torre Durán, the same assertion holds with the larger condition $2^j(r+2)^2 \le x^{(1-\delta)\varepsilon}$. In particular, for either choice of projector,

$$\mathcal{L}_E(x) = \sum_{1 \le r < t} \sum_{p \text{ odd prime}} \log |p^{k_{p,r}}(1 - e'_r)Q_{p,r}| + o(b^{1/2}). \tag{20.12}$$

Proof. Choose a fixed A such that $1/(5A) < \delta/2$. At an initial scale Y the two auxiliary primes have $\log(qd_0) \ll Y^{\varepsilon/5}\log^2(2Y)$. In selecting the common interval reserve the fixed additional factor A in the upper power before choosing these primes. The finitely many dyadic exceptional indices can then be avoided or placed at small twists on $[V, V^{3/2}]$ with $V \geq Y^A$. The earlier selection over the fields $K_\psi C_j$ is independent of the two primes and supplies room for the larger fixed power. The complete selection is proved in Lemma 19.12. All the conductors in the subfields above now have logarithm $O_{\psi,\varepsilon,\delta}(x^{\delta\varepsilon/2})$.

At odd primes the average over the two-power degree extension to E identifies the invariant strict group with the strict group of the chosen subfield. Its degree is at most $4\,\mathrm{ord}(\psi)2^j$. The cell estimate for its even K-group bounds the sum of logarithmic strict orders over all primes. With the displayed choice of $j(r)$, the sum over all $r < t$ is at most $\exp(C_{\psi,\varepsilon,\delta}x^{(1-\delta/2)\varepsilon})$, using the appropriate lattice bound. This is Theorem 19.13. Its ratio to b^a tends to zero for every fixed $a > 0$. All the projectors in (19.15) commute with e'_r, since $E/\mathbb{Q}$ is abelian. For each p, r, the logarithmic order removed by the additional projector is exactly $\log|p^{k_{p,r}}e'_rQ_{p,r}|$, bounded by the logarithmic order of the full invariant strict group. This proves (20.12) by addition. □

For example, in the second range any fixed $u, v > 0$ with $u+2v < 1$ are permitted simultaneously for $2^j \leq x^{u\varepsilon}$ and $r \leq x^{v\varepsilon}$, by taking $0 < \delta < 1-u-2v$ to absorb the constant from $r+2$. In the published lattice range the corresponding condition is $5(u+v) < 1$. Both statements apply to subfields containing the two auxiliary quadratic fields on the chosen interval.

Corollary 20.14 (Zero contribution above the large-prime cutoff)**.** *On every sufficiently distant admissible interval put $P = \exp(x^\varepsilon/12)$. At $p > P$, the entire summand of $\mathcal{S}_{p,r}(E)$ descending from $K_\psi C_j$ vanishes when*

$$2^j(r+2) \leq c_{\psi,\varepsilon}(\log x/\log\log x)^{1/5}, \qquad 0 \leq j \leq J.$$

There is no restriction on the order of the residual cyclotomic character in this assertion.

Proof. At odd primes restriction through the extension of degree at most two from $K_\psi C_j$ to $K_\psi C_j(i)$ is injective. This last field has modulus at most $2^{j+2}F$, independent of q, d_0. Its bound on the total logarithmic order is at most $x^{\varepsilon/2}$ under the indicated hypothesis for a sufficiently small $c_{\psi,\varepsilon}$. A single nonzero class at $p > P$ costs more than $x^\varepsilon/12$, which exceeds that bound eventually. The explicit estimates and the wider range using the cell count of de la Torre Durán are in Corollary 19.14. □

The full period field has $2^J \geq x^{2+8\varepsilon}/\,\mathrm{ord}(\psi)$, and the twist range extends to $\lfloor x^{401}\rfloor - 1$. In particular the field-degree bound in Theorem 20.13 does not reach the entire field even at the first twist. The sum on the right of (20.12) and the arithmetic lower estimate for the projected integral theta period at its original finite level remain to be bounded together on the common intervals.

20.9 One exceptional set on a whole period interval

At a single field the count in Theorem 20.9 sums separate upper bounds for the different coefficient primes. For each positive weight $k \geq 2$, the nonzero values $-L(1-k, \bar{\alpha})$ are algebraic numbers fixed by the choice of field and character. Factoring their numerator ideals lets us count the primes using a single integer for each k. We first give the resulting estimates for the actual complementary strict groups $M_{p,r}(E)$ from (20.12).

Theorem 20.15 (Simultaneous bounds on the full period fields)**.** *Write $t(x) = \lfloor x^{401}\rfloor$. On arbitrarily distant common intervals $[V, V^{3/2}]$ in Theorem 20.13, the following two assertions hold.*

1. *At any x in the interval there is a set $\mathcal{E}(x) \subseteq \{1, \dots, t(x)-1\}$ of size $O_{\psi,\varepsilon}(x^{401-3\varepsilon/2})$. For every $1 \le r < t(x)$ outside this set and every odd prime $p \le x^{399/2-5\varepsilon}$,*
$$p^{\lceil x^{203} \rceil} M_{p,r}(E_x) = 0.$$

2. *A single set $\mathcal{E}_* \subseteq \{1, \dots, t(V^{3/2})-1\}$ of size $O_{\psi,\varepsilon}(V^{401-3\varepsilon/2})$ works throughout the interval for the fixed cutoff $Y_* = V^{199-7\varepsilon}$. For every $x \in [V, V^{3/2}]$, every $1 \le r < t(x)$ outside $\mathcal{E}_*$, and every odd prime $p \le Y_*$,*
$$p^{\lceil V^{203} \rceil} M_{p,r}(E_x) = 0.$$

Both statements include the primes dividing the field degree or conductor. In each statement the sum of the full logarithmic orders over the indicated pairs is $o(\exp(x^{\varepsilon}/2))$, uniformly on the intervals.

Proof. We record the finite counting estimate first. Let the abelian field have degree n, modulus N, and twist cutoff t. For $p \nmid nN$, take $k \in [2, p]$ with $k \equiv -r \bmod (p-1)$. Let $J_k(E)$ be the product, over rational conjugacy orbits of characters α of parity $(-1)^k$, of the absolute norms of the numerator ideals of $B_{k,\bar{\alpha}}/k$ in the character value fields. Each conjugate contributes its positive p-adic valuation to $v_p(J_k(E))$. At each nontrivial residual character the finite Stickelberger annihilator has a bounded p-adic interpolation whose value at $1-k$ has this character's own valuation v. Interpolation at $2v+1$ distinct twists shows that at most $2v$ twists in its class escape the exponent bound $(1 + 2\lfloor \log_p t \rfloor)v$. The case $v = 0$ gives vanishing on the whole residue class. Summing over the primes uses $\sum_p v_p(J_k(E)) \log p = \log J_k(E)$ only once at each weight. The interpolation, the numerator formula, and the bound $\log J_k(E) \ll nk \log(2Nk)$ are proved in Lemma 25.18 and Theorems 25.19–25.20.

At an odd $p \mid nN$ use Corollary 25.13 on the p-Sylow subgroup and its prime-to-p complement. Summing the orbit bound (25.10) over at most $p-1$ residue classes gives at most $Cnp^2 \log(2Np)/\log p$ exceptional twists. The exponent outside these twists is bounded as in the proof of Theorem 20.9. Consequently for any $Y \ge 3$ the union $\mathcal{E}$ for all odd $p \le Y$ satisfies
$$|\mathcal{E}| \ll (1 + \omega(nN))\, nY^2 \log(2NY), \qquad p^{\lceil L \rceil} M_{p,r}(E) = 0$$
for $2 < p \le Y$ prime and $1 \le r < t$ outside $\mathcal{E}$. Here $\omega(m)$ counts the distinct prime factors of m and
$$L = CnY \log(2NY)(1 + \log(2t)).$$
Indeed the unramified sum of weighted counts uses (25.17) in Volume V, and each of the at most $\omega(nN)$ other primes costs at most $CnY^2 \log(2NY)$. Dividing an individual weighted count by $\log p > 1$ can only reduce it. The estimates for L include the scalar losses at the primes dividing n, bounded by $2(1 + \log_p n + \log_p t)$ in Theorem 20.9.

On our fields $n \ll_{\psi} x^{2+8\varepsilon}$, and the odd prime factors of nN divide the fixed conductor or order of ψ, or are one of q, d_0. In particular $\omega(nN) = O_{\psi}(1)$. Take the intervals of Lemma 19.12, with the fixed initial delay required in Theorem 20.13. They give $\log(2Nx^{401}) \ll_{\psi,\varepsilon} x^{\varepsilon/2}$; the same bound holds with V on the right at the largest level on $[V, V^{3/2}]$. For the latter assertion the quadratics are fixed on the interval, and the dyadic modulus is polynomial in V. More explicitly their log conductor is $O_{\psi,\varepsilon}(Y_0^{\varepsilon/5} \log^2(2Y_0))$ at the initial scale $Y_0 \le V$. Substituting $Y = x^{399/2-5\varepsilon}$ gives
$$nY^2 \log(2NY) \ll_{\psi,\varepsilon} x^{2+8\varepsilon+399-10\varepsilon+\varepsilon/2} = x^{401-3\varepsilon/2}.$$
Since $\log(2t) \ll_{\varepsilon} x^{\varepsilon/2}$ and $\varepsilon < 1/52$, one also has $L < x^{203}$ eventually. This proves the first assertion.

For the second, let E_* be the field at the largest dyadic level used anywhere on the interval, with the same K_ψ and the same two quadratic fields as before. Its degree is $O_\psi(V^{3+12\varepsilon})$. Every E_x embeds in E_* with relative degree a power of two. Use the finite counting estimate only once, for E_*, $t = t(V^{3/2})$, and $Y = Y_*$. The exponent for the number of exceptions is now

$$3 + 12\varepsilon + 2(199 - 7\varepsilon) + \varepsilon/2 = 401 - 3\varepsilon/2,$$

and for L the exponent is at most $202 + 6\varepsilon < 203$. Restriction carries strict classes to strict classes and commutes with complex conjugation. Corestriction after restriction is multiplication by $[E_* : E_x]$, a unit at every odd p. Hence the bound on $M_{p,r}(E_*)$ holds on $M_{p,r}(E_x)$ for every x, with exactly the chosen set of twists.

Finally a finite abelian p-group killed by p^a has logarithmic order at most a times the logarithmic order of its subgroup killed by p, by its elementary divisors. Lemma 19.18 bounds the latter here by $Cnp\log(2Np)$. In both ranges a, n, p, t, the number of primes, and $\log(2Np)$ are bounded by fixed powers of x. Their product is $o(\exp(x^\varepsilon/2))$, uniformly as V tends to infinity. □

Corollary 20.16 (Divisibility required of a surviving term)**.** *Write $\mathcal{D}_{p,r} = p^{k_{p,r}}(1 - e'_r)Q_{p,r}$ for the group on the right side of (20.12). All the pairs covered by either exponent bound of Theorem 20.15 have $\mathcal{D}_{p,r} = 0$. Moreover fix $A > 0$. Uniformly for sufficiently large x on the same intervals, if $p \nmid 2nN$ and $\mathcal{D}_{p,r} \neq 0$, then*

$$p^{1+v_p(r+k)} \mid J_k(E_x) \quad \text{for every integer } 2 \le k \le x^A \text{ with } p - 1 \mid r + k.$$

Proof. On the polynomial prime ranges of the theorem, Theorem 19.19 gives $k_{p,r} \ge \lfloor x^{-420} \exp(x^\varepsilon/3)\rfloor > \lceil x^{203}\rceil$ eventually. Each group before multiplication by $p^{k_{p,r}}$ is a summand of $M_{p,r}(E_x)$. This proves the first assertion. For the second, any k in the stated congruence gives $p \le t(x) + x^A + 1$, so the same lower bound on $k_{p,r}$ applies. Also $w = v_p(J_k(E_x)) \ll nk\log(2Nk)/\log p$ is polynomially bounded in x, hence eventually smaller than $k_{p,r}$. If $w < 1 + v_p(r + k)$, Theorem 25.19, gives $p^w M_{p,r}(E_x) = 0$, contradicting $\mathcal{D}_{p,r} \neq 0$. □

For example, at $E = \mathbb{Q}$ the numerator for $k = 2$ is one. The comparison therefore kills the rational p-primary summand at every positive even twist $r \equiv -2 \bmod (p - 1)$. The six rational residue classes and an imaginary quadratic example are computed in Corollary 25.21. In (20.12) a single surviving group can have large order. The exceptional-set count gives no bound for its full order, and if $p - 1 > r + x^A$ the divisibility test has no weight in its stated range. The estimate for the total of those remaining orders and the arithmetic lower bound for the designated Bessel pairing in Corollary 83.7 are still needed on the same interval.

20.10 Full orders at primes dividing the degree or conductor

Keep the fields E_x, the enclosing field E_*, and the integers $J_k(E_*)$ of Theorem 21.2. There are two reasons to track the character values integrally. The field conductor can be divisible by the coefficient prime, and at a divisor of the degree the character projectors can have denominators. The two losses are measured differently in the following result.

Theorem 20.17 (Full strict orders on the classes detected by a Bernoulli value)**.** *Fix $A > 0$. On the common intervals of Theorem 20.15 let $1 \le r < t(x)$, let p be any odd prime, and put $o = [K_\psi : \mathbb{Q}]$. Say that the pair (p, r) satisfies the following condition if for some integer $2 \le k \le V^A$ one has*

$$p - 1 \mid r + k, \qquad w = v_p(J_k(E_*)) < 1 + v_p(r + k).$$

Write $M = M_{p,r}(E_x)$ and $e_0 = |H_0|^{-1}\sum_{h\in H_0} h$, where $H_0 = \mathrm{Gal}(E_x/K_\psi C_J)$ has order four. For all sufficiently large V, every such pair satisfies

$$\begin{cases} p^w M = 0, & p \nmid o, \\ p^{w+v_p(o)}(1-e_0)M = 0, & p \mid o. \end{cases}$$

Uniformly for $x \in [V, V^{3/2}]$, the sum of the full $\log|M_{p,r}(E_x)|$ over all pairs satisfying the condition is $o(\exp(x^\varepsilon/2))$, counting each pair once.

Proof. The index $[E_x : K_\psi]$ is a power of two, so $v_p([E_x:\mathbb{Q}]) = v_p(o)$. In the comparison of Lemma 25.22, use all characters if $p \nmid o$, and project by $1-e_0$ if $p \mid o$. For such a divisor of the fixed integer o, we have $p \neq q, d_0$ for sufficiently large V. The inertia elements at q, d_0 generate H_0. Indeed $K_\psi C_J$ is unramified at both primes, and each of the two independent quadratic adjunctions ramifies at its own prime only among this pair. A character receiving a nonzero image from $1-e_0$ is nontrivial on one of these two involutions. Its reduction still takes the value -1 there, and the cyclotomic character is unramified there. Thus $\bar\alpha^{-1}\bar\kappa_p^{-r} \neq 1$. If $p \nmid o$, a character with trivial residual coefficient has a zero strict group by Theorem 24.6. In this case the character values can be taken in an unramified extension, since their orders are prime to p.

For every other participating character write $z = B_{k,\alpha^{-1}}/k$. Inflating the character along $\mathrm{Gal}(E_*/\mathbb{Q}) \to \mathrm{Gal}(E_x/\mathbb{Q})$ preserves its primitive character and its value z. Equation (25.16) therefore gives $v_p(z) \le w$. Theorem 25.23 also gives $v_p(z) \ge 0$, identifies it with $v_p(F(X_{1-k}))$, and supplies the annihilator $F(X_{r+1})$. An integral power series has $F(u)-F(v) \in (u-v)O$ when $u, v \in pO$, by subtracting monomials and passing to the limit. The valuation of $X_{r+1} - X_{1-k}$ is $1 + v_p(r+k)$ for $X_s = (1+p)^s - 1$. It follows that $v_p(F(X_{r+1})) = v_p(z) \le w$. Thus p^w kills this scalar group even in a ramified coefficient ring, since the scalar divides p^w there. The integral comparison proves both exponent assertions.

For the sum, a subgroup killed by p^a has logarithmic order at most $a\log|M[p]|$, by its cyclic decomposition. Lemma 19.18 bounds the latter logarithm by $C[E_x:\mathbb{Q}]p\log(2N_*p)$. All primes occurring here satisfy $p \le t_* + V^A + 1$, and all admissible w are at most $1+\log_3(t_*+V^A+1)$. The number of pairs is at most $t_*(t_*+V^A+1)$. These bounds, $[E_x:\mathbb{Q}]$, and $\log(2N_*)$ are polynomial in V for fixed A, ψ, ε. This accounts for all the stated exponent bounds simultaneously. For the finitely many primes dividing o, the remaining direct summand is $e_0 M$. Theorem 20.11 bounds the sum of its full logarithmic orders over these primes and *all* twists by $\exp(x^{2\varepsilon/3})$. The intervals of Lemma 19.12 retain precisely the growing odd-prime bound used there. Both the polynomial and this last bound are $o(\exp(x^\varepsilon/2))$, uniformly as claimed. □

Theorem 20.18 (A common divisor for all odd coefficient primes)**.** *Define $\mathcal{B}_p$ as in Theorem 21.2, now for each odd prime. For every fixed $A > 0$ and all sufficiently large V, simultaneously for every $2 \le k \le V^A$,*

$$\prod_{p \text{ odd prime}} \prod_{\substack{r\in\mathcal{B}_p \\ p-1\mid r+k}} p^{1+v_p(r+k)} \;\mid\; J_k(E_*).$$

The twists in $\mathcal{B}_p$ are counted once each on the entire interval, even when the corresponding strict groups survive at several fields.

Proof. Fix p, k with a factor in the product. For each participating twist choose a witnessing x, and put $d = k_{p,r}(x)$. As in Theorem 21.2, $p \le t_* + V^A + 1$ and $d \ge \lfloor x^{-420}\exp(x^\varepsilon/3)\rfloor$. A surviving group gives an element of $M_{p,r}(E_x)$ of order at least p^{d+1}. If $p \mid o$, the invariant summand satisfies $\log|e_0 M_{p,r}(E_x)| \le \exp(x^{2\varepsilon/3}) < d\log p$ by Theorem 20.11. It is therefore

already killed by p^d. The component of the element in $(1-e_0)M_{p,r}(E_x)$ still has order at least p^{d+1}.

The first comparison map of Lemma 25.22 sends this element, after extending scalars, to a tuple with some coordinate of order at least $p^{d+1-v_p(o)}$. Indeed its composite with the return map is multiplication by $[E_x:\mathbb{Q}]$. The map $m \mapsto m \otimes 1$ preserves orders since 1 belongs to a $\mathbb{Z}_p$-basis of O. The chosen scalar character has nontrivial residual coefficient by the proof of Theorem 20.17. Regard it as a character of E_*. The scalar group over $\mathbb{Q}$, its integral annihilator, and its negative special value depend only on this character, p and the indicated twist or residue class. Thus witnesses on different fields can be assigned to the same character.

For each fixed character occurring in this assignment, use its single series F from Theorem 25.23. An annihilator of an element of additive order at least $p^{d+1-v_p(o)}$ has valuation strictly greater than $d - v_p(o)$, including when O is ramified. At the nodes X_{r+1} these lower bounds exceed $t_*(1+\log_3(t_*+V^A+1))$, uniformly for large V. Any two different nodes in this set enlarged by X_{1-k} have difference of valuation at most $1+\log_3(t_*+V^A+1)$. Lemma 21.1 applies also in ramified O because division by a monic linear polynomial at a point of pO has integral quotient, and its Lagrange interpolation inequality uses only the normalized valuation. Consequently $v_p(F(X_{1-k}))$ is at least the sum of $1+v_p(r+k)$ over all the twists assigned to this character. It equals $v_p(B_{k,\alpha^{-1}}/k)$ by the unit formula of Theorem 25.23. Summing over the characters in equation (25.16) and multiplying over the finitely many participating primes proves the assertion. □

For a pair failing the strict inequality of Theorem 20.17, the higher finite differences in Proposition 25.24 can still bound the full scalar group. An example is given in its Corollary 25.25. A uniform bound for the surviving full orders in (20.12) and the comparison with the designated integral theta period remain necessary for Main Theorem 1.1.

20.11 Endpoint bounds on the same fields as the period

Theorem 20.19 (Full invariant orders up to a logarithmic endpoint)**.** *Use the polynomial modulus of Theorem 19.15. For every $a>0$ there is $c_a>0$, depending also on ψ,ε, for which the following holds. At each $1\le r<t(x)$ take the largest $0\le j\le J$ satisfying*

$$[2^j(r+2)]^5 \le c_a\,\frac{x^{\varepsilon}}{\log(2x)}.$$

Let $e(r)$ project to the classes coming from $L_j=K_\psi C_j(\sqrt{-q},\sqrt{-d_0})$, with $e(r)=0$ when the index does not exist. Then, uniformly on the interval,

$$\sum_{r<t(x),\ r\ge 1}\ \sum_{p\ \text{odd prime}} \log\lvert e(r)\mathcal{S}_{p,r}(E_x)\rvert = o\big(\exp(ax^{\varepsilon})\big).$$

Under the cell estimate in the second part of Theorem 20.2, one may replace the left side of the index condition by $2^j(r+2)^2$. Both conclusions include the full primary orders on both conjugation signs.

Proof. The extension E_x/L_j has two-power degree. At each odd prime restriction identifies the strict group of L_j with the invariants in E_x, by the global and local descent of Theorem 19.13. In either cell bound use $d=[L_j:\mathbb{Q}]\le 4o\,2^j$, $o=[K_\psi:\mathbb{Q}]$, and the modulus $N_x\le x^D$. Then $\log(2N_x d(r+2))\le C_1\log(2x)$, uniformly for all $r<x^{401}$. In the first bound the logarithm is multiplied by at most $C_2[2^j(r+2)]^5$. In the second it is multiplied by at most $C_2 2^j(r+2)^2$. Choose c_a to make either exponent at most $ax^{\varepsilon}/2$. Summing the resulting bounds on logarithmic orders costs at most x^{401}, and $x^{401}\exp(-ax^{\varepsilon}/2)\to 0$. □

Corollary 20.20 (One exceptional set at the enlarged coefficient cutoff)**.** *For every fixed $B > 0$ put*

$$Y_* = \frac{V^{199-6\varepsilon}}{(\log(2V))^{(B+1)/2}}.$$

There is one set of $O_{\psi,\varepsilon,B}(V^{401}/(\log(2V))^B)$ twists for the whole interval of Theorem 19.15. For every $x \in [V, V^{3/2}]$, every $1 \le r < t(x)$ outside this set and every odd prime $p \le Y_*$, the full complementary group $M_{p,r}(E_x)$ is killed by $p^{\lceil V^{203} \rceil}$. The sum of its logarithmic orders over these prime–twist pairs is $o(\exp(x^\varepsilon/2))$.

Proof. All E_x embed with two-power index in the largest field E_*. Its degree satisfies $n_* \ll_\psi V^{3+12\varepsilon}$, its modulus $N_* \le V^{3D/2}$, and $\omega(n_*N_*) \ll_\psi 1$, since only the two auxiliary primes and fixed prime divisors of $2oF$ can occur. Apply the finite counting estimate in the proof of Theorem 20.15 at this one field with $t_* = \lfloor V^{1203/2} \rfloor$. Its bound on the number of exceptional twists is $O_\psi(n_*Y_*^2 \log(2N_*Y_*))$. The exponent of V here is $3+12\varepsilon+2(199-6\varepsilon) = 401$, and the logarithm contributes at most one of the $B+1$ powers in the denominator. The bound on the exponent of the group is $p^{\lceil L \rceil}$ with $L \ll n_*Y_* \log(2N_*Y_*)(1+\log(2t_*))$. Since $202 + 6\varepsilon < 203$, this gives the asserted exponent. Restriction to E_* is injective at odd p, so the same list works for every E_x. Lemma 19.18 bounds $\log|M_{p,r}(E_x)[p]|$ by $Cn_*p\log(2N_*p)$. Multiplying by the exponent in powers of p and summing costs only a polynomial in V. This proves the order estimate. □

21 Residue data and exceptional twists

21.1 Several twists in the same Bernoulli numerator

Corollary 20.16 tests one surviving twist at a time. On a whole interval one can charge different twists to the same numerator, retaining their multiplicities. We first give the interpolation fact that permits this addition.

Lemma 21.1 (Simultaneous divisibility of an interpolated value)**.** *Let O be the integers of a finite unramified extension of $\mathbb{Q}_p$, with $v(p) = 1$, and let $F(X) \in O[[X]]$. Take distinct $a_0, a_1, \dots, a_m \in pO$. If, for each $i \ge 1$,*

$$v(F(a_i)) \;\ge\; v(a_0 - a_i) + \sum_{\substack{1 \le j \le m \\ j \ne i}} v(a_i - a_j),$$

then $v(F(a_0)) \ge \sum_{i=1}^m v(a_0 - a_i)$.

Proof. For $a \in pO$, the difference $F(X) - F(a)$ is divisible by $X - a$ in $O[[X]]$. Indeed for a monomial of degree n the quotient is $\sum_{j=0}^{n-1} X^j a^{n-1-j}$, and the sum defining each coefficient converges in O. Successive divisions give $F = R + H\prod_{i=1}^m (X - a_i)$, with $H \in O[[X]]$, $R \in O[X]$ and $\deg R < m$. For $m = 0$ the assertion is integrality. Otherwise interpolate R at $a_1, \dots, a_m$. At a_0 the term with coefficient $R(a_i) = F(a_i)$ has valuation

$$v(F(a_i)) + \sum_{j \ne i,\, 1 \le j \le m} \big(v(a_0 - a_j) - v(a_i - a_j)\big) \;\ge\; \sum_{j=1}^m v(a_0 - a_j).$$

The term involving $H(a_0)$ satisfies the same bound. □

Theorem 21.2 (One divisor for all surviving twists on an interval)**.** *Use the fields and intervals of Theorem 20.15. Let E_* be the largest field used on $[V, V^{3/2}]$, of degree n_* and modulus*

N_*, and put $t_* = t(V^{3/2}) = \lfloor V^{1203/2} \rfloor$. For each odd prime $p \nmid n_* N_*$, let $\mathcal{B}_p$ consist of the integers r for which some x on this interval has $1 \le r < t(x)$ and $\mathcal{D}_{p,r}(E_x) \neq 0$, with $\mathcal{D}_{p,r}$ as in Corollary 20.16. Fix $A > 0$. For sufficiently large V, simultaneously for every integer $2 \le k \le V^A$, one has the integer divisibility

$$\prod_{p \nmid 2 n_* N_*} \prod_{\substack{r \in \mathcal{B}_p \\ p-1 \mid r+k}} p^{\,1+v_p(r+k)} \;\mid\; J_k(E_*).$$

The outer product is over primes. The integer on the right is the product of the absolute norms of the numerator ideals of $B_{k,\bar\alpha}/k$, one per rational orbit of characters of E_* of parity $(-1)^k$.

Proof. Fix k, p with a factor on the left. Then $p \le t_* + V^A + 1$. At every witnessing x, restriction to E_* is injective on the strict group $M_{p,r}$. The local conditions and conjugation sign commute with restriction, and the composite of restriction with corestriction is multiplication by the power of two $[E_* : E_x]$. Nonvanishing of the stated image of $M_{p,r}(E_x)$ implies that $M_{p,r}(E_*)$ has an element of order at least $p^{k_{p,r}(x)+1}$. Theorem 19.19 gives $k_{p,r}(x) \ge \lfloor x^{-420} \exp(x^{\varepsilon}/3) \rfloor$, since this polynomial prime bound is eventually below $\exp(x^{\varepsilon}/12)$ throughout the interval. This lower bound exceeds $t_*(1 + \log_3(t_* + V^A + 1))$, uniformly in the chosen k, p, r, x.

Extend scalars to an unramified coefficient ring O containing all character values of $\mathrm{Gal}(E_*/\mathbb{Q})$. The idempotents are integral because $p \nmid n_*$. For each such r choose a character α whose component has an element of order at least $p^{k_{p,r}(x)+1}$. Such a component exists by faithful flatness and the direct sum decomposition. It has $\alpha(c) = (-1)^k$ and a nontrivial residual coefficient character by Lemma 25.18. Group the chosen twists by α.

For one such group take the bounded measure of that lemma with $\chi = \bar\alpha$ and $h = 1 - k \bmod (p-1)$. Its auxiliary integer can be fixed for the entire group since the residual character is fixed. The integral $A_b(s)$ annihilates the component at $s = r+1$, and at $s = 1-k$ it equals a p-adic unit times $B_{k,\bar\alpha}/k$. To apply the lemma above, put $X_s = (1+p)^s - 1$. There is one $F \in O[[X]]$ with $A_b(s) = F(X_s)$ on $\mathbb{Z}_p$. Indeed $\langle a \rangle = (1+p)^{u(a)}$ with $u(a) \in \mathbb{Z}_p$, since p is odd. In the integral of Lemma 25.18, expand the factor $\langle a \rangle^{-s}$ as $\sum_{j \ge 0} \binom{-u(a)}{j} X_s^j$. Each binomial coefficient is integral by continuity from nonnegative integers. The remaining character factors are units. Termwise integration is valid by uniform convergence on pO, and all coefficients of the resulting series are integral.

Take $a_0 = X_{1-k}$ and take the other nodes to be X_{r+1} for the distinct twists of this group. For distinct integers u, v one has $v_p(X_u - X_v) = 1 + v_p(u-v)$. In fact $(1+p)^h - 1$ has valuation one for $p \nmid h$, and taking the p-th power increases the valuation by one by binomial expansion. Inversion handles negative differences. There are fewer than t_* nodes besides a_0, and the integer differences have size at most $t_* + V^A + 1$. The order of the chosen element forces the annihilator at each of these nodes to have valuation at least $k_{p,r}(x) + 1$. The hypotheses of Lemma 21.1 therefore hold. It gives

$$v_p(B_{k,\bar\alpha}/k) \;\ge \sum_{r \text{ assigned to } \alpha} (1 + v_p(r+k)).$$

By the factorization of numerator ideals, the sum of the positive valuations over all embedded characters of the given parity is exactly $v_p(J_k(E_*))$. This is equation (25.16). Summing the last inequality and then multiplying over primes gives the claim. The bound on p makes the product finite. □

For example, at $k = 2$ the sum of $(1 + v_p(r+2)) \log p$ over the participating prime–twist pairs on the entire interval is at most $\log J_2(E_*)$, which is $O(n_* \log(2N_*))$ by Theorem 25.19. A pair

with $p-1 > r + V^A$ occurs in none of these products. For pairs that do occur, bounding the full logarithmic orders in (20.12) still requires control of their exponents beyond the sampled depth.

21.2 Frobenius orbits in the exceptional twist count

Work on one polynomial-conductor interval of Theorem 19.15. Write E_* for its largest field, N_* for its modulus, and $t_* = \lfloor V^{1203/2} \rfloor$. In particular $\log(2N_*) \ll_{\psi,\varepsilon} \log(2V)$. For a character α of $\mathrm{Gal}(E_*/\mathbb{Q})$ put $j(\alpha) = v_2(\operatorname{ord}\alpha)$. Write $J_{k,j}$ for the portion of the integer $J_k(E_*)$ in Theorem 25.19, obtained by using only rational character orbits of index $j(\alpha) = j$. The parity condition $\alpha(-1) = (-1)^k$ is retained.

Lemma 21.3 (A numerator for a fixed dyadic character order)**.** *For $k \geq 2$ one has $\log J_{k,j} \ll_\psi 2^j k \log(2N_*k)$. If p is an odd prime away from the field degree and modulus and $w(p) = \max(v_2(p-1), v_2(p+1))$, the orbit of such a character under $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ has size at least $\max(1, 2^{j-w(p)})$.*

Proof. The characters of the compositum are products of characters of its factors. Indeed a character of a subgroup of a finite abelian group extends to the group, by taking a root of its prescribed value when adjoining each generator. The factors other than the real cyclotomic tower give at most $4\operatorname{ord}(\psi)$ choices, all of bounded order. The tower factor is cyclic of two-power order. Once j exceeds the two-adic exponent of the orders of the other factors, the tower character must have exact order 2^j. For smaller j its order is bounded in terms of ψ. Thus in either case at most $C_\psi 2^j$ characters occur. For each rational orbit the numerator ideal of $B_{k,\bar{\alpha}}/k$ has log norm at most $[\mathbb{Q}(\alpha) : \mathbb{Q}]\, Ck\log(2N_*k)$, by the denominator and complex bounds in the proof of Theorem 25.19. The sum of these degrees counts the characters in the layer. This proves the first assertion.

The values generate the roots of unity of order $\operatorname{ord}\alpha$, prime to p. Frobenius raises them to the p-th power. If its orbit has size h, then $2^j \mid p^h - 1$. For odd h the two-adic valuation is $v_2(p-1)$. For even h it is $w(p) + v_2(h)$, by factoring successive differences of squares and using $v_2(p^2+1) = 1$. Both cases give the asserted lower bound. □

Theorem 21.4 (A common exceptional set for almost all coefficient primes up to a square-root cutoff)**.** *Fix $B > 0$ and $a > 1$. Put $L = \log(2V)$, $W = \lfloor a \log_2 L \rfloor$, where $\log_2$ denotes logarithm to base two, and set*

$$Y_0 = V^{199-6\varepsilon}/L^{(B+1)/2}, \qquad Y = V^{401/2}/L^{(B+a+1)/2}.$$

There is a single set of $O_{\psi,\varepsilon,a,B}(V^{401}/L^B)$ twists for the whole interval. For every $x \in [V, V^{3/2}]$ and every $1 \leq r < t(x)$ outside this set, the full group $M_{p,r}(E_x)$ is killed by $p^{\lceil V^{203} \rceil}$ at every odd prime $p \leq Y_0$, and also at every $Y_0 < p \leq Y$ with $p \not\equiv \pm 1 \pmod{2^{W+1}}$. The sum of its logarithmic orders over these pairs is $o(\exp(x^\varepsilon/2))$, uniformly in x. At most $O(Y/L^a + 1)$ primes up to Y fall in the two excluded residue classes.

Proof. Start with the exceptional set of Corollary 20.20 for $p \leq Y_0$. Consider an additional prime $Y_0 < p \leq Y$ with $w(p) \leq W$. It is prime to $[E_* : \mathbb{Q}]N_*$ for large V. The primes dividing the degree divide $2\operatorname{ord}(\psi)$. Of those dividing the modulus, only q, d_0 vary, and both exceed V^{401} by the selection in Theorem 19.15. Also $\log p \asymp \log V$ uniformly in this range.

Call (p, r) exceptional here if some x on the interval has $r < t(x)$ and $M_{p,r}(E_x)$ has an element of additive order greater than $p^{\lceil V^{202} \rceil}$. Restriction to E_* preserves its order since corestriction composed with restriction is multiplication by a power of two. Over the unramified coefficient

ring containing the character values, the integral idempotents split the strict group. Some scalar component has an element of order exceeding the same threshold. Its residual coefficient character is nontrivial by Lemma 25.18. Every local Frobenius conjugate has an element of the same order, since conjugating coefficients sends the cochains, local restrictions and cocycles to those for the conjugate character. Assign r to every character of one such orbit, once for this (p, r), and put $k \in [2, p]$ for the unique integer congruent to $-r$ mod $(p-1)$.

Fix p, k, α in this assignment, with $j = j(\alpha)$, and set $h = v_p(B_{k,\bar{\alpha}}/k)$, with $v_p(p) = 1$. This is a nonnegative integer by the integral interpolation formula and unramifiedness. Every member of the Frobenius orbit contributes the same h to $v_p(J_{k,j})$, by the norm factorization in equation (25.16), restricted to this layer. Hence the lemma and the bound on N_* give

$$h \le \frac{\log J_{k,j}}{\max(1, 2^{j-W}) \log p} \ll_{\psi,\varepsilon} 2^W Y.$$

In particular $h + 1 = O(V^{201})$ for sufficiently large V. There can be at most h distinct twists assigned to this character at this k. To see this, assume there are $h + 1$ and use their nodes $X_{r+1} = (1 + p)^{r+1} - 1$ and the comparison node X_{1-k}. Lemma 25.18, and the power-series construction in Theorem 21.2 give one integral series for this whole branch. Its value at the comparison node has valuation h. At every other node its value annihilates a scalar element of the stated order, hence has valuation greater than V^{202}. The valuation of a difference of distinct nodes is at most $1 + \log(t_* + Y + 1)/\log p = O(1)$, by the binomial valuation formula. Lemma 21.1 applies since the sum of at most $h + 1$ such valuations is less than V^{202}. It forces the comparison value to have valuation at least $h + 1$, a contradiction.

For fixed p, k, j, summing over characters therefore counts the assigned twists with their orbit sizes and gives at most $v_p(J_{k,j})$. Each pair assigned to layer j consumes at least $\max(1, 2^{j-W})$ of this count. Multiply by $\log p$, sum over the primes and use integer factorization. The number of additional pairs is bounded by

$$\frac{C}{\log V} \sum_j \frac{1}{\max(1, 2^{j-W})} \sum_{2 \le k \le Y} \log J_{k,j} \ll_{\psi,\varepsilon} (1 + \log V) 2^W Y^2.$$

Indeed there are $O_\psi(1 + \log V)$ layers by the degree bound, and $\log(2N_* Y) = O_{\psi,\varepsilon}(\log V)$. The definition of Y makes the last expression $O(V^{401}/L^B)$. Adding the twist from each such pair to the first set proves the uniform exponent bound. By Lemma 19.18 the logarithm of the subgroup killed by p is $O([E_* : \mathbb{Q}]p \log(2N_* p))$. Multiplication by the exponent in powers of p bounds the full logarithmic order by a polynomial in V, as does the number of pairs. This gives the claimed uniform little-oh. Each omitted residue class contains at most $1 + Y/2^{W+1}$ integers in the range. Since $a > 1$, these primes form a vanishing fraction of the primes up to Y, by the elementary lower bound $\pi(Y) \gg Y/\log Y$. □

For every pair covered by the theorem the depth in Theorem 19.19 exceeds $\lceil V^{203} \rceil$ for large V. Its term in (20.12) is therefore zero. An exceptional twist may still carry a large order.

21.3 Common coefficient primes for the cohomology and the Gram minors

Theorem 21.5 (Placing the auxiliary norm primes beyond the coefficient range)**.** *Fix $A > 0$ and an interval of Theorems 19.15 and 21.4. For each distinct period field in the interval the two split representatives $\mathfrak{p}, \mathfrak{q}$ allowed by Lemma 72.18, can be chosen above distinct rational primes exceeding $\exp(x^A)$ for every x in the interval. Their logarithmic norms are still bounded by a fixed power of x. The single additional prime in Theorem 94.15, can be placed above the same range, with its polynomial logarithmic bound for polynomial test depths.*

Use these choices in Corollary 94.19. At every rational coefficient prime $l \le \exp(x^A)$, every place $\mathfrak{l} \mid l$ of its coefficient field containing $F = E_x^+$, and $v = \mathfrak{l} \cap F$, the correction for a nonzero minor is

$$v_{\mathfrak{l}}(\det G_{I,J}) - v_{\mathfrak{l}}(\det G'_{I,J}) = \frac{e(\mathfrak{l}/v)}{2}\, v(\mathfrak{d}_F \mathfrak{a}_0^{-1}) \sum_{\tau} \left(\sum_{c \in I} D_{\tau,c} + \sum_{c \in J} D_{\tau,c} \right).$$

It is nonnegative and is zero when $l \nmid 2F_\psi q$, where F_ψ is the fixed character conductor. In particular, up to the cutoff Y of Theorem 21.4, every $l \nmid 2F_\psi$ has identical Gram-minor valuations. On the primes and twists covered by that theorem the corresponding cohomology orders have its uniform bound on these same fields.

Proof. We give the prime selection. Let $K/\mathbb{Q}$ be one of the fields F, E_x, let $d = [K : \mathbb{Q}]$, and fix a class in a narrow or ordinary ray class field of K, of finite modulus $\mathfrak{m}$. Take an odd rational prime s unramified in K and prime to the modulus. Every completion of K at s is unramified over $\mathbb{Q}_s$, whereas $\mathbb{Q}_s(\zeta_{s^b})$ is totally ramified of degree $\varphi(s^b)$. Thus $K(\zeta_{s^b})/K$ has this degree both globally and on inertia at any such place. Every nontrivial subextension ramifies there. The ray class field is unramified there, so the two fields intersect in K. Prescribe the desired ray class in the first and the identity in the second. For a lower cutoff $H \ge 2$, take b least with $s^b > H$. The abelian least-prime theorem of Thorner and Zaman gives a prime of absolute prime norm l in this class. Its cyclotomic Frobenius sends a root of unity to its l-th power, so $l \equiv 1 \pmod{s^b}$ and $l > H$. Its bound in logarithmic form is

$$\log l \ll 1 + \log |D_K| + \log N_{K/\mathbb{Q}}\mathfrak{m} + d \log(sH) + d \log(2d).$$

Indeed the largest conductor norm in this abelian compositum is at most $(N_{K/\mathbb{Q}}\mathfrak{m})s^{bd}$ by the norm calculation in Theorem 94.15. This argument works with the infinite real places included in the class modulus.

All original rational levels, including every terminal prime on the interval, have logarithms bounded by fixed powers of V, by Theorem 19.15 and Lemma 87.1. Start with $H = \exp(V^{B_0})$, choosing the fixed B_0 so that H exceeds these levels and $\exp(x^A)$ throughout. Over F apply the construction with finite modulus one to the narrow classes of $\mathfrak{d}_F$ and $\mathfrak{a}_0$, increasing H to the first prime before selecting the second. These classes have trivial character in E_x/F by Lemma 72.18, so their representatives are split. The same choice works whenever this period field occurs on the interval. For the last prime use the class of the ideal denoted by A in Theorem 94.15, now over E_x, and first increase H to exceed every rational prime in the specified test support. The number of rational prime divisors of the period modulus and the prescribed levels is bounded in terms of ψ. Thus s can in each case be chosen from a bounded list of primes. The degree, log discriminant, and the logarithm of every cutoff used here are polynomially bounded for the indicated depths, by the displayed estimate successively. The avoidance of all primes under the modulus also ensures the ray prime is coprime to it.

Finally $(u) = \mathfrak{d}_F \mathfrak{a}_0^{-1}/(\mathfrak{p}\mathfrak{q})$. Its numerator is Galois invariant: the different is invariant, and $\mathfrak{a}_0^2 = (d_0)$ uniquely determines the ideal $\mathfrak{a}_0$. All conjugates of the denominator are away from l in the asserted range. Consequently $v_{\mathfrak{l}}(\tau u) = e(\mathfrak{l}/v)\, v(\mathfrak{d}_F \mathfrak{a}_0^{-1})$ for every embedding τ, using the Galois group of the totally real field to identify its embeddings. Substitute this constant into the Gram-minor formula. Integrality and the support above $2F_\psi q$ were proved in Theorem 110.18. Since $q > V^{401} > Y$, only the fixed divisors of $2F_\psi$ can contribute below Y. Selecting the three split ideals changes no number field or strict local condition in the proof of Theorem 21.4. □

The comparison concerns the minors of the projected vectors. A lower bound for the designated signed period itself and the orders at the remaining exceptional twists are still needed for Main Theorem 1.1.

21.4 A test on the common interval and the prime 37

Theorem 21.6 (Testing the whole interval at a fixed conductor)**.** *Use a polynomial-conductor interval $[V, V^{3/2}]$ of Theorem 19.15, with largest field E_*, degree n_*, and modulus N_*. Fix $B > 0$ and set $H = \lceil V^{203} \rceil$. For each odd $p \le V^B$ with $p \nmid n_* N_*$, and each primitive character α of the Galois group of E_*, form the polynomial of Theorem 21.18 on each nontrivial residual branch of the appropriate parity. One polynomial tests all positive twists in that branch in every field of the interval on which α factors. At r, call its component detected when $P(X_{r+1}) \not\equiv 0 \bmod p^{H+v_p(H!)}O$.*

If every participating character of E_x at (p, r) is detected or has trivial residual coefficient, the whole strict group $M_{p,r}(E_x)$ is killed by $p^{H+v_p(H!)}$. Its contribution to (20.12) is zero. The sum of the full logarithmic orders of the groups satisfying this test is $o(\exp(x^\varepsilon/2))$ uniformly for $x \in [V, V^{3/2}]$. For a pair at which only some components are detected, each such component separately contributes zero to the remaining group after multiplication by $p^{k_{p,r}}$.

Proof. Take $2 \le k \le p$ congruent to $-r \bmod (p-1)$. Inflating a character to the largest field leaves its primitive conductor and all Bernoulli samples unchanged. Its scalar group is the strict group for the same coefficient character over $\mathbb{Q}$. Theorem 21.18 gives the asserted annihilation for each detected component. The trivial residual case has zero strict group by Lemma 25.18. All idempotents are integral here since $p \nmid n_*$. They give a direct sum after extension to the unramified coefficient ring, and faithful flatness descends the exponent when all components pass. The two-power projectors and quotients in (20.12) preserve this decomposition.

For $p \le V^B$, Theorem 19.19 gives $k_{p,r} \ge H + v_p(H!)$ throughout the interval eventually, since its lower bounds in both polynomial-prime ranges dominate every fixed power of x. Thus the asserted terms disappear. Lemma 19.18 bounds $\log |M_{p,r}(E_x)[p]|$ by $C n_* p \log(2N_* p)$. The cyclic decomposition bounds the full logarithmic order by this times $H + v_p(H!)$ on the detected pairs. The number of pairs is at most $V^B \lfloor V^{1203/2} \rfloor$, and n_*, N_* are polynomially bounded in V. The resulting polynomial is $o(\exp(x^\varepsilon/2))$ uniformly. The test itself uses H weights at most pH on each branch, each at the original conductor dividing N_*. □

Proposition 21.7 (An irregular branch with one exceptional class at each depth)**.** *For the rational character at $p = 37$, take $r \equiv 4 \bmod 36$ and $b = 2$. There exists $\xi \in \mathbb{Z}_{37}$ such that the annihilator from Theorem 25.23 has valuation $1 + v_{37}(r - \xi)$ on this branch, with $v_{37}(0) = +\infty$. In particular 37 kills the strict scalar group unless $r \equiv 1048 \bmod 1332$, and 37^2 kills it unless $r \equiv 11704 \bmod 49284$.*

Proof. Put $a_0 = 38^{-31} - 1$, $U = (X - a_0)/37$, and $G(U) = F(a_0 + 37U)/37$. The residual character ω^{32} is nontrivial and $2^{32} \not\equiv 1 \bmod 37$. Write $u_s = (38^s - 1 - a_0)/37$. For reproducibility the first three samples are displayed modulo $37^2 = 1369$:

k_i	32	68	104
u_{1-k_i}	0	186	409
$F(X_{1-k_i})/37$	451	376	745.

The first row of residues is obtained by exponentiating 38 modulo 37^3. For the second, compute $B_0 = 1$ and $B_j = -(j+1)^{-1} \sum_{i<j} \binom{j+1}{i} B_i$. For instance $B_{32} = -7709321041217/510$. Substituting the three values in $2^{1-k_i}(2^{k_i} - 1)(1 - 37^{k_i - 1})B_{k_i}/k_i$ gives $16687, 13912, 27565$ modulo 37^3, respectively.

All coefficients of G are integral, because its constant term is integral by the table and its coefficient of degree $j \ge 1$ is divisible by 37^{j-1}. Modulo 37 it is affine, and its values at $0, 1$ are $7, 6$. Thus its reduction is $7 - U$. The divided difference $(G(u) - G(v))/(u - v)$ is a unit

for all distinct $u, v \in \mathbb{Z}_{37}$, since its reduction is -1. This makes G a bijection at each residue depth, and hence an isometry onto $\mathbb{Z}_{37}$. The distance formula in Theorem 21.18 likewise makes $r \mapsto u_{r+1}$ an isometry of $\mathbb{Z}_{37}$ onto itself. Completeness gives a unique zero ξ of their composite. Its distance from any r gives the claimed valuation.

Here $u_{r+1} \equiv r+32 \bmod 37$, so the first exceptional class is $r \equiv 12 \bmod 37$, or $1048 \bmod 1332$ on the stated branch. To lift once, $u_{1049} \equiv 673 \bmod 1369$. Modulo 1369, G has degree at most two and is determined by the table, whose three nodes have distinct reductions. Quadratic interpolation gives $G(673) \equiv 1073 = 29 \cdot 37$. Increasing $r = 1048$ by $1332t = 36 \cdot 37t$ changes u_{r+1} by $36 \cdot 37t \bmod 1369$, by the binomial expansion, and changes G by $37t \bmod 1369$, since its derivative is $-1 \bmod 37$. Thus $t \equiv 8 \bmod 37$ gives the next exceptional class. This proves both exponent statements. The valuation computed here belongs to an annihilator; at the exceptional twists the order of the group still needs a bound. □

21.5 One set of Frobenius parameters on the whole interval

Corollary 21.8 (Common parameters on the support of strict cohomology)**.** *Fix one sufficiently distant interval $[Y, Y^{3/2}]$ of Theorem 11.9, with its two chosen auxiliary primes. For all x on it consider the large coefficient primes $\ell > \exp(x^{\varepsilon}/12)$, $1 \le r < t(x)$, and the complementary character summands of strict cohomology to which the ordinary rank-three construction applies. Keep those with nonzero strict group. For each resulting marked invariant ring D_i let d_i be the dimension of its special fiber. Put $d_* = \max_i d_i$, taking zero for the empty list. There are d_* distinct rational primes splitting completely in every E_x and in $\mathbb{Q}(i)$, unramified for every ring in the list, with the following property. For each i, its first d_i Frobenius trace differences make D_i a finite module over the power series ring in those d_i parameters over O_i. The same list can be chosen within any set of these split primes of positive upper natural density.*

Proof. The two auxiliary primes are fixed on this interval. The integer index of the real cyclotomic layer and the integer $t(x)$ each take only finitely many values. For each resulting field E and each r, the dual of the odd-primary strict group embeds prime by prime in the corresponding primary part of the finite group $K_{2r}(\mathcal{O}_E)$, by Theorem 25.1. Thus there are only finitely many ℓ for which a strict summand can be nonzero on the whole interval taken as a union. For each such (E, r, ℓ) the character list is finite. Fix the coefficient ring and a marking once per datum, using the same choices whenever the field and the data recur. This gives a finite list of ordinary rings. The compositum of the finitely many fields E_x and $\mathbb{Q}(i)$ is finite and Galois over $\mathbb{Q}$. Its completely split primes have positive natural density by Chebotarev. Deleting the finitely many ramified and coefficient primes preserves that density. Apply Theorem 34.15 to these primes, or to the indicated subset, for all the rings at once. The entries of the list are auxiliary observations of Frobenius at unramified primes. The local conditions on strict cohomology and the level defining the theta period are those for the given E_x throughout. □

For instance, if on every characteristic-ℓ curve through one of these rings the traces at its selected primes satisfied monic polynomial equations over the residue field, their images on the curve would be constant. Finiteness over the selected parameters would then force every element on the curve to be algebraic over the residue field, hence constant. Proposition 34.3 would give $d_i = 0$. Establishing such arithmetic control on the original points, and estimating their integral congruences to the diagonal, are further steps in the bound for (20.12).

21.6 One finite field for the large-prime strict orders

Fix a sufficiently distant common interval $[V, V^{3/2}]$ of Theorem 19.15. Its largest period field is E_*, of degree n_* and modulus N_*, and put $t_* = \lfloor V^{1203/2} \rfloor$. Let $\mathcal{P}$ be the coefficient primes occurring in a nonzero complementary strict group at some x on this interval with $\ell > \exp(x^{\varepsilon}/12)$. Theorem 25.1 gives finite support, since the fields form a finite nested list and $r < t_*$. At every $\ell \in \mathcal{P}$ take the list of (r, α) from these large-prime data. Repeated pairs are included once and one representative suffices from each orbit under residue-field Frobenius. One may include all the other complementary characters and twists of E_* with $1 \le r < t_*$ as well. Write $d_{\ell,r,\alpha}$ for the full O-length of the corresponding strict group, and $b_{\ell,\alpha} = [\mathbb{F}_\ell(\bar{\alpha}) : \mathbb{F}_\ell]$. Every ℓ in the list exceeds $2t_* + 3$ and N_* when V is large, since N_* is polynomial in V.

Theorem 21.9 (Simultaneous recovery of the full large-prime lengths)**.** *For any integers $h_\ell \ge 1$ there is a positive-density set of primes s, split in the original period fields, for which*

$$w_{h_\ell}(D_{s,h_\ell}(\alpha, r)) = \min(h_\ell, d_{\ell,r,\alpha}) \qquad \text{for every listed triple.}$$

The primes can also satisfy every splitting and power-residue condition of Theorem 21.17. In the set of primes split in the common field K defined below, a subset realizing the equalities has relative natural density exactly

$$\prod_{\ell,r,[\alpha]} (1 - \ell^{-b_{\ell,\alpha}}) \;\ge\; (2V)^{-C_{\psi,\varepsilon} n_* t_*}.$$

Here the product is over the distinct residual orbits in the list. In particular one finite field realizes all *large-prime orders throughout this interval if each h_ℓ exceeds the largest length at that prime.*

Proof. Take the cyclotomic field C_0 of Theorem 21.17 enlarged to contain the roots of unity of order $N_* \prod_{\ell \in \mathcal{P}} \ell^{h_\ell}$. As in that theorem, adjoin to C_0 the ℓ-th roots of the rational primes required to be power residues, for every listed ℓ, to form K. It is Galois over $\mathbb{Q}$. Complete splitting in K implies those residue conditions and all the congruences needed in Proposition 9.5. One can omit these radicals when only the moments are required.

For each listed orbit choose a primitive basis class u of Theorem 27.1. Its reduction is nonzero in $H^1(\mathbb{Q}, k_\alpha(\delta))$, where $k_\alpha = \mathbb{F}_\ell(\bar{\alpha})$ and $\delta = \bar{\alpha}\bar{\kappa}_\ell^{r+1}$. Indeed reduction of $H^1(U, T)$ has kernel $\ell H^1(U, T)$. The map to Galois cohomology at finite coefficients is injective in degree one by the low-degree sequence for the generic-point direct image. One may also perform this restriction over $\mathbb{Q}(\zeta_f)$ and take the exact character summand. Choose the conjugate bases for the conjugate characters. Their residual values are related by residue-field Frobenius.

We check that every such residual class remains nonzero on G_K. Over C_0 its coefficient is trivial. In the abelian group $\mathrm{Gal}(C_0/\mathbb{Q})$, conjugation at infinity acts on the coefficient by -1. Evaluating a cocycle at $cg = gc$ shows it is a coboundary, since 2 is invertible. Inflation–restriction therefore gives injectivity on restriction to C_0. The map sending an automorphism over C_0 to its quotients on the chosen radicals embeds $\mathrm{Gal}(K/C_0)$ into a product of groups of roots of unity. Conjugation acts on its ℓ-part by $\bar{\kappa}_\ell$. On inertia at ℓ the exponent of δ is $r+1$, strictly between 1 and $\ell - 1$. Thus no equivariant homomorphism from this radical group can contribute to the kernel of the second restriction. This proves the assertion even with the additional cyclotomic powers in C_0.

On G_K the residual evaluations are additive homomorphisms. Their joint image for a fixed ℓ is the full product of the additive groups k_α. In fact the image is stable under the finite abelian group of the residual character values. It surjects onto each factor, since a nonzero $\mathbb{F}_\ell$-subspace stable under all values of δ is stable under the field they generate. This is k_α, as $\bar{\kappa}_\ell$ has

values in $\mathbb{F}_\ell^\times$. Different r give inequivalent modules already on inertia at ℓ, and for fixed r the inequivalent modules are exactly the different Frobenius orbits of α. The finite group algebra in residue characteristic is semisimple and its central idempotents isolate these simple modules. Primary decomposition gives the full product across different ℓ as well. The joint kernel on G_K is open and normal in $G_{\mathbb{Q}}$. Among its finite quotient over K, the fraction of vectors with every coordinate nonzero is the stated product. These vectors form a conjugacy-stable set over $\mathbb{Q}$, so Chebotarev's theorem gives exactly that relative density among split primes. Theorems 27.1 and 9.5 now give the equalities, also for characters with length zero.

For the uniform lower bound, a prime in $\mathcal{P}$ contributes at least $\log 2$ to the sum of logarithmic strict orders over the twists of E_*. Indeed restriction from E_x is injective because its relative two-power degree is prime to ℓ. The first bound of Theorem 20.2, applied on E_* and summed up to t_*, gives $\#\mathcal{P} \le Z = \exp(V^C)$ for a fixed C. This follows since n_*, N_*, t_* are polynomial in V. The sum of $1/\ell$ over listed primes above Z is at most one. For primes below Z, put $\sigma = 1 + 1/\log Z$. Then $\sum_{\ell \le Z} 1/\ell \le e \log \zeta(\sigma) \le e \log(1 + \log Z)$, by the Euler product and the integral bound for the Dirichlet series. Thus the sum over the whole list is $O_{\psi,\varepsilon}(\log(2V))$. There are at most $n_* t_*$ factors at each ℓ. Taking logarithms and using $-\log(1 - \ell^{-b_{\ell,\alpha}}) \le 2/\ell$ proves the bound. □

There is an absolute size consequence for any test prime. Fix x in the interval and $s \equiv 1 \bmod N_*$. At every large $\ell \mid s-1$ take $h = v_\ell(s-1)$. For all complementary character orbits and twists of E_x whose moments at this precision are nonzero, the sum of their full logarithmic orders is at most

$$[E_x : \mathbb{Q}]\,(t(x) - 1)\log(s-1).$$

Indeed each orbit contributes $b_{\ell,\alpha} d_{\ell,r,\alpha} \log \ell$, and its length is at most h by Proposition 9.5. At each twist the sum of the orbit degrees is at most $[E_x : \mathbb{Q}]$. Now use $\sum_{\ell \mid s-1} v_\ell(s-1) \log \ell = \log(s-1)$. Choosing precisions above all lengths in the theorem gives one prime at which every supported large-prime component is counted. Its nonzero values remain nonzero if one passes to the precision $v_\ell(s-1)$, by compatibility of the cyclotomic class. The density estimate is relative to splitting in K. The size of a prime detecting the full support at these precisions is still uncontrolled on the scale required in (20.12).

21.7 Residue valuations over ramified coefficient rings

Let E_*, N_*, t_* be the largest field, modulus and twist cutoff on an interval of Theorem 19.15. Take any finite set of odd coefficient primes and positive precisions h_p. Let C be an abelian cyclotomic field containing the roots of order $N_* \prod_p p^{h_p}$. One may take $K = C$. More generally, for any of the listed $p > \max(N_*, 2t_* + 3)$, one may adjoin to C the p-th roots of any finite set of nonzero rationals, and let K be the compositum. This permits the power-residue requirements at the auxiliary primes in Theorem 21.17, after enlarging C for its further cyclotomic congruences.

For each prime s split completely in K, character α of E_* of conductor f, and $1 \le r < t_*$ with the complementary parity, choose a generator g of $\mathbb{F}_s^\times$. With $h = h_p$ and $w = g^{(s-1)/(fp^h)}$, set

$$D_j(s) = \sum_{\substack{1 \le a \le fp^h \\ (a, fp) = 1}} \alpha(a) a^r \operatorname{ind}_g(1 - w^a) \mod p^h O_\alpha, \qquad j = (p, r, [\alpha]).$$

The index is the discrete logarithm modulo p^h. For $y \in O_\alpha / p^h O_\alpha$ let $w_\pi(y)$ be the largest $v \le e_\alpha h$ such that y belongs to $\pi^v(O_\alpha / p^h O_\alpha)$. Put $W_j(s) = w_\pi(D_j(s))$.

Proposition 21.10 (The marginal law for every character lattice)**.** *Put $d_j = d_{p,r,\alpha}(N_*)$, and $m_j = \min(d_j, e_\alpha h)$. For $0 \le v \le e_\alpha h$, relative to the primes split in K,*

$$\Pr(W_j(s) \ge v) = p^{-b_\alpha \max(0, v - m_j)}.$$

This holds when several twists have the same residual character and when the character order is divisible by p.

Proof. Take a basis u of $H^1(U_{N_*}, T)$ from Theorem 27.3. Its residual class is nonzero since the kernel of reduction in cohomology is $\pi H^1(U_{N_*}, T)$. The residual module is unramified outside the open set's excluded primes, and inflation from the restricted Galois group to the absolute group is injective in degree one. Restriction to G_C keeps the class nonzero. In fact the abelian quotient $\mathrm{Gal}(C/\mathbb{Q})$ acts on the residual coefficient, and its central complex conjugation acts by -1. Evaluating a cocycle on the two expressions for a product with this central element shows that it is a coboundary on the quotient.

The group over C of the radical extension embeds in the product of the groups of roots of unity by taking quotients on the chosen roots. If no p-radicals are present, its order is prime to p. Otherwise its p-part has global conjugation character $\bar\kappa_p$, since the radicands are rational. The residual coefficient on inertia at this large p is $\bar\kappa_p^{r+1}$, distinct from $\bar\kappa_p$. Thus the kernel of restriction from G_C to G_K cannot contain the restricted class. Indeed such a class would factor as an equivariant additive homomorphism from the radical group into the residual coefficient. This proves nonvanishing on G_K in both cases.

On G_K the integral basis cocycle at precision p^h is an additive homomorphism into $O_\alpha/p^h O_\alpha$, since its coefficient character is trivial there. Its image is an ideal of this ring. To see this, conjugation by a global element preserves the image and acts by its value of $\alpha\kappa_p^{r+1}$. The image is additive, so is stable also under every p-adic integer modulo p^h. Removing the cyclotomic unit scalar leaves all values of α, which generate O_α over $\mathbb{Z}_p$. The image contains a unit by the residual nonvanishing, hence is the whole ring. Its kernel is open and normal over $\mathbb{Q}$. Divisibility by π^v is conjugacy-stable, so conditional Chebotarev gives the fraction $p^{-b_\alpha v}$ for the basis cocycle.

Finally specialize the actual class c on the same field. In the corestriction formula all embeddings at s send ζ_{fp^h} to the different w^a. The tensor factors contribute $\alpha(a)a^r$. Arithmetic Frobenius on a p^h-th root of a residue unit z gives the quotient $z^{(s-1)/p^h}$, with coordinate $\mathrm{ind}_g z$ in the basis w^f. Thus the moment is the evaluation of c, up to a basis unit, also when $p \mid f$. Multiplication of the primitive class by its coordinate shifts the valuation by d_j until it reaches $e_\alpha h$. This gives the asserted law. □

21.8 Frobenius orbits in the local cyclotomic sum

Fix the largest modulus N_* on one interval as in Theorem 8.3. Write $k = r + 1$, $f \mid N_*$ for the primitive character conductor, p for an odd coefficient prime, and $e = v_\pi(p)$. Take $v \ge 1$ and $h = \lceil v/e \rceil$. Let s be prime with $s \equiv 1 \bmod N_*$, $s \ne p$, and $p^h \mid s^k - 1$. Put $n = fp^h$, $\ell = \mathrm{ord}_n(s)$, and $A = (\mathbb{Z}/n\mathbb{Z})^\times$. In $\mathbb{F}_{s^\ell}$ choose a multiplicative generator g, and set $w = g^{(s^\ell - 1)/n}$.

Proposition 21.11 (Specialization without division by the residue degree)**.** *In a choice of coefficient basis, the unramified arithmetic Frobenius value of c modulo π^v is*

$$D_v(s) = \sum_{a \in A/\langle s \rangle} \alpha(a) a^r \, \mathrm{ind}_g(1 - w^a) \mod \pi^v.$$

The sum takes one representative in each multiplicative coset. The discrete logarithm is reduced modulo p^h. Its vanishing to any order at most v is independent of the choices. For fixed s, k every eligible calculation, including $p \mid f$, takes place in subfields of $\mathbb{F}_{s^{kN_*}}$.

Proof. At s the coefficient action of arithmetic Frobenius is $\alpha(s)s^k = s^k$, equal to one modulo π^v. The s-adic factors of the cyclotomic field of order n are unramified of degree ℓ. They correspond to orbits of $a \mapsto sa$ on the primitive roots w^a. Localizing the global corestriction sums the corestrictions of these factors. To see this on cocycles, partition the cosets in the transfer formula by the cycles of Frobenius. Choose successive powers of Frobenius times one initial representative around a cycle. All changes of representative cancel except the return step, which evaluates the conjugated cocycle on the ℓ-th power of Frobenius. Any power of Frobenius acting on its value is trivial on the target modulo π^v. This gives one contribution per orbit even if $p \mid \ell$.

At the representative a the Kummer unit specializes to $1 - w^a$. Arithmetic Frobenius to the power ℓ sends a p^h-th root of that unit to itself times $(1 - w^a)^{(s^\ell - 1)/p^h}$. Its coordinate in the basis $w^f = g^{(s^\ell - 1)/p^h}$ is the indicated discrete logarithm. The other Tate factors and the character basis have respective coordinates a^r and $\alpha(a)$, as in Proposition 21.10. Replacing a by sa raises the residue unit to its s-th power and multiplies the full term by $\alpha(s)s^{r+1} = 1 \bmod \pi^v$. Changing g to g^j with j prime to $s^\ell - 1$ permutes the root indices by $a \mapsto ja$ and scales the entire sum by $\alpha(j)^{-1}j^{-k}$, a unit.

The prime-to-p part of f divides $s - 1$. If $p \nmid f$, then $\ell \mid k$. Otherwise put $b_0 = v_p(f)$. Since $s^k \equiv 1 \bmod p^h$, the binomial theorem applied b_0 times gives $s^{kp^{b_0}} \equiv 1 \bmod p^{h+b_0}$. Thus $\ell \mid kp^{b_0} \mid kN_*$. In the common finite field one may obtain a generator of the degree-ℓ subfield by raising a generator to $(s^{kN_*} - 1)/(s^\ell - 1)$. The logarithm in the formula is taken with respect to that subfield generator. □

21.9 Orders of the detected strict classes on the period interval

At each x on the same original interval, use $E = E_x$, $t = \lfloor x^{401} \rfloor$, and let M_x be the integer in Theorem 34.22 formed with this field and this cutoff. Consider the triples at $\ell > \exp(x^\varepsilon/12)$ of that theorem, with one term per residue orbit. Write $d = v_\ell(L(1 - r, \alpha^*))$ and use v_j, h_0, b from Theorem 28.4. Put

$$H(x) = \exp(x^\varepsilon/2)/x^{820}, \qquad R_{\ell,r,\alpha} = \min\left(v_1, \frac{\log h_0}{b \log \ell}\right).$$

Let $\mathcal{J}_x$ consist of the triples with $R_{\ell,r,\alpha} \le x^3 H(x)$, and let $\mathcal{F}_x$ consist of those for which $v_1 = 0$ or $v_{d+1} \le d$.

Theorem 21.12 (A bound for orders on the original fields and intervals)**.** *Uniformly for all x of every sufficiently distant original interval the two estimates*

$$\sum_{\mathcal{J}_x} b \log \ell \ \operatorname{length}_O S^-[\ell^d] \ll_{\psi,\varepsilon} x^{-5} \exp(x^\varepsilon/2),$$
$$\sum_{\mathcal{F}_x} b \log \ell \ \operatorname{length}_O S^- \le \log M_x \ll_{\psi,\varepsilon} x^{812}$$

hold for the original complementary strict groups. The first estimate applies in particular to the full orders of the subgroups S^{ev} of Theorem 34.22. Its range includes every triple with $\exp(x^\varepsilon/12) < \ell \le H(x)$. Every component with $v_1 = 0$ vanishes.

Proof. The elementary-divisor decomposition of the finite O-module S^- shows that its ℓ^d-torsion has length at most $d \dim_{O/\ell} S^-[\ell]$, also when $d = 0$. Theorem 28.4 bounds the dimension by $R_{\ell,r,\alpha}$. The exponent bound in Theorem 34.22 puts S^{ev} in this same torsion group. Summing the length estimate on $\mathcal{J}_x$ costs at most $x^3 H(x) \log M_x$, by the prime valuation formula there on E_x. Its archimedean estimate gives $\log M_x \ll x^{812}$ with the field and conductor bounds of Theorem 19.15. This proves the first inequality.

To check the entire asserted prime range, the residual character cutting out K_0 has conductor dividing $f_\alpha \ell$ and order at most $[E:\mathbb{Q}](\ell-1)$. The latter follows by multiplying the orders of the finite character and of the residual cyclotomic character. The conductor–discriminant bound and the Minkowski ideal count in Theorem 34.21 therefore give

$$\log h_0 \ll [E:\mathbb{Q}]\ell \log(2 f_\alpha \ell).$$

For every prime under consideration $\log(2f_\alpha\ell) \ll \log \ell$ uniformly, since $f_\alpha \mid N_x$ and $\log N_x \ll x^{\varepsilon/4}$. Also $[E:\mathbb{Q}] \ll_\psi x^{2+8\varepsilon}$ with $2+8\varepsilon < 3$. Hence for large x one has $R_{\ell,r,\alpha} \le x^3 \ell$, which includes the claimed range in $\mathcal{J}_x$.

If $v_1 = 0$, Theorem 28.4 gives $S^- = 0$. In the other case of $\mathcal{F}_x$, its stopping test at $j = d+1$ bounds the length of the whole group by $v_{d+1} \le d$. Summing these lengths costs at most $\log M_x$ again. All local conditions in the argument are those of the original field by character descent. Each bound is pointwise in x with uniform constants on the period interval. □

For a contribution from S^{ev} outside the first estimate, one needs a positive valuation of $L(1-r,\alpha^*)$ and a valuation exceeding $x^3 H(x)$ of the primitive value at the reflected weight s_1, at the same prime $\ell > H(x)$. The remaining full strict orders also include classes above the controlled torsion levels. A bound for those orders and the comparison for the arithmetically normalized theta pairing are still required for the main theorem.

21.10 Summing full strict orders across weights

Use the period field $E = E_x$ of degree n and modulus N on the interval of Theorem 19.15, and put $t = \lfloor x^{401} \rfloor$. For $3 \le p \le Y$, $p \nmid nN$, take one α in each residue Frobenius orbit. Write $b_\alpha = [O/p : \mathbb{F}_p]$. Group the twists of this character by their residue modulo $p-1$, retaining the hypotheses of Theorem 28.8. A nonempty progression $\mathcal{T}$ consists of all $1 \le r < t$ in the chosen residue class. Let $k \in [2, p-1]$ satisfy $k \equiv -r \bmod (p-1)$, put $l = |\mathcal{T}|$, and define

$$v = v_p(L(1-k,\alpha^{-1})), \qquad \lambda_r = \mathrm{length}_O S_{\alpha,r}.$$

The character in the special value is primitive. Here $S_{\alpha,r}$ is the full original complementary strict group in this character component.

Theorem 21.13 (Full strict orders outside finitely many twists in each progression)**.** *There is a subset $D \subset \mathcal{T}$ with $|D| \le v$ and*

$$\sum_{r \in \mathcal{T}\setminus D} \lambda_r \;\le\; v(2l + v_p((l-1)!)).$$

A removed twist lies within p-adic distance strictly less than p^{-l} of a root in the coordinate specified below. Using these sets at all the primes and characters above gives

$$\sum_{p,[\alpha],\mathcal{T}} b_\alpha \log p \sum_{r \in \mathcal{T}\setminus D} \lambda_r \ll n(Y^2 + tY)\log(2NY),$$
$$\sum_{p,[\alpha],\mathcal{T}} b_\alpha \log p\, |D| \ll nY^2 \log(2NY).$$

In particular the first sum is $O_{\psi,\varepsilon}(x^{-2}\exp(x^\varepsilon/2))$ for $Y = x^{-3}\exp(x^\varepsilon/4)$, uniformly on the original intervals. It includes all twists and characters at $\exp(x^\varepsilon/12) < p \le Y$ except the individual triples removed by these sets.

Proof. Use one smoothing integer B and series F from Theorem 28.8 for the whole progression. Set $a = X_{1-k}$ and $G(U) = F(a + pU)$. Its i-th coefficient belongs to $p^i O$, by the binomial expansion at $a \in pO$. In particular the coefficients tend to zero. The constant coefficient has valuation v. Let μ be the minimum of the coefficient valuations and m the last index at which the minimum occurs. Then $m \le \mu \le v$. After dividing by p^μ and by a unit, the reduction of the series is a monic polynomial of degree m.

On the closed unit disk this series is a unit times a monic polynomial $P \in O[U]$ of that degree. Here is the lifting argument. Start with a monic lift of the reduction and unit factor one. Given a product correct modulo p^i, reduce its error divided by p^i modulo p. It is a polynomial since the series is restricted. Divide by the original monic reduction. Add p^i times lifts of the quotient to the unit factor and of the remainder to the polynomial. The product is now correct modulo p^{i+1}, with the same leading coefficient and unit reduction. The limits give the factorization. Its unit has unit value throughout the closed disk. Denote the roots of P, with multiplicity, by $\xi_1, \dots, \xi_m$ in a finite extension of J. They are integral since P is monic.

For $r \in \mathcal{T}$ put $u_r = (X_{1+r} - a)/p$. The binomial theorem at odd p gives $v_p(u_r - u_s) = v_p(r - s)$ for $r \ne s$. For each root choose r_i maximizing $v_p(u_{r_i} - \xi_i)$. Put r_i in D if this maximum is greater than l. At any $r \ne r_i$ the ultrametric inequality gives $v_p(u_r - \xi_i) \le v_p(r - r_i)$. Index $\mathcal{T}$ by $0, \dots, l-1$. Its step $p-1$ is a unit. Thus the sum of the latter upper bounds is $v_p(j!) + v_p((l-1-j)!) \le v_p((l-1)!)$, where j indexes r_i. If r_i is retained its own contribution for this root is at most l. For every retained twist, Theorem 28.8 gives

$$\lambda_r \le v_p(F(X_{1+r})) = \mu + \sum_{i=1}^{m} v_p(u_r - \xi_i).$$

A zero at an actual twist has already been removed. Summing gives $l\mu + m(l + v_p((l-1)!))$, which proves the first bound and the assertion about distances.

For fixed k, the sum of $b_\alpha v \log p$ over the participating primes and characters is at most $\log J_k(E)$ from (25.15). Indeed the rational numerator norm in that formula counts the valuations at p with their residue degrees. The Bernoulli polynomial estimate in Theorem 25.19 gives $\log J_k(E) \ll nk \log(2Nk)$. We have $l \le 1 + 2t/k$ since $k \le p$, and $v_p((l-1)!) \le (l-1)/(p-1)$. Sum first over $p, [\alpha]$, then over $2 \le k \le Y$. The two displayed estimates follow from $\sum_{k \le Y}(k + 2t) \ll Y^2 + tY$ and $\sum_{k \le Y} k \ll Y^2$. For the stated choice of Y we eventually have $t \le Y$. The common-field bounds $n \ll_\psi x^{2+8\varepsilon}$ and $\log(2NY) \ll_{\psi,\varepsilon} x^\varepsilon$ give the asserted order, since $9\varepsilon < 1$ in the standing range. In the displayed large-prime range p exceeds $n, N, t+2$ on sufficiently distant intervals, so every complementary character and twist qualifies. □

The estimate for $|D|$ counts triples with multiplicity $b_\alpha \log p$. Bounding the orders of the strict groups at those triples, and at larger primes, is still necessary for the uniform cohomology estimate in Section 6.6.

21.11 A single list of remaining twists on the period interval

Use the nested fields of Theorem 19.15 on an original interval $[V, V^{3/2}]$, and put $t_* = \lfloor V^{1203/2} \rfloor$. For a point x write $E = E_x$, $n = [E : \mathbb{Q}]$, $N = N_x$, $t = \lfloor x^{401} \rfloor$ and $Y = x^{-3} \exp(x^\varepsilon/4)$. Let $\mathcal{B}$ be the fixed odd prime divisors of the order of ψ. They are exactly the odd prime divisors of n, since the rest of the extension has degree a power of two.

Use $M_{p,r} = \frac{1}{2}(1 + (-1)^r c)\mathcal{S}_{p,r}(E)$ at odd p. Write $W_{p,r} = p^{k_{p,r}}(1 - e'_r)Q_{p,r} \subset M_{p,r}$ for the subgroup already retained in (20.12). The local length sum of Section 6.6 differs from $\sum_{p,r} \log |W_{p,r}|$ by $o(\exp(x^\varepsilon/2))$.

Theorem 21.14 (Full orders on one list for all fields of an interval)**.** *One can select exceptional twists once on $[V, V^{3/2}]$ so that the following assertions hold at every x. For $p \le Y$ outside $\mathcal{B}$, selection uses one set $D_{p,[\alpha],k}$ for each character orbit and $2 \le k \le p$ with $r \equiv -k \bmod (p-1)$ and the required parity. Globally trivial residual characters have empty sets. Otherwise, with e from Theorem 28.9, one has*

$$|D_{p,[\alpha],k}| \;\le\; v_p(L(1-k,\alpha^{-1})) - e(1+v_p(k-1)).$$

At $p \in \mathcal{B}$ a single set D_p suffices for the whole complementary group. In the first range the sum of the full logarithmic orders of all unselected components is $O_{\psi,\varepsilon}(x^{-2}\exp(x^{\varepsilon}/2))$. In the second range the sum of the full logarithmic orders of the unselected groups is bounded by a polynomial in x.

More precisely define $W'_{p,r}$ to equal $W_{p,r}$ for $p > Y$. At $p \le Y$ outside $\mathcal{B}$ retain in $W'_{p,r}$ only the orbit summands of $W_{p,r}$ for which $r \in D_{p,[\alpha],k}$. At $p \in \mathcal{B}$ retain $W_{p,r}$ if $r \in D_p$, and use zero otherwise. Then

$$\mathcal{L}(x) = \sum_{1 \le r < t} \sum_{p \text{ odd}} \log |W'_{p,r}| + o(\exp(x^{\varepsilon}/2)).$$

The additional removals described in Theorem 21.12 can be made in this formula as well.

Proof. Make the selection using the largest field E_* of the interval, the full twist range $r < t_*$, and the maximum of the cutoffs Y on the interval. For $p \notin \mathcal{B}$, character evaluation decomposes the integral group ring into unramified integer rings, including at primes ramified in E. A component of O-length λ_r therefore contributes $b_\alpha \lambda_r \log p$ to the logarithmic order of $M_{p,r}$, by Theorem 24.1. Theorem 28.6 kills the globally trivial residual case. In every other case use the root selection of Theorem 21.13 with the integral series F°. Theorem 28.9 bounds the full strict length by the valuation of this series wherever the valuation is finite. Its sample valuation is the displayed bound on $|D_{p,[\alpha],k}|$. A zero of the series at an integer twist is included by the selection rule.

A character occurring earlier on the interval inflates to E_* with the same primitive character, coefficient ring, and local conditions over $\mathbb{Q}$. Thus the sets just chosen apply throughout. At a fixed x sum only over characters of E_x and primes $p \le Y(x)$. The complete progression in the larger twist range has at most $1 + 2t_*/k$ terms. Bounding its retained sum also bounds that of its prefix at x. The numerator norm calculation (25.16) applies here even if $p \mid N$: it counts valuations in the character value fields, which are unramified at $p \nmid n$. The corrected valuation is no larger than the positive part of the primitive valuation. Consequently the weighted count of the selected triples at x is at most $\sum_{2 \le k \le Y} \log J_k(E_x)$. The logarithmic orders outside the selected triples sum to at most

$$C \sum_{2 \le k \le Y} (1 + 2t_*/k) \log J_k(E_x) \ll n(Y^2 + t_* Y)\log(2NY).$$

Uniformly on the interval $t_* \le x^{1203/2} \le Y$ eventually. The degree and conductor bounds in Theorem 21.13 now give the asserted estimate.

For each of the finitely many $p \in \mathcal{B}$, apply Theorem 20.9 at $x_* = V^{3/2}$. Its whole-field exceptional set D_p has size $O_\psi(n_* \log(2N_*))$, where $n_* = [E_* : \mathbb{Q}]$ and N_* is its modulus. Outside this set $p^{\lceil x_*^{202} \rceil}$ kills the whole complementary group on E_*. Restriction from E_x is injective since corestriction composed with restriction is multiplication by the relative degree, a power of two. Restriction preserves the local conditions and commutes with complex conjugation. At E_x, Lemma 19.18 bounds the logarithmic order at exponent p by $O_\psi(n \log(2Np))$. Multiplying

this by $\lceil x_*^{202} \rceil$ bounds each full logarithmic order in question. There are at most t terms per prime, and $x_* \le x^{3/2}$, proving the polynomial bound.

Each part discarded from $W_{p,r}$ lies in the corresponding part of $M_{p,r}$, so the same estimates pay for its removal. This proves the formula by (20.12). To see the last assertion, at $p > \exp(x^{\varepsilon}/12)$ discard a remaining component completely if it belongs to $\mathcal{F}_x$ of Theorem 21.12. On the remaining components in $\mathcal{J}_x$, quotient by the intersection with $S^-[p^d]$ from that theorem. The total costs are respectively at most $\log M_x$ and $O_{\psi,\varepsilon}(x^{-5}\exp(x^{\varepsilon}/2))$. Both are absorbed by the error, independently of overlaps with the earlier removals. □

The selected twists below Y and the remaining groups above Y enter with their actual orders. A uniform estimate for their sum and the arithmetic period comparison on this interval are still required.

21.12 One auxiliary field for the ordinary congruences

Corollary 21.15 (Simultaneous removal of auxiliary tame ramification)**.** *Fix a sufficiently distant period interval $[V, V^{3/2}]$. For every nonzero large-prime strict summand in Corollary 21.8 use its original E_x, ℓ, r, α. There are two rational primes s_1, s_2 which split in every E_x and in $K' = \mathbb{Q}(i)$, and one totally real abelian extension $L/\mathbb{Q}$ ramified only at these two primes, such that Theorem 34.16 supplies a cuspidal lift for each summand. The coefficient primes, all primes of the original field conductors and the period primes g_1, g_2, T split completely in L. On $K'L$ the corresponding adjoint is ordinary crystalline over ℓ, realizes the given residual diagonal and has prime-to-ℓ conductor $\mathfrak{f}(\alpha|_{G_{K'L}})^2$, where $\mathfrak{f}$ denotes the conductor ideal. On $E_xK'L$ it is unramified away from ℓ and remains cuspidal. All assertions use the same s_1, s_2, L throughout the interval.*

Proof. Corollary 21.8 proves that the list of data with nonzero strict group is finite once the interval is fixed. In particular the set P of coefficient primes occurring is finite. Let B consist of P, the prime divisors of the field conductors, and the period primes in the statement. The last list is finite too. The bounds for g_1, g_2, T in Theorem 93.17 are uniform on this bounded interval. Choose a modulus M divisible by the conductors of K' and all E_x and by every required $8N\ell^a$ in Lemma 21.19. Form the splitting field of the cyclotomic polynomial of order M and the finitely many polynomials $X^{\ell} - p$ for $\ell \in P$, $p \in B$. Chebotarev gives two distinct completely split primes outside all primes used so far. These serve as s_1, s_2. Each $p \in B$ is an ℓ-th power modulo each s_j for every $\ell \in P$.

For each pair s_j, ℓ, take the unique degree-ℓ subfield $L_{j,\ell} \subset \mathbb{Q}(\zeta_{s_j})$ and a character $\xi_{j,\ell}$ cutting it out. Existence and uniqueness follow from cyclicity of the multiplicative group modulo s_j. Its kernel consists of the ℓ-th powers in that group. As ℓ is odd, complex conjugation belongs to the kernel. The compositum L of these real fields thus has the indicated ramification and splitting. For the empty list take $L = \mathbb{Q}$. Apply Theorem 34.16 to each datum with its own two characters of order ℓ.

On $G_{K'L}$ the characters $\eta, \xi_{1,\ell}, \xi_{2,\ell}$ are trivial. Thus at every prime away from ℓ the inertia characters are $\alpha, 1, \alpha^{-1}$, with zero monodromy. The conductor exponent is twice that of α, since a character and its inverse have the same ramification groups as kernels. Restriction to $G_{E_xK'L}$ kills α. The ordinary flag and crystalline periods persist under these restrictions, and cuspidality follows by solvable base change as in Theorem 34.16. □

Theorem 21.16 (Descent of the original strict group from the same field)**.** *For one datum in the corollary, put $F_x = E_xK'L$ and $\Delta = \mathrm{Gal}(F_x/\mathbb{Q})$. Let O be the unramified coefficient DVR of the character, J its fraction field, and $A = (J/O)(\kappa_\ell^{-r}\alpha^{-1})$. For a number field D,*

write $S_D(A)$ for the classes in $H^1(D,A)$ trivial on inertia away from ℓ and on the whole decomposition groups at ℓ. For $j=1,2$ let I_j be inertia at s_j over $\mathbb{Q}$, and I_j' inertia over F_x using the same choice of place. There is an exact sequence

$$0 \longrightarrow S_{\mathbb{Q}}(A) \longrightarrow S_{F_x}(A)^{\Delta} \longrightarrow \bigoplus_{j=1}^{2} \mathrm{Hom}(I_j/I_j', A[\ell])$$

where exactness is asserted at the first two groups. The last module is isomorphic to $(O/\ell O)^2$. The same sequence holds with $A[\ell^n]$ as coefficients, for each $n \geq 1$. Thus descent to the original strict summand costs at most two units of O-length, independently of the degree of L, the character, the twist and the field on the interval. The same bound holds for the difference of lengths after multiplying both groups by any ℓ^j, $j \geq 0$.

Proof. Inertia over ℓ in G_{F_x} has the full residual cyclotomic image. Indeed E_xK' is unramified there and ℓ splits completely in L. Since $0 < r < \ell - 1$ and α is unramified at ℓ, some inertia element acts on A by a scalar whose difference from one is a unit of O. In particular $A^{G_{F_x}} = 0$, also for the finite coefficient submodules. Inflation–restriction now identifies $H^1(\mathbb{Q}, A)$ with $H^1(F_x, A)^{\Delta}$, even though ℓ may divide $|\Delta|$. Every invariant strict class upstairs has a unique global antecedent.

At ℓ the local degree of $F_x/\mathbb{Q}$ divides $[E_xK' : \mathbb{Q}]$, prime to ℓ in this large-prime range. Local restriction on degree-one cohomology is injective, since corestriction composed with restriction is multiplication by that degree. Away from ℓ, s_1, s_2 the index of inertia also divides $[E_xK' : \mathbb{Q}]$, since L is unramified there. The same argument gives injectivity on the inertia cohomology. The antecedent therefore satisfies every original local condition except possibly those at s_1, s_2.

The action on A at inertia I_j is trivial. Restrict the antecedent to I_j. Its restriction is a homomorphism vanishing on I_j', independent of any cocycle representative. The quotient I_j/I_j' is cyclic with ℓ-part of order exactly ℓ. Indeed E_xK' splits at s_j; the character fields from the other auxiliary prime are unramified there. At s_j the fields from this prime are subfields of $\mathbb{Q}(\zeta_{s_j})$ with exactly one factor of degree ℓ and the remaining factors of distinct prime degrees. They are totally ramified there. The image of the homomorphism is therefore in $A[\ell]$, and the Hom module for this prime is one copy of $O/\ell O$. The two restrictions vanish precisely when the antecedent is strict. This proves exactness and the length bound. If the first two groups are $M \subset B$, multiplication gives a surjection $B/M \to \ell^j B/\ell^j M$, proving the assertion at depth j. In particular, on any collection of character summands for which $\ell^j M \neq 0$, the sum of the logarithmic orders upstairs lies between the corresponding sum downstairs and three times that sum. Indeed a nonzero module has length at least one, and both logarithmic orders use the same factor $\log|O/\ell O|$ per unit of length. The proof uses the same invariants and the same inertia quotients for $A[\ell^n]$. The identification of $S_{\mathbb{Q}}(A)$ with the original character summand over E_x is the prime-to-degree descent in Theorem 24.1. □

The comparison thus retains the original strict group, with its full primary exponents, on a field supporting the stated cuspidal adjoints. A bound for the orders of the invariant groups in this sequence is still needed in (20.12). The signed integral period comparison concerns the original field E_x throughout.

21.13 One prime detecting all the integral dual classes

Theorem 21.17 (Simultaneous detection subject to the period splitting conditions)**.** *Fix a sufficiently distant interval of Corollary 21.15 and all its nonzero large-prime strict summands. There is a positive-density set of rational primes s satisfying every individual congruence of*

Proposition 36.1 and splitting in every E_x and $K' = \mathbb{Q}(i)$. For every coefficient prime ℓ, every rational prime listed for splitting in Corollary 21.15 is an ℓ-th power modulo s. For every datum one can fix an integral class d as in Lemma 36.2 so that its reduction evaluates nontrivially at Frobenius at every such s. The reduction character is trivial locally at s, so nonvanishing is independent of the Frobenius representative.

Proof. There are finitely many data on this interval by Corollary 21.8. Denote the coefficient primes by P and the list of primes required to split by B. Take a cyclotomic field C_0 containing all the original fields, K', and the roots of unity for every prescribed modulus $8N\ell^a$. Let K be obtained from C_0 by adjoining an ℓ-th root of every $p \in B$ for each $\ell \in P$. This is Galois over $\mathbb{Q}$.

Fix one residual character $\delta = \bar{\kappa}_\ell^{r+1}\bar{\alpha}$ and denote its module by $D = k_\ell(\delta)$. Restriction $H^1(\mathbb{Q}, D) \to H^1(K, D)$ is injective. Indeed D is trivial over C_0. For the finite abelian group $G = \mathrm{Gal}(C_0/\mathbb{Q})$, a central element acting by a scalar different from one makes $H^1(G, D) = 0$. Writing a cocycle at $zg = gz$ expresses it as a coboundary. The group $\mathrm{Gal}(K/C_0)$ embeds in a product of the groups $\mu_{\ell'}$ for $\ell' \in P$ by its action on the chosen radicals. Conjugation on each $\mu_{\ell'}$ coordinate is cyclotomic, since the radicands are rational. Thus its ℓ-part has scalar action $\bar{\kappa}_\ell$. On inertia at ℓ, the exponent $r + 1$ lies strictly between 1 and $\ell - 1$ and α is unramified. Consequently δ is neither trivial nor $\bar{\kappa}_\ell$. There are no G-equivariant homomorphisms from $\mathrm{Gal}(K/C_0)$ to D. Two applications of inflation–restriction prove injectivity.

Take one character from each orbit under residue-field Frobenius for each ℓ, and choose the class of Lemma 36.2. Conjugate characters use conjugate classes. Indeed the restriction to inertia at ℓ determines $r + 1$ in the above range, and prime-to-ℓ finite characters lift uniquely from their residues. Use the same class whenever the datum repeats. On G_K each reduction is a nonzero additive homomorphism to k_ℓ. Its image is stable under multiplication by $\delta(G_\mathbb{Q})$, by the cocycle identity under conjugation. Those values generate the entire minimal residue field over $\mathbb{F}_\ell$. Thus each image is full.

Their joint image is the full product. For a fixed ℓ it is a submodule of the sum of the D's for the finite abelian group of residual character values. This group has order prime to ℓ. Its group algebra over $\mathbb{F}_\ell$ is a product of finite fields, with nonconjugate characters in distinct factors. The corresponding idempotents separate the images, each of which is full. Different coefficient primes separate by primary decomposition of the finite additive image. Hence one can choose $g \in G_K$ with every evaluation nonzero. The common kernel on G_K is open and normal in $G_\mathbb{Q}$ by conjugation equivariance. Chebotarev applied to the conjugacy class of g in this finite quotient gives the desired positive-density set. Its primes split in K, giving all the stated splitting and power conditions. Conjugation multiplies each evaluation by a unit. A finite set of ramified or previously used primes may be discarded. For an empty list ordinary complete splitting in C_0 suffices. □

21.14 Interpolation at a fixed conductor

Fix an odd prime p, a primitive character $\chi = \alpha^{-1}$, and one admissible branch $2 \le k \le p$ of Theorem 25.23. Thus its residual coefficient character is nontrivial. Let O be the integer ring of the coefficient field, put $X_s = (1 + p)^s - 1$, and take the same smoothing integer b at all weights in this branch.

Theorem 21.18 (Recovery of the strict annihilator from finitely many weights)**.** *For $H \ge 1$, set $k_i = k + i(p - 1)$, $a_i = X_{1-k_i}$ for $0 \le i < H$. Let P be the polynomial of degree less than H with*

$$P(a_i) = b^{1-k_i}(b^{k_i} - \chi(b)^{-1})(1 - \chi(p)p^{k_i-1})B_{k_i,\chi}/k_i.$$

Then $P \in O[X]$. If F is the annihilating series in Theorem 25.23, then on every admissible twist $r \geq 1$,

$$F(X_{r+1}) \equiv P(X_{r+1}) \pmod{p^{H+v_p(H!)}O}.$$

In particular a value of P of valuation $w < H + v_p(H!)$ gives $p^{\lceil w \rceil} S_{\alpha,r} = 0$. The same H samples determine every coefficient of the restricted series $F(a_0 + pU)$ modulo $p^H O$.

Proof. For $a \in pO$ and $F \in O[[X]]$, subtract $F(a)$ and divide by $X - a$. The resulting series is integral: the coefficient at degree j is $\sum_{n>j}[X^n]F\, a^{n-1-j}$, which converges in O. Apply this division successively at $a_0, \ldots, a_{H-1}$. Newton's formula gives $F = P_0 + \prod_i (X - a_i)G$ for $P_0 \in O[X]$ of degree less than H and $G \in O[[X]]$. The nodes are distinct, and Theorem 25.23 gives exactly the specified values there. Thus $P = P_0$.

For integers $s \neq t$, $v_p(X_s - X_t) = 1 + v_p(s - t)$. This follows by factoring out the unit $(1 + p)^t$: a power prime to p preserves the valuation of $(1 + p) - 1$, and each subsequent p-th power increases it by one by the binomial expansion, since p is odd. Among H successive terms $r + k + i(p - 1)$, at least $\lfloor H/p^j \rfloor$ are multiples of p^j for each $j \geq 1$. Consequently the product of $X_{r+1} - a_i$ has valuation at least $H + \sum_{j\geq 1}\lfloor H/p^j \rfloor$. This is the stated precision. Equal residues to this precision and one valuation below it imply equal valuations. Dividing $p^{\lceil w \rceil}$ by the annihilator gives an element of O, which proves the exponent bound.

Finally every $a_0 + pU - a_i$ has both coefficients in pO. The substitution of $a_0 + pU$ into G converges to a restricted integral series, since both coefficients of the argument are divisible by p. This proves the coefficientwise assertion. For explicit numerical evaluation, the denominator $\prod_{j\neq i}(a_i - a_j)$ in Lagrange's formula has valuation $H - 1 + v_p(i!(H - 1 - i)!)$. The other polynomial factors are integral. It suffices, for instance, to compute each sample modulo $p^{2H+2v_p(H!)}O$ to retain the displayed precision. □

There is also a description by residue classes when O is unramified. Write $F(a_0 + pU) = \sum_m d_m U^m$. Here $v_p(d_m) \geq m$, by expanding $(a_0 + pU)^n$. The constant coefficient is nonzero by the Bernoulli value and the functional equation for its primitive character. Put $\mu = \min_m v_p(d_m)$, and let $s \leq \mu$ be the degree of the nonzero reduction of $p^{-\mu}\sum d_m U^m$. If $s = 0$, all values on $\mathbb{Z}_p$ have valuation μ. For $s > 0$ and $l \geq 1$, twists of valuation strictly greater than $\mu + sl$ occupy at most s residue classes modulo p^l inside the fixed branch modulo $p - 1$.

Indeed start with the normalized integral series. At an allowed residue $c \in \mathbf{F}_p$ where its reduction is nonzero all values are units. At a root of multiplicity e, first translate by an integer lift of c. The coefficient of degree e is a unit, and all lower coefficients are divisible by p. Now substitute pU. The new minimum valuation is between one and e, and after division by that power of p the degree of the reduction is at most e. At every stage the sum of the positive degrees over the surviving discs is therefore at most s. A branch ending by stage l has valuation at most $\mu + sl$. There are at most s continuing discs at stage l. The map $r \mapsto (X_{r+1} - a_0)/p$ preserves distances on integers by the valuation formula above. As $p - 1$ is a unit, the twists in the fixed branch run through all residues at each depth. This proves the claim.

21.15 Cuspidal congruences with prescribed auxiliary characters

Fix an integer $k \geq 2$, a primitive Dirichlet character χ of conductor N with $\chi(-1) = (-1)^k$, and a prime $\ell > \max(k + 1, (8N)^3)$. Fix an embedding of the character values into $\overline{\mathbb{Q}}_\ell$. Put $h = 8N$. We use the Fourier variable $Q = \exp(2\pi i z)$.

Lemma 21.19 (Two independent cuspidal Eisenstein congruences)**.** *There is an integer $a \geq 1$ such that the following holds for any two distinct primes $s_1, s_2 \equiv 1 \bmod h\ell^a$. At level $\Gamma(h) \cap \Gamma_0(s_1 s_2)$ there are two independent cusp forms in residue characteristic ℓ, of weight k, with the*

transformation law of χ at level $\Gamma_0(Ns_1s_2)$. Each has eigenvalue $1+\chi(p)p^{k-1}$ reduced modulo the maximal ideal for every Hecke operator T_p with $p \nmid hs_1s_2$, including $p=\ell$.

Proof. Except when $(k,\chi)=(2,1)$, take the normalized holomorphic Eisenstein series $E_k(1,\chi)$ at level N. Its first Fourier coefficient is one and its coefficient at $n\geq 1$ is $\sum_{d|n}\chi(d)d^{k-1}$. Its constant terms at the cusps of $\Gamma(h)$ are algebraic by the algebraic Fourier expansion principle. These standard formulas use the classical normalization of T_p. [11] Choose a so that ℓ^a times every one of these finitely many constants has positive valuation. For $s=s_1,s_2$, put $F_s(z)=E(z)-E(sz)$. At a cusp represented by the first column (u,v) of $\gamma\in\mathrm{SL}_2(\mathbb{Z})$, put $d=\gcd(su,v)$, so $d=1$ or s. The first column of $\mathrm{diag}(s,1)\gamma$ is d times the primitive column $(su/d,v/d)$. Complete this column to γ' of determinant one. Then $(\gamma')^{-1}\,\mathrm{diag}(s,1)\gamma$ is upper triangular with diagonal $d,s/d$. Thus the constant of $E(sz)|_k\gamma$ is $(d/s)^k$ times that of $E|_k\gamma'$. Both primitive columns agree modulo h, since $s\equiv 1 \bmod h$. Their completions modulo h differ on the right by an upper unitriangular matrix, which lifts to an integral translation. The two constants of E are consequently equal. Multiplication by $1-(d/s)^k$ makes the constant vanish after reduction at every cusp by the choice of a.

For $(2,1)$ use the normalized weight-two Eisenstein series $E=-1/24+\sum_{n\geq 1}\sigma_1(n)Q^n$ and take $F_s(z)=E(z)-sE(sz)$. Its weight-two transformation formula cancels the nonmodular term, giving a form on $\Gamma_0(s)$. The same formula at the cusp zero gives $F_s|_2\left(\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right)=E(z)-s^{-1}E(z/s)$. Its two cusp constants are $(s-1)/24$ and $-(1-s^{-1})/24$, both zero after reduction.

In each case the expansion at infinity has integral coefficients. At this prime-to-ℓ level the smooth compact modular curve with fixed Weil pairing has geometrically integral special fiber. The expansion at one cusp suffices for integrality. Indeed a generic-fiber holomorphic section could have a pole only on the whole special fiber, which its integral expansion excludes. The vanishing constants at all cusps now make its reduction cuspidal. We use the good reduction, Tate cusp charts and Fourier expansion principle for modular curves. Conrad, *Arithmetic moduli of generalized elliptic curves*. The Hecke formula for the divisor sums gives the stated eigenvalues. Replacing z by sz commutes with every indicated T_p. In weight two with trivial character the same Fourier formula applies directly to F_s. The two reductions have coefficient one at Q, while their coefficients at Q^{s_1} differ by one up to sign, since $s_1\equiv 1 \bmod \ell$. They are independent. □

Theorem 21.20 (An ordinary newform of exact auxiliary conductor)**.** *Keep s_1,s_2 as in Lemma 21.19. For each $j=1,2$ choose any Dirichlet character ξ_j of conductor s_j and order ℓ. There is a normalized cuspidal newform f of weight k, exact level Ns_1s_2 and nebentype $\chi\xi_1\xi_2$, with a place over ℓ such that*

$$a_p(f)\equiv 1+\chi(p)p^{k-1} \pmod{\mathfrak{m}} \qquad (p\nmid hs_1s_2).$$

In particular f is ordinary at ℓ.

Proof. Write $s=s_1s_2$, $\xi=\xi_1\xi_2$. Work over the integers of a finite extension of $\mathbb{Q}_\ell$ containing the relevant roots of unity and cusp parameters. On the compact curve X of level $\Gamma(h)\cap\Gamma_0(s)$ the cover which chooses generators of the two cyclic subgroups is an étale torsor for $Z=(\mathbb{Z}/s\mathbb{Z})^\times$. On the smooth elliptic locus this follows since s is invertible and the full level h removes automorphisms. At a cusp (u,v) a stabilizing translation of width w has lower-left entry $-v^2w$ and lower-right entry $1+uvw$. For $p\mid s$, either $p\mid v$ or $p\mid w$. Thus its lower-right entry is one modulo every $p\mid s$. As s is squarefree the width stays the same after choosing both generators. In the tame Tate charts the parameter maps therefore have degree one and the residue extensions are étale. This proves the assertion on the compactification. Descent along

this torsor gives a line bundle L_ξ whose sections have the prescribed diamond character on the cover. It has degree zero, since its ℓ-th power is trivial. Its reduction is canonically trivial, since both characters reduce to one. These statements follow by trivializing the torsor étale locally and using the character for the transition functions, also when ℓ divides $|Z|$.

Let C be the cusp divisor and ω the Hodge bundle. The reduction of integral sections of $\omega^k(-C) \otimes L_\xi$ injects into $H^0(X_{\mathrm{sp}}, \omega^k(-C))$. Its image has codimension at most one. To see this, the module of integral sections is finite free over the coefficient DVR, with rank the generic-fiber dimension. The injection follows from multiplication by a uniformizer on the line bundle. The two Euler characteristics agree by Riemann–Roch, since the fibers have the same genus and the line bundles have the same degree. By Kodaira–Spencer, $\Omega^1 = \omega^2(-C)$. Serre duality identifies special-fiber H^1 with the dual of $H^0(X_{\mathrm{sp}}, \omega^{2-k})$. This has dimension zero for $k > 2$, because the modular discriminant gives a positive cusp divisor for ω^{12}, and one for $k = 2$, because the fiber is geometrically connected. This proves the codimension bound. Katz, *p-adic properties of modular schemes and modular forms*. In particular some nonzero vector in the two-dimensional space of Lemma 21.19 lifts.

The change of full h-level to $\Gamma_0(N)$ acts through a subgroup of $\mathrm{SL}_2(\mathbb{Z}/h\mathbb{Z})$ of order less than ℓ. Representatives can be chosen to act trivially modulo s by the Chinese remainder theorem and surjectivity of reduction for $\mathrm{SL}_2(\mathbb{Z})$. This action commutes with the auxiliary diamonds. Average a lift against the inverse of χ on this finite group. The denominator is a unit and the reduction, already of character χ, is preserved. We have obtained a nonzero residual Hecke eigenvector in the reduction of the classical cusp lattice at level Ns of character $\chi\xi$. The Hecke operators away from hs preserve this lattice and its reduction agrees on the chosen vector with the usual Fourier formula, since ξ reduces to one. This includes T_ℓ, whose coefficient at Q^n is $a_{\ell n} + \chi\xi(\ell)\ell^{k-1}a_{n/\ell}$, where the second coefficient is zero if $\ell \nmid n$.

The commutative algebra generated by these Hecke operators on the lattice is finite and torsion-free over the DVR. A minimal prime under the residual eigencharacter has characteristic zero because a uniformizer is a nonzero divisor. Passing to the fraction field of this finite domain and choosing a prime above the eigencharacter gives characteristic-zero eigenvalues with the desired reductions. They occur on the cusp space because the Hecke algebra acts faithfully there, so its localization at this generic factor has a nonzero eigenspace after scalar extension. Newform decomposition realizes that system in a primitive form of level dividing Ns. The character $\chi\xi$ has conductor Ns, forcing equality. At ℓ the eigenvalue is one modulo the maximal ideal. □

22 Relative orders through the norm map

22.1 Strict orders on one cyclotomic field per interval and precision

Fix the auxiliary primes on an interval of Section 6.6. Let E_* be its largest field, so $E_x \subseteq E_*$ with relative degree a power of two throughout the interval. For an odd p and $h \geq 1$ put $L_h = E_*(\mu_{p^h})$, $F_h = L_h^+$, $T_h = \widetilde{C}(F_h)$, and $\Delta_{x,h} = \mathrm{Gal}(L_h/E_x)$. Let $B_{x,h,r}$ be the quotient of T_h by p^h and by the relations $\delta - \kappa_p(\delta)^{-r} \bmod p^h$ for $\delta \in \Delta_{x,h}$. Only the action on μ_{p^h} is used to evaluate this scalar. Write $S_{x,r}$ for $\mathcal{S}_{p,r}(E_x)^{c=(-1)^r}$.

Theorem 22.1 (All twists and all fields of one interval)**.** *For every x on the interval one has $S_{x,r}[p^h] \simeq \mathrm{Hom}(B_{x,h,r}, \mathbb{Z}/p^h)$. The number $m_{x,h,r}$ of cyclic factors of $S_{x,r}$ of order at least p^h is $\dim_{\mathbb{F}_p} p^{h-1}B_{x,h,r}$. If $d_p = [E_*(\mu_p) : E_*]$, then for $t \geq 1$ integral*

$$\sum_{1\leq r<t} m_{x,h,r} \leq \left\lceil \frac{t-1}{d_p} \right\rceil \dim_{\mathbb{F}_p}(p^{h-1}T_h/p^hT_h), \qquad \sum_{1\leq r<t} \log_p |S_{x,r}| = \sum_{h\geq 1} \sum_{1\leq r<t} m_{x,h,r}.$$

There is also a fixed-field formula for full orders. Write $b = \log_p \exp T_1$. Whenever $p^b \mid r$, the full group $S_{x,r}$ is dual to

$$T_1 \Big/ \sum_{\delta \in \Delta_{x,1}} (\delta - \omega(\delta)^{-r}) T_1,$$

where ω is the Teichmüller lift of the action on μ_p. These assertions include odd primes dividing $[E_x : \mathbb{Q}]$.

Proof. Apply Theorem 22.5 first over E_*. Restriction to E_* identifies strict classes over E_x with the $\mathrm{Gal}(E_*/E_x)$-invariants. Indeed at the odd prime the degree is a unit, so restriction and averaging give descent in global cohomology and injectivity on each required local group, including the inertia groups away from p. This also follows from Lemma 19.4. All restriction maps in Theorem 22.5 are equivariant. Thus descending to E_x imposes precisely the equivariance for all lifts to $\Delta_{x,h}$, with the indicated action on the coefficients. The quotient formula follows. For finite abelian p-groups, duality into $\mathbb{Z}/p^h$ preserves the elementary divisors of exponent at most p^h. Multiplication by p^{h-1} counts the summands of exact order p^h at this precision. Summing over h counts the length of each summand in the full strict group. These groups are finite for the positive twists by Proposition 11.4.

The group $\mathrm{Gal}(L_h/E_*)$ is a subgroup of $(\mathbb{Z}/p^h)^\times$. Its subgroup of order prime to p is cyclic of order d_p and acts through roots of unity on the coefficient. Its character idempotents are integral since d_p is a unit and all d_p-th roots lie in $\mathbb{Z}_p$. Consequently $B_{x,h,r}$ is a quotient of the single ω^{-r}-component of $T_h/p^h T_h$. The d_p residues of r give all these components once. Multiplying each quotient by p^{h-1} gives the inequality by counting their occurrences up to $t-1$.

For the fixed-field assertion take $h = b+1$. The principal unit part of κ_p^{-r} is one modulo p^h when $p^b \mid r$, by binomial expansion on $1 + p\mathbb{Z}_p$. Thus Theorem 22.5 can use L_1 over E_* at this precision. Descend through the same group of order a power of two. Every resulting quotient has exponent at most p^b, hence the p^{b+1}-torsion has no element of order p^{b+1}. An element of any greater order would have a multiple of that order. It follows that this torsion already gives the full group. Duality can now be taken into $\mathbb{Q}_p/\mathbb{Z}_p$. □

At fixed p, h all tests above use the same real field F_h for every twist and every E_x on the interval. Theorem 28.11 bounds its contribution by ordinary class data and a determinant of local cyclotomic logarithms. A bound on the sum of the surviving lengths as p, h and the interval vary is still needed for Section 6.6.

22.2 A common quotient bound for the residual twists

Fix a whole interval in Section 6.6, an odd prime p, and integers $h > b \geq 0$, $T \geq 2$. Use the largest field E_* on this interval. Put $M = \widetilde{C}((E_*(\mu_{p^h}))^+)/p^h$, as in Theorem 22.1, and $d = [E_*(\mu_p) : E_*]$. In the infinite cyclotomic extension over E_*, the principal-unit image is $1 + p^a\mathbb{Z}_p$ for an integer $a \geq 1$. Take a generator u of this group and a Galois element γ with cyclotomic value u. Write M_τ for the summand of M on which the finite subgroup of order d acts by the character τ. All lengths below are over $\mathbb{Z}_p$.

For each τ list in increasing order the weights $1 \leq r < T$ with tame character $\omega^{-r} = \tau$ on this subgroup. The list is an arithmetic progression $r_i = r_0 + di$, $0 \leq i < k_\tau$. For a nonempty list put

$$w_i = ai + v_p(i!), \qquad D_\tau = w_{k_\tau - 1}.$$

For a field E_x on the interval let $S_{x,r} = \mathcal{S}_{p,r}(E_x)^{c=(-1)^r}$.

Theorem 22.2 (All residual lengths at one finite precision)**.** *If $b \geq D_\tau$ for every nonempty list, then*

$$\sum_{1 \leq r < T} \max_x \operatorname{length}_{\mathbb{Z}_p} \left((S_{x,r}/S_{x,r}[p^b])[p^{h-b}] \right) \;\leq\; \sum_{\tau : k_\tau > 0} \operatorname{length}_{\mathbb{Z}_p} \left(p^{b-D_\tau} M_\tau \right).$$

In particular it bounds the same sum for the surviving direct summands cut out by $1 - J_{p,r}$ in Section 6.6. At a point x of every sufficiently distant common interval one may use that section's $T = \lfloor x^{401} \rfloor$ and its original cutoff $b = b_0(x)$ for $p \leq P(x)$, $b = 0$ for $p > P(x)$. The exponents $w_0, \ldots, w_{k_\tau - 1}$ are the exact elementary divisor valuations of polynomial evaluation at the full list of wild characters, before reduction modulo p^h.

Proof. Because p is odd, its cyclotomic image is the direct product of the tame subgroup and the stated principal-unit group. Indeed the image is closed of finite index in $\mathbb{Z}_p^\times$; taking limits of powers separates its prime-to-p and pro-p parts. Character averages split M over $\mathbb{Z}_p$, since $d \mid p - 1$. For each weight choose any field E_{x_i} from the interval. By Theorem 22.1, the finite group $S_{x_i,r_i}[p^h]$ is dual to a quotient B_i of M_τ. On this quotient γ acts as the scalar $z_i = u^{-r_i}$ modulo p^h. The same element acts for every field, since it fixes E_*. On cyclic factors one checks that the length in the theorem is $\operatorname{length}(p^b B_i)$: a factor of exponent e contributes $\max(0, \min(e, h) - b)$ to either length.

For $i \geq 0$ set $P_i(Z) = \prod_{l<i}(Z - z_l)$, with empty product one. For distinct integral indices j, l one has $v_p(z_j - z_l) = a + v_p(j - l)$. In fact raising a principal unit of depth a to an exponent prime to p leaves its depth unchanged, and raising to p increases it by one, by binomial expansion for odd p. Also $p \nmid d$. It follows that for $j \geq i$ the value $P_i(z_j)$ has valuation at least w_i, with equality for $j = i$: the product of the i successive nonzero integers ending at j is a multiple of $i!$, equal to $i!$ at $j = i$. For $j < i$ the value is zero. Changing the monomial basis of degrees below k_τ to the monic polynomials P_i is integral unimodular. In their evaluation matrix, dividing column i by p^{w_i} gives a lower triangular integral matrix with units on its diagonal. This proves the elementary divisor assertion, since the w_i are nondecreasing.

Let Y be the image of $p^{b-D_\tau} M_\tau$ in $\bigoplus_i B_i$. Filter Y by requiring its first i coordinates to vanish. The quotient at stage i is the image of the i-th coordinate on that subgroup. For any $m \in M_\tau$, the image of $p^{b-w_i} P_i(\gamma) m$ belongs to this subgroup since $w_i \leq D_\tau$. Its i-th coordinate is p^b times a unit times the image of m. These coordinates therefore contain $p^b B_i$, including when the power is zero in the quotient. Additivity of length gives the proposed bound on this list. The fields were chosen independently, so we may maximize the individual lengths and add over the lists. The possible E_x form a finite chain. Passing to a direct summand of a finite abelian group decreases the displayed truncated length.

Finally the p-part of the index of the cyclotomic image is p^{a-1}, bounded by $[E_* : \mathbb{Q}]$ by restriction from the absolute Galois group of $\mathbb{Q}$. This field degree is polynomially bounded in V on $[V, V^{3/2}]$: the common biquadratic factors have bounded degree and the dyadic real layer has degree at most $2(V^{3/2})^{2+8\varepsilon}$ in the field construction. Thus $D_\tau \leq T(1 + \log_p[E_* : \mathbb{Q}] + 1/(p-1))$, eventually less than $b_0(x) = \lfloor \exp(x^\varepsilon/8) \rfloor$ uniformly for the small primes. For $p > P(x) = \exp(x^\varepsilon/12)$, $d \geq (p-1)/[E_* : \mathbb{Q}] > T$ eventually. Those lists contain at most one term, so their losses are zero. □

The result counts the twists together without a multiplicity factor in front of the length of a common real class group. A bound for the right side uniform in the precision, with the weighted sum over p required in Section 6.6, is still needed to control the full residual orders.

22.3 Full relative strict orders in progressions of twists

Fix one of the intervals of Section 6.6 and its largest field E_*. Fix an odd prime p and a subfield $F_0 \subseteq E_*$ of relative degree a power of two. For $F_0 \subseteq F \subseteq E \subseteq E_*$, write $S_r(E)$ for the sign $(-1)^r$ summand of the strict group. Put

$$U_r(E/F) = (1 - e_F)S_r(E), \qquad e_F = |\operatorname{Gal}(E/F)|^{-1} \sum_{\delta \in \operatorname{Gal}(E/F)} \delta.$$

All the fields here are abelian over $\mathbb{Q}$. In particular complex conjugation acts on their cohomology.

Use $L_h = E_*(\mu_{p^h})$ and its real logarithmic class group $T_h = \widetilde{C}(L_h^+)$ from Theorem 22.1. For a subfield A between F_0 and E_*, let $B_h(A, u)$ be the quotient of T_h/p^h by all the relations $\delta - \kappa_{p,h}(\delta)^{-u}$ for $\delta \in \operatorname{Gal}(L_h/A)$, where $\kappa_{p,h}$ is the action on μ_{p^h}. Define

$$D_h(E/F, u) = \ker\big(B_h(E, u) \longrightarrow B_h(F, u)\big), \qquad M_h = \operatorname{lcm}\big(2,\ |\kappa_{p,h}(\operatorname{Gal}(L_h/F_0))|\big).$$

The arrow imposes the extra relations over F.

Theorem 22.3 (Full strict orders from one relative quotient)**.** *Let $u \geq 1$ and $h \geq 1$. If $p^{h-1}D_h(E_*/F_0, u) = 0$, then for every positive $r \equiv u \bmod M_h$ and every $F_0 \subseteq F \subseteq E \subseteq E_*$, the full group $U_r(E/F)$ has the elementary divisors of $D_h(E/F, u)$. For every fixed u such an h exists. For $h = 1$ the test is just the vanishing of the relative quotient modulo p. For the whole $S_r(E)$ the same statements use $B_h(E, u)$ in place of the relative quotients and the test at E_*.*

Proof. Restriction to E_* identifies $S_r(A)$ with the $\operatorname{Gal}(E_*/A)$-invariants in $S_r(E_*)$. Indeed averaging is exact in degree a power of two at the odd prime p. Inflation–restriction gives this assertion in global degree one. Restriction on the local groups above p is injective by corestriction, so the criterion of local triviality descends as well. The same argument applies to the unramified conditions outside p. All maps commute with the sign projection. This also proves the assertion for a real subfield, where the negative sign part is zero.

The finite-precision identification of Theorem 22.1 thus identifies $S_u(A)[p^h]$ with the characters of $B_h(A, u)$ into $\mathbb{Z}/p^h$. One may fix a generator for the coefficient module at this precision. Under restriction from F to E a character of T_h is the same character subject to fewer equivariance conditions. Dualizing restriction gives exactly the quotient arrow above. Since e_F is an integral projection, $D_h(E/F, u)$ is dual to $U_u(E/F)[p^h]$. In particular the test at E_*/F_0 holds precisely when this largest relative group has no element of order p^h. For a finite abelian p-group this means that its full exponent divides p^{h-1}. By finiteness at the positive twist u in Proposition 11.4, we can choose h above the exponent valuation.

If $r \equiv u \bmod M_h$, all the defining scalars are identical at precision h, by Lagrange's theorem on the image of $\kappa_{p,h}$, and the sign agrees as well. Consequently every quotient and every arrow just used is identical at that precision. The test now bounds the full exponent at r over E_*/F_0. Under restriction each $U_r(E/F)$ lies in $U_r(E_*/F_0)$, since averaging first over $\operatorname{Gal}(E_*/F)$ and then over the larger group fixing F_0 gives the latter average. Hence the same exponent bounds every smaller relative group. Its subgroup killed by p^h is the whole group, and the dual identification gives the claimed elementary divisors. Omitting the two averages gives the assertion for $S_r(E)$. □

For the small-twist range one can take F_0 to be the smallest L_x on the interval and use $E = E_x, F = L_x$. For the large twists at $p \in \Pi$, use the smallest $B(x)$ and $F = B(x)$. For $J_{p,r} = 0$ use the whole-group version. At a given x, let N_x count the integers in the applicable

range $1 \le r < t(x)$ in a progression tested by the theorem. Put $b = b_0(x)$ for $p \le P(x)$ and $b = 0$ otherwise. Its exact contribution to the residual length sum of Proposition 6.11 is

$$N_x(\log p)\ \mathrm{length}_{\mathbb{Z}_p}(p^b D_h(E_x/F, u)),$$

with $B_h(E_x, u)$ in the whole-group case. This follows on each cyclic factor by removing its subgroup killed by p^b. The relative test can succeed even when the invariant summand has larger exponent. A bound for the weighted sum over all progressions and primes on these intervals is still required.

22.4 What two class groups determine about every twist

Fix the auxiliary primes and let E_* be the largest CM field on one interval of Section 6.6. Fix an odd prime p. Write $L_\infty = E_*(\mu_{p^\infty})$, $F_\infty = L_\infty^+$ and $F_0 = (E_*(\mu_p))^+$. Let F_j/F_0 be the subextension of degree p^j in F_∞. This is the cyclotomic $\mathbb{Z}_p$-extension of F_0. Indeed $L_\infty = E_*(\mu_p)\mathbb{Q}_\infty$, where $\mathbb{Q}_\infty$ is the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$. Taking real parts gives $F_\infty = F_0\mathbb{Q}_\infty$, since the quadratic extension $E_*(\mu_p)/F_0$ is imaginary. Put $H = \mathrm{Gal}(F_\infty/F_0)$. Via restriction, a topological generator γ of H has a unique lift to $\mathrm{Gal}(L_\infty/E_*(\mu_p))$. Write $a \in 1 + p\mathbb{Z}_p$ for its cyclotomic character.

Take the finite prime-to-p subgroup D' of a decomposition group at p in $\mathrm{Gal}(F_\infty/\mathbb{Q})$. It is the same for every prime above p, by commutativity. Set

$$e = 1 - \frac{1}{|D'|}\sum_{g \in D'} g, \qquad C_j = e\ \mathrm{Cl}(F_j)\{p\} \quad (j = 0, 1).$$

Braces denote the primary subgroup. Let Δ_0 be the tame subgroup of $\mathrm{Gal}(L_\infty/E_*)$. The cyclotomic character identifies it with a subgroup of the $(p-1)$-st roots of unity in $\mathbb{Z}_p^\times$. For a character τ of Δ_0 with these values, use the usual integral character idempotent e_τ, acting on the class groups through restriction to the real field. Define

$$C_{j,\tau} = e_\tau C_j, \qquad K_\tau = \ker(\mathrm{N} : C_{1,\tau} \longrightarrow C_{0,\tau}), \qquad b_\tau = \dim_{\mathbf{F}_p}(K_\tau/pK_\tau).$$

For $E = E_x$ on the interval, let $A_r(E)$ be the Pontryagin dual of the complementary strict group of Theorem 22.1, in its *untwisted class group coordinates*. Thus the relation for $\delta \in \mathrm{Gal}(L_\infty/E)$ in these coordinates is action by $\kappa_p(\delta)^{-r}$. Put $B_r(E) = eA_r(E)$, $\tau = \kappa_p^{-r}|_{\Delta_0}$ and $s_r = v_p(a^{-r} - 1)$.

Theorem 22.4 (Two ordinary class groups and all positive twists)**.** *For every E_x on this interval and every positive r, the norm defining K_τ is onto, $B_r(E_x)/p^{s_r}B_r(E_x)$ is a quotient of $C_{0,\tau}$, and at most b_τ cyclic factors of $B_r(E_x)$ have order greater than p^{s_r}. If $K_\tau = 0$, the full group in question is*

$$B_r(E_x) \simeq C_{0,\tau}/\overline{\sum_{\delta \in \mathrm{Gal}(L_\infty/E_x)} (\delta - \kappa_p(\delta)^{-r})C_{0,\tau}}.$$

The finite group on the right uses the action on F_0. The same assertions hold after imposing any further integral character idempotent commuting with the field action, applied to all the modules in the statements.

Proof. Let $\mathcal{N}$ be the maximal abelian pro-p extension of F_∞ unramified away from p and split at every prime over p. Write $X = \mathrm{Gal}(\mathcal{N}/F_\infty)$. Conjugation acts on X through $\mathrm{Gal}(F_\infty/\mathbb{Q})$, since the local conditions are preserved by that group and X is abelian. For each j there is a canonical isomorphism

$$X/(\gamma^{p^j} - 1)X \simeq \widetilde{C}(F_j).$$

To see this, the Galois group of $\mathcal{N}/F_j$ is an extension of the procyclic group H^{p^j} by X. It is pro-p. A lift of a topological generator defines a continuous section because its closed cyclic subgroup maps isomorphically onto H^{p^j}. The commutator subgroup after closure is $(\gamma^{p^j}-1)X$, which is already compact. The maximal abelian subextension allows at p only subextensions of the local cyclotomic tower, and is unramified elsewhere. Conversely any finite abelian p-extension of F_j with these conditions becomes split at p and unramified elsewhere after adjoining F_∞. Its compositum with F_∞ is abelian over F_∞, so it lies in $\mathcal{N}$. Taking the kernel of the map to H^{p^j} gives the stated isomorphism by the definition of the degree-zero logarithmic class group. Inclusion of Galois groups induces the quotient map on X when j decreases. Under class field reciprocity this inclusion on abelianizations is the norm on ideles.

At each finite level D' fixes every prime over p. Its action on each local cyclotomic degree group is trivial because the cyclotomic Galois group is abelian. In the exact sequence of Theorem 28.11, e therefore kills the entire local kernel and the quotient of the global degree group. Further, inverting p in the ordinary ideal class group kills precisely the subgroup generated by classes of primes above p, which e also annihilates. Projection by an integral idempotent is exact. These identifications give, compatibly with norms, for $M = e_\tau e X$,

$$C_{0,\tau} = M/(\gamma-1)M, \qquad C_{1,\tau} = M/(\gamma^p-1)M.$$

In particular the norm is onto. Put $U = (\gamma-1)M$ and $N_\gamma = 1+\gamma+\cdots+\gamma^{p-1}$. The norm kernel is canonically $U/N_\gamma U$.

Theorem 22.1 identifies $B_r(E_x)$ with the quotient of M by all the displayed character relations for $\mathrm{Gal}(L_\infty/E_x)$. In detail, modulo p^h the kernel of the action on $E_*(\mu_{p^h})$ has trivial twisting scalar. Its relation on X gives precisely the logarithmic group of the corresponding finite real layer by the preceding isomorphism. The remaining relations are those of that theorem. Projecting by e_τ retains the whole e-part of the quotient because Δ_0 already acts there by τ. Passing over all h recovers the compact quotient with the closed relation subgroup. Its finite quotients of p-power exponent separate its points, and the strict group is finite by Proposition 11.4.

Under $M \to B = B_r(E_x)$, the image of U is $(a^{-r}-1)B = p^{s_r}B$. The image of $N_\gamma U$ is $p^{s_r+1}B$, since $1 + a^{-r} + \cdots + a^{-(p-1)r}$ has valuation one. Indeed $a^{-r} = 1+z$, $z \in p\mathbb{Z}_p$, and the sum is $p + \binom{p}{2}z + \cdots + z^{p-1}$, congruent to p mod p^2 for odd p. It follows that $B/p^{s_r}B$ is a quotient of $C_{0,\tau}$, and $p^{s_r}B/p^{s_r+1}B$ is a quotient of K_τ/pK_τ. The latter dimension counts the indicated cyclic factors exactly.

If $K_\tau = 0$, then $U = N_\gamma U$. On any finite continuous H-stable quotient of U, N_γ acts nilpotently. Modulo p it acts as $(\gamma-1)^{p-1}$, and the action of γ has p-power order. A power of N_γ therefore maps the finite quotient into its multiple by p, and iteration kills it. Surjectivity forces the quotient to vanish. These quotients separate points: intersect a separating open subgroup with all its H-translates. The orbit of the subgroup is finite by continuity and compactness (an open subgroup of H preserves it, by applying compactness to the subgroup of U and then using inverses). Thus $U = 0$, so $M = C_{0,\tau}$ with trivial action of H. The full quotient formula follows. Commuting integral projectors preserve all the quotient maps and identities above. □

22.5 Real logarithmic class groups at arbitrary precision

Let p be odd. For a number field D, let $X(D)$ be the maximal abelian pro-p Galois quotient unramified outside p in which the decomposition map at each $w \mid p$ factors through the local cyclotomic $\mathbb{Z}_p$-extension. Let Γ_D be the Galois group of the cyclotomic $\mathbb{Z}_p$-extension of D. Its character is the principal unit part $\langle \kappa_p \rangle$ of the cyclotomic character. The quotient $X(D) \to \Gamma_D$

is surjective. Write $\widetilde{C}(D)$ for its kernel, the logarithmic class group of degree zero at p. It is finite for fields abelian over $\mathbb{Q}$, by the abelian case of the Gross–Kuz'min theorem. For the identification with logarithmic classes and this finiteness result see K. Belabas and J.-F. Jaulent, *The logarithmic class group package in PARI/GP*, Section 1. The connection of these classes with twists of wild kernels is developed by J.-F. Jaulent and A. Michel, *Approche logarithmique des noyaux étales sauvages des corps de nombres*.

Fix an abelian field $E/\mathbb{Q}$, $r \geq 1$, $h \geq 1$, and $R_h = \mathbb{Z}/p^h$. Let L be a finite cyclotomic extension of E inside $E(\mu_{p^\infty})$, Galois over $\mathbb{Q}$, containing μ_p, such that $\kappa_p^{-r} \bmod p^h$ is trivial on G_L. One may always take $E(\mu_{p^h})$. Put $F = L^+$, $\Delta = \mathrm{Gal}(L/E)$, and let $\theta : \Delta \to R_h^\times$ be the induced character $\kappa_p^{-r} \bmod p^h$. Use compatible cyclotomic coordinates on the coefficients.

Theorem 22.5 (The complementary strict group on a real field)**.** *Let Δ act on $\widetilde{C}(F)$ by restriction of its automorphisms to F. Form the finite module*

$$B_{h,r} = \frac{\widetilde{C}(F)}{p^h\widetilde{C}(F) + \sum_{\delta\in\Delta}(\delta - \theta(\delta))\widetilde{C}(F)}.$$

In this expression scalar residues can be lifted arbitrarily to $\mathbb{Z}_p$ since the denominator contains $p^h\widetilde{C}(F)$. With c complex conjugation there is an isomorphism

$$(\mathcal{S}_{p,r}(E)^{c=(-1)^r})[p^h] \simeq \mathrm{Hom}(B_{h,r}, R_h).$$

The formula allows p to divide $|\Delta|$ and $[E:\mathbb{Q}]$.

Proof. Let G be the Galois group over E unramified outside p, allowing all archimedean places, and put $N = \ker(\kappa_p|G)$, $J = G/N$. The image J is a closed subgroup of $\mathbb{Z}_p^\times$ with an open procyclic pro-p part. For $D_h = R_h(\kappa_p^{-r})$, restriction induces

$$H^1(G, D_h)/\inf H^1(J, D_h) \simeq \mathrm{Hom}(N, D_h)^J.$$

Indeed N acts trivially and $H^2(J, D_h) = 0$ in inflation–restriction. For the latter fact a copy of $\mathbb{Z}_p$ has the length-one completed group-ring resolution given by multiplication by $\gamma - 1$, followed by augmentation. Identifying its completed group ring with $\mathbb{Z}_p[[T]]$ sends $\gamma - 1$ to T, proving exactness. Passing to J takes invariants under a finite group of order prime to p, an exact operation by averaging.

Let $\mathfrak{X}$ be the maximal abelian pro-p quotient of N after killing the images of the local cyclotomic kernels at all places over p and their conjugates in G. Lemma 24.11 now identifies the full strict p^h-torsion with $\mathrm{Hom}_J(\mathfrak{X}, D_h)$. In detail the finite class must restrict to zero on each such kernel, where the coefficient action is trivial. The quotient by global cyclotomic classes in that lemma is precisely the kernel of restriction to N above. Outside p the unramified condition is already imposed in G.

Over L the same N and $\mathfrak{X}$ occur. In fact L/E lies in the cyclotomic tower and is unramified away from p. The maximal extensions unramified outside p over the two fields coincide, as is seen by taking the compositum of the conjugates over E of each finite extension over L. At a place over p the absolute local cyclotomic kernel already fixes L_w. Ranging over all places of L gives the same collection of kernels up to conjugation. Write $J_L = \kappa_p(G_L)$. Since D_h is trivial over L, the J_L-invariant homomorphisms out of $\mathfrak{X}$ identify naturally with $\mathrm{Hom}(\widetilde{C}(L), R_h)$ in the untwisted coordinates. To see this, apply the same restriction calculation over L to the trivial finite module. Its numerator consists of characters on $X(L)$, as each local character factors through the cyclotomic image at p. Its denominator consists of the pullbacks of characters on Γ_L. Restriction from $X(L)$ to its degree-zero kernel realizes their quotient, since $X(L) \to \Gamma_L \simeq$

$\mathbb{Z}_p$ splits as a map of abelian pro-p groups by lifting a topological generator. The restriction map is canonical and is equivariant under field automorphisms. Requiring equivariance under all of J imposes $f(\delta z) = \theta(\delta) f(z)$ for $\delta \in J/J_L = \Delta$. This argument takes no average over Δ.

On the coefficient, complex conjugation acts by $(-1)^r$. Thus in the desired eigenspace the corresponding untwisted character satisfies $f(cz) = f(z)$. The untwisted invariant characters of $\widetilde{C}(L)$ are exactly those on $\widetilde{C}(F)$. Here are the local details. Restriction identifies R_h-valued global characters over F with the invariant characters over L, since L/F has order two. At each place away from p its inertia subgroup after restriction has index at most two in the original inertia subgroup. A character zero on the former is zero on both. At a place over p, intersect the kernel of $\langle \kappa_p \rangle$ with the local absolute group of L. This intersection again has index at most two in that kernel, proving descent of the local condition in both directions. The pro-p global cyclotomic images for L, F agree by the same index argument. Taking invariants is exact at the odd prime p, so the identification remains valid on quotienting by the global cyclotomic characters. All these maps commute with Δ. Factoring a homomorphism to R_h with the stated equivariance through $B_{h,r}$ now gives the required isomorphism. □

22.6 An interval bound outside the factors detected by the norm kernel

Use the fields and the class groups of Theorem 22.4 on $[V, V^{3/2}]$, with the same pair of auxiliary primes that occurs in the periods. For each odd prime p write $B_{p,r}$ for the summand $B_r(E_x)$ in that theorem, and put

$$t = \lfloor x^{401} \rfloor, \qquad Y = x^{-3} \exp(x^{\varepsilon}/4), \qquad n_* = [E_* : \mathbb{Q}].$$

Write the elementary divisor exponents of $B_{p,r}$ in decreasing order as $v_1(p,r), v_2(p,r), \ldots$, padded by zeros. For each p, r use $b_{p,\tau} = \dim_{\mathbf{F}_p} K_\tau / pK_\tau$ and $s_{p,r} = v_p(a^{-r} - 1)$ from that theorem. Define the nonnegative integer

$$D_{p,r} = \sum_i \min\{v_i(p,r), s_{p,r}\}.$$

Theorem 22.6 (A uniform bound for the part determined by the first layer)**.** *At every sufficiently large x on the common intervals,*

$$\sum_{\substack{2<p\le Y \\ p \text{ prime}}} (\log p) \sum_{1\le r<t} D_{p,r} \ll_{\psi,\varepsilon} x^{-2} \exp(x^{\varepsilon}/2).$$

The difference between the left side and the corresponding sum of the full logarithmic orders of $B_{p,r}$, taken as full sum minus displayed sum, is exactly

$$\sum_{2<p\le Y} (\log p) \sum_{1\le r<t} \sum_{i=1}^{b_{p,\tau}} (v_i(p,r) - s_{p,r})_+, \qquad \tau = \kappa_p^{-r}|_{\Delta_0}.$$

Here the outer sum is over primes and $z_+ = \max(z, 0)$. Consequently entire summands satisfying the two-layer norm isomorphism test enter the first bound simultaneously at all their positive twists below t.

Proof. For a fixed prime, $D_{p,r} \log p$ is the logarithm of the order of $B_{p,r}/p^{s_{p,r}} B_{p,r}$. Theorem 22.4 bounds it by $\log |C_{0,\tau}|$. The integral character idempotents for Δ_0 are orthogonal and sum to one, so summing $\log |C_{0,\tau}|$ once over all characters gives $\log |e \operatorname{Cl}(F_0)\{p\}|$. As r varies, every character occurs at most $1 + t/d_p$ times, with

$$d_p = |\Delta_0| = [E_*(\mu_p) : E_*] \ge (p-1)/n_*.$$

This degree bound follows by intersecting E_* with $\mathbb{Q}(\mu_p)$. The count therefore uses a single ordinary class number at each prime, even though the field in the period varies along the interval.

Write N_* for a cyclotomic modulus for E_* as in Theorem 19.15. Since $F_0 \subseteq \mathbb{Q}(\zeta_{pN_*})$, its degree d is at most n_*p and the conductor–discriminant formula gives $|\operatorname{disc}(F_0)| \le (pN_*)^d$. Minkowski's theorem supplies an integral ideal of norm at most $A = (4/\pi)^d |\operatorname{disc}(F_0)|^{1/2}$ in every ideal class. The number of such ideals is at most $A^2\zeta_{F_0}(2)$; this follows by bounding each indicator by $A^2/(\mathrm{N}\mathfrak{a})^2$. The Euler product gives $\zeta_{F_0}(2) \le \zeta(2)^d$ because the number of prime ideals over a rational prime is at most d. In particular

$$\log|\operatorname{Cl}(F_0)| \ll n_*p\log(2pN_*).$$

Summing over the integers from 3 to Y bounds the desired sum by $O((n_*Y^2+n_*^2tY)\log(2N_*Y))$, using $p/(p-1) \le 2$. On the specified interval, $n_* \ll_\psi V^{3+12\varepsilon} \le C_\psi x^{3+12\varepsilon}$. This follows from the dyadic degree at its upper endpoint and the fixed degree of the other factors. The modulus consists of the same fixed character conductor, two fixed auxiliary primes, and a power of two of polynomial size in V. Thus $\log(2N_*Y) \ll_{\psi,\varepsilon} x^{\varepsilon}$, by the conductor bounds of Section 6.6. The first summand is $O_{\psi,\varepsilon}(x^{-3+13\varepsilon}\exp(x^{\varepsilon}/2))$. The second is bounded by a fixed power of x times $\exp(x^{\varepsilon}/4)$. Both satisfy the asserted bound since $0 < \varepsilon < 1/52$.

Finally the same two-layer theorem gives $v_i(p,r) \le s_{p,r}$ for $i > b_{p,\tau}$. Subtracting the truncated length on each cyclic factor proves the exact expression for the excess. If $K_\tau = 0$ the inner sum is empty. □

The estimate covers the summand away from the trivial action of the prime-to-p decomposition group. It leaves the excess orders in the formula, the invariant summand, and primes above Y to the other arithmetic estimates of Section 6.6.

22.7 The strict group at each cyclotomic norm level

Fix a power interval and use its largest field E_*, as in Section 6.6. Fix an odd prime p and write $L_\infty = E_*(\mu_{p^\infty})$, $F_\infty = L_\infty^+$, $F_0 = E_*(\mu_p)^+$. Let F_j/F_0 be the layer of degree p^j in F_∞. Write $T_j = \widetilde{C}(F_j)$ for the degree-zero logarithmic class group. Here the subscript counts layers above F_0. For $E = E_x$, put $G_x = \operatorname{Gal}(L_\infty/E)$ and let $A_{x,r}$ be the Pontryagin dual of $\mathcal{S}_{p,r}(E)^{c=(-1)^r}$, in the untwisted class group coordinates of Theorem 22.1. Thus the character on these coordinates is $\eta_r(\delta) = \kappa_p(\delta)^{-r}$. For a compact module T with the indicated action set

$$Q_{x,r}(T) = T/\overline{\sum_{\delta\in G_x}(\delta - \eta_r(\delta))T}.$$

On T_j the field action is the one on F_j. The scalar uses the indicated lift to L_∞.

Theorem 22.7 (The exact strict quotient at a fixed norm level)**.** *Let a be the cyclotomic value of a topological generator γ of $\operatorname{Gal}(L_\infty/E_*(\mu_p))$. Write $s_r = v_p(a^{-r}-1)$. For every positive r, every $j \ge 0$, and every field E_x on the interval there is an isomorphism of finite abelian groups*

$$Q_{x,r}(T_j) \simeq A_{x,r}/p^{s_r+j}A_{x,r}. \tag{22.1}$$

In particular the base-p logarithm of $|Q_{x,r}(T_{j+1})|/|Q_{x,r}(T_j)|$ counts the cyclic factors of $A_{x,r}$ of order greater than p^{s_r+j}. If the two orders agree, $Q_{x,r}(T_j)$ already gives the full order and all the elementary divisors of $A_{x,r}$. This applies to every tame character, including the invariant part for the prime-to-p decomposition group.

Proof. The intersection of $E_*(\mu_p)$ with the field of all p-power roots of unity has degree p^u over $\mathbb{Q}(\mu_p)$ for some $u \geq 0$. Indeed the cyclotomic group over $\mathbb{Q}(\mu_p)$ is $1 + p\mathbb{Z}_p \simeq \mathbb{Z}_p$. Its subgroup of index p^u is $1 + p^{u+1}\mathbb{Z}_p$. Thus $v_p(a-1) = u+1$, and p^u divides $[E_*(\mu_p) : \mathbb{Q}(\mu_p)] \leq [E_* : \mathbb{Q}]$. In the tower one consequently has

$$E_*(\mu_{p^{u+1+i}})^+ = F_i \qquad (i \geq 0).$$

The extension before taking real parts has degree p^i over $E_*(\mu_p)$. Taking real parts preserves that degree because both fields are CM. If $z \in p\mathbb{Z}_p$ has valuation d, the binomial expansion shows that $(1+z)^p - 1$ has valuation $d+1$, and that raising $1+z$ to an exponent prime to p preserves d. Inverting a unit preserves the valuation of its difference from one. It follows that

$$s_r = u + 1 + v_p(r), \qquad v_p(a^{-rp^j} - 1) = s_r + j.$$

For use with the norm, let X be the Galois group of the maximal abelian pro-p extension of F_∞ unramified away from p and split at the places over p. The conjugation action is well defined on this abelian group. Recall the class field argument in Theorem 22.4. Over F_i the group upstairs is an extension of $\langle \gamma^{p^i} \rangle \simeq \mathbb{Z}_p$ by X. A lift of its topological generator supplies a section. The closed commutator subgroup is therefore $(\gamma^{p^i} - 1)X$. Abelianizing, then taking the kernel of the map to the cyclotomic group, gives $T_i = X/(\gamma^{p^i} - 1)X$. In fact a finite abelian extension with the indicated local cyclotomic conditions splits at the places over p after adjoining F_∞, and the converse follows by restriction at each completion. Under reciprocity, inclusion from the higher field gives the norm. Hence for $k \geq j$ the norm $T_k \to T_j$ is onto with kernel $(\gamma^{p^j} - 1)T_k$.

Set $h = s_r + j$ and $k = j + v_p(r)$. Then $E_*(\mu_{p^h})^+ = F_k$. The finite-coefficient description in Theorem 22.1, dualized using $1 \mapsto p^{-h} \bmod \mathbb{Z}_p$ on $\mathbb{Z}/p^h$, identifies $A_{x,r}/p^h A_{x,r}$ with $Q_{x,r}(T_k)/p^h Q_{x,r}(T_k)$. All lifts of a given automorphism of $E_*(\mu_{p^h})$ give the same scalar modulo p^h. On this quotient the operator $\gamma^{p^j} - 1$ acts by $a^{-rp^j} - 1$, which is zero modulo p^h. Thus passage by norm to T_j imposes precisely relations already satisfied, giving $Q_{x,r}(T_j)/p^h Q_{x,r}(T_j)$. On T_j itself γ^{p^j} acts trivially. Its character relation kills $(a^{-rp^j} - 1)Q_{x,r}(T_j) = p^h Q_{x,r}(T_j)$. This proves (22.1) with the asserted precision.

For a cyclic group of order p^v, the quotient modulo p^h has order $p^{\min(v,h)}$. Its order increases by a factor of p at the next precision exactly when $v > h$. Multiplication over the cyclic factors proves both final assertions, since $A_{x,r}$ is finite by Proposition 11.4. □

22.8 The total contribution of the primes required to split

Fix a field $E = E_x$ on the interval in Section 6.6 and write $n = [E : \mathbb{Q}]$. For each odd prime p form $F_\infty = (E_*(\mu_{p^\infty}))^+$ using the same largest field E_* on this interval. Let M_p be the Galois group of the maximal everywhere unramified abelian pro-p extension of F_∞. Let X_p be its quotient obtained by imposing complete splitting at the primes above p. Use $Q_{x,r}$ and $A_{p,x,r}$ as in Theorem 22.7. Put $U_{p,x,r} = Q_{x,r}(M_p)$. The following estimate compares the full orders at all primes using only the degree of the original field and the range of weights.

Theorem 22.8 (The cost of the splitting condition at all odd primes)**.** *For every positive r there is a natural surjection of finite groups $U_{p,x,r} \longrightarrow A_{p,x,r}$. Write e_p for the ramification index of p in $E/\mathbb{Q}$. This map is an isomorphism whenever $p - 1 > e_p r$. For every integer $t \geq 2$,*

$$0 \leq \sum_{p>2} \sum_{1 \leq r < t} \log \frac{|U_{p,x,r}|}{|A_{p,x,r}|} \leq 6n(t-1)\log(2nt). \tag{22.2}$$

Here p runs over primes. At each pair (p, r), one may also apply multiplication by any power $p^{k_{p,r}}$ with $k_{p,r} \geq 0$ to both groups and use the orders of their images in the same inequality.

Proof. First identify $Q_{x,r}(X_p)$. In the notation of Theorem 22.7 the logarithmic class group at level j is $X_p/(\gamma^{p^j}-1)X_p$. On its twisted quotient the additional relation coming from $\gamma^{p^j}-1$ is multiplication by $a^{-rp^j}-1$. It generates the ideal $p^{s_r+j}\mathbb{Z}_p$. The finite quotients of $Q_{x,r}(X_p)$ modulo p^{s_r+j} are therefore the quotients of $A_{p,x,r}$ at exactly those precisions, by (22.1). The identifications use restriction of characters and norm between layers, so they commute with reduction. A compact abelian pro-p group is the inverse limit of these quotients. Indeed every finite quotient has bounded exponent, and compactness gives surjectivity to the inverse limit. This identifies $Q_{x,r}(X_p)$ with $A_{p,x,r}$, which is finite by Proposition 11.4.

The primes above p in F_∞ form a finite set $\mathcal{P}$, and each has finite residue field. In fact the underlying real cyclotomic tower of $\mathbb{Q}$ has one such prime with residue field $\mathbb{F}_p$, and F_∞ has degree at most $[E_* : \mathbb{Q}]$ over this tower. At $w \in \mathcal{P}$ the local unramified pro-p group is generated by arithmetic Frobenius on the residue field. Denote its image in M_p by ϕ_w. This element is independent of the chosen prolongation since M_p is abelian. A field automorphism sends ϕ_w to $\phi_{\delta w}$, because its action on residues carries the power map defining one arithmetic Frobenius to the other. Consequently the kernel D_p of $M_p \to X_p$ is the image of the permutation module $\mathbb{Z}_p[\mathcal{P}]$ under $[w] \mapsto \phi_w$. Its image is compact, hence closed. Quotienting by the character relations is right exact. Lifting the relations on $X_p = M_p/D_p$ gives the quotient by D_p and the same relations on M_p. Thus the kernel of $U_{p,x,r} \to A_{p,x,r}$ is a quotient of $Q_{x,r}(\mathbb{Z}_p[\mathcal{P}])$.

Write $G_x = \mathrm{Gal}(E_*(\mu_{p^\infty})/E)$. The primes of $\mathcal{P}$ in a single G_x-orbit contribute at most one cyclic summand to the latter quotient. Indeed $[\delta w] = \kappa_p(\delta)^{-r}[w]$ there. Every value $1-\kappa_p(\delta)^{-r}$ for a stabilizer element kills this generator. To bound its order, extend w to the CM tower and let v be its restriction to E. The image of the local absolute Galois group of E_v fixes this prolongation and hence w. Its cyclotomic image is

$$H_v = \mathrm{Gal}(\mathbb{Q}_p(\mu_{p^\infty})/(E_v \cap \mathbb{Q}_p(\mu_{p^\infty}))) \;\subseteq\; \mathbb{Z}_p^\times.$$

The index is the degree of the intersection. This finite intersection is totally ramified over $\mathbb{Q}_p$, so its degree divides e_p. Write $H_v = \mu_d \times (1+p^h\mathbb{Z}_p)$, where $d \mid p-1$ and $h \geq 1$. This decomposition follows by projecting a closed subgroup of $\mu_{p-1} \times (1+p\mathbb{Z}_p)$ to its prime-to-p and pro-p factors, as in Theorem 9.16. In particular

$$\frac{p-1}{d}\,p^{h-1} \;\mid\; e_p.$$

The quantities d, h are the same above each v, since $E/\mathbb{Q}$ is Galois. If $d \nmid r$, some element of μ_d gives a unit among the annihilators, so the generator vanishes. If $d \mid r$, a generator of $1+p^h\mathbb{Z}_p$ gives an annihilator of valuation $h + v_p(r)$ by the binomial formula at an odd prime. These bounds show the kernel is finite, and they prove the asserted isomorphism whenever $p-1 > e_p r$.

The number of orbits is the number of primes of E^+ above p. Indeed restriction identifies G_x with $\mathrm{Gal}(F_\infty/E^+)$, since $EF_\infty = E_*(\mu_{p^\infty})$ and $E \cap F_\infty = E^+$. The number of primes of E^+ is at most the number of primes of E, which is at most n/e_p. Put $m = \lfloor (t-1)/d \rfloor$. The sum of $v_p(r)$ over the positive multiples $r = di < t$ equals $\sum_{j \geq 1} \lfloor m/p^j \rfloor \leq m/(p-1)$. The total logarithmic kernel order at p is therefore at most

$$\frac{n}{e_p}\frac{t-1}{d}\left(h + \frac{1}{p-1}\right)\log p \;\leq\; n(t-1)\frac{\log p}{p-1}\left(1 + \frac{1}{p-1}\right).$$

For the last inequality use $e_p d \geq (p-1)p^{h-1}$ and $h \leq p^{h-1}$. All the kernels vanish if $p > 1 + n(t-1)$. For $M = 1 + n(t-1)$ the elementary bound $\sum_{p \leq M} (\log p)/p \leq 2 \log M$ follows from $\lfloor M/p \rfloor \geq M/(2p)$ and $\sum_{p \leq M} \lfloor M/p \rfloor \log p \leq \log(M!)$. For $p \geq 3$, $p/(p-1) \leq 3/2$ and $1 + 1/(p-1) \leq 3/2$. These estimates imply (22.2). Finally $p^k U_{p,x,r} \to p^k A_{p,x,r}$ is onto, and

its kernel is a subgroup of the original kernel. This proves the estimate at all the stated precisions. □

On the intervals of Section 6.6, $n \le [E_* : \mathbb{Q}] \ll_\psi x^{3+12\varepsilon}$ and $t = \lfloor x^{401} \rfloor$. Thus even the full correction is $O_{\psi,\varepsilon}(x^{404+12\varepsilon}\log(2x))$. This also bounds the change in the excess above the precisions of Theorem 9.16. It leaves the sizes of the ordinary unramified specializations themselves to be estimated.

22.9 Strict classes killed by one integer throughout an interval

Fix an interval $[V, V^{3/2}]$ of Theorem 19.15 and $0 < \varepsilon < 1/52$. At x write $E = E_x$, $g = [E : \mathbb{Q}]$, $t = \lfloor x^{401} \rfloor$, and let N be the cyclotomic modulus used for the theta periods. For an odd prime p put

$$M_{p,r}(E) = \tfrac{1}{2}(1 + (-1)^r c)\mathcal{S}_{p,r}(E), \qquad P = \exp(x^\varepsilon/12).$$

Here c is complex conjugation on the field. If B is a positive integer, $M[B]$ denotes the kernel of multiplication by B on M. The prime powers occurring in B can have very different exponents. We estimate their contributions using the same integer at every weight.

Theorem 22.9 (Order of the strict subgroup killed by a common integer)**.** *On every sufficiently distant such interval, for $Y \ge P$ and $B \ge 1$,*

$$\sum_{\substack{p \le Y \\ p \text{ odd prime}}} \sum_{1 \le r < t} \log |M_{p,r}(E)[B]| \ \ll\ g\left\{tP\left(1 + \frac{\log(2N)}{\log 2}\right) + Y\left(1 + \frac{\log(2N)}{\log P}\right)\right\}\log B.$$

The implicit constant is absolute. Take $B = M_*$, the single positive integer formed from the primitive critical values in Theorem 34.22 on the largest field of the interval. Then, uniformly in x on the entire interval, the left side with

$$Y = Y(x) = x^{-1240}\exp(x^\varepsilon/2)$$

is $O_{\psi,\varepsilon}(x^{-15}\exp(x^\varepsilon/2))$. This also holds with $B = M_*B_*$, where B_* is the positive integer for the two critical groups in Corollary 34.25. With $B = M_x$ formed on the individual field, the sum up to $x^{-820}\exp(x^\varepsilon/2)$ is $O_{\psi,\varepsilon}(x^{-5}\exp(x^\varepsilon/2))$.

Proof. Write $v = v_p(B)$. In a cyclic group of order p^a, the subgroup killed by B has order $p^{\min(a,v)}$. Summing over cyclic factors gives $\log|M[B]| \le v\log|M[p]|$ for each of the finite groups in the statement, also when $v = 0$. For $p \le P$, Lemma 19.3 gives $\log|M_{p,r}(E)[p]| \ll gp\log(2Np)$ separately at each r. For $p > P$, Lemma 19.18 gives the same bound for the *sum* over r. Its simultaneous estimate applies because $p > t + 1$ and $p \nmid gN$ on these intervals. The different weights then use distinct character components in the first layer of the real cyclotomic class group. Now

$$vp\log(2Np) = (v\log p)\,p\left(1 + \frac{\log(2N)}{\log p}\right).$$

In the first range the last two factors have product at most $P(1 + \log(2N)/\log 2)$, and in the second at most $Y(1 + \log(2N)/\log P)$. Sum the weights $v_p(B)\log p$, whose sum over all primes is $\log B$. This proves the first assertion.

For the second, the field bounds give $g \ll_\psi x^{2+8\varepsilon}$, $\log(2N) \ll_{\psi,\varepsilon} x^{\varepsilon/4}$, and $t \le x^{401}$. At the upper endpoint write g_*, N_*, t_* for these parameters. Theorem 34.22 gives

$$\log M_* \ll g_* t_*^2 \log(2N_*t_*) \ll_{\psi,\varepsilon} V^{1220} \le C_{\psi,\varepsilon}x^{1220}.$$

Indeed $g_* \ll V^{3+12\varepsilon}$, $t_*^2 \le V^{1203}$, and $\log(2N_*t_*) \ll V^{3\varepsilon/8} + \log V$. For large V we have $Y \ge P$ and $\log(2N)/\log P \le 1$. The first term in the asserted bound is at most a constant times $x^{1625}\exp(x^{\varepsilon}/12)$, and the second at most a constant times $x^{1223}Y$. Both have the required size. Corollary 34.25 gives the same polynomial bound for $\log B_*$ directly from Lemma 11.3. Finally $\log M_x \ll x^{812}$ by the same primitive-value estimate on E_x. Substitution into the first assertion at the larger cutoff gives the last bound, using $g \ll x^3$. □

Corollary 22.10 (Full orders of the classes detected by even orthogonal points)**.** *At every x on the same interval, consider all $P < p \le Y(x)$, all $1 \le r < t$, and all complementary character orbits $[\alpha]$. Give each orbit its minimal unramified coefficient ring O_α of degree b_α. The sums $S^{\mathrm{ev}}_{p,r,\alpha}$ of the classes in Theorem 34.22 satisfy*

$$\sum_{p,r,[\alpha]} b_\alpha \log p \,\operatorname{length}_{O_\alpha} S^{\mathrm{ev}}_{p,r,\alpha} \ll_{\psi,\varepsilon} x^{-15}\exp(x^{\varepsilon}/2).$$

In the full complementary order at x, removing $M_{p,r}(E)[M_*]$ at every odd $p \le Y(x)$ costs at most this same upper bound, with a possible change of the implicit constant.

Proof. Theorem 34.22 kills the entire detected subgroup by $p^{v_p(L(1-r,\alpha^*))}$. The valuation identity there shows that this prime power divides M_*, also for characters inflated from E_x. Since $p > g$, the ring $\mathbb{Z}_p[\mathrm{Gal}(E/\mathbb{Q})]$ splits into the unramified integer rings indexed by the residue Frobenius orbits. Restriction identifies the strict character group over $\mathbb{Q}$ with its factor in $M_{p,r}(E)$. Indeed averaging over the field group gives descent in degree one and commutes with all the local restrictions, as in Lemma 24.8. A simple factor of an O_α-module has p^{b_α} elements. Thus the left side is the sum of the logarithmic orders of subgroups of distinct factors of $M_{p,r}(E)[M_*]$. The theorem bounds it. Theorem 21.12 gives a further componentwise range for the detected subgroups. The common-integer estimate here includes the M_*-torsion in every character component, even when its individual primitive value is a p-adic unit. For the final assertion use the exact sequence with subgroup $M_{p,r}(E)[M_*]$ and quotient by that subgroup, separately at each prime and weight. The terms left over are the orders of those quotients and the full orders above $Y(x)$. □

22.10 Simultaneous vanishing at the marked coefficient primes

Use the polynomial-conductor intervals of Theorem 19.15. Fix one such interval $[V, V^{3/2}]$, with its single pair of quadratic primes. The fields E_x are nested there, since only the index in the real cyclotomic tower varies. Denote their largest member by E_*, and choose its cyclotomic modulus $N_* \le V^{3D/2}$ from that theorem. All subfields considered below lie in this one cyclotomic field. We use the full strict group $\mathcal{S}_{p,r}$ of Section 19.1.

Theorem 22.11 (Selecting the period primes with vanishing descended groups)**.** *Fix $0 < 9\theta_g < \varepsilon$ and $0 < 9\theta_T < 1/2 + 15\varepsilon/16$. On every sufficiently distant interval just specified, and at every x on it, both auxiliary primes g_1, g_2 of Theorem 7.11 and the common terminal prime T of Theorem 9.13 may be chosen with the following additional property. For $p = g_1, g_2$ use $\theta = \theta_g$, and for $p = T$ use $\theta = \theta_T$. Then*

$$\mathcal{S}_{p,r}(L) = 0 \quad \text{for every totally imaginary } L \subseteq E_* \quad \text{and } r \ge 1 \text{ with } [L:\mathbb{Q}](r+2) \le V^{\theta}.$$

For $L \subseteq E_x$ the full $\mathrm{Gal}(E_x/L)$-invariant subgroup of $\mathcal{S}_{p,r}(E_x)$ is also zero. The terminal choices still number $Y^{1-o(1)}$ for the same selected family of words and for the prescribed admissible factors Γ_c fixed before selecting T.

Proof. For any fixed $\theta > 0$, form an exceptional set of rational primes for the whole interval. Include each $p > 3^{4V^\theta}$ for which one of the pairs (L, r) in the displayed range has $\mathcal{S}_{p,r}(L) \neq 0$. For one pair put $d_L = [L : \mathbb{Q}]$, $n = 4(r+2)$. We have $3^{nd_L} \leq 3^{4V^\theta}$. Lemma 19.2, with $M = N_*$, bounds the sum of the logarithmic orders of all its strict groups above this threshold by $\exp(C(nd_L)^9 \log(2N_* nd_L))$. Each nontrivial group contributes at least $\log 2$. Thus the number of excluded primes for this pair is at most that bound divided by $\log 2$.

Write $G = \mathrm{Gal}(E_*/\mathbb{Q})$. Its order is at most N_*. Any subgroup can be generated by at most $\lceil \log_2 |G| \rceil$ elements, since adjoining an element outside a generated subgroup at least doubles its size. Counting lists of generators, padded with identities, gives at most $\exp(O_{\psi,\varepsilon}((\log V)^2))$ subgroups. There are at most V^θ possible r. Adding the bounds over all pairs gives the following upper bound for the size of the single exceptional set:

$$\exp\Big(O_{\psi,\varepsilon,\theta}(V^{9\theta}\log(2V) + (\log V)^2)\Big).$$

Use this once for each of the two fixed exponents.

For the auxiliary primes the proof of Theorem 7.11 provides $U^{1-o(1)}$ candidates in $(U, 2U]$, where $\log U \asymp_\varepsilon x^\varepsilon$. They exceed $3^{4V^{\theta_g}}$ for large V, and the exceptional set has size $U^{o(1)}$. After the first prime is chosen, the additional exclusions for the second number $O(r_0^3(1+U^{3/4}))$, with r_0 the row rank, bounded by a fixed power of x. This leaves $U^{1-o(1)}$ choices with the required disjointness. For these primes carry out the word selection in Theorem 9.13 with the stated factors. It gives $Y^{1-o(1)}$ eligible primes in one window for the selected words, with

$$\log Y \gg m x^\varepsilon \gg V^{1/2+15\varepsilon/16}.$$

These candidates exceed $3^{4V^{\theta_T}}$, and the second exceptional set has size $Y^{o(1)}$. Removing it proves the simultaneous assertions. The fields and the quadratic primes were chosen before either exceptional set was formed.

Finally $[E_* : \mathbb{Q}] \leq V^{3D/2} < p$ for all three chosen primes once V is large. On global H^1 with coefficients $\mathbb{Q}_p/\mathbb{Z}_p(-r)$, restriction to E_x identifies the group over L with the invariants. Indeed the two outside terms of inflation–restriction in degrees one and two vanish for a quotient of order prime to p, by averaging. The same argument gives injection upon restriction on local H^1 at p. At every other place it gives injection for the inertia groups, since the index of the smaller inertia group divides the local extension degree. Consequently a class whose restriction is unramified outside p and locally zero above p already has both properties over L. Applying the global identification to these kernels proves the assertion about invariants. □

For instance one may take $\theta_g = \varepsilon/10$ and $\theta_T = 1/18$. For the actual period field this includes every layer $K_\psi C_j(\sqrt{-q}, \sqrt{-d_0}) \subseteq E_x$ for which $4\,\mathrm{ord}(\psi)2^j(r+2) \leq V^\theta$, since the three constituent degrees multiply to at most the coefficient on the left. This gives zero contribution at the designated coefficient primes in either conjugation eigenspace of these descended parts. In particular it applies at the same T as the period transport in Theorem 71.21, with no truncation of the cohomology exponent. The relative summands of larger degree, the other coefficient primes and the full range $r < x^{401}$ still enter the length required in Section 6.6.

22.11 Vanishing of the critical sign at every required weight

Use E_*, V and the two exceptional sets of Theorem 22.11. Put $t_* = \lfloor V^{(3/2)401} \rfloor$. For an odd prime p write $e_n = (1 + (-1)^n c)/2$, where c denotes complex conjugation in the field group.

Theorem 22.12 (The full critical sign at the three period primes)**.** *The choices of g_1, g_2, T in Theorem 22.11 can simultaneously satisfy, at each of these three coefficient primes and for*

every $1 \le r < t_*$,

$$e_{r+1}\mathcal{S}_{p,r}(L) = 0 \quad \textit{for every CM subfield } L \subseteq E_*.$$

At the same primes all the complementary strict subgroups detected by the even orthogonal specializations of Theorem 34.22 are zero throughout its range. These choices retain the same number of terminal candidates in the window for the selected words.

Proof. Use the single larger CM field $E'_* = E_*(i)$ of Corollary 34.25, and the positive integer

$$B_* = \prod_{n=2}^{2t_*+1} |D_n(E'_*)|$$

defined there. For every odd p prime to B_*, the strict critical-sign group over E'_* vanishes for $n = r+1$ in the displayed range. Indeed in the proof of Theorem 11.1 the length of its dual for each fixed n, p is bounded by a finite multiple of $v_p(D_n(E'_*))$, using the injection of Lemma 11.2. For the complementary detected subgroups Theorem 34.22 supplies the annihilating integer M_*. Multiplication by M_* is an automorphism of any finite p-group if $p \nmid M_*$, so each such subgroup then vanishes as well.

The two integer bounds in Theorem 22.9 give $\log(B_*M_*) \ll_{\psi,\varepsilon} V^{1220}$. The number of their distinct prime divisors is at most this logarithm divided by $\log 2$. Add these primes to both exceptional sets in Theorem 22.11 before either auxiliary prime is selected. A fixed polynomial in V is $U^{o(1)}$ and $Y^{o(1)}$ in the notation of that theorem. Its proof therefore gives the same counts with the extra exclusions. Finally each chosen p exceeds $[E'_* : \mathbb{Q}]$ for large V. Restriction from any indicated L to E'_* is injective on strict groups since corestriction followed after restriction multiplies by the prime-to-p degree. It preserves complex conjugation, as these fields are abelian over $\mathbb{Q}$. This proves the first assertion on every L, including all of the actual E_x. □

Thus the coefficient primes used by the exchange formulas in Theorem 71.25 can have zero critical-sign length over the full period fields up to the entire weight cutoff. On the complementary sign Theorem 22.11 also removes the indicated descended components at their full exponent. The full sum over complementary relative classes at all coefficient primes remains in Proposition 6.11.

22.12 The full complementary order outside the class norm exceptions

Fix the largest field E_* on $[V, V^{3/2}]$ as in Section 6.6. For every odd prime p use its real cyclotomic tower F_i, split class module X_p, generator γ and tame group Δ_0 from Theorem 22.7. Put $n_* = [E_* : \mathbb{Q}]$, $j = \lfloor \log_p n_* \rfloor$ and $B_i = \widetilde{C}(F_i)$. In this subsection use the whole of B_i, including the invariant part for the decomposition group. Let g_i be the number of primes over p in F_i. Set

$$K_j = \ker(\mathrm{N} : B_{j+1} \longrightarrow B_j), \qquad C_i = \mathrm{Cl}(\mathcal{O}_{F_i}[1/p])\{p\}.$$

Proposition 22.13 (The local degree contribution to a class norm kernel)**.** *Every prime above p in F_{j+1} is fixed by $\mathrm{Gal}(F_{j+1}/F_j)$. The map $K_j \to C_{j+1}$ has image in the kernel of the ordinary norm to C_j. Its kernel is killed by p and has dimension at most $g_{j+1} - 1$ over $\mathbf{F}_p$. In particular*

$$\log|K_j| \le \log|\ker(C_{j+1} \to C_j)| + (g_{j+1} - 1)\log p.$$

The same kernel assertion holds on each integral tame character summand. The dimensions of these kernels sum to at most $g_{j+1} - 1$.

Proof. At every finite layer F_i the number of primes above p is at most n_*, by total ramification in the real cyclotomic field used in the proof of Theorem 9.16. The restriction maps between the finite prime sets are onto. Their sizes are therefore nondecreasing and bounded, so their inverse limit has at most n_* elements. Every orbit of the procyclic pro-p group generated by γ has size a power of p at most n_*. All its orbit sizes divide p^j. Hence γ^{p^j} fixes every such prime, including after restriction to F_{j+1}.

At that level the kernel of $B_{j+1} \to C_{j+1}$ is a quotient of the degree-zero local lattice of rank $g_{j+1} - 1$ in Theorem 28.11. The cyclic group of the indicated extension acts trivially on that lattice. It fixes each prime and its action on the local cyclotomic degree group is conjugation in an abelian group. For a degree-zero logarithmic class z, extension of its norm equals the sum of its conjugates. Indeed on an idele the local product for the norm, embedded back into the higher field, is the product of the conjugate ideles. Principal ideles, local norm kernels and the degree maps respect these operations, so the identity passes to the class group. On the local kernel this composition is multiplication by p. An element in that kernel with zero norm is consequently killed by p. The p-torsion of a finite quotient of a free $\mathbb{Z}_p$-module of rank $g_{j+1}-1$ has dimension at most this rank, by its cyclic decomposition. The map to the ordinary class group commutes with norm by the same idele calculation. Projection onto the distinct Δ_0 characters is integral and exact, giving the last assertion. □

Write $d = v_p(\kappa_p(\gamma) - 1)$, $s_r = d + v_p(r)$ and take $t_* = 2 + \lceil V^{602} \rceil$ and $H = d + \lfloor \log_p t_* \rfloor$. As before $A_{p,x,r}$ is the dual of the complementary strict cohomology group on E_x. For each character τ of Δ_0 put $k_{p,\tau} = \log_p |e_\tau K_j|$.

Theorem 22.14 (A bound from a finite class norm in every tame character)**.** *There are sets $D_{p,\tau}$ in the progressions $\kappa_p^{-r}|_{\Delta_0} = \tau$, $1 \le r < t_*$, with $|D_{p,\tau}| \le k_{p,\tau}$. For every x on the interval and all unselected weights in their respective progressions,*

$$\log_p |p^{s_r+j} A_{p,x,r}| \le H k_{p,\tau}.$$

This uses the full order above the specified precision, through every exponent. The bound of Proposition 22.13 applies to the sum of $k_{p,\tau} \log p$ over all characters, even when p divides the conductor or the degree of E_*.

Proof. Put $M = e_\tau X_p$ and $U = (\gamma^{p^j} - 1)M$. These are finitely generated over $\mathbb{Z}_p$ by Theorem 28.13. With $N(Y) = \Phi_{p^{j+1}}(Y)$, the cyclotomic polynomial, the group $U/N(\gamma)U$ equals $e_\tau K_j$. Indeed $B_i = X_p/(\gamma^{p^i} - 1)X_p$, the norm is the quotient map, and $Y^{p^{j+1}} - 1 = (Y^{p^j} - 1)N(Y)$. For $b_r = \kappa_p(\gamma)^{-r}$, the map $M \to A_{p,x,r}$ is onto. Its quotient by $\gamma - b_r$ is the full group on E_* in this progression before imposing the additional field relations from E_x. The image of U is $(b_r^{p^j} - 1)A_{p,x,r} = p^{s_r+j} A_{p,x,r}$. On the rational span of M and its stable subspace spanned by U, $\gamma - b_r$ is injective by finiteness of the strict group on E_*.

For a primitive p^{j+1}-th root ζ put $e' = p^j(p-1)$ and $O = \mathbb{Z}_p[\zeta]$. Via evaluation of Y at γ, $(U \otimes O)/(\gamma - \zeta)(U \otimes O) = U/N(\gamma)U$. The extension has ramification degree e' and residue field $\mathbf{F}_p$. Apply Lemma 28.15 to U at ζ and all the b_r of the progression. For the resulting monic polynomial P, $v_p(P(\zeta)) = k_{p,\tau}/e'$. Every b_r has $v_p(b_r - \zeta) = 1/e'$. Roots α with $v_p(\alpha - \zeta) < 1/e'$ contribute the same sum S to the valuation at every b_r. There are at most $k_{p,\tau} - e'S$ other roots, counted with multiplicities. For each of them choose one closest b_r when the progression is nonempty. Away from that selection its valuation at any other b_r is at most H, since two distinct sample points have difference of valuation $d + v_p(r - r') \le H$. Hence $v_p(P(b_r)) \le S + H(k_{p,\tau} - e'S) \le H k_{p,\tau}$ outside the union of the selected weights. This bounds the length of $U/(\gamma - b_r)U$ and hence of its indicated image on every E_x. □

Corollary 22.15 (The full strict orders outside the norm selections)**.** *Use the polynomial-conductor intervals, $t = \lfloor x^{401} \rfloor$, $Y = x^{-3}\exp(x^{\varepsilon}/4)$, and $Z = x^{-3}\exp(x^{\varepsilon}/6)$. For each odd $p \le Z$ use $D_{p,\tau}$ above. For $Z < p \le Y$ use the first selection D^0_{τ} in Theorem 28.16. Denote the applicable selection by $D(p,\tau;x)$. Then, for each fixed $0 < \varepsilon < 1/52$, uniformly at sufficiently large x on these intervals,*

$$\sum_{\substack{2<p\le Y\\ p \text{ prime}}} \sum_{\substack{1\le r<t\\ r\notin D(p,\kappa_p^{-r}|_{\Delta_0};x)}} \log|A_{p,x,r}| \ll_{\psi,\varepsilon} x^{-2}\exp(x^{\varepsilon}/2).$$

All selections of weights use E_* and the interval cutoff t_*. Only the numerical ranges Z, Y in which they are applied vary with x. They may be intersected with the earlier exceptional component selections of Theorem 21.14 when retaining terms in the residual length sum.

Proof. For $p \le Z$, one has $p^{j+1} \le n_* Z \le Y$ eventually, since n_* is bounded by a fixed power of x. The sum of the orders in logarithmic scale through precision $s_r + j$ is therefore bounded by Theorem 9.16, which includes the invariant part. Beyond this precision use Theorem 22.14. Summing its bound over the weights costs at most $1+tn_*/(p-1)$ repetitions per tame character. For $p \le n_*$, the fields F_{j+1} have degrees at most $n_* p^{j+2} \le n_*^2 p^2$ and cyclotomic moduli at most $N_* n_*^2 p^2$. Here $p^{d-1} \le n_*$ as in Theorem 22.7. The conductor and class number bound of Theorem 9.16, together with Proposition 22.13, bounds the entire cost in this range by a fixed power of x, including H and the number of weights. For $n_* < p \le Z$ one has $j = 0$. The logarithmic size of K_0 is $O(n_* p^2 \log(2N_* n_* p^2) + n_* \log p)$. Multiplying by $H(1+tn_*/(p-1))$ and summing costs $O_{\psi,\varepsilon}(n_* x^{\varepsilon}\log(2x)(Z^3 + tn_* Z^2))$. This is within the bound, by the calculation in Corollary 28.17.

For $Z < p \le Y$, eventually $p > t_* + 2$ and $p > N_*$. Indeed both t_* and N_* are bounded by fixed powers of V, while Z grows faster than each such power uniformly for $x \ge V$. Now E_* is unramified at p and disjoint from the p-power cyclotomic field, since its modulus is prime to p. The latter extension is totally ramified at p, also after unramified local base change. Hence the full tame group of order $p-1$ acts by inertia at p, also on restriction to the real tower. Its action on the real tower is faithful because the only possible nontrivial kernel element, complex conjugation, acts nontrivially on the CM field E_*. Thus the image of Δ_0 is contained in the prime-to-p decomposition subgroup D'. Every $1 \le r < t$ gives a nontrivial τ, since $r < p-1$. Averaging over D' kills this summand. The group denoted $eA_{p,x,r}$ in Corollary 28.17 is the entire $A_{p,x,r}$ at these weights. Its first selection and bound finish the sum. For the final assertion, terms discarded by either theorem have nonnegative logarithmic orders, and the union of the two discarded sums costs at most the sum of their bounds. □

The estimate leaves the selected full orders and the primes above Y. Proposition 28.18 shows why class group orders and maps between the underlying norm groups alone do not bound a selected order, even with just one exceptional weight.

22.13 The local conditions at the conductor

Fix one of the intervals $[V, V^{3/2}]$ of Theorem 19.15. Write $E = E_x$, $n = [E:\mathbb{Q}]$, $t = \lfloor x^{401} \rfloor$, and let N_* be the cyclotomic modulus of the largest period field E_* on the interval. We use this same modulus even for characters coming from a smaller E_x.

Fix an odd prime ℓ, $1 \le r < t$, and a character α of $G = \mathrm{Gal}(E/\mathbb{Q})$ with values in $\overline{\mathbb{Q}}_\ell$. Set $O_\alpha = \mathbb{Z}_\ell[\alpha(G)]$, write J_α for its fraction field, e_α for its ramification index, and put $D = (J_\alpha/O_\alpha)(\alpha^{-1}\kappa_\ell^{-r})$. The character group of a finite abelian extension is viewed as a group of characters of the absolute Galois group by inflation. Let $S(\alpha, r)$ consist of the classes in

$H^1(\mathbb{Q}, D)$ unramified away from ℓ and zero at ℓ. In $S^N(\alpha, r)$ require in addition that the class be zero on the decomposition group at every $q \mid N$, $q \neq \ell$. Write $\lambda^N_{\ell,r,\alpha} = \operatorname{length}_{O_\alpha} S^N(\alpha, r)$. These are the local conditions on the scalar group underlying the rank-three argument. The distinction matters even for divisible coefficients when the finite character has ramified ℓ-power image.

Lemma 22.16 (The correction at one finite prime)**.** *For $q \neq \ell$, let I_q denote inertia, and choose a lift F_q of arithmetic Frobenius. The possible local values of an unramified class belong to a group of length zero unless $\alpha(I_q)$ has nontrivial ℓ-power order and no prime-to-ℓ part. If this image has order ℓ^a, $a \geq 1$, the ambient unramified local group has O_α-length*

$$\min\left\{ \frac{e_\alpha}{\varphi(\ell^a)},\ v_{\pi_\alpha}(\alpha(F_q)^{-1} q^{-r} - 1) \right\}.$$

Here v_{π_α} assigns value one to a uniformizer. The quotient $S(\alpha, r)/S^N(\alpha, r)$ injects into the direct sum of these local groups for $q \mid N$, $q \neq \ell$.

Proof. Inflation–restriction identifies the unramified subgroup with $D^{I_q}/(F_q - 1)D^{I_q}$. Indeed the procyclic residue Galois group acts on D^{I_q}, and a cocycle is specified by its value on arithmetic Frobenius modulo the values of coboundaries. Every value defines a continuous cocycle because it lies in a finite stable submodule, and a multiple of the order of the action times the exponent of that submodule makes the cyclic norm of the value zero. The cyclotomic character is unramified at q. If inertia has trivial image then $D^{I_q} = D$ and the scalar $\alpha(F_q)^{-1} q^{-r} - 1$ is nonzero. In fact $q^r > 1$ and $\alpha(F_q)$ is a root of unity. A nonzero scalar acts surjectively on J_α/O_α. If inertia has nontrivial prime-to-ℓ image, some inertia eigenvalue differs from one by a unit and $D^{I_q} = 0$.

In the remaining case a generator of the inertia image is a primitive ℓ^a-th root ζ. Its difference from one has valuation $e_\alpha/\varphi(\ell^a)$. This follows by evaluating the cyclotomic polynomial at one. The product of the $1 - \zeta^j$ for j prime to ℓ modulo ℓ^a equals ℓ, and each has the same valuation. Thus $D^{I_q} = D[\zeta - 1]$ is cyclic of this length. Its quotient by $F_q - 1$ has the displayed length by the elementary divisor theorem. Changing the lift of Frobenius preserves its action on D^{I_q}. Finally localization at the indicated primes on $S(\alpha, r)$ has kernel exactly $S^N(\alpha, r)$. □

Theorem 22.17 (Full character lengths on the period fields)**.** *Let $M_{\ell,r}(E) = \mathcal{S}_{\ell,r}(E)^{c=(-1)^r}$. For every x on these intervals put*

$$Z_{\ell,r}(E) = \sum_{\substack{\alpha \in \widehat{G}(\overline{\mathbb{Q}}_\ell) \\ \alpha(c) = (-1)^r}} \frac{\lambda^{N_*}_{\ell,r,\alpha}}{e_\alpha}.$$

All the character groups here have finite length. For $\ell \nmid n$ one has $\operatorname{length}_{\mathbb{Z}_\ell} M_{\ell,r}(E) = Z_{\ell,r}(E)$. More generally, uniformly on the interval,

$$\sum_{\ell > 2} (\log \ell) \sum_{1 \leq r < t} \left| \operatorname{length}_{\mathbb{Z}_\ell} M_{\ell,r}(E) - Z_{\ell,r}(E) \right| \ll_\psi t\, n^2 \log(2N_*).$$

The sum over geometric characters in $Z_{\ell,r}$ can equivalently be taken over the $\mathbb{Q}_\ell$-orbits, with coefficient $[O_\alpha/\pi_\alpha : \mathbf{F}_\ell]$ multiplying each $\lambda^{N_*}_{\ell,r,\alpha}$.

Proof. Choose the integer ring O of a finite extension of $\mathbb{Q}_\ell$ containing all the character values, with uniformizer π, residue field k and ramification index e. A finite free extension of coefficients commutes with the global and local cochains and the kernels under consideration. This follows

in a basis of the extension, including for the divisible coefficients by writing $(J_\alpha/O_\alpha)\otimes_{O_\alpha} O = \mathrm{Frac}(O)/O$. After this extension put

$$A = M_{\ell,r}(E)\otimes_{\mathbb{Z}_\ell} O, \qquad B = \bigoplus_{\alpha(c)=(-1)^r} S(\alpha,r)\otimes_{O_\alpha} O.$$

By Lemma 25.22 the character evaluation and its inverse up to scalar give maps $A \to B \to A$ whose composites in both orders equal multiplication by n. The local assertion in that lemma uses the inertia cosets on restriction of the induced representation, so applies also at primes ramified in E. When $\ell \nmid n$ these maps are isomorphisms after dividing one by n. No inertia image of any α then has nontrivial ℓ-power order. Lemma 22.16 identifies $S(\alpha,r)$ with $S^{N_*}(\alpha,r)$, giving the asserted equality upon dividing the O-lengths by e.

It remains to bound the kernels when $m = v_\ell(n) > 0$. The extension E/K_ψ has degree a power of two, so $\ell^m \mid \mathrm{ord}(\psi)$. In particular both ℓ and m are bounded in terms of ψ. The kernels of the two maps are contained in $A[\ell^m]$ and $B[\ell^m]$, respectively. The group A is finite by Proposition 11.4. The Kummer estimate in the proof of Theorem 11.5 gives $\dim_{\mathbf{F}_\ell} M_{\ell,r}(E)[\ell] \ll_\psi n\log(2N_*)$.

Here is a bound for the other kernel that also proves its finiteness. Put $\Sigma = \{q : q \mid \ell N_*\}$, and write $G_{\mathbb{Q},\Sigma}$ for the Galois group of the maximal extension unramified at all other finite primes. Outside Σ the coefficient is unramified, and an unramified cocycle is zero on inertia. Thus the scalar groups lie in the cohomology of $G_{\mathbb{Q},\Sigma}$. By the coefficient sequence for multiplication by π, each scalar π-torsion group over O has dimension at most that of $H^1(G_{\mathbb{Q},\Sigma}, k(\bar\alpha^{-1}\bar\kappa_\ell^{-r}))$. Let P be the ℓ-Sylow of G and put $F' = E^P(\mu_\ell)$. Its degree divides $(\ell-1)n/|P|$ and is prime to ℓ. Restriction to F' is injective by corestriction, and the residual coefficient becomes trivial there. In a basis of k the resulting dimension over k is bounded by the $\mathbf{F}_\ell$-dimension of $H^1(G_{F',\Sigma},\mu_\ell)$, since $\mu_\ell \subset F'$. Kummer theory bounds this by the dimension of the Σ-units modulo ℓ and the ℓ-rank of the Σ-class group. The unit rank and number of inverted places are $O_\psi(n\log(2N_*))$. The field has cyclotomic modulus dividing $N_*\ell$ and degree $O_\psi(n)$. The conductor–discriminant formula and the Minkowski ideal count used in Theorem 11.5 give the same bound for the logarithm of its class number. This proves $\dim_k B[\pi] \ll_\psi n^2\log(2N_*)$, since there are at most n characters.

For any π-primary module of finite socle dimension d, the subgroup killed by π^j has length at most jd, since multiplication by π^{i-1} embeds each successive quotient of π^i-torsion by π^{i-1}-torsion in the socle. Hence $B[\ell^m]$ is finite. The map to A now gives finiteness of B. Using the two maps in opposite directions bounds $|\mathrm{length}_O A - \mathrm{length}_O B|/e$ by $m\max(\dim_k A[\pi], \dim_k B[\pi])$. For A its socle dimension is the number of $\mathbb{Z}_\ell$-cyclic factors of $M_{\ell,r}(E)$, by base change of its elementary divisors. This proves an $O_\psi(n^2\log(2N_*))$ bound at each such prime and twist. Passing to S^{N_*} costs at most one unit of normalized length per character and prime dividing N_* by Lemma 22.16. Summing over r and the fixed prime divisors of $\mathrm{ord}(\psi)$ gives the claim. Finally an orbit has $e_\alpha[O_\alpha/\pi_\alpha : \mathbf{F}_\ell]$ members, and conjugation identifies their lengths. □

In the source the divisible character module and the modulus used for its local conditions are specified in `Development/AutomorphicArithmetic/AutomorphicVarieties/CharacterLevelBounds/ShaFamMono.lean`, line 30. Theorem 22.17 bounds the change of local conditions and of integral character lattices. A bound for the scalar lengths themselves is still needed.

22.14 Ordinary class groups at every precision of the strict group

Fix the fields $E = E_x \subseteq E_*$ on the interval of Section 6.6. Write $n = [E:\mathbb{Q}]$ and $n_* = [E_*:\mathbb{Q}]$. Fix an odd prime p. Use the real cyclotomic tower $F_0 \subset F_1 \subset \cdots \subset F_\infty$ of Theorem 22.7,

with $[F_j : F_0] = p^j$. In the full CM tower $L_\infty = E_*(\mu_{p^\infty})$, the group over $E_*(\mu_p)$ restricts isomorphically to $\Gamma = \mathrm{Gal}(F_\infty/F_0)$. Choose a topological generator γ, put $a = \kappa_p(\gamma)$, and put $s_r = v_p(a^{-r} - 1)$ for each positive integer r. The ordinary group used below is

$$C_j = \mathrm{Cl}(\mathcal{O}_{F_j}[1/p])\{p\}.$$

It is obtained from the ideal class group of F_j by killing the classes of the primes above p and taking the p-primary part. Write $T_j = \widetilde{C}(F_j)$ for the degree-zero logarithmic class group. For $G_x = \mathrm{Gal}(L_\infty/E)$, define

$$Q_{r,m}(Y) = Y \Big/ \overline{p^m Y + \sum_{\delta \in G_x} (\delta - \kappa_p(\delta)^{-r}) Y} \qquad (m \geq 1).$$

The action on each class group is induced by restriction to its field. Let $A_{p,x,r}$ be the Pontryagin dual of $\mathcal{S}_{p,r}(E)^{c=(-1)^r}$ in the untwisted class group coordinates of Theorem 22.7.

Lemma 22.18 (Local degrees under norm after the primes cease splitting)**.** *There is an integer $\sigma_p \geq 0$, with $p^{\sigma_p} \leq n_*$, such that restriction gives a bijection on the primes above p from F_∞ to F_j for every $j \geq \sigma_p$. Let $g_p \leq n_*$ be their number in these layers. For each such j there is a natural surjection $T_j \to C_j$ whose kernel K_j is a quotient of*

$$P^0 = \{(z_w)_{w|p} \in \mathbb{Z}_p^{g_p} : \sum_w z_w = 0\}.$$

The field action on this lattice permutes the places. For each integer $i \geq 0$ one has $N_{j+i,j} K_{j+i} = p^i K_j$.

Proof. Write $u = v_p(a - 1) - 1$. As in the proof of Theorem 22.7, $F_j = (E_*(\mu_{p^{u+1+j}}))^+$. Its degree over $\mathbb{Q}(\mu_{p^{u+1+j}})^+$ is at most n_*, by the compositum degree bound and the fact that both CM fields have index two over their real subfields. The real cyclotomic field has a unique prime over p. Thus the number of places above p in each layer is at most n_*. These finite sets map onto one another, so their inverse limit has at most n_* elements. The decomposition subgroup of a place in Γ consequently has finite index $p^{\sigma_p} \leq n_*$. It is the same subgroup for all places, since $F_\infty/\mathbb{Q}$ is abelian and transitive on the places. For $j \geq \sigma_p$, the group $\Gamma_j = \mathrm{Gal}(F_\infty/F_j)$ lies in this stabilizer. Each place of F_j then has a unique extension to F_∞ and its local degree group is all of Γ_j. This is the degree group for the local cyclotomic extension because F_∞ is the compositum of F_j with the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$.

By local reciprocity a local factor at $w \mid p$ maps onto this degree group. In the global class group defined by the locally cyclotomic condition, killing all these local factors gives C_j by ideal class field theory. The global cyclotomic degree of a tuple of the local factors is the sum of its local degrees. Since one local factor already maps onto Γ_j, any lift of a class in C_j can be corrected to have degree zero. The resulting surjection from T_j has as kernel the image of the tuples of degree sum zero, exactly as in Theorem 28.11. Use γ^{p^j} as generator in each coordinate. Conjugation acts trivially on the cyclotomic group and permutes the places, which proves the asserted lattice description. By functoriality of local reciprocity the norm on local degrees is the inclusion $\Gamma_{j+i} \subseteq \Gamma_j$. In these coordinates each entry is multiplied by p^i, at the same place. The image of all degree-zero tuples from above is therefore exactly $p^i P^0$ below. Taking images in the logarithmic class group proves the norm assertion, including in the presence of relations from units. □

Let $v \mid p$ in E. Write the cyclotomic image of its local absolute Galois group as $\mu_d \times (1 + p^h \mathbb{Z}_p)$, with $d \mid p - 1$ and $h \geq 1$. This open subgroup splits into its prime-to-p and pro-p factors by

taking the corresponding projections in its finite cyclic quotients. Its index $(p-1)p^{h-1}/d$ divides the ramification index $e_p(E/\mathbb{Q})$, since the intersection of E_v with the local cyclotomic tower is totally ramified. The quantities are independent of the place by Galois conjugacy. Define

$$b = b_{p,x,r,m} = \begin{cases} 0 & d \nmid r, \\ \min\{m, h + v_p(r)\} & d \mid r. \end{cases}$$

Theorem 22.19 (Recovery from ordinary ideal classes at a specified layer)**.** *Fix $r, m \geq 1$, put $A = A_{p,x,r}/p^m A_{p,x,r}$, and choose $j \geq \max\{\sigma_p, m - s_r, 0\}$. There is a subgroup $B \subseteq A$ generated by at most $g_p - 1$ elements and killed by p^b such that, compatibly with norm, for every $i \geq 0$*

$$Q_{r,m}(C_{j+i}) \simeq A/p^i B.$$

In particular the layer $j+b$ recovers A exactly. Equality of the orders of the ordinary quotients at two consecutive layers $j+i, j+i+1$ already certifies recovery of A at precision m. At fixed p, m the single layer $F_{m+\lfloor \log_p n_* \rfloor}$ suffices for every E_x in the interval and every positive weight.

Proof. Theorem 22.7 identifies $Q_{r,m}(T_{j+i})$ with A because $s_r + j + i \geq m$. These identifications use restriction of characters and are compatible with norm, which induces the identity on A. The quotient functor $Q_{r,m}$ is right exact. Taking the quotient by K_{j+i} before imposing the scalar and precision relations has the same effect as imposing all these relations in one quotient. Its kernel on the surjection to the ordinary group is consequently the image of K_{j+i}. Denote the image of K_j in A by B. The lemma and the norm identification show that the image of K_{j+i} is exactly $p^i B$. The lattice in the lemma gives the claimed generator bound.

Choose a prolongation of v to L_∞. The local Galois group at v restricts into G_x and fixes that place. Its elements fix every place over p in F_∞, since the Galois group over $\mathbb{Q}$ is abelian. They therefore act trivially on P^0. In the twisted quotient each of the scalars $1 - \kappa_p(\delta)^{-r}$ for these elements annihilates B. If $d \nmid r$, a tame generator gives a unit. Otherwise a generator of $1 + p^h\mathbb{Z}_p$ gives a scalar of valuation $h + v_p(r)$ by binomial expansion at the odd prime p. The precision also kills $p^m B$. Thus $p^b B = 0$. If consecutive ordinary orders agree, then $p^i B = p^{i+1} B$, and iteration in the finite group gives $p^i B = 0$.

Take $j = \max\{\sigma_p, m - s_r, 0\}$. When $j = \sigma_p$, one has $j + b \leq \lfloor \log_p n_* \rfloor + m$. In the other case use $s_r = 1 + u + v_p(r)$, $p^{h-1} \leq e_p \leq n_*$, and $b \leq h + v_p(r)$ to obtain the same inequality. Every larger layer gives the same quotient, proving the common-field assertion. □

Corollary 22.20 (Total error over all odd primes, independent of precision)**.** *For $t \geq 2$ integral, choose for each $p > 2$ prime and $1 \leq r < t$ any $m \geq 1$, any j as in the theorem and any integer $k \geq 0$. With $A = A_{p,x,r}/p^m A_{p,x,r}$ at each pair,*

$$0 \leq \sum_{p>2} \sum_{1 \leq r < t} \log \frac{|p^k A|}{|p^k Q_{r,m}(C_j)|} \leq 6 n_* n (t-1) \log(2nt).$$

At $t = \lfloor x^{401} \rfloor$ the right side is polynomial in x uniformly on the fields of Section 6.6.

Proof. The restricted surjection on the images of p^k has kernel contained in B, whose order is at most $p^{(g_p - 1)b}$. A positive discrepancy requires $d \mid r$, so $p - 1 \leq e_p r$ and $p \leq 1 + n(t-1)$. At this prime put $M = \lfloor (t-1)/d \rfloor$. The sum of $v_p(r)$ over these weights is $v_p(M!) \leq M/(p-1)$, because d is prime to p. Using $g_p - 1 \leq n_*$, $e_p \leq n$ and $h \leq p^{h-1}$, the logarithmic contribution is at most

$$n_* n (t-1) \frac{\log p}{p-1} \left(1 + \frac{1}{p-1}\right).$$

For integral $X \geq 2$, the inequality $\sum_{p \leq X} \lfloor X/p \rfloor \log p \leq \log(X!)$ gives $\sum_{p \leq X} (\log p)/p \leq 2 \log X$. Apply it with $X = 1 + n(t-1)$, using $p/(p-1) \leq 3/2$ and $1 + 1/(p-1) \leq 3/2$. This proves the displayed bound. The degree estimate from Theorem 19.15 gives the last assertion. □

The ordinary quotient at the common layer accounts for all classes in the complementary sign at the prescribed precision. The remaining cohomological estimate in Section 6.6 asks for an upper bound on the orders of the surviving quotients themselves as the precisions and weights vary.

22.15 The exceptional weights at small coefficient primes

We now locate the weights where the full complementary group at a small prime can exceed a polynomial bound. The set of weights will be determined by ordinary ideal classes in finitely many fields attached to the largest field E_* of the interval. The same set will work on every E_x. Keep F_j, C_j, T_j, γ, a and $\sigma = \sigma_p$ from Section 22.14 at an odd prime p. Let X be the abelian pro-p class module over F_∞ unramified away from p and split at the primes over p. Write $T = \gamma - 1$ for the Iwasawa variable. The class field description in Theorem 22.7 gives

$$T_j = X/((1+T)^{p^j} - 1)X,$$

with norm induced by the quotient map. Indeed abelianizing over F_j imposes the commutators with γ^{p^j}, and the kernel of the cyclotomic degree in that abelianization is the displayed quotient.

The group of L_∞/E_* is a subgroup of $\mathbb{Z}_p^\times$ under the cyclotomic character. It is the product of its finite prime-to-p part Δ and the closed subgroup generated by γ. The order of Δ divides $p-1$. Thus for each character τ of Δ the idempotent $e_\tau = |\Delta|^{-1} \sum_{\delta \in \Delta} \tau(\delta)^{-1} \delta$ is integral over $\mathbb{Z}_p$. These idempotents split every module in the following calculation. Take $M_\tau = e_\tau X$ and $P(Y) = \Phi_{p^{\sigma+1}}(Y)$. Define nonnegative integers from the ordinary group at a finite level by

$$D_\tau = e_\tau C_{\sigma+2}/P(\gamma) e_\tau C_{\sigma+2}, \qquad h_\tau = \log_p |D_\tau|.$$

Lemma 22.21 (An ordinary class group at a primitive cyclotomic character)**.** *There is an isomorphism $M_\tau/P(\gamma)M_\tau \simeq D_\tau$. At the preceding level one has*

$$\sum_\tau h_\tau \log p \leq \log |C_{\sigma+1}| + (g_p - 1) \log p.$$

These statements apply also at primes dividing the conductor or degree of E_*.

Proof. The polynomial $P(Y)$ divides $Y^{p^j} - 1$ whenever $j \geq \sigma + 1$. Hence $X/P(\gamma)X$ identifies with $T_j/P(\gamma)T_j$ at all these levels, compatibly with norm. On the kernel $K_{\sigma+1}$ of $T_{\sigma+1} \to C_{\sigma+1}$, the element γ^{p^σ} acts trivially, by the local lattice of Lemma 22.18. Consequently $P(\gamma) = \sum_{i=0}^{p-1} \gamma^{ip^\sigma}$ acts there as multiplication by p. The image of this kernel after imposing $P(\gamma) = 0$ therefore has order at most $p^{g_p - 1}$. The surjection to the corresponding quotient of $C_{\sigma+1}$ gives the order bound for $X/P(\gamma)X$.

The norm from level $\sigma + 2$ sends its local kernel onto $pK_{\sigma+1}$ by the same lemma. The latter maps to zero after imposing $P(\gamma) = 0$, and norm on the specialized logarithmic groups is an isomorphism. The upper local kernel therefore has zero image. Right exactness identifies the upper ordinary quotient with $X/P(\gamma)X$. Projecting onto e_τ gives the isomorphism. The orders of the summands multiply to the order of the whole group, proving the inequality. □

For an integer $R \geq 2$ put $w = v_p(a-1)$, $W = w + \lfloor \log_p R \rfloor$, and

$$I_\tau = \{1 \leq r < R : \ \kappa_p^{-r}|_\Delta = \tau\}, \qquad H_\tau = W h_\tau, \qquad m_p = 1 + \max_\tau H_\tau.$$

Compute the ordinary quotients on the right below at $j_p = m_p + \lfloor \log_p n_* \rfloor$, with G_x replaced by $\mathrm{Gal}(L_\infty/E_*)$ in Q_{r,m_p}. Define

$$\mathcal{E}_{p,\tau} = \{r \in I_\tau : \ \log_p |Q_{r,m_p}(C_{j_p})| > H_\tau\}.$$

Thus testing membership uses the action on ordinary ideal classes at a specified finite level and scalar congruences modulo p^{m_p}.

Theorem 22.22 (A finite exceptional set for every tame character)**.** *One has $|\mathcal{E}_{p,\tau}| \le h_\tau$. For every field E_x of the interval and every $r \in I_\tau \setminus \mathcal{E}_{p,\tau}$, the full order satisfies $\log_p |A_{p,x,r}| \le H_\tau$. At E_* the exceptional set consists exactly of the weights whose full length exceeds H_τ.*

Proof. For any finite abelian p-group B and integers $m > H \ge 0$, one has $\log_p |B| > H$ if and only if $\log_p |B/p^m B| > H$. Indeed any cyclic factor cut short by reduction still contributes $m > H$, and if none is cut short the orders agree. Apply Theorem 22.19 with $E = E_*$ to prove the exact identification of the exceptional set. In the progression I_τ, put $t_r = a^{-r} - 1$. Imposing the field and scalar relations on X first over E_* gives $A_{p,*,r} = M_\tau/(T - t_r)M_\tau$, as in the proof of Theorem 22.8. Indeed the tame relations project onto e_τ, and equivariance for the topological generator gives equivariance for its closed subgroup by continuity. The corresponding group on E_x imposes all of these relations and possibly further ones. It is a quotient of $A_{p,*,r}$. It remains to count the weights of large length at E_*.

Choose a primitive $p^{\sigma+1}$-th root of unity ζ. The ring $O = \mathbb{Z}_p[\zeta]$ has uniformizer $\pi = \zeta - 1$ and ramification degree $e = p^\sigma(p-1)$, by the Eisenstein polynomial $P(1+T)$. Evaluation at $T = \pi$ maps $\Lambda = \mathbb{Z}_p[[T]]$ onto O with kernel $(P(1+T))$, by division by this monic distinguished polynomial. The lemma gives $M_\tau \otimes_\Lambda O = D_\tau$. Its O-length is h_τ, since the residue field has order p.

We give the presentation argument to keep track of the integral length. The reduction of M_τ modulo (p, T) is finite dimensional, as it is a quotient of D_τ. Lifts of a basis generate M_τ over Λ. In fact the submodule they generate is closed by compactness of a finite free Λ-module. The quotient Y then satisfies $Y = (p, T)Y$. Its finite Γ-stable quotients separate points. To see this, an open subgroup contains a smaller open subgroup stable under Γ, obtained by intersecting its translates. There are only finitely many translates because continuity and compactness of the open subgroup make its stabilizer open. On any finite stable quotient of Y, the action of γ has p-power order. Modulo p, some power of $T = \gamma - 1$ is zero, by the binomial formula in characteristic p. Since the finite quotient is also killed by a power of p, some power of (p, T) kills it. Thus all these quotients vanish, proving generation.

Take a surjection $\Lambda^q \to M_\tau$ from the chosen generators. If $q = 0$, all the groups in question are zero. Otherwise its relations map at π onto a full-rank sublattice of O^q with cokernel D_τ. This follows by right exactness and surjectivity of $\Lambda \to O$. Lift a basis of the sublattice to relation columns over Λ, and let $f(T)$ be their determinant. For the valuation normalized by $v(p) = 1$, Smith reduction gives $v(f(\pi)) = h_\tau/e$. Evaluation at any t_r gives relation columns on the full group $A_{p,*,r}$. Therefore its length is at most $v(f(t_r))$ whenever this determinant is nonzero.

Factor $f = p^\mu U \prod_i (T - \beta_i)$ by Weierstrass preparation over $\mathbb{Z}_p$, allowing a finite extension for the roots. The unit power series U has valuation zero at all these arguments, and the roots, with multiplicities, have positive valuation. Since $v(\pi) = 1/e < 1$, a root with $v(\beta_i) \ge 1$ contributes exactly $1/e$ at π. There are at most h_τ such roots. For each, in a nonempty progression choose one r_i maximizing $v(t_{r_i} - \beta_i)$, allowing an infinite maximum. At every other weight,

$$v(t_r - \beta_i) \le v(t_r - t_{r_i}) = w + v_p(r - r_i) \le W.$$

The equality uses the binomial formula for a principal unit at an odd prime. For a root with $v(\beta_i) < 1$, its contribution at every t_r is $v(\beta_i) \le e\,v(\pi - \beta_i)$. Indeed if $v(\beta_i) < 1/e$ the two valuations coincide, and otherwise $e\,v(\pi - \beta_i) \ge 1$. Away from the chosen weights every individual contribution to $v(f(t_r))$, including μ, is consequently at most eW times its contribution at π. In particular the determinant is nonzero there and $v(f(t_r)) \le Wh_\tau$. Every weight in $\mathcal{E}_{p,\tau}$ must be among the at most h_τ chosen weights. □

Corollary 22.23 (Simultaneous vanishing of the residual groups at small primes)**.** *Take $0 < \varepsilon < 1/52$ and a polynomial-conductor interval $[V, V^{3/2}]$ of Theorem 19.15. Set $R = \lfloor V^{1203/2} \rfloor$ and $Y = V^{100}$. There is a set $\mathcal{E}_V \subset [1, R) \cap \mathbb{Z}$ determined by the finite ordinary groups above, of size*

$$|\mathcal{E}_V| \ll_{\psi,\varepsilon} V^{306+24\varepsilon} \log(2V).$$

On every sufficiently distant such interval, for all $x \in [V, V^{3/2}]$, all odd primes $p \le Y$, and all $1 \le r < \lfloor x^{401} \rfloor$ outside $\mathcal{E}_V$, the residual group $R_{p,r}$ of Section 6.6 is zero. The full complementary groups in this range have total weighted length bounded by a fixed power of V.

Proof. Let N_* be the cyclotomic modulus of E_*. The real field $F_{\sigma+1}$ has degree at most $n_*^2p^2$ and admits the modulus $N_*p^{u+\sigma+2} \le N_*n_*^2p^2$. Indeed $p^u, p^\sigma \le n_*$, and its degree over F_0 is $p^{\sigma+1}$, with $[F_0 : \mathbb{Q}] \le n_*(p-1)$. For a real abelian field of degree d and modulus N, the conductor–discriminant formula gives $|\mathrm{disc}| \le N^d$. Every ideal class contains an integral ideal of norm at most $\sqrt{|\mathrm{disc}|}$ by Minkowski. The number of these ideals is at most $|\mathrm{disc}|\zeta_F(2) \le (2N)^d$, using the Euler factors. Lemma 22.21 therefore gives

$$\sum_\tau h_\tau \log p \ll n_*^2p^2 \log(2N_*n_*p).$$

Take $\mathcal{E}_V$ to be the union of the finite sets $\mathcal{E}_{p,\tau}$ for $2 < p \le Y$. Summing the count in the theorem over primes using $\sum_{p \le Y} p^2 \le Y^3$ gives $O(n_*^2Y^3 \log(2N_*n_*Y))$. Now $n_* \ll_\psi V^{3+12\varepsilon}$ and $\log(2N_*) \ll_{\psi,\varepsilon} \log(2V)$, which give the displayed cardinality. In particular it is $o(V^{401})$, even at the smallest weight cutoff of this interval.

Here $W \le 1 + \log_p n_* + \log_p R$. Thus every H_τ in the stated prime range is bounded by a fixed power of V. For large V, $Y < P(x) = \exp(x^\varepsilon/12)$ and every $H_\tau < b_0(x) = \lfloor \exp(x^\varepsilon/8) \rfloor$, uniformly for $x \ge V$. At a weight outside the union, the full complementary group has length at most H_τ and hence is killed by $p^{b_0(x)}$. This kills its summand $U_{p,r}$ in the definition of $R_{p,r}$, so the residual quotient is zero. For the final assertion, there are at most YR prime and weight pairs, each with log order bounded by $(\max_{p,\tau} H_\tau) \log Y$. Their product bound is polynomial. □

Membership in $\mathcal{E}_V$ can be tested without locating any root of an Iwasawa power series. The calculation bounds the number of exceptional weights. Their full orders, including on the smaller fields E_x, still enter the sum in Section 6.6.

22.16 A fixed level for the rational strict groups

Write $S_{p,r} = \mathcal{S}_{p,r}(\mathbb{Q})$. Its coefficients are $A_{p,r} = (\mathbb{Q}_p/\mathbb{Z}_p)(-r)$. A class is unramified away from p and has zero restriction to $G_{\mathbb{Q}_p}$. If $v \ne p$ is a finite prime, the unramified local group is $A_{p,r}/(\mathrm{Frob}_v - 1)A_{p,r}$. This is zero for $r \ge 1$, since multiplication by the nonzero scalar $v^{-r} - 1$ on $\mathbb{Q}_p/\mathbb{Z}_p$ is surjective. Requiring zero localization at any additional such primes therefore gives the same strict group.

Lemma 22.24 (The automorphic labels for the trivial character)**.** *Put $K = \mathbb{Q}(\sqrt{-3})$ and $u = 7$, and fix one place of K above u. For every even $r \ge 2$ form the multiset of Theorem 30.11*

with this K, u, level $N = 2$, and the unique character modulo two. Set $d_r = 1 + u^r + u^{-r}$. For every prime $p \geq 11$ with $p-1 \nmid 2r$, the one-character comparison of Theorem 54.13 for $S_{p,r}$ has the following form. There is a submultiset $\mathcal{T}_{p,r}$ of the labelled trace values at this fixed level, with their coefficient embeddings, such that

$$\operatorname{length}_{\mathbb{Z}_p} S_{p,r} \;\leq\; 2 \sum_{b \in \mathcal{T}_{p,r}} v_p(b - d_r), \qquad v_p(p) = 1.$$

Proof. Use the initial character of conductor one in Theorem 19.15. In Proposition 36.3 take $s = 3, u_1 = 7, u_2 = 13$. The last two primes are 1 mod 3, so split in K. The Minkowski bound for K is $2\sqrt{3}/\pi < 2$, giving $|\mathrm{Cl}(K)| = 1$. Fix p, r as in the lemma. Choose an interval far enough that $r < t(V)$ and its two moving ramified primes exceed p. Its upper field has degree a power of two and its modulus is supported at two and at those two moving primes. Consequently $p \nmid su_1 N_*[E_* : \mathbb{Q}]|\mathrm{Cl}(K)|$, as required in Theorem 54.13. The trivial tame character has a singleton residue orbit, coefficient ring $\mathbb{Z}_p$ and the complementary sign at this even weight. The strict scalar group in the comparison is $S_{p,r}$ by the local calculation above. In particular, this group is independent of the chosen interval.

For this one character, the proof of Theorem 54.13 applies the intersection inequality of Proposition 41.4 before it sums over characters or weights. With the multiplicities of Lemma 54.2, this bounds the strict length by twice the sum of $v_p(b - d_r)$ over nonsplit geometric trace points. Equivalently, each of these points occurs once in the determinant of multiplication by the good Frobenius difference on the torsion-free augmentation ideal, as in Theorems 54.3 and 44.44. The hypothesis $p - 1 \nmid 2r$ is exactly what makes the three residual inertia characters distinct. If the strict group is zero we can take the empty submultiset.

It remains to verify the level at which we count the points. At an irreducible point Proposition 44.42 gives a conjugate-self-dual cuspidal representation over K. At each finite place away from p its Galois representation has finite inertia of order prime to p, by the tame condition in Theorem 54.13. The three residual characters on this inertia are trivial, since the tame character is trivial and the cyclotomic character is unramified there. For every inertia element, all its eigenvalues thus reduce to one. They have order prime to p, and reduction is injective on roots of unity of such order. The element is diagonalizable in characteristic zero since it has finite order. It follows that the entire inertia group acts trivially. The Tate twist used in descent is unramified at these places. Thus the associated Weil–Deligne parameters have trivial inertia and zero monodromy. At places above p, crystallinity from Proposition 54.11 gives the same assertion about the Weil–Deligne parameters. The local–global compatibility, weight calculation and spherical level criterion used in Theorem 36.18 now give hyperspecial fixed vectors at every finite place and coefficient weights of absolute value at most $4(r + 2)$. In particular the representation has vectors of level $U_K(2)$.

At each remaining nonsplit point Proposition 40.11 gives a primitive cuspidal form of weight $2r + 1$ and level equal to the conductor of the quadratic character of K, namely three. Its normalized trace in the arithmetic convention is $1 + u^{-r} a_u(f)$. Both this trace and the inverse convention are among the plane labels of Theorem 30.8 at $N = 2$, since $3 \mid 2|D_K|$. For both types of points the full embedded automorphic label with Frobenius convention determines at most one trace point by Proposition 44.42. Distinct labels which have the same numerical trace remain separate factors in the multiset. This proves the asserted inclusion with multiplicity and hence the inequality. □

Theorem 22.25 (A polynomial logarithmic bound for the rational groups)**.** *There are absolute constants $C, A > 0$ and, for each even $r \geq 2$, a positive integer H_r such that*

$$|K_{2r}(\mathbb{Z})| \mid H_r^2, \qquad \log H_r \leq C(r + 2)^A.$$

Consequently the normalized sum of strict lengths in (20.5) *is at most* $2C(r+2)^A$*, uniformly in the coefficient rings and in the finite set of primes.*

Proof. Let H_r be the absolute value of the integer $I_{u,H,r}$ of Theorem 30.11 for the data of Lemma 22.24, where $H = (\mathbb{Z}/2\mathbb{Z})^\times$. The integer is the product, over the full labelled list with conjugates, of $u^{18h+1}(b - d_r)$, with $h = 4(r+2)$. Each factor is an algebraic integer and Galois permutes the factors. None vanishes since $|b| \le 3 < d_r$ under complex embeddings. Theorem 30.11 bounds its logarithm as asserted because u, K, N are fixed. For every $p \ge 11$ with $p - 1 \nmid 2r$, all factors are integral at p and the power of u is a unit. The lemma gives

$$\operatorname{length}_{\mathbb{Z}_p} S_{p,r} \le 2v_p(H_r).$$

By Proposition 20.6, $S_{p,r}$ is dual to the p-part of $K_{2r}(\mathbb{Z})$ for odd p, this part is zero if $p - 1 \mid 2r$, and there is no factor at two. For completeness the primes five and seven also contribute zero at every even r. Their maximal real cyclotomic fields have degrees two and three and respective discriminants 5 and 7^2 by the conductor–discriminant formula. Their Minkowski bounds are $\sqrt{5}/2$ and $6 \cdot 7/27$, both less than two. Thus both real class groups are trivial, and Proposition 11.19 makes the corresponding quotient of $K_{2r}(\mathbb{Z})$ modulo p zero. The group is finite, so its p-part is zero. The prime three always satisfies $p - 1 \mid 2r$. Multiplication of the local divisibilities gives the asserted divisibility of ordinary integers. Equation (20.5) then gives the coefficient statement. □

Corollary 22.26 (Rational classes on the period fields)**.** *Let the original character ψ be arbitrary and let E_x be its fields on $[V, V^{3/2}]$. For each odd p and each even $1 \le r < t = \lfloor x^{401} \rfloor$, let $D_{p,r}(E_x)$ be the image of $S_{p,r}$ under restriction. Then, uniformly on these intervals,*

$$\sum_{p>2} \sum_{\substack{1 \le r < t \\ 2 \mid r}} \log |D_{p,r}(E_x)| \ \ll \ (t+2)^{A+1}.$$

For every sufficiently distant interval, $R_{p,r}^{\mathrm{Gal}(E_x/\mathbb{Q})} = 0$ for every odd $p \le P(x)$ and every $1 \le r < t$, with R as in Proposition 6.11.

Proof. Restriction preserves vanishing at the places over p and unramifiedness elsewhere. Each image has order at most that of its source, so summing the preceding theorem over the weights proves the first assertion. Put $G = \mathrm{Gal}(E_x/\mathbb{Q})$. For odd r complex conjugation acts as minus one on the complementary summand, and two is invertible on its p-group. There are therefore no invariants. For even r with $p \nmid |G|$, the norm divided by $|G|$ is an integral projection onto invariants and commutes with $J_{p,r}$. On strict groups, restriction identifies $S_{p,r}$ with the invariants over E_x. Indeed the two restriction and corestriction composites are $|G|$ and the sum of G. Corestriction preserves strictness, since its local restrictions are sums of local corestrictions and a strict class is zero at every finite place. The latter assertion follows by the same unramified calculation as above with the local residue cardinality. Thus the invariant part of $U_{p,r}$ has length at most $2C(r+2)^A/\log p < b_0$ for large V. In taking $U_{p,r}/U_{p,r}[p^{b_0}]$, the integral averaging projection is exact and its entire image is killed by the truncation.

Finally, every odd prime dividing $|G|$ divides the order of ψ and belongs to the fixed set Π in Proposition 6.11. At each weight for such a p, $J_{p,r}$ is the average over a subgroup of two-power order. This average is the identity on every G-invariant element of the quotient as well, whereas it is zero on $U_{p,r} = (1 - J_{p,r})M_{p,r}$ and on all of its quotients by G-stable subgroups. This proves the assertion at these primes. □

The remaining complementary classes can transform under nontrivial characters of the period field. The preceding argument treats the trivial character and supplies a single integer at each weight on every interval, independently of its moving ramified primes.

22.17 Odd quadratic and quartic characters on the common fields

Let $S(\alpha, r)$ be the strict group on $\mathbb{Q}$ with coefficients $(J/O)(\alpha^{-1}\kappa_p^{-r})$, where κ_p is the p-adic cyclotomic character and O is the ring generated over $\mathbb{Z}_p$ by the values of the finite character α in its fraction field J. We use zero localization at p and zero restriction to inertia elsewhere. The extra conductor conditions in Theorem 22.17 define a subgroup of this group. Write η_p for the unique quadratic character of conductor p. At $r \equiv (p-1)/2 \bmod (p-1)$ the reduction of κ_p^{-r} is η_p.

Proposition 22.27 (Two conductor bounds at the half residue)**.** *Let α have primitive conductor a, let p be an odd prime with $p \nmid a$, and suppose $\alpha(-1) = (-1)^r$ and $r \equiv (p-1)/2 \bmod (p-1)$.*

1. *If α is quadratic, then, given $0 < \delta < 4$, one has $S(\alpha, r) = 0$ whenever $a \le (4-\delta)p$ and p is sufficiently large in terms of δ alone.*
2. *Suppose α is odd of order four. Write $a_2 = \operatorname{cond}(\alpha^2)$ and $Y = \max\{1, 3a\sqrt{a_2}\,p/32\}$. If $Y(1+\log Y)^3 < p^2$, then $S(\alpha, r) = 0$.*

For each fixed odd quadratic or quartic character these conclusions cover every sufficiently large prime at which an odd complementary weight lies in the half residue.

Proof. Let $\lambda = \alpha^{-1}\eta_p$ and let L be the field cut out by λ. The parity condition makes L totally real. The two conductor factors are coprime, and inertia at p has image of order two. The residual character $\bar{\lambda}$ has the same image order m as λ since $m = 2$ or 4 is prime to p. If the strict group is nonzero, Lemma 55.33 gives

$$p^{\operatorname{ord}_m(p)} \mid h_L,$$

where h_L is the ordinary class number. To recall the divisibility, a strict class of order p lifts to a residual class. The coefficient invariants vanish globally and at p because some inertia element acts by a scalar different from one modulo p. Thus the residual class is still zero locally at p. At the other finite places the inertia action on the coefficient group has order prime to p. Its invariants are either the divisible group or zero, so passage to its p-torsion preserves the unramified condition. Restriction to G_L is injective by averaging over the quotient of order m. The resulting homomorphism factors through the ordinary class group by reciprocity, since it is unramified everywhere and p is odd. Equivariance makes its nonzero image a vector space over the field generated by a primitive m-th root in characteristic p, of degree $\operatorname{ord}_m(p)$.

In the quadratic case the conductor–discriminant formula gives $D = \operatorname{disc} L = ap$. We record the uniform estimate

$$h_L \le \left(\frac{1}{2} + O\!\left(\frac{\log\log(3D)}{\log(3D)}\right)\right)\sqrt{D}.$$

Indeed, if $\epsilon > 1$ is a fundamental unit, then $\epsilon - \epsilon'$ is a nonzero integral multiple of $\sqrt{D}$. Since $|\epsilon'| = \epsilon^{-1}$, it follows that $\epsilon + \epsilon^{-1} \ge \sqrt{D}$, whence $2\log\epsilon \ge \log D - O(1/D)$ as $D \to \infty$. For the primitive character χ_D, its sum on an interval is $O(\sqrt{D}\log(2D))$. This follows by the additive Fourier expansion modulo D, since the primitive Gauss sums have absolute value $\sqrt{D}$ at unit frequencies and vanish at the other frequencies, and the geometric sum at frequency $1 \le j < D$ has absolute value at most $D/(2\min(j, D-j))$. Partial summation at $y = \lceil \sqrt{D}\log^2(2D) \rceil$ bounds the tail of $L(1, \chi_D)$ by $O(1/\log(2D))$. The initial sum is at most $1 + \log y$. The

quadratic class number formula $2h_L \log \epsilon = \sqrt{D} L(1, \chi_D)$ now gives the estimate. Under the displayed condition on a, $h_L/p \le (1/2+o(1))\sqrt{4-\delta} < 1$ uniformly as $p \to \infty$. This contradicts the divisibility.

In the quartic case r is odd, hence $p \equiv 3 \bmod 4$ and $\mathrm{ord}_4(p) = 2$. The three nontrivial characters of L have conductors ap, a_2, ap, respectively. Thus $\operatorname{disc} L = a^2 a_2 p^2$. Minkowski's bound for an integral ideal in each class of this real quartic field is $(4!/4^4)\sqrt{\operatorname{disc} L} \le Y$. The number of ideals of norm k is at most the number of ordered factorizations of k into four positive factors, by comparison of Euler factors with those of $\zeta(s)^4$. Sum first over three factors, bounding the number of choices of the last by Y divided by their product. This gives $h_L \le Y(1+\log Y)^3$, contradicting $p^2 \mid h_L$ under the stated condition. At fixed a, this upper bound is $O_a(p(1+\log p)^3) = o(p^2)$. □

Let $C_\infty = \bigcup_j C_j$ be the real cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}$, and let D be the subfield of $K_\psi C_\infty$ cut out by all its characters of order dividing four. This is a fixed finite abelian field of two-power degree. Indeed its ambient Galois group has an open procyclic subgroup isomorphic to $\mathbb{Z}_2$, whose fourth powers form another open subgroup. Every character in question kills those fourth powers, and the resulting joint character quotient has exponent dividing four. In particular $D \subset B_J = K_\psi C_J$ for all sufficiently large J.

Theorem 22.28 (All odd weights on the fixed subfield of exponent four)**.** *Take the actual fields and intervals of Theorem 19.15, and set $t = \lfloor x^{401} \rfloor$. There is a constant A, depending only on the original data, such that uniformly there*

$$\sum_{p>2} \sum_{\substack{1 \le r < t \\ r \text{ odd}}} \log \left| \mathcal{S}_{p,r}(D)^{c=-1} \right| \ll_{\psi,\varepsilon} V^A + \exp(x^{2\varepsilon/3}).$$

For every such odd weight and every odd $p \le P(x)$, one has

$$R_{p,r}(E_x)^{\mathrm{Gal}(E_x/D)} = 0$$

on every sufficiently distant interval.

Proof. There are finitely many characters of D. Its odd characters have order two or four. Choose a fixed p_0 exceeding their conductors, all primes in the finite set of Lemma 9.31, the prime divisors of $[K_\psi : \mathbb{Q}]$, and the thresholds in Proposition 22.27 for these finitely many characters. At each $p > p_0$ and each odd half-residue weight the full minus summand on D vanishes. To see the character comparison at this fixed field, extend coefficients to contain fourth roots of unity. The degree of D is a unit at p, so the character projections on the cochains are integral. Restriction identifies each scalar strict group with the corresponding character summand over D by inflation and restriction with a prime-to-p quotient. This holds on local decomposition groups at p and on inertia elsewhere as their quotients also have order prime to p. Equivalently one can use Shapiro's lemma with the regular representation and then project to a character. Each odd character summand is therefore zero by the proposition. The scalar extension used here is faithfully flat.

The zero residue modulo $p-1$ contains no odd weights. Thus every other possible pair with $p > p_0$ satisfies $p - 1 \nmid 2r$. For all sufficiently distant intervals $D \subset E_*$, the actual upper endpoint field. The full orders at all these separated pairs on D have product dividing $J(V)$ by Lemma 9.31, because $t \le \lfloor V^{1203/2} \rfloor$. The logarithmic sum for $p > p_0$ is at most $\log J(V) \ll V^A$.

For $2 < p \le p_0$ restrict from D to the actual B_J inside E_x. Its kernel is killed by $[B_J : D]$, whose p-adic valuation is at most $s_p = v_p([K_\psi : \mathbb{Q}])$. For fixed p, D, the order of $\mathcal{S}_{p,r}(D)[p]$ is bounded independently of r. Indeed it is bounded by the order of the global degree-one

group with coefficients $\mathbb{F}_p(-r)$ unramified away from p, using the multiplication-by-p sequence. Restriction to $D(\mu_p)$ is injective since the relative degree divides $p-1$. On this field the coefficient module is isomorphic to μ_p. Kummer theory puts the unramified-away-from-p group between the group of p-units modulo p-th powers and the p-torsion of the ideal class group with primes over p inverted. Both are finite and independent of r. Successive multiplication by p now bounds the logarithm of the kernel on restriction to B_J by a constant depending only on p, D, s_p. Summing these losses costs $O_\psi(t)$. The image lies in the corresponding complementary group on B_J. For sufficiently large V the growing prime range of Theorem 20.4 contains every $p \le p_0$. Its bound on the same interval gives total logarithmic order of all these images at most $\exp(x^{2\varepsilon/3})$. This proves the first assertion.

For the second let $H = \mathrm{Gal}(E_x/D)$. When $p \nmid |H|$, restriction and corestriction identify the H-invariants in the strict group with the strict group on D, as in Corollary 22.26. Its minus part has length bounded by the preceding display divided by $\log p$, including the implied constant. This is less than $b_0 = \lfloor \exp(x^\varepsilon/8) \rfloor$ uniformly for large V, since $V \le x$ and $x^{2\varepsilon/3} = o(x^\varepsilon)$. The averaging operator over H commutes with all the field projections and passes exactly to invariants in their quotients. The truncation in Proposition 6.11 thus kills the whole invariant image. If $p \mid |H|$, then p belongs to the fixed set Π there. The field of its averaging operator $J_{p,r}$ contains D, since both candidate fields contain any fixed subfield of $K_\psi C_\infty$ for sufficiently large V. The subgroup used in this average is contained in H. Its average fixes every H-invariant class and acts as zero on the entire residual quotient by definition. This also proves vanishing. □

Corollary 22.29 (Every complementary weight over a fixed imaginary quadratic field)**.** *Let $F \subset K_\psi C_\infty$ be any imaginary quadratic field. On the same intervals, for some fixed A',*

$$\sum_{p>2} \sum_{1 \le r < t} \log \left| \mathcal{S}_{p,r}(F)^{c=(-1)^r} \right| \ll_{\psi,\varepsilon} V^{A'} + \exp(x^{2\varepsilon/3}).$$

The sum divided by $\exp(x^\varepsilon/2)$ tends uniformly to zero. At every odd $p \le P(x)$ and every weight $1 \le r < t$, the invariants of the actual $R_{p,r}(E_x)$ under $\mathrm{Gal}(E_x/F)$ are zero for large V.

Proof. For odd weights $F \subset D$ and restriction to D is injective since $[D : F]$ is a power of two. Invariants under $\mathrm{Gal}(E_x/F)$ are in particular invariants under $\mathrm{Gal}(E_x/D)$. Apply the theorem. At an even weight c generates $\mathrm{Gal}(F/\mathbb{Q})$, so the plus group on F is the rational strict group by prime-to-p descent. Sum Theorem 22.25 over these weights and use $t \le V^{1203/2}$. An invariant residual class under $\mathrm{Gal}(E_x/F)$ is already fixed by c at this weight. Together these elements generate $\mathrm{Gal}(E_x/\mathbb{Q})$. Corollary 22.26 therefore gives zero. Finally both terms of the displayed upper bound are $o(\exp(x^\varepsilon/2))$ since $x \ge V \to \infty$. □

The bound for D concerns all its odd characters and all odd weights on the original intervals. The quadratic fields added at the two moving ramified primes need not be contained in D.

22.18 Normalized Frobenius values on the original period fields

We now evaluate the full groups $\mathcal{S}_{\ell,r}(E_x)$ of Section 6.4. Fix a common algebraic closure of $\mathbb{Q}$. First let $E/\mathbb{Q}$ be a finite abelian field unramified at the odd prime ℓ, with $\ell \nmid [E : \mathbb{Q}]$, and let $r \ge 1$. Write $M = (\mathbb{Q}_\ell/\mathbb{Z}_\ell)(-r)$, $\chi = \kappa_\ell^{-r}$, and $S = \mathcal{S}_{\ell,r}(E)$. We inflate cocycles to G_E. Choose a decomposition group $D_v \subset G_E$ at one place over ℓ. For a finite abelian ℓ-group U, put $U^\vee = \mathrm{Hom}(U, \mathbb{Q}_\ell/\mathbb{Z}_\ell)$, using the additive coefficient group.

Lemma 22.30 (A normalization at the coefficient prime)**.** *Every $c \in S$ has precisely one representing cocycle y_c which is zero on D_v. The correspondence is additive, and a class killed*

by ℓ^a has normalized values in $M[\ell^a]$. With $H = G_{\mathbb{Q}^{\mathrm{ab}}}$ there is a surjection

$$H \longrightarrow S^\vee, \qquad n \longmapsto (c \longmapsto y_c(n)).$$

Proof. By strictness, subtracting a global coboundary makes a representative zero on D_v. Locally $E_v/\mathbb{Q}_\ell$ is unramified, whereas the ℓ-power cyclotomic tower of $\mathbb{Q}_\ell$ is totally ramified. Thus the cyclotomic image of inertia is all of $\mathbb{Z}_\ell^\times$, also over E_v. The invariants of D_v in M are therefore the same as the global invariants. A global coboundary vanishing on D_v is identically zero. This proves uniqueness; addition and multiplication by ℓ^a preserve the normalization.

The group H is contained in G_E and acts trivially on M, since all roots of unity belong to $\mathbb{Q}^{\mathrm{ab}}$. Suppose y_c vanishes on H. It descends to a cocycle on the abelian quotient $B = \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/E)$. On this quotient, for z in the image of inertia at v and $g \in B$, the equation $zg = gz$ and $y_c(z) = 0$ give $(\chi(z) - 1)y_c(g) = 0$. The inertia image under χ is the full global image. Thus all values are globally invariant, and the descended cocycle is a homomorphism. Its image is finite, because it is a continuous map from a compact group to a discrete group. It vanishes on every inertia group away from ℓ by the original unramified condition. All inertia images in B at places above ℓ agree, since $\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}$ is abelian and $E/\mathbb{Q}$ is Galois. The homomorphism is unramified there as well.

A nonzero image would give an extension E'/E of degree ℓ, unramified at all finite places, with $E'/\mathbb{Q}$ abelian. The ℓ-primary subgroup of $\mathrm{Gal}(E'/\mathbb{Q})$ would have order ℓ. Each finite inertia group injects into $\mathrm{Gal}(E/\mathbb{Q})$ and consequently projects trivially onto that primary subgroup. The degree-ℓ field fixed by the complementary subgroup would be unramified at every finite prime of $\mathbb{Q}$, contradicting Minkowski's discriminant bound. We conclude that $y_c = 0$. The group S is finite by the argument of Proposition 11.4 for odd ℓ. The evaluation map on H is a homomorphism, and the argument just given says its image has zero annihilator in S. A proper subgroup of the finite group $S^\vee$ has nonzero annihilator by finite abelian duality. This proves surjectivity. □

Theorem 22.31 (Full strict groups at one list of rational primes)**.** *Take a nonempty finite list of triples (E_i, ℓ_i, r_i) as above, writing $S_i = \mathcal{S}_{\ell_i, r_i}(E_i)$. Let $C/\mathbb{Q}$ be any finite abelian extension containing all the E_i, and prescribe an element $\sigma_0 \in \mathrm{Gal}(C/\mathbb{Q})$ fixing them all. Put $b = \#\{i\}$, $d_i = \dim_{\mathbb{F}_{\ell_i}} S_i[\ell_i]$, and $d = \max_i d_i$. There exist*

$$h = d + \lceil \log_2(2b) \rceil$$

distinct good rational primes with this prescribed Frobenius in C. At one compatible choice of places above them let $s_1, \ldots, s_h$ be their Frobenius elements. For every i the normalized values give an injection

$$S_i \longrightarrow (\mathbb{Q}_{\ell_i}/\mathbb{Z}_{\ell_i})^h, \qquad c \longmapsto (y_c(s_j))_{1 \le j \le h}.$$

In particular the exact additive order of each class is the largest of the orders of its displayed values. One can avoid any finite set of primes.

Proof. Lift σ_0 to $\sigma \in G_{\mathbb{Q}}$. It lies in every G_{E_i}. For Haar-uniform $n \in H$, the functional $c \mapsto y_c(n)$ is uniform on $S_i^\vee$ by Lemma 22.30. The functional at σn is obtained by multiplication by the unit $\chi_i(\sigma)$ and addition of the fixed functional at σ, by the cocycle identity. It too is uniform. Take h independent such elements of the coset. For a fixed i, their reductions modulo $\ell_i S_i^\vee$ are independent uniform vectors in a vector space of dimension d_i. If these vectors fail to span, they lie in a hyperplane. For $d_i > 0$ there are $(\ell_i^{d_i} - 1)/(\ell_i - 1)$ hyperplanes; the probability that all vectors lie in any particular one is ℓ_i^{-h}. For $d_i = 0$ failure has probability zero. Summing the resulting bounds over the indices gives at most $b\,2^{d-h} < 1$. This uses

no independence between different groups. Fix a tuple for which every reduction spans. The integral functionals generate $S_i^\vee$: the quotient by their span is a finite ℓ_i-group equal to its multiple by ℓ_i, and is therefore zero. Finite duality now gives the asserted injections at the chosen group elements.

For each i take the exponent $\ell_i^{a_i}$ of S_i, omitting trivial groups. All normalized representatives have values killed by $\ell_i^{a_i}$. The finite semidirect product recording the character modulo $\ell_i^{a_i}$ and the values of the cocycles on a generating set of S_i gives a finite quotient of G_{E_i}. This follows directly from the cocycle law. Take the compositum of the normal closures of its fixed fields over $\mathbb{Q}$ for all i, together with C. For each chosen coset element, Chebotarev gives infinitely many rational primes with that conjugacy class in the finite Galois group. A choice of place realizes the specified element itself. All the elements restrict to σ_0 in C, and every normalized evaluation is preserved. Excluding previous choices and all bad primes proves the assertion. Orders are preserved by an injection, and the order of a tuple of elements of ℓ_i-power order is their largest order. □

Corollary 22.32 (The weighted lengths on the common interval)**.** *Use the fields in Section 59.3 on $[V, V^{3/2}]$, with $N^\natural$ the common conductor modulus and $n_* = [E_* : \mathbb{Q}]$ at the largest layer. Fix $A_0 > 0$. For all the distinct triples*

$$E = E_x, \qquad 1 \le r < t(x), \qquad 2 < \ell \le V^{A_0}, \qquad \ell \nmid n_* N^\natural,$$

one list of $V^{O(1)}$ rational primes in a prescribed compatible finite abelian Frobenius class suffices in Theorem 22.31. In particular they can all split in every period and starting field, with any given cyclotomic depth at each coefficient prime. The number of primes has the stated bound independently of those depths. For each triple write s_j for the resulting Frobenius at the chosen place, and put

$$u_{\ell,r,E,j} = \log_\ell \#\{y_c(s_j) : c \in \mathcal{S}_{\ell,r}(E)\}.$$

For every subset of these triples the sum of $(\log \ell)\,\mathrm{length}_{\mathbb{Z}_\ell} \mathcal{S}_{\ell,r}(E)$ over the subset is at most the sum of $(\log \ell)\sum_{j=1}^{h} u_{\ell,r,E,j}$ over that same subset. Also $\ell^{\max_j u_{\ell,r,E,j}}$ is exactly the exponent of the corresponding strict group.

Proof. All degrees divide n_*, and each conductor divides $N^\natural$. Thus each triple satisfies the lemma. The number of different fields on the interval is at most $1 + \log_2 n_*$, since consecutive distinct fields in this nested tower differ by degree at least two. The number of twists is at most $V^{1203/2}$, and the number of coefficient primes is at most V^{A_0}. The degree n_* and $\log(2N^\natural)$ are polynomially bounded on the intervals of Theorem 19.15. The Kummer estimate in the proof of Theorem 11.5 gives uniformly

$$d_i \log \ell_i \ \ll \ n_* \ell_i \log(2N^\natural \ell_i).$$

It bounds the dimension of the ℓ_i-torsion via the units and the class group of $E_i(\mu_{\ell_i})$. Hence both d and h meet the claimed bound. For the splitting assertion take C to contain all the period fields, the finite abelian starting fields of Corollary 61.19, and the indicated roots of unity, and take $\sigma_0 = 1$.

Each coordinate image is a finite subgroup of $\mathbb{Q}_\ell/\mathbb{Z}_\ell$, hence cyclic of order $\ell^{u_{\ell,r,E,j}}$. The group embeds into the product of those cyclic images. Taking logarithms of their orders and summing gives the stated inequality. The exponent of the subgroup is at most the largest coordinate order and at least the exponent of each coordinate image, proving equality. □

The value $y_c(s_j)$ uses the normalization at the chosen place over ℓ. Ordinary localization at a good split rational prime q would take its value in $M/(q^{-r} - 1)M$, which is zero: multiplication

by the nonzero ℓ-adic scalar $q^{-r}-1$ is surjective on $\mathbb{Q}_\ell/\mathbb{Z}_\ell$. The theorem uses finite quotients determined by the actual strict groups. It gives no upper bound for the orders in the coordinate images or the sizes of the rational primes chosen. An estimate for those orders, or an integral formula relating them to the projected periods, is still needed for the remaining lengths in Section 6.6.

22.19 The genus field contribution to the full strict length

Let $E/\mathbb{Q}$ be finite abelian. Write T_E for its genus field, the maximal extension of E abelian over $\mathbb{Q}$ and unramified at all finite places over E. For every prime ℓ, including two, and $r \geq 1$, set $M = (\mathbb{Q}_\ell/\mathbb{Z}_\ell)(-r)$, $H = G_{\mathbb{Q}^{\mathrm{ab}}}$, and

$$S = \mathcal{S}_{\ell,r}(E), \qquad K_{\ell,r}(E) = \ker\bigl(S \longrightarrow \mathrm{Hom}_{\mathrm{cont}}(H, M)\bigr).$$

The restriction makes sense on classes since H acts trivially on M. We compute this kernel without a restriction on the ramification of E at ℓ.

Lemma 22.33 (The genus field on the varying interval)**.** *Let $\psi = \prod_{p|F} \psi_p$ be the decomposition of the original primitive character into its prime-power conductor factors. Put*

$$T_\psi = \prod_{p|F} K_{\psi_p}, \qquad g_\psi = \frac{\prod_{p|F} \mathrm{ord}(\psi_p)}{\mathrm{ord}(\psi)}.$$

Here a product of fields is their compositum, and the empty product gives $T_\psi = \mathbb{Q}$ and $g_\psi = 1$. For the period fields of Theorem 19.15,

$$T_{E_x} = E_x T_\psi, \qquad [T_{E_x} : E_x] \mid g_\psi.$$

Proof. We give the Dirichlet character description of the genus field using finite primes throughout. Leopoldt (1953). For an abelian field E inside $\mathbb{Q}(\mu_N)$, let X be its group of Dirichlet characters. For each $p \mid N$, let X_p consist of their components at p, viewed as characters of the single p-power factor. In the cyclotomic Galois group the inertia group at p is precisely this local factor: the p-power cyclotomic extension is totally ramified there and all the other factors are unramified. Its image in the Galois group of E has character group X_p, by restriction of characters of a finite abelian group. Thus $e_p(E/\mathbb{Q}) = |X_p|$.

Let T have character group generated by all the X_p. It contains E, since each character is the product of its components. Distinct factors are independent, so $[T : \mathbb{Q}] = \prod_p |X_p|$, and its inertia index at each p is still $|X_p|$. It follows that T/E is unramified at every finite place. Conversely, if B/E is any finite extension unramified at finite places with $B/\mathbb{Q}$ abelian, then all its finite inertia groups have orders $e_p(E/\mathbb{Q})$. They generate $\mathrm{Gal}(B/\mathbb{Q})$, since their fixed field is unramified at all finite primes of $\mathbb{Q}$ and hence is $\mathbb{Q}$ by Minkowski's bound. The group is abelian, so $[B : \mathbb{Q}] \leq \prod_p e_p(E/\mathbb{Q})$. Applying the same bound to BT, which is still unramified over E, gives $B \subset T$. This proves $T = T_E$.

The characters of E_x are generated by ψ and the characters of its three factors $C_J, \mathbb{Q}(\sqrt{-q}), \mathbb{Q}(\sqrt{-d_0})$. Each of the latter characters is supported at a single prime, respectively $2, q, d_0$. For the quadratic fields this follows from $q, d_0 \equiv 3 \bmod 4$, so their discriminants are $-q, -d_0$. Taking all local components therefore adjoins exactly the ψ_p to this group. This gives $T_{E_x} = E_x T_\psi$. The single-prime components of ψ are independent in the product of cyclotomic factors, so $[T_\psi : K_\psi] = g_\psi$. Since $K_\psi \subset E_x$, the degree of its base change divides g_ψ. □

Theorem 22.34 (The strict classes vanishing on the absolute commutator subgroup)**.** *Fix a place $v \mid \ell$ of E, with absolute decomposition group D_v. Let $U = M^{D_v}$ and set*

$$C_{E,\ell} = \mathrm{Gal}(T_E/E)/\langle \mathrm{Frob}_v(T_E/E)\rangle.$$

The action on U factors through $C_{E,\ell}$. Inflation induces an isomorphism

$$H^1(C_{E,\ell}, U) \;\simeq\; K_{\ell,r}(E), \qquad \mathrm{length}_{\mathbb{Z}_\ell} K_{\ell,r}(E) \le v_\ell(|C_{E,\ell}|).$$

In particular for each x on the period interval,

$$\sum_{\ell} (\log \ell) \sum_{1 \le r < t(x)} \mathrm{length}_{\mathbb{Z}_\ell} K_{\ell,r}(E_x) \;\le\; (t(x)-1)\log g_\psi.$$

Proof. Set $B = \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/E)$. In B divide out by the closed subgroup J generated by the images of D_v and of inertia at all finite primes away from ℓ. Inertia at all places over ℓ has the same image, since $E/\mathbb{Q}$ is Galois and the larger extension is abelian over $\mathbb{Q}$. Dividing out first by all finite inertia gives $\mathrm{Gal}(T_E/E)$, by the definition just proved. The image of D_v there is generated by its unramified Frobenius. Hence $B/J = C_{E,\ell}$. Inertia away from ℓ acts trivially on M, so $M^J = U$. This is a finite cyclic ℓ-group: the local cyclotomic image contains an open subgroup of $\mathbb{Z}_\ell^\times$, and a unit of infinite order there has a nontrivial r-th power. Its difference from one kills only a finite subgroup of $\mathbb{Q}_\ell/\mathbb{Z}_\ell$.

Take $c \in K_{\ell,r}(E)$. A representative y vanishes on H, since all coboundaries do and its restriction is zero. It therefore descends to B. Strictness permits subtraction of a coboundary so that $y = 0$ on D_v. At the remaining finite primes away from ℓ it is zero on inertia, as the original cocycle factors through the quotient unramified there and inertia acts trivially on M. Thus the adjusted cocycle vanishes on J. Its values belong to M^J, by applying the cocycle identity to $jg = gj$. It descends to a cocycle of $C_{E,\ell}$ with coefficients U. Conversely, inflating any such cocycle gives an unramified class away from ℓ and zero restriction at every place above ℓ, since the images of their decomposition groups in B are the same. Inflation is injective: if an inflated cocycle is the coboundary of $m \in M$, then its vanishing on J forces $m \in U$. This proves the isomorphism.

For any finite group C acting on a finite cyclic ℓ-group U, restriction to an ℓ-Sylow subgroup P is injective in first cohomology, by corestriction. We prove $\mathrm{length}\, H^1(P,U) \le \log_\ell |P|$ by induction. For nontrivial P take a central subgroup Z of order ℓ. The kernel of restriction to Z is the inflation of $H^1(P/Z, U^Z)$, bounded by induction since U^Z is cyclic. Evaluation at a generator of Z makes $H^1(Z,U)$ a subquotient of U; restriction to the trivial subgroup followed by corestriction shows it is killed by ℓ. Its length is at most one. The trivial group starts the induction. This proves the stated bound and, by Lemma 22.33, the inequality for each r with $v_\ell(g_\psi)$ on the right. Summing uses $\sum_\ell v_\ell(g_\psi)\log \ell = \log g_\psi$. □

Corollary 22.35 (Common split primes for every strict group up to the genus contribution)**.** *Fix one of the intervals and a finite list of its triples (E_x, ℓ, r), now allowing every coefficient prime. At one list of good rational primes split in any prescribed finite abelian field containing the E_x, the normalized evaluations give homomorphisms on each S with common kernel exactly $K_{\ell,r}(E_x)$. Normalization requires the representing cocycle to vanish on the chosen D_v. The values at the selected primes are independent of the choice of such a representative. The number of primes may be taken as $d + \lceil \log_2(2b) \rceil$, where $b \ge 1$ is the number of triples and d is the largest minimal number of generators of any $S/K_{\ell,r}(E_x)$ in the list. For $\ell \le V^{A_0}$ it is polynomial in V for each fixed A_0; unrestricted prescribed finite cyclotomic depths are allowed. A finite list can also include every nonzero strict group on the interval, without a size restriction on ℓ.*

Proof. The restriction pairing on H has annihilator K by definition. Therefore $H \to (S/K)^\vee$ is onto, as in Lemma 22.30. The hyperplane count in Theorem 22.31 selects the stated number of group elements of H giving generation for all the quotient duals together. For each $c \in S$ choose a representing cocycle with value zero on D_v. Any two choices differ by the coboundary of an element of the finite group $U = M^{D_v}$ from the theorem. Add to the common splitting field enough ℓ-power roots of unity to make all the characters at the chosen primes act trivially on these groups U, as well as the roots requested in the statement. At such a Frobenius the difference of the two representatives is exactly zero.

Each selected representative has finite image by compactness. At a finite coefficient precision containing that image, its values and character are recorded by a finite semidirect product. There are only finitely many classes in each group by Proposition 11.4. Apply Chebotarev to the joint normal closures and the finite abelian splitting field, matching each selected element of H with a rational Frobenius and a choice of place. All evaluations agree with their values on H. Thus they are additive and their joint kernel is precisely K. The same rank estimate from Theorem 11.5 as in Corollary 22.32 applies also to the ramified primes and to two; a quotient of a finite abelian ℓ-group has at most as many generators as the group itself. Finally there are only finitely many fields and weights on each interval. Proposition 11.4 gives finite prime support for each pair. This proves the last assertion. □

For these evaluations let $I_{\ell,r}(E_x)$ denote the image of the whole group in its product of coordinate groups. Its order has the exact relation

$$\log|S| = \log|I_{\ell,r}(E_x)| + \log|K_{\ell,r}(E_x)|.$$

The total second term on an interval, summed at each x over all primes and permitted weights, is at most $(t(x)-1)\log g_\psi$, a polynomial in x. For a character of prime-power conductor, or for the trivial character, $g_\psi = 1$ and the common tests recover the full groups even at the ramified primes. Bounding the orders of the images $I_{\ell,r}(E_x)$ on the scale required by Section 6.6 and comparing the signed integral periods there are the remaining arithmetic estimates.

22.20 Local unit tests at arbitrary precision on the period fields

Fix the fields $E = E_x \subseteq E_*$ of Section 6.6 on one of its intervals. Write $\kappa = \kappa_p$ for the cyclotomic character at an odd prime p. For a CM field F let $D_p(F) = \mathcal{S}_{p,-1}(F)^{c=-1}$. Its coefficients are μ_{p^∞}. Theorem 24.13 uses the group $D_p(E(\mu_p))$ through precision $1 + v_p(r+1)$. To go beyond that precision we need descent through extensions of p-power degree. We carry this out on the fields

$$B_k = E_*(\mu_{p^k}) \quad (k \geq 1), \qquad B_\infty = \bigcup_{k \geq 1} B_k.$$

They depend only on p and the chosen interval.

Lemma 22.36 (Descent of strict classes in a cyclotomic tower)**.** *Let F be a number field, $F_\infty = F(\mu_{p^\infty})$, and $A = (\mathbb{Q}_p/\mathbb{Z}_p)(s)$ with $s \neq 0$. Write $S(F,A)$ for the classes in $H^1(F,A)$ trivial on inertia away from p and on the full local groups at p. If $F \subseteq K \subset F_\infty$ is finite over F, then restriction identifies $S(F,A)$ with $S(K,A)^{\mathrm{Gal}(K/F)}$.*

Proof. Put $\Gamma = \mathrm{Gal}(F_\infty/F)$. Its image in $\mathbb{Z}_p^\times$ is open and is the product of a group of order dividing $p-1$ and a procyclic copy of $\mathbb{Z}_p$. If g generates the latter, $\kappa(g)^s - 1$ is nonzero and multiplication by it on A is surjective. The two-term resolution for the procyclic group over its completed group ring, with differential $g-1$, gives zero in degrees one and two. Averaging

over the finite factor therefore gives $H^1(\Gamma, A) = H^2(\Gamma, A) = 0$. The cyclotomic image at each $w \mid p$ is also open, so its first cohomology vanishes by the same proof.

Since G_{F_∞} acts trivially on A, inflation and restriction identify $H^1(F, A)$ with the Γ-invariants in $\mathrm{Hom}_{\mathrm{cont}}(G_{F_\infty}, A)$. At a place above p, local injectivity says exactly that the homomorphism must vanish on the corresponding local subgroup of G_{F_∞}. Away from p, inertia already lies in G_{F_∞} and must also be killed. These are the same subgroups when one starts at K: the infinite field is the same, the places above p are all taken, and K/F is unramified away from p. Passing from the invariants for $\mathrm{Gal}(F_\infty/K)$ to the invariants for Γ proves the lemma. □

Theorem 22.37 (The exact ideal-class subgroup at every precision)**.** *For $r, m \geq 1$ put $k = \max\{1, m - v_p(r+1)\}$ and $M_{p,r}(E) = \mathcal{S}_{p,r}(E)^{c=(-1)^r}$. Then $\kappa^{r+1} \bmod p^m$ defines a character ξ of $\mathrm{Gal}(B_k/\mathbb{Q})$. With a choice of compatible Tate-module bases one has*

$$M_{p,r}(E)[p^m] \simeq \{z \in D_p(B_k)[p^m] : \sigma z = \xi(\sigma) z \text{ for all } \sigma \in \mathrm{Gal}(B_k/E)\}.$$

To calculate $D_p(B_k)[p^m]$, take $F = B_k$ in the following map and compute its kernel:

$$\mathrm{Cl}(F)[p^m]^- \longrightarrow \left(\prod_{w \mid p} \frac{\mathcal{O}_{F_w}^\times}{\mu(F_w)_p \, (\mathcal{O}_{F_w}^\times)^{p^m}} \right)^- .$$

Represent the ideal class by $\mathfrak{a}$ prime to p, write $\mathfrak{a}^{p^m} = (a)$, and take the minus projection of the tuple of a at $w \mid p$. For fixed p, m one may use B_m for every pair E_x, r on the interval.

Proof. The extension E_*/E has two-power degree. Restriction identifies p-primary cohomology over E with the invariants over E_* by averaging. At a place above p restriction is injective by local corestriction. The same holds on inertia elsewhere, since its index divides this two-power degree. Thus this identification respects strictness, even when a place ramifies. Apply Lemma 22.36 to B_k/E_*. By transitivity of invariants we may now impose the full $\mathrm{Gal}(B_k/E)$-action on the strict classes over B_k.

For $u \in 1 + p^k\mathbb{Z}_p$, binomial expansion gives $v_p(u^{r+1} - 1) \geq k + v_p(r+1)$. This proves the assertion about ξ. On the subgroup G_{B_k}, the actions κ^{-r} and κ agree modulo p^m. Apply the proof of the lemma to both over B_k. At this precision the homomorphisms on G_{B_∞} take values in the same cyclic group, subject to the same local vanishing and equivariance conditions. On conjugating such a homomorphism by an element over $\mathbb{Q}$, the two actions on its argument agree. The ratio of the actions on its value, from twist $-r$ to twist $+1$, is $\kappa^{r+1} \bmod p^m$. Thus the former invariants give exactly the indicated ξ-eigenvectors. The original sign of c becomes $(-1)^r(-1)^{r+1} = -1$. The argument applies to every larger k as well, giving the common layer B_m.

For the ideal formula use Proposition 24.12. Here are the details that allow the local conditions to be tested on any generators. Weak approximation supplies a representative prime to p. Changing the representative multiplies a by a p^m-th power and a global unit. For a global unit u, every conjugate of the algebraic integer $u/c(u)$ has absolute value one. It is a root of unity by Kronecker's theorem. Since 2 is invertible on the target and a prime-to-p root is a p^m-th power, the minus part of the global unit disappears there. The displayed map is therefore well defined and additive. If its value is zero, $e^-[a]$, with $e^- = (1 - c)/2$ on the Kummer group modulo powers, has image in $\mu(F_w)_p F_w^{\times p^m}/F_w^{\times p^m}$ at every $w \mid p$. It has divisible valuations away from p. These are precisely the conditions of Proposition 24.12, and its ideal class is $e^-[\mathfrak{a}] = [\mathfrak{a}]$. The converse follows by taking a generator supplied by that proposition. This proves the formula at all finite places. □

The local power test is finite. In F_w, normalize the valuation by $v_w(\mathfrak{p}_w) = 1$ and put $e = v_w(p)$. For $b = 1 + \lfloor e/(p-1) \rfloor$, the logarithm and exponential identify $1 + \mathfrak{p}_w^b$ with $\mathfrak{p}_w^b$. Hence $1 + \mathfrak{p}_w^{b+me} = (1 + \mathfrak{p}_w^b)^{p^m}$. One can test the images of local roots and p^m-th powers in the units modulo $\mathfrak{p}_w^{b+me}$.

Proposition 22.38 (Equality of two local kernels controls all higher layers)**.** *Let $h \geq 1$ be such that the cyclotomic image of $G_{E_*(\mu_p)}$ is $1 + p^h\mathbb{Z}_p$, and fix $k \geq h$. If $|D_p(B_{k+1})| = |D_p(B_k)|$, then restriction identifies $D_p(B_k)$ with $D_p(B_i)$ for every $i \geq k$. For all E_x, r, the full group $M_{p,r}(E_x)$ is then isomorphic to the eigenspace in Theorem 22.37 in $D_p(B_k)[p^{k+v_p(r+1)}]$ at precision $k + v_p(r+1)$.*

Proof. Lemma 22.36 at twist $+1$ gives inclusions of the finite $D_p(B_i)$ identifying each earlier group with the corresponding fixed subgroup. Put $Z = \bigcup_i D_p(B_i)$ under these maps. Choose γ with cyclotomic value $1 + p^k$ generating $\mathrm{Gal}(B_\infty/B_k)$. Then $Z^\gamma = D_p(B_k)$ and $Z^{\gamma^p} = D_p(B_{k+1})$. By inclusion and equality of orders these fixed subgroups agree. Let $T = \gamma - 1$, $N = 1 + \gamma + \cdots + \gamma^{p-1}$. If $NTz = 0$, then $\gamma^p z = z$, hence $Tz = 0$. Consequently N acts injectively on TZ.

Each z lies in a finite stable p-group on which γ has p-power order, say dividing p^a. On its reduction modulo p, $T^{p^a} = 0$ and $N = T^{p-1}$. A power of N therefore maps the finite group into its multiple by p. Iteration gives zero. Injectivity on TZ now forces $Tz = 0$ for every z. This proves stabilization. Each element of a strict group has finite p-power order. Apply the theorem at its precision using a sufficiently high layer. Its image in Z is fixed by γ, while γ acts on it by $(1 + p^k)^{r+1}$. The difference from one has valuation $k + v_p(r+1)$, again by binomial expansion. This bounds the exponent and proves the stated full comparison. □

Proposition 22.39 (The quadratic summand of discriminant -1208)**.** *Let $F = \mathbb{Q}(\sqrt{-302})$. For every positive odd r, $M_{3,r}(F)$ is cyclic of order three or nine. It has order three when $r \equiv 5 \bmod 6$. Among the two progressions $r \equiv 1, 3 \bmod 6$, at most one can have order nine. Its order is constant on each progression. For the original quadratic character of discriminant -1208 these are the full orders of the $\mathrm{Gal}(E_x/F)$-invariant summands on every one of its period fields.*

Proof. The class number of F is 12. For verification, a reduced primitive positive binary quadratic form (a, b, c') of discriminant -1208 has $a \leq \sqrt{1208/3}$, $|b| \leq a \leq c'$, and $b \geq 0$ on either boundary. Checking $4a \mid b^2 + 1208$ gives the pairs

$$(1,0), (2,0), (3,\pm2), (6,\pm4), (9,\pm4), (13,\pm12), (17,\pm4).$$

The form–ideal correspondence gives the asserted number. Proposition 24.15 constructs a nonzero class in $D_3(F)[3]$ from the generator $73 + 9\sqrt{-302}$. Thus $D_3(F)$ has order three. Since $r+1$ is even, Theorem 24.13 gives $|M_{3,r}(F)[3]| = 3$, and it gives the whole group when $3 \mid r+1$.

For the other progressions we need an upper bound at higher precision. Let χ be the quadratic character of F and $f = 1208$. Since $3 \nmid 2f$ and the minus character of $\mathrm{Gal}(F/\mathbb{Q})$ is χ, Lemma 25.18 applies to the whole group under consideration. The required Bernoulli values are

k	3	5	9	11	15	17
$(B_{k,\chi}/k) \bmod 27$	9	18	9	18	9	18.

Here is an integer and rational calculation of the table. Set $S_j = \sum_{a=1}^{f} \chi(a) a^j$. Skip even a and multiples of 151. For the remaining a, give the sign $+1$ to a mod 8 equal to $1, 7$ and the

sign -1 to $3,5$. Multiply by $+1$ or -1 according as $a^{75} \bmod 151$ is 1 or -1. This is χ since $-1208 = 8(-151)$. Starting with $b_0 = 1$, the two finite formulas used are

$$b_i = -\frac{1}{i+1}\sum_{j=0}^{i-1}\binom{i+1}{j}b_j, \qquad \frac{B_{k,\chi}}{k} = \frac{1}{kf}\sum_{i=0}^{k}\binom{k}{i}b_i f^i S_{k-i}.$$

The latter is the defining sum of the Bernoulli polynomial at a/f. For example it gives 839844 and -364139453484 at the first two indices. All six entries have valuation two. Every odd r with $3 \nmid r+1$ has $-r \bmod 18$ in the six columns. For that k, $2 < 1+v_3(r+k)$, so the cited lemma gives $9M_{3,r}(F) = 0$. The order-three subgroup at precision one now implies cyclicity. The finite coefficient comparison of Lemma 24.11 at precision two shows that each order depends only on $r \bmod 6$.

To distinguish how many progressions can attain the upper bound, apply Theorem 22.37 with $E = E_* = F$ and with the common field $F(\mu_9)$ at precision two. The proof of that theorem applies to this constant field as well. Here $F \cap \mathbb{Q}(\mu_9) = \mathbb{Q}$, since the latter field has unique quadratic subfield $\mathbb{Q}(\sqrt{-3})$. Choose the element γ over F with cyclotomic residue 4 mod 9. The involution over F with residue -1 fixes the desired classes since $r+1$ is even. In the subgroup fixed by this involution, the elements also fixed by γ form $D_3(F)$ by Lemma 22.36. All the elements of order three belonging to the eigenspaces in the theorem are in this line, as $4^{r+1} \equiv 1 \bmod 3$.

If both remaining progressions had order nine, choose classes y_1, y_2 of order nine in the two eigenspaces, rescaled so that $3y_1 = 3y_2 = v \neq 0$. On the two progressions, $4^{r+1} \equiv 1+3(r+1) \bmod 9$, with $r+1$ equal to 1 and 2 modulo three in some order. Thus $(\gamma-1)(y_1+y_2) = (1+2)v = 0$, whereas $3(y_1+y_2) = 2v \neq 0$. This would give an element of order nine in $D_3(F)$, a contradiction. Finally E_x/F has two-power degree for this original character. Restriction, corestriction and averaging, including at the local subgroups as in the theorem, identify $M_{3,r}(F)$ with the invariant summand on E_x. □

In particular the weighted contribution of this summand at three over odd $r < t$ is bounded by $\lceil (t-1)/2 \rceil \log 9$ on the original intervals. For general fields the theorem gives the actual subgroup at each depth. A uniform upper bound for the sizes of the groups persisting to greater depths, and the upper comparison for the integral projected periods in Section 6.6, are still required.

22.21 The exact order of the quadratic summand at three

The upper bound in Proposition 22.39 leaves open the possibility of order nine. To decide it we use the ordinary class groups in a real quadratic tower. This also gives a bound for a collection of quadratic characters at all their weights on the original intervals.

Let α be a quadratic character with $\alpha(-1) = (-1)^r$, where $r \geq 1$. Write κ for the 3-adic cyclotomic character, ω for its quadratic Teichmüller part, and $\langle\kappa\rangle = \kappa/\omega$. The character $\beta = \alpha\omega^r$ is even. When $\beta \neq 1$ write R for its real quadratic field and let

$$Q_n = \mathbb{Q}(\zeta_{3^{n+1}})^+, \qquad R_n = RQ_n, \qquad R_\infty = \bigcup_{n\geq 0} R_n.$$

Let $S(\alpha, r)$ denote the cohomology classes over $\mathbb{Q}$ with coefficient $A = (\mathbb{Q}_3/\mathbb{Z}_3)(\alpha^{-1}\kappa^{-r})$ whose restrictions to inertia away from three and to the local group at three are zero.

Lemma 22.40 (A bound from the ordinary class numbers of the real layers)**.** *Write $h_{3,n} = |\operatorname{Cl}(R_n)\{3\}|$. Every finite subgroup of $S(\alpha, r)$ has order at most $h_{3,n}$ for some n. In particular, if $h_{3,n} \leq H$ at every layer, then $|S(\alpha, r)| \leq H$ for every r giving the same β.*

Proof. The coefficient character is $\theta = \beta^{-1}\langle\kappa\rangle^{-r}$. It is trivial on G_{R_∞}. The group $\mathrm{Gal}(R_\infty/\mathbb{Q})$ is the product of a group of order two and $\mathbb{Z}_3$, since R is quadratic and each Q_n has degree a power of three. A generator of the infinite factor acts on A by a scalar $u \neq 1$. Since $(u-1)A = A$, every continuous cocycle of that factor is a coboundary, as is seen by matching its value at the generator. Averaging over the finite factor therefore gives zero first cohomology of the quotient. Restriction now injects the global classes into $\mathrm{Hom}_{\mathrm{cont}}(G_{R_\infty}, A)$.

Choose cocycles representing generators of a finite subgroup of $S(\alpha, r)$. Each cocycle z has finite image by compactness. On one decomposition group at three it has the form $z(g) = (\theta(g) - 1)b$ for some $b \in A$. On a conjugate decomposition group the cobounding element can be taken to be $\theta(s)b - z(s)$, where s conjugates the first group to the second. All these elements and all the cocycle images are killed by a common power of three. Take n large enough that $\theta(G_{R_n})$ fixes that coefficient torsion. Each restriction to G_{R_n} is then a homomorphism and vanishes on every decomposition group above three. At a prime away from three it vanishes on inertia: its original restriction was a coboundary there, and on inertia over R_n both factors of θ are trivial.

By global class field theory the homomorphisms so obtained factor through the 3-part of the ideal class group of $\mathcal{O}_{R_n}[1/3]$. This group is the quotient of $\mathrm{Cl}(R_n)\{3\}$ by the 3-primary images of the primes over three. Infinite places affect only the prime two. After restriction to G_{R_∞}, all our generators belong to the image of the character group of this one finite quotient. Its character group into $\mathbb{Q}_3/\mathbb{Z}_3$ has the same order as the quotient. The initial restriction was injective, proving the finite-subgroup assertion. Each global class has finite order by the finite-image argument, so any finite list generates a finite subgroup. The uniform bound follows. □

Theorem 22.41 (Order three at every positive odd weight)**.** *Let $F = \mathbb{Q}(\sqrt{-302})$. For every positive odd integer r,*

$$M_{3,r}(F) \simeq \mathbb{Z}/3\mathbb{Z}.$$

For the period fields of the character of discriminant -1208, this is the whole $\mathrm{Gal}(E_x/F)$-invariant summand of $M_{3,r}(E_x)$. Its contribution at the odd weights $1 \leq r < t$ to the sum of logarithmic orders is exactly $\lfloor t/2 \rfloor \log 3$.

Proof. Take α to be the character of F. At every odd weight, $\beta = \alpha\omega$ cuts out

$$R = \mathbb{Q}(\sqrt{906}), \qquad \mathrm{disc}(R) = 3624.$$

Indeed ω cuts out $\mathbb{Q}(\sqrt{-3})$, and 906 is squarefree and is 2 mod 4. Restriction from $\mathbb{Q}$ to F identifies $S(\alpha, r)$ with $M_{3,r}(F)$. To see this, averaging over the quadratic extension identifies global cohomology with the invariants of its twisted action. Removing the twist over F gives the α-eigenspace, which is the minus part for odd r. Restriction at three and restriction on inertia away from three are injective on the corresponding downstairs local cohomology by corestriction, since their indices divide two. Thus the identification preserves both directions of the strict local conditions.

We specify the external class-number input. For a positive quadratic discriminant $f \equiv 0 \bmod 3$, Mercuri, Paoluzi and Schoof identify the order of the 3-class group in layer n with the order of

$$C(f)/((1+T)^{3^n} - 1)C(f), \qquad C(f) = \mathbb{Z}_3[[T]]/J.$$

This uses equality of the orders of the class group component and the unit quotient by cyclotomic units, followed by finite duality and their formula for C_n in Section 2. Their discriminant table records $[3624, 0, [T, 3]]$. Here 0 denotes the stabilization level and the last entry gives generators of J. This is the level-zero case in the first column of their Table 3.1. Thus $C(3624)$ has

order three and T acts by zero. The displayed quotient has order three for every n, including $n = 0$. [12, 13]

Lemma 22.40 gives $|M_{3,r}(F)| \leq 3$. For the lower bound, Proposition 24.15 constructs a nonzero class from $73 + 9\sqrt{-302}$ at precision one and transfers it to every positive odd weight. This proves equality. Restriction from F to E_x gives the invariant summand by Proposition 22.39. There are $\lfloor t/2 \rfloor$ positive odd integers less than t. □

Corollary 22.42 (Quadratic contributions with bounded real discriminant)**.** *For each x in the original interval and each $1 \leq r < t(x)$, consider the quadratic characters of $E_x/\mathbb{Q}$ with the prescribed parity for which $\beta \neq 1$ and $\operatorname{disc}(R) < 100000$. For all these pairs together one has*

$$\sum_{r,\alpha} \log |S(\alpha, r)| \ll t(x)$$

with an absolute implied constant. The same bound applies to the sum of logarithmic orders of their restriction images on E_x. When $3 \nmid [E_x : \mathbb{Q}]$, these images give the whole indicated character summands.

Proof. Mercuri, Paoluzi and Schoof, Theorem 1.1, prove boundedness of the 3-class numbers in the cyclotomic tower of every real quadratic field in this discriminant range. [12] Let H be the maximum of the finitely many resulting bounds. For each r, multiplication by ω^r is injective on quadratic characters, so each real quadratic field occurs at most once. The lemma bounds each order by H. There are fewer than 100000 choices of discriminant, giving an upper bound $100000\, t(x) \log H$. Restriction can only decrease the order. When the degree of E_x is prime to three, restriction followed by averaging identifies global and local conditions with invariants just as for F in the theorem. Removing the coefficient twist gives exactly the corresponding character summand. □

This bound controls the stated part of the sum on the original fields. The remaining character components and the integral upper comparison for the projected theta periods in Section 6.6 still require estimates there.

22.22 The exact change in strict cohomology at split primes

Fix one of the intervals of Section 6.6. Write E_* for its largest period field, N_* for a cyclotomic modulus for E_*, $n_* = [E_* : \mathbb{Q}]$, and t_* for the largest twist cutoff. Let $\mathcal{P}$ be any finite set of the large coefficient primes. We use $\ell \nmid 4N_*$, $\ell > n_* t_*$ and $\ell > 2t_* + 3$ for $\ell \in \mathcal{P}$. These conditions hold in the large-prime range of Theorem 32.1 throughout sufficiently distant intervals by the polynomial bounds for N_*, n_*, t_*. For each ℓ work over the integers $\mathcal{O}$ of a finite unramified extension $J/\mathbb{Q}_\ell$ containing all the values of characters of $\mathrm{Gal}(E_*/\mathbb{Q})$.

For $1 \leq r < t_*$ and $\alpha(c) = (-1)^r$, put

$$\theta = \alpha^{-1}\kappa_\ell^{-r}, \qquad \lambda = \theta^{-1}\kappa_\ell, \qquad M_m = (\mathcal{O}/\ell^m)(\theta), \qquad D_m = (\mathcal{O}/\ell^m)(\lambda).$$

Use arithmetic Frobenius. Denote by S_m the classes of $H^1(\mathbb{Q}, M_m)$ which vanish at ℓ and are unramified at all other finite primes. For a finite set Q of good primes away from ℓ, let S_m^Q allow all local classes at Q and keep the other conditions. Write S and S^Q for the same groups with coefficients $(J/\mathcal{O})(\theta)$. Theorem 8.1 proves exact preservation for one auxiliary prime on the nonzero summands. The issue for several primes is that global reciprocity pairs the sum of their local contributions with each dual class.

Lemma 22.43 (A primitive odd class)**.** *There is an integral class $w \in H^1(\mathbb{Q}, \mathcal{O}(\lambda))$ unramified at every finite prime different from ℓ whose reduction modulo ℓ has nonzero restriction to $H = G_{\mathbb{Q}^{\mathrm{ab}}}$.*

Proof. Take S_0 to consist of infinity and the primes dividing $4N_*\ell$, and write $G_{\mathbb{Q},S_0}$ for the Galois group of the maximal extension unramified outside S_0. The integral argument of Lemma 36.2 applies also when the original strict group vanishes. Indeed its global Euler characteristic formula for $V = J(\lambda)$ gives

$$\dim_J H^1(G_{\mathbb{Q},S_0}, V) - \dim_J H^2(G_{\mathbb{Q},S_0}, V) = 1.$$

Indeed the global invariants vanish and c acts by -1, so the minus space at the real place has dimension one. The integral degree-one group for the lattice $T = \mathcal{O}(\lambda)$ is finitely generated by the usual finiteness theorem for Galois cohomology with restricted ramification. It spans the rational group, as a continuous cocycle on a compact group has bounded image. It is torsion-free since $H^0(G_{\mathbb{Q},S_0}, V/T) = 0$, again by the action of c. A basis member w has nonzero reduction by the long exact sequence for multiplication by ℓ. [1]

At $p \neq \ell$, pass locally to the field cut out by α; its degree is prime to ℓ. There inertia acts trivially on T, so the inertia restriction is a homomorphism. Its only possible contribution is from the pro-ℓ tame quotient $\mathbb{Z}_\ell(1)$. If the residue field has order q, Frobenius acts on that quotient by q and on T by q^{r+1}. The nonzero scalar $q^r - 1$ therefore kills its image in a torsion-free module. Restriction on inertia cohomology across this finite extension is injective by inflation–restriction and averaging. Thus w is unramified over $\mathbb{Q}_p$.

On H the coefficients are trivial, so restriction of a cocycle is a homomorphism independent of the representative. If the reduction of w vanished there it would descend to the abelian quotient. For a cocycle v on that quotient, the equality $cg = gc$ gives $(\lambda(c) - 1)v(g) = (\lambda(g) - 1)v(c)$ modulo ℓ. The first multiplier is -2, a unit. This makes v a coboundary, contradicting the choice of w. □

Theorem 22.44 (Split primes and the change of local conditions)**.** *Assign any integers $s_\ell \geq 1$ to the primes of $\mathcal{P}$. There is an infinite set of rational primes split completely in $\mathbb{Q}(\mu_{4N_*})$ with $v_\ell(q-1) = s_\ell$ for every $\ell \in \mathcal{P}$. For any $k \geq 1$ distinct members forming Q, any of the indicated (ℓ, r, α), and every $m \geq 1$,*

$$S_m^Q / S_m \;\simeq\; \left(\mathcal{O}/\ell^{\min(m,s_\ell)}\right)^{k-1}. \tag{$*$}$$

Under local Tate duality its image is the kernel of addition in k copies of the dual of $\mathcal{O}/\ell^{\min(m,s_\ell)}$.

Proof. Choose $\sigma \in G_{\mathbb{Q}}$ acting trivially on $\mathbb{Q}(\mu_{4N_*})$ and by $1 + \ell^{s_\ell}$ on $\mu_{\ell^{s_\ell+1}}$ for each ℓ. Such an element exists by the Chinese remainder theorem and the cyclotomic Galois isomorphism. For each character and twist choose a cocycle representing the class in Lemma 22.43. We can choose $h \in H$ so that every one of these cocycles takes a nonzero value modulo ℓ on $\gamma = \sigma h$. In fact the joint image of H under their residual homomorphisms is a finite abelian group. Its parts at different primes form a direct product. On the part at ℓ, cancellation of one value $\bar{w}(\sigma) + \bar{\lambda}(\sigma)\bar{w}(h)$ excludes at most a fraction $1/\ell$, because the homomorphism has nonzero image. There are at most $n_*(t_* - 1) < \ell$ pairs at that prime, counting each character of E_* just once per twist. Their excluded sets cannot cover the image. Independent choices in its primary parts give the required h.

Form a finite Galois extension of $\mathbb{Q}$ as follows. Include the cyclotomic fields just used and record every D_j-valued cocycle on $G_{\mathbb{Q},S_0}$ for $1 \leq j \leq s_\ell$, for every indicated pair at every ℓ. There are finitely many because $H^1(G_{\mathbb{Q},S_0}, D_j)$ and the group of coboundaries are finite. A cocycle v is recorded by the homomorphism $g \mapsto (v(g), \lambda(g) \bmod \ell^j)$ into a finite affine group.

Take the compositum of the corresponding fixed fields of the kernels. Chebotarev's theorem supplies infinitely many primes with the conjugacy class of γ in this extension, after omitting all the primes in the sets S_0. Choose at each of them a place giving the actual image of γ as Frobenius. These primes have the required splitting and exact depths.

At each $q \in Q$, evaluation at the chosen Frobenius identifies the unramified local group for D_m with

$$U = \mathcal{O}/(\ell^m, q^{r+1} - 1) = \mathcal{O}/\ell^{\min(m, s_\ell)}.$$

Here $\alpha(q) = 1$, and the binomial expansion of q^{r+1} gives $v_\ell(q^{r+1} - 1) = s_\ell$ since $\ell \nmid r + 1$. The image of the old dual Selmer group in U^k is exactly the diagonal. To see the inclusion, this dual group has the local conditions orthogonal to those of S_m. At every prime outside S_0 its classes are unramified, since the two unramified conditions on unramified dual modules are exact annihilators. Its classes thus come from $G_{\mathbb{Q},S_0}$. For $m \le s_\ell$ all their Frobenius values agree by construction. For $m > s_\ell$ reduce the cocycles to level s_ℓ, which induces an isomorphism on these local unramified quotients. This proves the inclusion at every level.

The chosen integral w reduces to a member of the old dual Selmer group at every level. At ℓ the primal condition is zero. At all other finite places both w and the primal classes are unramified, and their cup product vanishes by inflation from the procyclic unramified quotient of cohomological ℓ-dimension one. The real place contributes zero for odd ℓ. The common value of w in U is a unit by our choice of h. Its $\mathcal{O}$-multiples supply the entire diagonal.

For clarity, the change-of-conditions sequence from finite Poitou–Tate duality identifies the image of

$$S_m^Q \longrightarrow \bigoplus_{q \in Q} H^1(\mathbb{Q}_q, M_m)/H^1_{\mathrm{unr}}(\mathbb{Q}_q, M_m)$$

with the exact annihilator of these restrictions of the old dual Selmer group. Indeed the obstruction to lifting a tuple of new local classes, with the old conditions at the other places, is its sum of local pairings against that group. This is the middle localization sequence of global duality after quotienting by the old local subgroups. Its kernel on global classes is S_m. Locally the displayed summands are the duals of U. The trace pairing on the unramified coefficient ring is perfect, so we can equally use $\mathcal{O}$-linear duals with values in $\ell^{-m}\mathcal{O}/\mathcal{O}$. The annihilator of the diagonal consists of tuples whose sum is zero. Its first $k - 1$ entries are arbitrary and determine the last. This proves $(*)$. [1] □

Corollary 22.45 (Elementary divisors on the original fields)**.** *For the same Q there is a noncanonical decomposition restricting to the given inclusion of S,*

$$S^Q \simeq S \oplus (\mathcal{O}/\ell^{s_\ell})^{k-1}.$$

It holds on each α-component of the original groups over every E_x through which α factors. Each prime of Q alone leaves the full strict group on this component unchanged. For k primes, removing the subgroup killed by ℓ^a from each of the two groups increases the resulting length by exactly $(k-1)\max(s_\ell - a, 0)$, for every integer $a \ge 0$.

Proof. Let $A = (J/\mathcal{O})(\theta)$ and identify M_m with $A[\ell^m]$ by division by ℓ^m. Inertia at ℓ acts through a nontrivial residual cyclotomic power, so $A^{G_\ell} = A^{G_{\mathbb{Q}}} = 0$. For $p \neq \ell$, A^{I_p} is divisible. Indeed the inertia character has order prime to ℓ, giving either A or zero as invariants. The long exact sequences for multiplication by ℓ^m, globally, on G_ℓ, and on I_p, now give $S_m = S[\ell^m]$ and $S_m^Q = S^Q[\ell^m]$. The resulting subquotients S_m^Q/S_m inject into S^Q/S. Their union is the whole quotient, since a continuous cocycle with discrete coefficients on a compact group has finite image. By $(*)$ their orders are constant for $m \ge s_\ell$. A basis of the quotient of the asserted type thus lifts already to $S^Q[\ell^{s_\ell}]$. Sending its generators to these lifts gives an $\mathcal{O}$-linear splitting.

Since $[E_x : \mathbb{Q}]$ is prime to ℓ, restriction and averaging identify cohomology on $\mathbb{Q}$ for the twist by α^{-1} with the α-part of cohomology on E_x for the untwisted module $(J/\mathcal{O})(-r)$. This identification also identifies the local conditions. On decomposition groups above ℓ and on inertia away from ℓ, restriction has zero kernel because the finite indices are prime to ℓ. The relaxed condition allows all classes on both sides at every place over Q. Finally on each new cyclic summand the quotient by its ℓ^a-torsion has length $\max(s_\ell - a, 0)$. Additivity in the direct sum proves the last assertion. □

In particular the increase in the sum of retained lengths in (6.6), when the same retained triples are compared, is obtained by multiplying these increments by $\log \ell$ and summing them. For $k = 2$ and $r = 1$, the same two primes may also be used in Theorem 32.23. The construction prescribes their Frobenius evaluations and leaves their sizes unrestricted. The original summand S still enters the absolute length in Section 6.6.

22.23 Division of strict classes by allowing tame ramification

Keep $E_*, N_*, t_*, \mathcal{P}, \theta, \lambda, M_m, D_m$ of Section 22.22. Write $O = \mathbb{Z}_\ell[\alpha]$ for the minimal unramified coefficient ring, with fraction field J and residue field k_α. We make the local choices over this ring. Extension to the common unramified coefficient ring commutes with all the cohomology groups and localization kernels below, since it is finite free. Use S, S_m, S^Q, S^Q_m with the same meaning as in that section. The set $\mathcal{P}$ can contain the full support of the nonzero large-prime summands on the given interval by Corollary 21.8.

Lemma 22.46 (Finite layers of the odd dual group)**.** *Let C be the group of classes with coefficients $(J/O)(\lambda)$ unramified away from ℓ, with the full local condition at ℓ. The Selmer group dual to the local conditions defining S_m, with coefficients D_m, equals $C_m = C[\ell^m]$ under division by ℓ^m. Its length is*

$$\operatorname{length}_O C_m = m + \operatorname{length}_O S[\ell^m].$$

The divisible subgroup of C is one copy of J/O. The finite quotient by that subgroup has the elementary divisors of S. The compatible reductions w_m of a primitive class w as in Lemma 22.43 generate the ℓ^m-torsion of the divisible subgroup.

Proof. At a finite place $p \neq \ell$ where the characters are unramified, local Tate duality makes the unramified subgroups exact annihilators. Where they are ramified, both inertia characters have prime-to-ℓ order and are nontrivial after reduction. Both groups of local invariants vanish, so the entire local degree-one groups vanish by local duality and the local Euler characteristic. At ℓ the annihilator of the zero condition is the full group. Global invariants of $(J/O)(\lambda)$ vanish by oddness, and its inertia invariants away from ℓ are either zero or divisible. The exact sequence for multiplication by ℓ^m now identifies the finite dual Selmer group with $C[\ell^m]$.

Apply the finite Selmer order formula to M_m, D_m, as in the proof of Theorem 28.1. The two global invariant groups are zero. For $p \neq \ell$ finite the order of the unramified condition equals the order of the local invariants. At ℓ both the condition on M_m and its invariants are zero, the latter by cyclotomic inertia. The real local condition is zero and the real invariants are all of M_m, since $\theta(c) = 1$. Thus $|S_m|/|C_m| = 1/|O/\ell^m|$. Corollary 22.45 identifies S_m with $S[\ell^m]$. [1]

The Pontryagin dual of C is a finitely generated O-module: its quotient by ℓ is dual to the finite group $C[\ell]$, and lifts of a basis generate by compact Nakayama. Equivalently, the closed span of the lifts has a compact pro-ℓ quotient equal to its multiple by ℓ, and such a quotient has no nonzero finite quotient. The group S is finite by Proposition 11.4 and prime-to-degree

descent. Apply the structure theorem over O and take successive differences of the displayed lengths. For large m the difference is one, giving the divisible rank of C. At each m the difference in excess of one counts the elementary divisors of S of exponent at least m. Finally w_m defines a class of order ℓ^m, since $\ell^{m-1}w_m = w_1 \neq 0$ in C. Its compatible lifts at all larger exponents put it in the divisible subgroup. There it generates the indicated layer. □

Proposition 22.47 (Prescribing the residual dual evaluations)**.** *For each (ℓ, r) take one α from each orbit under residue-field Frobenius. Choose any positive depths s_ℓ. On every C_1 one may prescribe an arbitrary k_α-linear functional. Infinitely many good rational primes split in $\mathbb{Q}(\mu_{4N_*})$, have $v_\ell(q-1) = s_\ell$ simultaneously, and realize all these functionals as evaluation of unramified classes at Frobenius at a choice of place. For a conjugate character the evaluations are given by conjugation.*

Proof. Let $H = G_{\mathbb{Q}^{\mathrm{ab}}}$. On H each residual cocycle is a homomorphism independent of its representative. Restriction of C_1 is injective by the argument with the central element c in Lemma 22.43. Evaluation therefore maps H to $C_1^* = \mathrm{Hom}_{k_\alpha}(C_1, k_\alpha)$ with image whose annihilator in C_1 is zero. We verify that the joint image on all the factors is the full product.

At a fixed ℓ this additive image is stable under conjugation by $G_{\mathbb{Q}}$. Conjugating an element of H multiplies its functional on each factor by the scalar $\bar{\lambda}(g)$. The finite abelian group acting in this way is a quotient of $\Delta = \mathrm{Gal}(E_*/\mathbb{Q}) \times \mathbb{F}_\ell^\times$, with every element of Δ available. Indeed the cyclotomic conductors N_* and ℓ are coprime. The characters of Δ on the respective factors are $(a, u) \mapsto \bar{\alpha}(a)u^{r+1}$. Their orbits are distinct: restricting to the second factor determines $r+1 < \ell-1$, and the prime-to-ℓ values of α lift uniquely from their residues. The group algebra $\mathbb{F}_\ell[\Delta]$ is a product of fields with one factor for each such orbit of characters of Δ. This follows by diagonalizing the finite abelian group over $\overline{\mathbb{F}}_\ell$ and adding the character idempotents in each Frobenius orbit, using $\ell \nmid |\Delta|$. The orbit idempotents consequently separate all the projections of the image. In each projection the acting field is k_α, which is generated by the character values. An image with zero annihilator that is a k_α-subspace of C_1^* is all of C_1^*. Distinct ℓ's are separated by the primary decomposition of the finite additive image.

Take σ with the cyclotomic actions specified in the proof of Theorem 22.44. It acts trivially on each residual coefficient, so evaluation there is a well-defined linear functional on classes. Multiplying σ by an element of H adds an arbitrary joint functional by the preceding paragraph. Record the residual cocycles and the prescribed cyclotomic actions in the finite extension used for Chebotarev, now using only level one for the cocycles. Choosing a place with the specified Frobenius proves the assertion. □

Theorem 22.48 (Division by a prescribed power on the same interval)**.** *Put $d_{\ell,r,\alpha} = \dim_{k_\alpha} S[\ell]$ and choose an integer $h \geq 1 + \max_{\ell,r,\alpha} d_{\ell,r,\alpha}$ for a nonempty list of coefficient primes. For any depths $s_\ell \geq 1$ there are h common split rational primes Q of these exact depths with the following properties on every indicated original component. Writing $s = s_\ell$ and $P = S^Q$, one has*

$$S = \ell^s P, \qquad P/S \simeq (O/\ell^s)^{h-1}.$$

If $b_1, \ldots, b_{h-1}$ are the exponents of S, padded by zeros, the elementary divisors of P have exponents $s + b_1, \ldots, s + b_{h-1}$. In particular every strict class of order ℓ^a, $a \geq 1$, is ℓ^s times a class of order ℓ^{a+s} ramified at most at these additional primes in the sense of the original local conditions. Only residual cohomology is used to select the Frobenius evaluations at the h primes.

Proof. For each representative in Proposition 22.47, choose a basis of C_1 beginning with w_1. The dimension is $1 + d$, where $d = d_{\ell,r,\alpha}$, by Lemma 22.46. Choose h rows with first entry one

that span the dual. For example take the first coordinate functional, its sum with each other coordinate functional in turn, and repeat the first row if needed. Use Proposition 22.47 for each simultaneous row, excluding the previously chosen primes. The residual localization $C_1 \to k_\alpha^h$ is then injective and the value of w at each chosen Frobenius is a unit. Finite Poitou–Tate duality as in Theorem 22.44 gives

$$\dim_{k_\alpha} P[\ell] = d + (h - \dim_{k_\alpha} C_1) = h - 1.$$

This uses $S_1^Q = P[\ell]$, as proved for finite and divisible coefficients in Corollary 22.45 independently of the particular good primes.

Next consider a level $m \geq s$. At each chosen prime the unramified dual group is O/ℓ^s, and reduction from level m to level s is an isomorphism on this local group. On the global groups $C_m \to C_s$, the same reduction corresponds to multiplication by ℓ^{m-s} on $C[\ell^m]$. For all sufficiently large m it kills the finite quotient of C and its image is exactly the ℓ^s-torsion of the divisible line. Here the statement about the image follows also by splitting the divisible line off as an injective O-module. Lemma 22.46 identifies that layer with $(O/\ell^s)w_s$. The joint unramified local image is therefore a single vector with h unit entries and all of its multiples. Its annihilator in the h local ramification quotients is isomorphic to $(O/\ell^s)^{h-1}$, by solving for the last coordinate. Finite global duality identifies S_m^Q/S_m with this annihilator. These subquotients inject into P/S and exhaust it, so their eventual common order and isomorphism type give $P/S \simeq (O/\ell^s)^{h-1}$. In particular P is finite.

The equality $\dim_{k_\alpha} P[\ell] = h - 1$ says that P requires $h - 1$ generators over the discrete valuation ring O. Thus $P/\ell^s P$ has length at most $s(h-1)$. It surjects onto P/S, which has exactly that length, since the latter is killed by ℓ^s. This proves $S = \ell^s P$, and all $h - 1$ cyclic summands of P have length at least s. Multiplying them by ℓ^s gives exactly the stated relation of elementary divisors. Any lift of a nonzero class of order ℓ^a under this multiplication has order ℓ^{a+s}. Prime-to-degree restriction and character projection carry the whole calculation to each E_x, by the descent in Corollary 22.45. □

Corollary 22.49 (The layers contributing to the length sum)**.** *Choose Q as in Theorem 22.48, and a disjoint set Q' of the same cardinality and depths as in Theorem 22.44. For every $m \geq 1$,*

$$\operatorname{length}_O S_m^{Q'} - \operatorname{length}_O S_m^Q = \operatorname{length}_O S[\ell^m] - \operatorname{length}_O S[\ell^{\max(m-s_\ell,0)}].$$

In particular for $s_\ell = 1$ the difference counts exactly the cyclic summands of the original group of length at least m.

Proof. Put $s = s_\ell$. Corollary 22.45 gives $\operatorname{length}_O S_m^{Q'} = (h-1)\min(m,s) + \operatorname{length}_O S[\ell^m]$. For the other set, sum $\min(m, b_i + s) = \min(m,s) + \min((m-s)_+, b_i)$ over the elementary divisors in Theorem 22.48. Subtraction proves the formula. Both sets can avoid any further finite set of primes. □

For $s_\ell = 1$, summing these differences for $m > a$ gives the exact length after removal of the part killed by ℓ^a in (6.6). All but finitely many terms vanish for each triple. The local construction gives no bound on the last nonzero m, which is still needed for the absolute estimate.

22.24 Measurement of the total residual length by ordinary class groups

We now include the primes dividing the field degree or the conductor, and $p = 3$, in the measurement of Proposition 6.11. The important degree in the finite averaging argument is

the relative degree from the chosen field to the largest field in its interval. These relative degrees are powers of two even when p divides $[E_* : \mathbb{Q}]$.

Fix $x \in [V, V^{3/2}]$, $E = E_x$, and let $R = t_*$ and $n_* = [E_* : \mathbb{Q}]$. Fix an odd $p \le 2R + 1$. As in Theorem 22.7, set

$$L_\infty = E_*(\mu_{p^\infty}), \qquad F_0 = (E_*(\mu_p))^+, \qquad F_\infty = L_\infty^+.$$

Write F_j for the relative degree p^j layer and $C_j = \mathrm{Cl}(\mathcal{O}_{F_j}[1/p])\{p\}$. Let $\Gamma = \mathrm{Gal}(L_\infty/E_*(\mu_p))$, choose its topological generator γ, and write $a = \kappa_p(\gamma)$, $u = v_p(a-1) - 1$, $l = \lfloor \log_p n_* \rfloor$. We have $p^u \le n_*$. Write $\mathcal{T}$ for the subgroup of elements of finite order prime to p in $\mathrm{Gal}(L_\infty/\mathbb{Q})$. It is finite since it injects into the finite quotient by $\Gamma \simeq \mathbb{Z}_p$.

For $D = E$, or for either field used for the average $J_{p,r}$, put

$$T_D = \mathcal{T} \cap \mathrm{Gal}(L_\infty/D), \qquad d_{D,r} = \frac{1}{|T_D|} \sum_{\delta \in T_D} \kappa_p(\delta)^r \delta.$$

These are idempotents in $\mathbb{Z}_p[\mathcal{T}]$. Set $e_r = d_{E,r}$ if the original average is zero, and $e_r = d_{E,r} - d_{D,r}$ if it is the average for E/D. Here $D = L_x$ or $B(x)$ according to Section 6.6.

Lemma 22.50 (The original averages in the cyclotomic class coordinates)**.** *Put $j = m + l$ for any integer $m \ge 1$. The finite dual, through precision m, of the complementary strict group over E after applying $1 - J_{p,r}$ has the same elementary divisors as*

$$e_r C_j / (p^m, \gamma - a^{-r}) e_r C_j.$$

Each e_r is an integral idempotent. The assertion includes the primes at which the full Galois group of $E/\mathbb{Q}$ has nontrivial p-Sylow subgroup.

Proof. For every D above, E_*/D has degree a power of two. Thus $E_*(\mu_p)/D$ has degree prime to the odd prime p. The abelian group $G_D = \mathrm{Gal}(L_\infty/D)$ is the direct product of Γ and T_D. To see this, let h be the order of its quotient by Γ. For $g \in G_D$ there is a unique $z \in \Gamma$ with $z^h = g^h$, since the h-th power acts bijectively on $\mathbb{Z}_p$. Then gz^{-1} has order dividing h. This also gives $T_D/T_E = \mathrm{Gal}(E/D)$ when $D \subset E$.

Theorem 22.19 identifies the full complementary dual at precision m with the quotient of $C_j/p^m C_j$ by the relations $\delta = \kappa_p(\delta)^{-r}$ for $\delta \in G_E$. On its finite prime-to-p factor these relations project onto $d_{E,r}$. On its procyclic factor the single relation $\gamma = a^{-r}$ suffices, by continuity. This construction is compatible with the field action: on equivariant homomorphisms to the twisted coefficient the action of a lift s sends $f(z)$ to the function $z \mapsto \kappa_p(s)^{-r} f(s^{-1}z)$. On the dual untwisted class coordinates it therefore acts by $\kappa_p(s)^r s$. This calculation commutes with restriction and norm in the finite-layer identification. Lifts differing by G_E induce the same action.

On the $d_{E,r}$-summand the average of these operators over T_D/T_E is exactly $d_{D,r}$, as is seen by summing first over T_E. Also $d_{D,r} d_{E,r} = d_{D,r}$. Averaging and taking its complement commute with the precision and cyclotomic quotients, since they are direct summand projections. Dualizing a finite-group average gives the average of the inverse actions, which is the same projector. This proves the stated identification. □

Decompose the finite abelian prime-to-p algebra $\mathbb{Z}_p[\mathcal{T}]$ by its Frobenius orbit idempotents e_ν. On each factor e_r is zero or one. Put

$$\mathcal{W}_\nu = \{1 \le r < t(x) : e_\nu e_r = e_\nu\}, \qquad P_x(Y) = \sum_\nu e_\nu \prod_{r \in \mathcal{W}_\nu} (Y - a^{-r}).$$

Each empty product is one. For this x, p define

$$Z_m = C_{m+l}/(p^m, P_x(\gamma))C_{m+l}, \qquad h_p = \max_{\nu,\ r\in\mathcal{W}_\nu} \sum_{r'\in\mathcal{W}_\nu\setminus\{r\}} (1 + u + v_p(r - r')),$$

with zero for the empty maximum.

Theorem 22.51 (A finite measurement for the entire residual local sum)**.** *For $X > 0$ put $b = b_0(x)$, $m_p = b + \lfloor X/\log p\rfloor + 1$ and form the two natural logarithmic sums*

$$A_- = \sum_{2<p\le 2R+1} \log|p^{b+h_p} Z_{m_p}|, \qquad A_+ = \sum_{2<p\le 2R+1} \log|p^{b-h_p} Z_{m_p}|$$

over primes. For all sufficiently large V, $b \ge h_p$ for every prime in these sums. There is a fixed $C = C_{\psi,\varepsilon}$ such that independently of x, X

$$0 \le A_+ - A_- \ll_{\psi,\varepsilon} V^C,$$
$$A_+ + \log J(V) \le X \implies \mathcal{R}(x) \le X, \qquad \mathcal{R}(x) \le X \implies A_- \le X.$$

In particular these quantities account for the full range of odd coefficient primes in the residual sum of Section 6.6.

Proof. Let Y_m be the direct sum over weights of the finite groups in Lemma 22.50. On each orbit ν apply the interpolation maps of Theorem 57.59 to the distinct values a^{-r} for $r \in \mathcal{W}_\nu$. Their difference valuations are $1 + u + v_p(r - r')$ by the binomial theorem at an odd prime. Thus the two composites are p^{h_p}, and

$$|p^{b+h_p} Z_m| \le |p^b Y_m| \le |p^{b-h_p} Z_m|.$$

Here $h_p \le R(1+l+\log_p R)$, which is polynomial in V and less than b uniformly. The difference between the two outer logarithms to base p is at most $2h_p \dim_{\mathbb{F}_p} Z_m/pZ_m$. As P_x reduces to a power of $Y-1$ of degree at most R on each factor, the filtration by $\gamma-1$ bounds this dimension by $R\dim_{\mathbb{F}_p} C_{m+l}/(p, \gamma-1)C_{m+l}$.

We bound the last dimension without assuming total ramification at the bottom. In the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$, inertia at p surjects onto the whole Galois group. Passing to inertia of a completion of F_0 reduces its image by an index dividing the ramification index of that completion: the local inertia subgroup has precisely that index in the original inertia group. The p-part of this index is at most n_* since $[F_0 : \mathbb{Q}]$ divides $n_*(p-1)$. Under the cyclotomic identification, the subgroup Γ^{p^l} is therefore in this inertia image. Indeed relative to the generator $1 + p$ of the whole cyclotomic direction it has index p^{u+l}. It follows that every prime over p in F_l is totally ramified in F_{m+l}/F_l.

The dimension of $C_{m+l}/(p, \gamma-1)C_{m+l}$ is at most that of the quotient by $p, \gamma^{p^l} - 1$. Over F_l the split class field argument in Theorem 57.59 applies to this latter quotient with γ^{p^l} as generator. It gives the bound $v_p(h_{F_l}) + g_l - 1$, where g_l is the number of primes of F_l above p. Both quantities are polynomially bounded in V, uniformly for $p \le 2R + 1$. Indeed $[F_l : \mathbb{Q}] \le n_*(p-1)p^l$, and by Theorem 22.7 its conductor divides $N_* p^{u+1+l}$. Here $p^l, p^u \le n_*$. Apply the conductor-discriminant and Minkowski bounds of Corollary 57.52. Summing the width with factors $\log p$ over at most $2R + 1$ primes proves the uniform polynomial estimate.

All primes in the finite test are below $P(x)$ for large V. Hence $p^b Y_{m_p}$ measures exactly the residual tail there with each elementary divisor capped at m_p. A divisor longer than this cap would already contribute more than X to the capped total, by the choice of m_p. If $A_+ + \log J(V) \le X$, the capped total is therefore the true total through $2R + 1$. For larger

primes the separated-weight bound of Lemma 9.31 applies at all the weights and costs at most $\log J(V)$, including primes above $P(x)$. Its fixed excluded primes are all below $2R+1$ eventually. This proves the first implication; the capped total is always at most the true one, which proves the second. □

For example one can take $X = \frac{1}{4}\exp(x^{\varepsilon}/2)$, the sufficient budget in Proposition 6.11. The polynomial width is smaller than any fixed positive fraction of this budget eventually, uniformly on the interval. An arithmetic upper bound for A_+ at this scale is still required. The width estimate bounds the difference of the two measured sums and is compatible with both sums exceeding the budget. The signed period comparison must also hold for the same original data.

22.25 Which prime ideals can detect the residual strict classes?

Fix an interval of Theorem 19.15 and a point x in it. Write $E = E_x$, $n = [E : \mathbb{Q}]$, $t = t(x)$, $R = t_*$ and $n_* = [E_* : \mathbb{Q}]$. Use the fields, the action of γ, and the idempotents of Lemma 22.50. For each odd $p \le 2R+1$ choose an arbitrary precision $m_p \ge 1$, set $j = m_p + \lfloor \log_p n_* \rfloor$, and write

$$Q_{p,r} = e_r C_j/(p^{m_p}, \gamma - a^{-r})e_r C_j \qquad (1 \le r < t).$$

There is a surjection from the ordinary ideal class group of F_j to $Q_{p,r}$. It kills the primes above p, takes the p-primary projection, and then applies the displayed projection and quotient. For a rational prime s, let $H_{p,r}(s)$ be the subgroup generated by the images of the prime ideals above s. For a finite set S of rational primes put $H_{p,r}(S) = \sum_{s\in S} H_{p,r}(s)$. The ramification index, residue degree and number of places of E over s are denoted by e_s, f_s, g_s. These satisfy $e_s f_s g_s = n$, since $E/\mathbb{Q}$ is Galois.

Lemma 22.52 (An integer annihilating the projected prime classes)**.** *For $s \ne p$, the group $H_{p,r}(s)$ has at most g_s generators and is annihilated by $s^{f_s r} - 1$. For $s = p$ the group is zero. These assertions include primes s ramified in E and primes p dividing $[E_* : \mathbb{Q}]$.*

Proof. Let $G_E = \mathrm{Gal}(L_\infty/E)$. Its action on $Q_{p,r}$ is scalar multiplication by κ_p^{-r}. Indeed Lemma 22.50 imposes this relation on the finite subgroup T_E and on a generator of the procyclic factor. It persists under the field average because the entire Galois group is abelian.

Fix a prime of F_j above $s \ne p$ and prolong it to an algebraic closure containing L_∞. Write v for the place it induces on E. An arithmetic Frobenius lift at v preserves the chosen prime of F_j. On all p-power roots of unity its action is raising to s^{f_s}. In fact reduction is injective on roots of unity of order prime to s, and arithmetic Frobenius on the residue field raises to the cardinality of the residue field of v. This also proves independence of the lift in the presence of inertia. Thus on the image of this ideal class the same element acts both as the identity and as $s^{-f_s r}$. Multiplication by the p-adic unit $s^{f_s r}$ gives the asserted annihilator. The cyclotomic Frobenius formula also appears in `ReciprocityTheory/GaloisValuations/Global.lean`, line 364.

The image of G_E on F_j is $\mathrm{Gal}(F_j/(E \cap F_j))$, by Galois correspondence. Its orbits on the primes above s thus correspond to the primes of $E \cap F_j$ above s. Each extends to a prime of E, so there are at most g_s orbits. The class map is equivariant, and scalar multiplication on a finite abelian p-group preserves the cyclic subgroup generated by each element. One prime per orbit therefore suffices. The case $s = p$ follows from the definition of C_j. □

Theorem 22.53 (The total contribution of a set of rational primes)**.** *Let S be finite. The full natural logarithmic order of its images, summed over all measured coefficient primes and weights, satisfies*

$$\sum_{2<p\le 2R+1} \sum_{1\le r<t} \log |H_{p,r}(S)| \;\le\; \frac{n\,t(t-1)}{2} \sum_{s\in S} \frac{\log s}{e_s}.$$

For any integer $b \geq 0$, the same bound holds for the decrease of $\sum_{p,r} \log |p^b Q_{p,r}|$ when the primes over S are inverted in the ordinary class groups. The bounds are uniform in the precisions m_p.

Proof. For $s \neq p$, the preceding lemma bounds $\log |H_{p,r}(s)|$ by $g_s v_p(s^{f_s r} - 1) \log p$. For fixed s, r this is the valuation of a single positive integer, with a multiplier independent of p. Summing over p gives at most

$$g_s \log(s^{f_s r} - 1) \;\leq\; (n/e_s)\, r \log s.$$

The formula includes the integer one, whose logarithm is zero. The product of the groups for the individual s surjects onto their sum. Addition over S and then over r proves the first assertion.

Inverting all the primes over S quotients the ideal class group by their classes. This subgroup is stable under every field automorphism. Primary projection, the idempotent and the scalar quotient therefore give $Q_{p,r}/H_{p,r}(S)$. For $Q = Q_{p,r}$ and $H = H_{p,r}(S)$ the kernel of $p^b Q \longrightarrow p^b(Q/H)$ is $H \cap p^b Q$. Its logarithmic order is bounded by $\log |H|$, proving the second assertion. □

For instance, on our interval one may invert all rational primes dividing pN_* in the class group for p. The primes above p have already been removed, so the additional set can be chosen as $S = \{s : s \mid N_*\}$, independent of p and x. Its cost in the actual capped residual sum is at most $n_* R^2 \log N_*/2$. This is polynomial in V and includes the two moving quadratic primes. The same conclusion holds for any set with $\sum_{s \in S} \log s \leq V^A$ for a fixed A.

Corollary 22.54 (Cyclotomic splitting forced by a surviving prime class)**.** *Put $b = b_0(x)$ and $k_p = \max\{0, b - \lfloor \log_p(n_* R) \rfloor\}$. Map the class group to the tail $p^b Q_{p,r}$ by multiplying the original class map by p^b. For $s \neq p$ a nonzero image of a prime above s requires s to split completely in the degree-p^{k_p} subfield of $\mathbb{Q}(\mu_{p^{k_p+1}})$. Its size must also satisfy*

$$f_s r \log s > (b+1) \log p.$$

In particular every prime with $\log s \leq b_0(V) \log 3/(n_* R)$ has zero image in all these tail maps, simultaneously throughout the interval.

Proof. If z is the projected class, $p^b z \neq 0$ forces its order to be at least p^{b+1}. Hence $p^{b+1} \mid s^{f_s r} - 1$. This proves the strict size inequality. Let d be the order of s mod p. It divides $f_s r$ and $p - 1$. For an odd p, binomial expansion at 1 gives

$$v_p(s^{f_s r} - 1) = v_p(s^{p-1} - 1) + v_p(f_s r).$$

Indeed raising s^d to an exponent prime to p preserves the valuation of its difference from one, and each subsequent p-th power increases it by one. Since $f_s r \leq n_* R$, the valuation on the right coming from $s^{p-1} - 1$ is at least $1 + k_p$ when $k_p > 0$. Modulo p^{k_p+1}, the residue of s then lies in the subgroup of order $p - 1$. This is exactly the Frobenius criterion for complete splitting in the indicated subfield. When $k_p = 0$ that field is $\mathbb{Q}$. The size inequality, $p \geq 3$, and $b_0(x) \geq b_0(V)$ give the last assertion. □

This splitting restriction concerns the rational primes which can represent nonzero elements under the tail map. Even a set of primes of very small density can represent every class of a finite quotient. An absolute bound for the order of the quotient in Theorem 22.51 is still needed, as is the signed period comparison (6.3) on the same fields.

22.26 Recovering strict torsion from ray characters

Fix an interval of Theorem 19.15 and x in that interval. Put $E = E_x$ and use its common modulus N_*. Let p be odd and $1 \le r < t(x)$. Write $\mathrm{Gal}(E/\mathbb{Q}) = P \times \Delta$, where P is its p-Sylow subgroup. Take a finite extension $J/\mathbb{Q}_p$ containing the values of all characters of this group. Let O, π, k, e be its ring of integers, a uniformizer, its residue field and $v_\pi(p)$, respectively. Write $A = J/O$, $R_h = O/\pi^h O$. For characters α of Δ and η of P, inflated to the absolute Galois group, put

$$\theta = \kappa_p^{-r}\alpha^{-1}\eta^{-1}, \qquad \Sigma = \{v : v \text{ is a prime dividing } pN_*\}.$$

Let $S(\theta) \subset H^1(\mathbb{Q}, A(\theta))$ be the classes trivial on the decomposition groups at Σ and on inertia elsewhere. These are the strong scalar local conditions of Section 22.13. Their source definition is `Development/AutomorphicArithmetic/AutomorphicVarieties/CharacterLevelBounds/ShaFamMono.lean`, line 30.

Write H for the fixed field of the kernel of $\chi = \theta \bmod \pi$, and $\Delta_H = \mathrm{Gal}(H/\mathbb{Q})$. This group embeds in $k^\times$. Denote by $\widetilde{\chi}$ the lift of χ to roots of unity of order prime to p. Normalize all local valuations of π-adic character values by $v_\pi(\pi) = 1$, with $v_\pi(0) = +\infty$, and define

$$c_H = \min_{g \in G_H} v_\pi(\theta(g) - 1), \qquad c_w = \min_{g \in G_{H_w}} v_\pi(\theta(g) - 1) \quad (w \mid \Sigma).$$

Here G_H, G_{H_w} denote absolute Galois groups. We have $1 \le c_H \le c_w < \infty$. At $w \mid p$ the cyclotomic image contains an open subgroup of $1 + p\mathbb{Z}_p$, even after killing the finite characters. Elsewhere the value of the cyclotomic character at Frobenius is the residue cardinality, whose r-th power is greater than one and is not a root of unity.

For $1 \le h \le c_H$ put $u = \lceil h/e \rceil$. For $w \mid p$ write $e_w = v_w(p)$ with $v_w(H_w^\times) = \mathbb{Z}$. Form the ray modulus

$$\mathfrak{m}_h = \prod_{w \mid p} \mathfrak{p}_w^{1 + \lfloor e_w/(p-1) \rfloor + u e_w} \prod_{\substack{w \mid \Sigma \\ w \nmid p}} \mathfrak{p}_w.$$

At $w \mid \Sigma$ define the following character with values in the additive group of R_h by the formula

$$\ell_w(g) = \frac{\theta(g) - 1}{\pi^{c_w}} \pmod{\pi^h} \quad (g \in G_{H_w}).$$

Indeed the discarded cross term in the product rule has valuation at least $c_w \ge h$ after division. One value of ℓ_w is a unit, so ℓ_w spans a free R_h-line. Write $\mathrm{Cl}_{\mathfrak{m}_h}(H)$ for the ray class group. Let L_h be the following explicitly defined finite O-module. Take the homomorphisms

$$\varphi : \mathrm{Cl}_{\mathfrak{m}_h}(H) \longrightarrow (R_h, +), \qquad \varphi(\delta z) = \widetilde{\chi}(\delta)\varphi(z) \quad (\delta \in \Delta_H).$$

Retain those whose pullback by reciprocity at each $w \mid \Sigma$ is in $R_h \ell_w$. These are finite linear conditions. Under local reciprocity one can evaluate them on a uniformizer and generators of the unit group modulo the specified principal units. Both sides factor through these quotients.

Theorem 22.55 (The finite torsion of a strict character group)**.** *For $1 \le h \le c_H$ there are isomorphisms of O-modules*

$$S(\theta)[\pi^h] \;\simeq\; \begin{cases} L_h, & \chi \neq 1, \\ L_h / R_h \ell_H, & \chi = 1. \end{cases}$$

In the second line $H = \mathbb{Q}$ and $\ell_H(g) = (\theta(g) - 1)/\pi^{c_H} \bmod \pi^h$. The residual field is the same for all η and all weights congruent to r modulo $p - 1$ at fixed α.

Proof. Identify $A[\pi^h]$ with R_h by $\pi^{-h}z + O \mapsto z \bmod \pi^h$. The action modulo π^h is trivial on G_H. It factors through Δ_H on which it is $\widetilde{\chi} \bmod \pi^h$, since the kernel of reduction on units of R_h is a p-group. Inflation–restriction identifies the global finite-coefficient cohomology with the equivariant continuous homomorphisms on G_H displayed above, initially without a conductor condition. The outer cohomology groups of Δ_H in degrees one and two vanish by averaging over its order, a unit in O. At each rational prime restriction to H_w likewise detects the zero class for the divisible coefficients, by restriction followed by corestriction.

The coefficient sequence for multiplication by π^h on $A(\theta)$ maps finite-coefficient cohomology onto the subgroup killed by π^h. Its kernel is the image under the connecting map of the invariants modulo π^h times the invariants. At H_w the invariants are $\pi^{-c_w}O/O$. Lifting their generator to $\pi^{-c_w-h} + O$ in the coefficient sequence gives exactly ℓ_w. Thus the image of a finite class in divisible cohomology vanishes locally precisely when its restriction lies on this line. At primes outside Σ both the character and $H/\mathbb{Q}$ are unramified. On inertia all of A is invariant and divisible, so the connecting map there vanishes. The finite class must itself vanish on inertia. At a real place the positive cohomology is zero since p is odd.

Global class field theory now describes the finite characters unramified outside Σ. Away from p the higher units are pro-residue-characteristic and have no nonzero image in R_h. Above p put $s_w = 1 + \lfloor e_w/(p-1) \rfloor$. The local logarithm and exponential are inverse between $1 + \mathfrak{p}_w^{s_w}$ and $\mathfrak{p}_w^{s_w}$. Raising to p^u therefore maps this unit group onto $1 + \mathfrak{p}_w^{s_w+ue_w}$. Every additive character with values in R_h kills those powers. These facts give exactly all the required characters from the stated ray group. They apply to the local characters ℓ_w as well.

Finally, if $\chi \neq 1$, some $\theta(g) - 1$ is a unit and the global invariants vanish. If $\chi = 1$, the global connecting map gives the line $R_h\ell_H$, by the same calculation as at w. Its restriction is $\pi^{c_w - c_H}\ell_w$, hence it belongs to L_h. This gives the asserted quotient. The character of P reduces to one and $\bar{\kappa}_p$ has order $p-1$, which proves the assertion about H. □

Corollary 22.56 (Two consecutive precisions)**.** *Let $d_0 = 0$ and let d_h be the O-length of the displayed quotient at precision h. If $d_h = d_{h-1}$ for some $1 \le h \le c_H$, then $\pi^{h-1}S(\theta) = 0$ and $S(\theta)$ has length d_h. Writing $n_* = [E_* : \mathbb{Q}]$, the ray groups used for these tests satisfy, for $n_H = [H : \mathbb{Q}] \le (p-1)n_*$,*

$$\log |\mathrm{Cl}_{\mathfrak{m}_h}(H)| \ll n_H\{\log(2pN_*n_H) + (2 + \lceil h/e \rceil)\log p\}.$$

Proof. The two successive torsion subgroups are nested and finite, so equality of lengths gives equality of subgroups. Every cohomology class is killed by a power of π, since a continuous cocycle on a compact group has finite image in A. Any element of order π^j with $j \ge h$ would give an element of order exactly π^h by multiplication. This proves the first assertion. The field H is contained in $E^P(\mu_p)$ and has conductor dividing pN_*. Its absolute discriminant is at most $(pN_*)^{n_H}$ by the conductor–discriminant formula. Minkowski's bound gives an ideal of norm at most $2^{n_H}|\operatorname{disc} H|^{1/2}$ in each ordinary class. The number of ideals of norm at most y is at most $y^2\zeta_H(2) \le y^2\zeta(2)^{n_H}$. The ray group adds a factor at most the norm of its modulus. Away from p this is at most $N_*^{n_H}$. Above p it is at most $p^{(2+u)n_H}$, since $1 + \lfloor e_w/(p-1) \rfloor \le 2e_w$ and $\sum_{w|p} e_w f_w = n_H$. These inequalities prove the bound. □

Theorem 22.57 (Descent on the integral character block)**.** *Write $|P| = p^a$. Let M_α be the α-eigenspace for Δ in $\mathcal{S}_{p,r}(E) \otimes_{\mathbb{Z}_p} O$. For $b \ge a$,*

$$|p^b M_\alpha| \;\le\; \prod_{\eta \in \widehat{P}} |p^{b-a} S(\kappa_p^{-r}\alpha^{-1}\eta^{-1})|.$$

In particular $p^b M_\alpha = 0$ if every η satisfies the consecutive-precision test at some h_η with $h_\eta - 1 \le e(b-a)$.

Proof. Over E the coefficient is $A(\kappa_p^{-r})$. At a finite place $w \nmid p$ its unramified local group is $A/((Nw)^{-r}-1)A = 0$, since the nonzero scalar acts surjectively. Thus the strict kernel there also satisfies the strong condition at all places above Σ. Extending coefficients commutes with these kernels since O is finite free over $\mathbb{Z}_p$. Twist the descent by α^{-1}. Restriction to E from E^{Δ} identifies the strict kernel with M_α. Indeed averaging gives descent on global cohomology and injectivity on local cohomology, including on inertia. Shapiro's lemma from E^{Δ} to $\mathbb{Q}$ now identifies this group with the strong kernel on $O[P] \otimes_O A(\kappa_p^{-r}\alpha^{-1})$. On a decomposition group the induced module splits over its cosets into induced local modules. The same holds on inertia, so the asserted kernel is preserved under Shapiro.

Character evaluation $O[P] \to \bigoplus_\eta O(\eta^{-1})$ has an integral reverse map given by the inverse Fourier matrix multiplied by $|P|$. Orthogonality makes both composites multiplication by p^a. Tensoring these identities with the twisted coefficient and taking the strong kernels preserves the identities. In particular $p^b M_\alpha$ is contained in the image under the reverse map of $p^{b-a}\bigoplus_\eta S(\theta)$. The order bound and the vanishing assertion follow. □

These tests apply at the cutoff $b = b_0(x)$ of Section 6.6, also to any further direct summand of the indicated block when $b_0(x) \geq a$. Their validity requires no change of period field or interval. An upper bound for the sum of the blocks for which no test has yet given stabilization is still needed for the full local estimate.

22.27 Ordinary class groups before cyclic descent

Fix x on an interval of Theorem 19.15, write $E = E_x$, and let p be odd. Write $\mathrm{Gal}(E/\mathbb{Q}) = P \times \Delta$, with P its p-Sylow subgroup. Set $K = E^{\Delta}$. This is the cyclic p-power subfield of the fixed character field K_ψ, including $K = \mathbb{Q}$. Indeed E/K_ψ has degree a power of two. In particular K is totally real and its ramified primes form a set independent of x.

Let O be an unramified extension of $\mathbb{Z}_p$ containing the values of the characters of Δ, let $k = O/pO$, and put $A = O[1/p]/O$. For $1 \leq r < t(x)$ let α be a character of Δ with $\alpha(c) = (-1)^r$, where c is complex conjugation. Write

$$M = \left(\mathcal{S}_{p,r}(E) \otimes_{\mathbb{Z}_p} O\right)_\alpha, \qquad \theta = \kappa_p^{-r}\alpha^{-1}, \qquad \chi = \bar{\kappa}_p^{-r}\bar{\alpha}^{-1}.$$

We regard α, θ, χ as characters of the absolute Galois group by inflation where necessary. The residual field $H = \overline{\mathbb{Q}}^{\ker\chi}$ is totally real, since $\chi(c) = 1$, and $\Delta_H = \mathrm{Gal}(H/\mathbb{Q})$ has order prime to p. Thus H and K are disjoint. Write $\widetilde{\chi}$ for the Teichmüller lift of χ and $R_h = O/p^hO$. For $L = H$ or KH set

$$D_h(L) = \{\varphi : \mathrm{Cl}(L) \longrightarrow (R_h, +) \mid \varphi(\delta z) = \widetilde{\chi}(\delta)\varphi(z) \text{ for every } \delta \in \Delta_H\}.$$

The maps are homomorphisms of groups. On KH the action of Δ_H fixes K. Use $D_\infty(L)$ for the same definition with target A. Its exponent and order are finite. For the local hypotheses below, D_v denotes an absolute decomposition group at the rational prime v.

Theorem 22.58 (Torsion on the entire p-Sylow block)**.** *Suppose $\chi(D_p) \neq 1$. For $1 \leq h \leq 1 + v_p(r)$ one has*

$$M[p^h] \simeq D_h(KH)$$

as O-modules with P-action. The action on the character group on the right is by precomposition with the inverse action on the class group. If p^d is the exponent of $D_\infty(KH)$, with $d = 0$ for the zero module, then $v_p(r) \geq d$ implies $p^d M = 0$ and $M \simeq D_\infty(KH)$.

Proof. First descend through E/K. Since its degree $|\Delta|$ is a unit in O, global restriction identifies the group on the indicated eigenspace with cohomology over K twisted by α^{-1}. The same averaging gives injectivity on local restrictions. More precisely the resulting group S_K consists of classes in $H^1(K, A(\theta))$ which vanish at the places over pN_* and on inertia elsewhere. Over E these conditions are the original ones. At a place $u \nmid p$ the unramified local subgroup on E is $A/((Nu)^{-r} - 1)A = 0$. This proves the claim about the kernels by applying restriction to each decomposition or inertia group. The coefficient extension commutes with kernels since O is finite free over $\mathbb{Z}_p$. The descent is equivariant for P with the usual cohomological action. In particular it retains the integral p-Sylow action throughout.

Let $w \mid p$ in K. The subgroup $G_{K_w} \subset D_p$ has p-power index, while χ has order prime to p. Hence its restriction has the same nontrivial image. Some local value of $\theta - 1$ is a unit, and $A(\theta)$ has no invariants at w or globally over K. The sequence for multiplication by p^h thus identifies $S_K[p^h]$ with finite-coefficient classes that vanish at every $w \mid p$ and are unramified at every $w \nmid p$. To verify the latter assertion, the inertia image of θ away from p has order prime to p. If it is nontrivial there are no inertia invariants, in either coefficient module. If it is trivial the divisible module of inertia invariants is A. In both cases the finite-to-divisible map on inertia cohomology is injective. An unramified finite class maps to zero on the whole local group in divisible cohomology, since the latter's unramified subgroup is zero. In the unramified-coefficient case the scalar on Frobenius is a root of unity times $(Nw)^{-r}$ and differs from one, which proves this last statement.

For $h \le 1 + v_p(r)$ the finite action is $\widetilde{\chi} \bmod p^h$. Indeed α takes prime-to-p roots of unity as values, and for $u \in 1 + p\mathbb{Z}_p$ one has $u^r \equiv 1 \bmod p^{1+v_p(r)}$ by binomial expansion. Restrict from K to KH. Inflation–restriction and averaging identify the finite classes with $\widetilde{\chi}$-equivariant additive characters there, as $[KH : K]$ is prime to p. Unramifiedness is detected by restriction on inertia since the local inertia index divides this degree. Local vanishing at p is detected in the same way on decomposition groups. Class field theory gives the ordinary ideal class group for everywhere-unramified characters, real places imposing no further condition at odd p. Moreover each prime ideal over p has trivial image under every equivariant character. Its stabilizer in Δ_H has nontrivial χ-image by the local calculation at w. One element of the stabilizer acts on the target by a root whose difference from one is a unit. Thus the character vanishes on the ideal class, exactly the additional splitting condition at this place. This gives the isomorphism.

For the P-action one may use representatives in G_H, since KH/H maps isomorphically to $K/\mathbb{Q}$. They act trivially on $R_h(\theta)$ in this range, so conjugation of ideal classes gives the stated dual action. Finally $D_h(KH) \simeq D_\infty(KH)[p^h]$ via $z \bmod p^h \mapsto z/p^h + O$. Under the exponent hypothesis the orders of $M[p^d]$ and $M[p^{d+1}]$ agree, taking $M[1] = 0$. Every cohomology class is killed by a power of p since a continuous cocycle on a compact group has finite image in A. An element of greater exponent would yield one of order exactly p^{d+1}. This proves the assertion about the whole module. □

Theorem 22.59 (A vanishing test on the prime-to-p field)**.** *Assume in addition that $\chi(D_v) \neq 1$ at every finite prime ramified in $K/\mathbb{Q}$. With $s = 1 + v_p(r)$ one has*

$$(M[p^h])^P \simeq D_h(H) \quad (1 \le h \le s), \qquad M = 0 \iff D_1(H) = 0.$$

The number of indecomposable summands of the $k[P]$-module $M[p]$ is $\dim_k D_1(H)$. In particular $\dim_k M[p] \le |P| \dim_k D_1(H)$.

Proof. Use the finite coefficient $R_h(\theta)$ of the preceding proof. There are no global invariants over K, so inflation–restriction identifies its first cohomology over $\mathbb{Q}$ with the P-invariants over

K. At primes outside p and the ramification of K, unramifiedness descends because the inertia groups are the same. At a ramified prime $v \neq p$ the unramified finite subgroup over K_w is zero. Indeed a nontrivial residual inertia value kills the invariants. If inertia acts trivially, the nontrivial residual local character has Frobenius value different from one and the unramified quotient is zero. The same alternatives hold over $\mathbb{Q}_v$. The character image stays nontrivial over K_w by the p-power index argument. Restriction on local first cohomology is injective here, and at p, since local coefficient invariants over K_w vanish. Thus the finite local conditions descend exactly. The first theorem's finite class field calculation over $\mathbb{Q}$ now gives $D_h(H)$.

The finite space $M[p]$ is a module over $k[P] \simeq k[T]/(T^{|P|})$, with $T = \sigma - 1$ for a generator of the cyclic group. On each nilpotent Jordan block the kernel of T is one-dimensional. This proves the count, the dimension bound and the equivalence at precision one. Since M is p-primary torsion, its vanishing is detected by $M[p]$. □

Corollary 22.60 (The test throughout the deep dyadic layers)**.** *Write $\alpha = \beta\nu$, with β from C_J of order 2^j and ν of order dividing* $\operatorname{lcm}(2, o)$*, where $o = \operatorname{ord}\psi$. Put*

$$\mathcal{B}_p = \{p\} \cup \{v : v \text{ ramifies in } K/\mathbb{Q}\}, \qquad j_p = \max_{v \in \mathcal{B}_p} \big(v_2(v^2 - 1) - 3\big) + v_2(\operatorname{lcm}(2, o, p - 1)).$$

Both theorems apply for $j > j_p$ at every weight of the specified sign, for every x on the original intervals and with either choice of each moving quadratic character. If $p - 1 \mid 2r$, the fields KH for these tests have degree at most $2[E : \mathbb{Q}]$ and conductor dividing pN_*.

Proof. The characters of E are generated by the original character, the dyadic characters and the two quadratic characters. This gives the decomposition with the asserted order bound. All primes in $\mathcal{B}_p$ are odd since a quotient of $(\mathbb{Z}/2^a\mathbb{Z})^\times$ has no odd-order character. The Frobenius of such a prime v acts on the real dyadic tower by the class of v modulo signs. Represent that class by the choice of v or $-v$ congruent to one modulo four. The valuation of its difference from one is $v_2(v^2 - 1) - 1$. The group $1 + 4\mathbb{Z}_2$ is generated topologically by 5, and $v_2(5^{2^a} - 1) = a + 2$ by repeated squaring. In the quotient of order 2^j, the Frobenius therefore has order $2^{\max(0, j - (v_2(v^2-1)-3))}$. The dyadic character is faithful on that quotient and unramified at v. In the residual character all the other factors on a Frobenius lift have order dividing $\operatorname{lcm}(2, o, p - 1)$. For $j > j_p$ they cannot cancel its two-part. This proves the local hypotheses, including for $v = p$. At $p - 1 \mid 2r$ the cyclotomic character modulo p to exponent r has order at most two. The compositum KH then lies in the compositum of E with the quadratic subfield of $\mathbb{Q}(\mu_p)$, giving both asserted bounds. □

For the cubic character of conductor 3367 in Section 26.10, one has $p = 3$, $\mathcal{B}_p = \{3, 7, 13, 37\}$, and $j_p = 2$. Thus every dyadic character of order at least eight satisfies these tests at every positive weight of the prescribed sign. For an even weight and $\nu = 1$, the residual field is C_j. The class number of C_j is prime to three for every j by Fukuda and Komatsu, Corollary 1.1 of their paper on Weber's class number problem [14]. Theorem 22.59 therefore kills the entire cubic Sylow block above this dyadic character, even though the invariant block of the original cubic field in Theorem 26.23 is nonzero. For a moving quadratic twist the class group in the vanishing test is the one for its own residual character. Controlling the groups that survive these tests in all weights remains necessary in Section 6.6.

23 References

[1] J. S. Milne, *Arithmetic Duality Theorems*, 2nd ed., 2006, Chapters I and II. Book.

[2] K. Iwasawa, *On $\mathbb{Z}_\ell$-extensions of algebraic number fields*, Ann. of Math. **98** (1973), 246–326.

[3] C. A. Weibel, *The K-book*, AMS, 2013. Chapter VI, Section 8.

[4] B. Kahn, *The Quillen–Lichtenbaum conjecture at the prime 2*. Theorem 1.

[5] E. Bayer-Fluckiger, V. Emery and J. Houriet, *Hermitian lattices and bounds in K-theory of algebraic integers*, Doc. Math., Extra Volume Merkurjev (2015), 71–83. Paper, especially Section 3.1 and Corollary 5.2.

[6] A. Mathew, *Torsion exponents in stable homotopy and the Hurewicz homomorphism*, Algebr. Geom. Topol. **16** (2016), 1025–1041. Theorem 1.3.

[7] B. Ferrero and L. C. Washington, *The Iwasawa invariant μ_p vanishes for abelian number fields*, Ann. of Math. **109** (1979), 377–395. Paper.

[8] L. C. Washington, *The non-p-part of the class number in a cyclotomic $\mathbb{Z}_p$-extension*, Invent. Math. **49** (1978), 87–97. Theorem, p. 87.

[9] A. de la Torre Durán, *Perfect forms and torsion bounds in algebraic K-theory over totally real and CM fields*, preprint, November 2026. Theorem 3.9 and Remark 4.2.

[10] C. A. Weibel, *The K-book*, Graduate Studies in Mathematics 145, AMS, 2013. Chapter VI, Corollary 9.8.

[11] 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.

[12] P. Mercuri, M. Paoluzi and R. Schoof, *Greenberg's conjecture for real quadratic number fields*, Journal of Experimental Mathematics **1** (2025), 207–217. Theorem 1.1, Section 2 and Table 3.1. Published paper.

[13] P. Mercuri, M. Paoluzi and R. Schoof, data accompanying *Greenberg's conjecture for real quadratic number fields*, file *Ideals with discriminant 0 mod 3.txt*, entry for 3624. Authors' data repository.

[14] 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.